# PigMail+PigProxy
## Конфигурация почтового и прокси сервера для малого и среднего предприятия

## Оглавление

# Постановка задачи

## *Почтовый сервер*

Имеется небольшая фирма, состоящая из головного офиса и нескольких удалённых филиалов. Также имеются штатные иногородние представители без офиса и деловые партнёры, с которыми происходит интенсивный обмен конфиденциальной информацией. Имеется ограниченное число (чаще всего один) почтовых доменов. Число пользователей также ограничено - несколько десятков. Почтовый сервер располагается непосредственно в головном офисе и подключён к интернету по выделенной линии.

Большинство пользователей подключаются из локальной сети головного офиса, но некоторые постоянно находятся за её пределами (удалённый филиал, представители, партнёры), некоторые могут подключаться извне (мобильные пользователи).

Большая часть почтовых адресов доступна для всех, но некоторые специальные адреса являются секретными - только для своих. Часть пользователей может отправлять почту за пределы домена, часть - только своим.

Для повышения степени защищённости имена учётных записей пользователей (логины) могут не совпадать с открытыми именами почтовых ящиков.

Для организации "безличной" связи контрагентов с отделами продаж, закупок, поддержки клиентов и т.д. применяются списки рассылки. Списки рассылки также могут быть общедоступными и скрытыми. Некоторые списки рассылки, в основном, предназначенные для рассылки информации вовне, могут быть авторизуемыми - это означает, что посылать сообщения в эти списки могут только определённые отправители, при этом им, возможно, потребуется подтвердить истинность своего обратного адреса.

Ряд адресов может иметь псевдонимы; алиасинг действует по той же схеме, что и в Eserv/2.

На время отсутствия (отпуск, болезнь), а также в других специальных случаях любому локальному получателю может быть сопоставлен автоответчик, высылающий штампованные извещения о невозможности немедленного ответа.

Защита от спама строится на использовании системы чёрных и белых списков, а также фильтрации содержимого писем. Белые списки имеют приоритет над чёрными. Для некоторых особо доверенных отправителей из белого списка возможно отключение обязательной для большинства спам-фильтрации. Для ряда отправителей из чёрного списка возможен приём почты в карантин с последующим ручным анализом. Некоторые локальные адреса имеют статус "специальных" (abuse). На эти адреса принимаются даже письма от заблокированных отправителей попавших в чёрные списки; в этом случае письма не подвергаются спам-фильтрации. Особо злостные спамеры могут быть лишены и этого права.

Для надёжного опознания "своих" используется SMTP-авторизация (хотя в некоторых экзотических случаях может и не применяться). У некоторых локальных пользователей установлено специальное программное обеспечение - клиентские программы дилерских и банковских систем, агенты диагностики и мониторинга сетевой инфраструктуры; возможно, не все они умеют корректно авторизоваться на почтовом сервере. Таких отправителей необходимо независимо от прочих настроек безопасности автоматически авторизовать, основываясь на обратном адресе и IP-адресе.

Имеется группа администраторов. Пользователь, авторизованный как администратор, имеет право указывать любой обратный адрес и обходить ограничение на число получателей. Некоторые администраторы имеют право отправлять письма на адреса из чёрного списка получателей. Для безопасности администраторские привилегии могут быть предоставлены только клиентам, подключающимся из локальной сети.

Отправлять почту за пределы домена, а также на "закрытые" адреса своего домена, могут только авторизованные пользователи, причём право отправки за пределы домена предоставлено не всем.

Существование "закрытых" адресов скрывается от не доверенных отправителей.

Ограничения на размер письма задаются динамически зависимости от адреса подключения, а также сочетания адресов отправителя и получателей.

Будучи принятой сервером, почта, которая не может быть доставлена по любой причине (спам, превышение ограничения на размер, отсутствие допустимых получателей), не удаляется, а оставляется для последующего анализа.

## *Прокси-сервер*

Прокси-сервер обслуживает только клиентов локальной сети (включая тех, кто входит в локальную сеть извне с помощью модема и сервера удалённого доступа, если таковой имеется). Требования к нему достаточно стандартны: обеспечить доступ к ресурсам, размещённым в глобальной сети, и при этом дифференцировать доступ в соответствии с расположением ресурса (возможно, вплоть до каталога или даже файла на сервере) и подключившимся пользователем и приложением.

Возможно применение локального кэширования загруженных из глобальной сети объектов. Режим кэширования должен выбираться в зависимости от запрашиваемого ресурса - вплоть до каталога или даже файла на сервере.

## *HTTP-сервер*

HTTP-сервер обслуживает публичный web-сайт компании (возможно, несколько различных сайтов одновременно), а также приватный сайт внутреннего назначения, доступный только сотрудникам фирмы. Поэтому обязательным требованием является поддержка так называемых виртуальных серверов, когда в зависимости от способа обращения (обычно в качестве ключевого элемента выступает символическое имя сервера) посетителю предоставляется доступ к одному из размещённых на сервере сайтов.

Обязательна поддержка сценариев, выполняемых на сервере. При этом для защиты от уязвимостей, которые почти наверняка найдутся в мало-мальски сложном сценарии, необходима возможность запускать их от имени определяемого настройками пользователя с минимально необходимыми для работы данного конкретного сценария правами.

Необходимо выполнять авторизацию пользователей - либо на основании IP-адреса, либо средствами протокола - и по данным авторизации обеспечить разграничение прав доступа к различным сайтам и разделам сайтов.

## *FTP-сервер*

FTP-сервер обслуживает публичный FTP-сайт компании, а также приватный сайт внутреннего назначения, доступный только сотрудникам фирмы. Поэтому обязательным требованием является поддержка так называемых виртуальных серверов, когда в зависимости от способа обращения (обычно в качестве ключевого элемента выступает IP-адрес подключения) посетителю предоставляется доступ к одному из размещённых на сервере сайтов.

Протокол FTP требует обязательной авторизации пользователей. На основании данных авторизации желательно обеспечить разграничение прав доступа к различным сайтам и разделам сайтов. Кроме того, каждому пользователю можно предоставить так называемый виртуальный корневой каталог - отдельный раздел сайта, где он волен хозяйничать, но за пределы которого выйти не может. Необходимо предусмотреть возможность гостевой авторизации - аналога анонимного подключения, доступного в других протоколах. При этом гостей необходимо ограничить в правах - обычно им разрешается только просматривать некоторые каталоги и читать размещённые в них файлы.

# Как это сделано

PigMail+PigProxy/2 является продолжением развития линейки PigMail+PigProxy/1, но представляет собой полностью самодостаточную сборку, основу которой составляют базовые компоненты стандартной конфигурации Eserv/3.

На сегодняшний день почтовый сервер состоит из двух относительно независимых служб - SMTP-сервера и POP/IMAP-сервера. Всю работу по приёму, анализу и маршрутизации почты выполняет SMTP-сервер, он же выполняет доставку сообщений в почтовые ящики локальных пользователей. Доставка исходящей почты за пределы локальных доменов выполняется специальным сервисом в составе SMTP-сервера либо, в особых случаях, внешним агентом (в поставку PigMail+PigProxy/2 включены **smtpsend.exe**, **smtpsend3.exe** и **smtpsend4.exe**), запуском которого также управляет SMTP-сервер. POP/IMAP-сервер занят исключительно обслуживанием локальных почтовых ящиков.

Работа SMTP-сервера начинается с анализа IP-адреса подключившегося к нему почтового клиента или агента доставки почтовой службы (для простоты будем кратко называть его клиентом). На основании системы чёрных и белых списков принимается решение о приёме или отклонении подключения. Если адрес находится в белом списке, а в настройках сервера отсутствует требование явной авторизации на сервере SMTP, то выполняется так называемая IP-авторизация - пользователь назначается в соответствии с содержимым списка. Одновременно могут быть выставлены некоторые дополнительные параметры. Если после проверки по чёрному и белому спискам остаётся неопределённость, адрес проверяется с помощью размещённых в интернете баз данных открытых релеев (MAPS, CBL, CWHOIS и других), причём выбором таких баз данных можно управлять. Такие проверки на начальном этапе позволяют отсечь до 20% спама.

Следующим шагом является взаимное представление клиента и сервера. При этом клиент сообщает своё имя, а сервер отвечает перечислением своих возможностей.

После обмена любезностями клиент может выполнить процедуру явной авторизации на сервере. Авторизоваться или нет - это решение принимает сам клиент. Сервер не может побудить клиента к авторизации, он может только отвергнуть письмо, если клиент не авторизовался, в то время как это, по мнению сервера, необходимо, либо авторизовался, но не так, как этого ожидал сервер.

Далее клиент сообщает обратный адрес письма. Здесь вариантов уже существенно больше. Во-первых, отправителем может быть один из локальных пользователей - в этом случае существует возможность тонкой настройки его прав. Отправитель может попасть под действие чёрного либо белого списков. Во-вторых, отправитель может быть либо авторизован, либо нет. Некоторые отправители на этом этапе могут быть авторизованы автоматически (в том случае, когда авторизация обязательна, а клиент её выполнять не умеет), факт авторизации некоторых других отправителей, напротив, может быть дополнительно с пристрастием проверен. Наконец, адреса, не попавшие ни в какие списки, проверяются на корректность - как на простое присутствие в них запрещённых символов, так и на корректность почтового домена.

Если адрес отправителя принят, клиент сообщает адреса получателей письма, которые проверяются на соответствие примерно таким же условиям - разумеется, вместо авторизации получателя проверяется опять-таки факт правильной авторизации отправителя. В результате часть адресов может быть отвергнута как не соответствующая его правам. По ходу дела проверяется, не выполняется ли переадресация, не является ли получатель списком рассылки. Если получатель принадлежит одному из локальных доменов, проверяется существование пользователя - если такового не оказывается, существует несколько возможных способов реакции.

После указания адресов клиент начинает передачу письма. При этом выполняется (или не выполняется - в зависимости от выбранного метода передачи) анализ заголовков и тела письма. Затем успешно принятое письмо подвергается (или, в зависимости от настроек, не подвергается) различным видам анализа - на наличие вирусов, на признаки спама, на соответствие ограничениям по размеру. Отправитель получает либо подтверждение успешного приёма письма, либо отказ с соответствующим случаю пояснением, но само письмо с сервера не удаляется - оно перемещается на хранение до момента, когда у администратора дойдут руки проанализировать ситуацию. В отдельных случаях - например, обнаружение вируса - формируются автоматические письма-извещения.

Прорвавшееся сквозь оборонительный частокол письмо проходит процедуру доставки. Именно здесь выполняется реальная переадресация и обработка списков рассылки, здесь же обрабатываются назначенные локальным получателям автоответчики. Если получатель локальный, то письмо помещается в его почтовый ящик. Если получатель определён как внешний, письмо перемещается в специальный каталог исходящих писем, и сервер запускает программу-агента для доставки этого письма. Если сервер не смог принять определённого решения относительно какого-либо получателя, письмо сохраняется до вмешательства администратора. Частью процедуры доставки является формирование автоматических извещений отправителям. На этом работа SMTP-сервера заканчивается.

POP/IMAP-сервер также начинает с анализа IP-адреса подключившегося клиента. Точно так же в зависимости от нахождения в чёрном либо белом списке подключение может быть либо принято, либо отклонено. Однако при этом не выполняется IP-авторизация и дополнительный анализ адреса.

В отличие от SMTP-сервера, явная авторизация на POP/IMAP-сервере является обязательной - только на основании её результатов сервер может определить, какой именно почтовый ящик следует обрабатывать.

Если клиент успешно прошёл авторизацию, и почтовый ящик удалось открыть, то далее всё просто - клиент получает оглавление почтового ящика и принимает решение о дальнейших действиях. Любое сообщение может быть загружено клиентом, удалено, перемещено, клиент также может запросить дополнительную информацию о сообщениях.

Прокси-сервер в минимальном варианте совмещает в себе три службы, обслуживающие три различных протокола - HTTP-прокси, FTP-прокси и Socks-прокси. HTTP-прокси предназначен в основном для web-сёрфинга посредством браузеров (или, по довольно удачному определению редмондских лингвистов - обозревателей), он же обеспечивает тем же браузерам доступ к FTP-серверам. FTP-прокси предназначен для использования специальными FTP-клиентами, каковыми являются, например, FAR Manager или FreeCommander; он позволяет более полно использовать возможности популярного протокола передачи файлов. Socks-прокси базируется на универсальном протоколе Socks, позволяющем организовывать соединения туннельного типа - прокси-сервер не анализирует ни данные, ни служебную информацию, передаваемые по таким соединениям. Соответственно, Socks-прокси может быть использован коммуникационными программами самого различного профиля; пожалуй, самая популярная в этом классе программа - интернет-пейджер ICQ.

Дополнительно к этим трём службам можно подключить старое доброе отображение портов TCP и UDP. С его помощью также можно организовать туннельное соединение для любого протокола на базе TCP/IP. Конечно, с этим может справиться и Socks-прокси, но использовать его возможности научились ещё не все интернет-клиенты, а в ряде случаев настроить прямое статическое отображение бывает гораздо проще.

Ещё одна служба, которая может быть задействована дополнительно, - POP3-прокси; с её помощью можно опрашивать почтовые ящики на произвольном множестве серверов.

Работа всех служб прокси-сервера начинается с анализа IP-адреса подключающегося клиента. Анализ требуется гораздо более пристрастный, чем для любого другого сервера, входящего в состав PigMail+PigProxy, - малейшая оплошность в настройке может превратить прокси-сервер в открытый (Open Proxy), что неминуемо влечёт за собой счета на весьма приличные суммы. Поэтому анализируется не только IP-адрес клиента, но и адрес сетевого интерфейса, к которому происходит подключение. Обычно подключения принимаются только на интерфейсы, принадлежащие локальной сети, хотя возможны разные варианты, вплоть до самых экзотических. На основании системы чёрных и белых списков принимается решение о приёме или отклонении подключения. Если адрес находится в белом списке, то при соответствующем разрешении в настройках сервера выполняется так называемая IP-авторизация - пользователь назначается в соответствии с содержимым списка. Одновременно могут быть выставлены некоторые дополнительные параметры.

Для отображения портов TCP или UDP весь анализ на этом заканчивается - поскольку отображение статическое, порт и сетевой интерфейс, к которым обратился клиент, однозначно определяют целевой сервер и его порт. Служба устанавливает соединение и выпускает клиентскую программу наружу.

HTTP-прокси принимает от клиентской программы сложный запрос, содержащий множество параметров - указатель на искомый сетевой ресурс (так называемый URL - Uniform Resource Locator), режимы приёма, информацию о клиенте, хранимые параметры сессии и, возможно, данные авторизации на внешнем сервере и прокси-сервере. В зависимости от настроек сервера и содержимого запроса он может быть либо принят, либо отвергнут. Если запрос принимается, прокси-сервер сам обращается по указанному адресу и возвращает клиенту ответ. Если запрос не принимается, клиенту возвращается заранее заготовленный для такого случая стандартный ответ.

FTP-прокси не требует обязательной авторизации, поскольку это не определено стандартом. Тем не менее, поддержка авторизации на FTP-прокси существует. Клиент передаёт адрес целевого сервера и параметры авторизации на нём; эти параметры также могут содержать необязательную информацию для авторизации на прокси-сервере. Прокси-сервер анализирует эти параметры, выполняет подключение и обеспечивает передачу данных.

Клиент Socks-прокси вначале выполняет (или не выполняет) авторизацию. Это зависит также от используемой версии протокола Socks - авторизация поддерживается только в версиях не ниже 5. Затем клиентская программа задаёт адрес целевого сервера и номер порта, а также требуемый метод соединения. Если запрос допустим, прокси-сервер устанавливает соединение с сервером и обеспечивает передачу данных.

POP3-прокси получает от клиента в запрос, содержащий имя целевого сервера и имя учётной записи пользователя на целевом сервере. Если подключение разрешено настройками, прокси-сервер устанавливает соединение, инициирует процедуру авторизации на внешнем POP-сервере и в дальнейшем обеспечивает обмен командами и данными между клиентской программой и целевым сервером.

Работа HTTP-сервера начинается с анализа IP-адреса подключающегося клиента. На основании системы чёрных и белых списков принимается решение о приёме или отклонении подключения. Если адрес находится в белом списке, то при соответствующем разрешении в настройках сервера выполняется так называемая IP-авторизация - пользователь назначается в соответствии с содержимым списка. Одновременно могут быть выставлены некоторые дополнительные параметры.

HTTP-сервер принимает от клиентской программы сложный запрос, содержащий множество параметров - указатель на искомый ресурс сервера (так называемый URI), режимы приёма, информацию о клиенте, хранимые параметры сессии и, возможно, данные авторизации. В зависимости от настроек сервера и содержимого запроса он может быть либо принят, либо отвергнут. Если запрос принимается, сервер преобразует URI в реальный физический путь и проводит дополнительный анализ запроса. В зависимости от расположения и типа запрошенного объекта может быть выполнен сценарий, результаты действия которого получит клиент. Может быть передан сам запрошенный файл. Запрос может быть отвергнут, если у обратившегося посетителя нет прав на его выполнение. Если запрос не принимается, клиенту возвращается заранее заготовленный для такого случая стандартный ответ.

Работа FTP-сервера начинается с анализа IP-адреса подключающегося клиента. На основании системы чёрных и белых списков принимается решение о приёме или отклонении подключения. Если адрес находится в белом списке, то при соответствующем разрешении в настройках сервера выполняется так называемая IP-авторизация - пользователь назначается в соответствии с содержимым списка. Одновременно могут быть выставлены некоторые дополнительные параметры. Правда, поскольку FTP - протокол с обязательной явной авторизацией клиента, толку от IP-авторизации немного.

На основании результатов авторизации сервер устанавливает базовые параметры сессии - например, в стучае гостевой авторизации пользователь получает возможность только просматривать каталоги и читать размещённые в них файлы. Далее сервер анализирует поступающие команды протокола. Для каждой команды выполняется преобразование логического пути к запрошенному файлу или каталогу в физический путь на диске сервера и анализируются права доступа пользователя. В зависимости от этого запрос либо выполняется, либо нет.

Теперь можно более подробно присмотреться к работе отдельных механизмов сервера.

## *Авторизация*

Назначение авторизации - однозначная идентификация подключившегося клиента. Порядок действия прост - клиент передаёт имя своей учётной записи (логин) и пароль, а сервер ищет их в своих списках. При обнаружении переданных данных клиент считается авторизованным, в противном случае - нет. Имя учётной записи обязательно должно быть уникальным. Пока сервер обслуживает один почтовый домен, это условие обеспечивается легко - ведь почтовые адреса также должны быть уникальны, и даже если в качестве имени учётной записи использовать имя почтового ящика, уникальность будет обеспечена. Если же сервер обслуживает несколько почтовых доменов, обеспечение уникальности становится проблемой. В качестве выхода все включённые в PigMail+PigProxy/2 серверы предоставляют возможность передавать составное имя учётной записи вида **имя@домен**. Здесь домен представляет собой домен авторизации, его имя не обязательно совпадает с именем почтового домена.

Каждому домену авторизации сопоставлен свой **источник авторизации** с уникальным именем. Источник авторизации, в свою очередь характеризуется способом авторизации и дополнительными параметрами. На сегодняшний день доступны четыре способа авторизации:

- Авторизация в домене Active Directory. В качестве домена может выступать и компьютер, на котором установлен сервер. В качестве дополнительного параметра указывается имя домена Active Directory или имя локального компьютера.
- Авторизация по списку пользователей формата Eserv/2. Дополнительный параметр задаёт имя файла с таким списком. Это может быть как отдельный список, вырезанный из конфигурационного файла Eserv.ini, так и сам конфигурационный файл.
- Авторизация по списку пользователей формата Eserv/3. Дополнительный параметр задаёт имя файла с таким списком. Это файл стандартного текстового списка (см. раздел **Назначение и формат управляющих списков**), в котором, помимо имени учётной записи и пароля, зашифрованного по алгоритму MD5 (то есть, не поддающегося обратной расшифровке), хранится дополнительная информация.
- Авторизация по списку пользователей, хранящемуся в базе данных, доступной через ODBC-подключение. Дополнительные параметры задают реквизиты для доступа к базе данных и расположение файла с текстом запроса к базе данных.

В процессе авторизации первым делом производится разделение переданного составного имени учётной записи на собственно имя и домен. Если домен не был указан, используется домен авторизации по умолчанию, задаваемый в настройках сервера. Это может быть как жёстко определённый для всех вариантов подключения параметр, так и назначаемый в зависимости от того, на какой из сетевых интерфейсов было выполнено подключение (в последнем случае используется специальный управляющий список). Если домен отсутствует в списке локальных доменов либо не обнаруживается заданный в его параметрах источник авторизации, применяется заданный в настройках сервера альтернативный метод авторизации. На сегодняшний день доступны четыре метода авторизации (только что описанный обобщённый метод с использованием имени домена можно считать пятым или нулевым - в зависимости от точки зрения на нумерологию):

- Авторизация в домене Active Directory. В качестве домена может выступать и компьютер, на котором установлен сервер. Имя домена для этого случая задаётся в настройках сервера.

- Авторизация по списку пользователей формата Eserv/2. Это может быть как отдельный список, вырезанный из конфигурационного файла Eserv.ini, так и сам конфигурационный файл. Имя файла задаётся в настройках сервера.
- Авторизация по списку пользователей формата Eserv/3. Это файл стандартного текстового списка (см. раздел **Назначение и формат управляющих списков**), в котором, помимо имени учётной записи и пароля, зашифрованного по алгоритму MD5 (то есть, не поддающегося обратной расшифровке), хранится дополнительная информация. Имя файла задаётся в настройках сервера.
- Авторизация по заданному в настройках сервера источнику авторизации.

Для POP/IMAP-сервера на этом всё и заканчивается, поскольку авторизация на нём обязательна - иначе невозможно определить, с каким почтовым ящиком будет работать подключившийся клиент. Для SMTP-сервера всё несколько сложнее, поскольку далеко не все клиенты могут быть авторизованы. Разумеется, если сервер предназначен исключительно для внутреннего использования, можно требовать авторизацию от всех клиентов. Но если сервер обслуживает реальный почтовый домен (то есть, его имя или IP-адрес указаны в публичных таблицах DNS в качестве почтового сервера домена), то примерно половина подключений будет приходиться на внешние почтовые серверы, по определению доставляющие почту анонимно. В такой ситуации разумно настаивать на авторизации только тех клиентов, которые отправляют почту за пределы почтового сервера. В этой версии конфигурации требование усилено - проверяется не только сам факт успешной авторизации, но и соответствие между именем учётной записи и обратным адресом. Аналогично можно управлять авторизацией клиентов, отправляющих почту на секретные локальные адреса. При желании можно вообще не настаивать на авторизации - в этом случае, принимая решение о разрешении или запрете маршрутизации письма, сервер будет ориентироваться только на сочетание почтовых адресов отправителя и предполагаемого получателя и IP-адрес клиента.

## *Группы пользователей*

Группы пользователей представляют собой способ определения шаблонов прав (они же профили) доступа. В ситуации, когда права реальных пользователей достаточно часто меняются, гораздо удобнее настроить профили для групп, пользователи же будут получать права групп, в которые они входят. В соответствии с общепринятыми правилами, эффективные права пользователя получаются суммированием прав всех групп, в которые он входит, а также прав, назначенных для пользователя индивидуально.

Механизм групп поддерживается для всех способов авторизации - в соответствии с их устройством. Обычно предполагается, что пользователи и группы принадлежат одному домену авторизации; в большинстве случаев этого вполне достаточно. Если же это условие оказывается слишком жёстким (чаще всего в случае авторизации по списку домена Active Directory, когда PigMail+PigProxy работает не на контроллере домена - в этом случае определение принадлежности пользователя к группе затруднено), существует возможность включить механизм кроссдоменной группировки. Надстройка позволяет объединять в группы пользователей из различных доменов, использующих разные способы авторизации. При этом не обязательно, чтобы группы пользователей были определены на уровне соответствующих источников авторизации. Более того - можно описать группы пользователей, принадлежащие фиктивным, вовсе не описанным доменам. Правда, увлекаться созданием лишних, сверх необходимого, сущностей, не рекомендуется с достаточно давних времён.

## *Автоматическая авторизация*

Это дополнительная возможность, которую предоставляет SMTP-сервер для разрешения противоречащих друг другу требований к системе. Сейчас уже достаточно типична схема, при которой часть локальных (логически - с точки зрения почтового сервера) пользователей постоянно или достаточно часто находится вне пределов локальной сети (и даже вне пределов доверенных сетей). Поэтому для отделения "агнцев от козлищ" совершенно необходима явная авторизация отправителя на сервере SMTP. Вместе с тем нередки случаи использования различных унаследованных приложений - различных агентов, клиентов, роботов, - отсылающих информацию по электронной почте, но не обученных премудростям авторизации. Достаточно часто информацию требуется отправлять именно за пределы локального домена либо скрытому получателю, а в этом случае авторизация обязательна. Если обновить приложения до более "продвинутых" версий не представляется возможным, используется автоматическая авторизация.

Механизм автоматической авторизации запускается на этапе анализа адреса отправителя при совпадении двух условий - во-первых, её использование разрешено в настройках сервера, и, во-вторых, подключившийся отправитель не авторизовался явным образом. Адрес электронной почты отправителя и IP-адрес подключения ищутся в особом списке авто-авторизации. Если подходящая пара обнаружена, отправитель считается авторизовавшимся.

## *Локальные пользователи и почтовые ящики*

Собственно, с точки зрения сервера, пользователь и почтовый ящик - это две разные ипостаси одного и того же субъекта. POP/IMAP-сервер выясняет пользователя и подключает его к именному почтовому ящику, а конечная задача SMTP-сервера состоит в доставке письма опять же в почтовый ящик. Пользователи

перечислены как в списках авторизации, так и в специальном списке локальных почтовых ящиков, используемом SMTP-сервером для тонкой настройки прав. Почтовые ящики представляют собой каталоги, в которых хранятся файлы писем. Обычно каталоги почтовых ящиков располагаются в общем почтовом каталоге соответствующего домена - это соответствует системе почтовой адресации и вполне понятно интуитивно. Если пользователь и его ящик существуют, то никаких проблем нет. Хуже, если пользователь отсутствует в списках или для него почему-то не заведён почтовый ящик. POP/IMAP-сервер в такой ситуации предлагает клиенту особый аварийный ящик, всегда пустой.

SMTP-сервер при необнаружении отправителя тоже не особо церемонится - отвергает адрес как неверный (подобный трюк с использованием поддельных адресов, якобы принадлежащих локальному домену, довольно часто применяют спамеры). А вот с отсутствующим получателем можно обойтись по-разному. Наиболее распространённый вариант - отказ в приёме такого адреса. Однако нередки и ситуации, когда почту для несуществующих локальных получателей необходимо принимать (например, когда SMTP-сервер выступает в качестве транзитного, выполняющего пересылку на какую-то другую почтовую систему). Это можно реализовать несколькими способами. Во-первых, можно автоматически создавать почтовые ящики для таких пользователей в расчёте на то, что администратор сервера это заметит и примет меры (если он, к примеру, просто забыл добавить пользователя в списки). Во-вторых, можно перенаправить такие письма в специальный почтовый ящик (тому же администратору). В-третьих, можно их просто складировать в отдельном каталоге - опять же до рассмотрения администратором.

Бывают также довольно экзотические ситуации, когда почтовый домен получателя в списках не значится, но публичные таблицы DNS упрямо указывают на наш сервер. Это следствие либо ошибки в настройках самого сервера, либо ошибки или даже злого умысла администратора DNS-сервера. Обычно на такие провокации поддаваться не следует, но если сервер ещё не окончательно настроен, можно разрешить приём писем на такие адреса - до выяснения ситуации и ликвидации проблемы.

## *Алиасы или псевдонимы*

Алиасы предоставляют возможность сопоставить одному почтовому ящику несколько почтовых адресов. Их действие распространяется только на адреса получателей. Подобно обычным локальным адресам, алиасы могут быть общедоступные и закрытые.

В описываемой конфигурации, в отличие от стандартной, алиасы являются именно алиасами - попытка определить перенаправление на несколько адресов вызовет ошибку. Списки рассылки реализованы отдельно.

Алиасы не обладают свойством рекурсии - этим можно воспользоваться, чтобы вывести из-под действия группового алиаса конкретный адрес.

При анализе адреса первым делом проверяется именно наличие алиаса - если он существует, то, все дальнейшие проверки предпринимаются уже в отношении перенаправленного адреса. Поэтому алиасы не помогут в ситуации, когда почту, приходящую на локальный адрес, необходимо временно перенаправить на некоторый внешний почтовый ящик. Первое же входящее письмо будет отвергнуто, поскольку внешним отправителям не разрешено использовать сервер для транзитной пересылки почты (так сделано - описываемая конфигурация предназначена для корпоративного почтового сервера). Для этого надо использовать списки рассылки.

## *Списки рассылки*

Списки рассылки - весьма удобный механизм для отправки писем на множество адресов. Указав в письме один-единственный адрес, можно осчастливить корпоративными новостями несметное число сетян - за что он в большом почёте у спамеров-любителей (профессионалы используют гораздо более изощрённые системы).

В описываемой конфигурации списки рассылки выступают в роли локальных получателей, поэтому отправлять сообщения в списки могут и внешние отправители - это позволяет наряду с личными адресами (публиковать которые не всегда желательно) организовать и "безличные", типа **support@**, **sales@**, **info@**, которые в разное время будут обслуживаться разными реальными получателями.

Подобно обычным локальным получателям, списки рассылки могут быть общедоступные и закрытые. Существует возможность закрыть список ещё сильнее, разрешив отправку в него сообщений только определённым отправителям и даже проверяя правильность их авторизации. Таким способом обязательно следует защищать списки рассылки, нацеленные за пределы локального домена - дабы ими не воспользовались какие-нибудь посторонние злоумышленники.

Список рассылки может быть временно выключен - тогда использовать его не сможет никто. Существует также возможность сделать список "невидимым". Это связано с особенностями реализации - дело в том, что списки рассылки обрабатываются сразу вслед за алиасами, поэтому список рассылки может "закрыть" реально существующий локальный адрес - например, для временной переадресации поступающей почты на внешний адрес. Если такую переадресацию периодически требуется то включать, то отключать, режим невидимости списка очень пригодится - это гораздо удобнее, чем удалять список, а потом создавать заново.

Как и алиасы, списки рассылки не поддерживают рекурсию. То есть, если в списке рассылки указать его собственный адрес, будет выполнена попытка доставить письмо в указанный локальный ящик. Таким способом можно сохранять на сервере копию временно переадресованной почты - чтобы после возвращения получатель мог её заново просмотреть, если на то будет его воля.

Имеется возможность делать временные исключения из списка рассылки. Если сотрудник отдела поддержки уходит в отпуск, ему совершенно незачем получать предназначенную для отдела оперативную рассылку. А если он, как это довольно часто бывает, подписан на несколько подобных рассылок сразу, то исключить его из всех таких списков будет уже проблематично, а ещё сложнее будет по его возвращении вспомнить, на какие рассылки он был подписан. Гораздо проще добавить его адрес в один-единственный дополнительный список.

Списки рассылки обслуживаются специальным плагином **maillists**, загрузкой которого при старте сервера можно управлять с помощью специального параметра конфигурационного файла PigMail2.ini. Этот же параметр позволяет временно отключать использование списков рассылки в случае возникновения проблем.

## *Автоответчики*

Автоответчики реализуют две возможности. Во-первых, отправители иногда желают получать подтверждения о доставке своих писем. Чаще всего такие подтверждения формирует почтовая программа получателя, однако можно научить этому и SMTP-сервер. Если у письма несколько получателей, как локальных, так и внешних, то сервер подтверждает только доставку писем в локальные почтовые ящики - за внешних адресатов пускай отдуваются обслуживающие их серверы.

Вторая - несомненно, гораздо более полезная, - функция автоответчиков заключается в посылке неких стандартных сообщений в ответ на поступающие по определённому локальному адресу письма. Например: "Уважаемый отправитель, ваше письмо поступило в отдел продаж и будет рассмотрено в самое ближайшее время, благодарим за проявленный интерес". Отвечающими адресами могут быть как списки рассылки, так и личные локальные почтовые ящики (в этом случае автоответы, как правило, повествуют о временном отсутствии получателя). Такой автоответчик срабатывает только при явном обращении отправителя по его адресу (включая, однако, и случай использования алиаса), но не реагирует на поступление письма через собственный список рассылки.

При формировании автоответов в качестве обратного используется специальный адрес "отскока". Почта на этот адрес обычно не принимается (хотя любопытства ради можно изменить стандартную настройку сервера - тогда письмо будет принято, но никаких дополнительных автоответов, даже если они заказаны, отправлено не будет). Это сделано для того, чтобы исключить возможность переписки между двумя роботами - ведь письмо вполне может придти от какой-нибудь автоматической системы. По этой же причине существует специальный список отправителей, которым никогда не отправляется автоответ.

Автоответчики обслуживаются специальным плагином **autoresponders**, загрузкой которого при старте сервера можно управлять с помощью специального параметра конфигурационного файла PigMail2.ini. Этот же параметр позволяет временно отключать использование автоответчиков в случае возникновения проблем.

## *Почтовые роботы*

Почтовые роботы - это особые программы, обрабатывающие поступающие к ним письма, обычно имеющие специальный формат. С помощью роботов можно выполнять любую обработку почты - от простой доставки в нужный почтовый ящик до выполнения сложных запросов к различным информационным системам с последующей отправкой сформированного ответа. Например, автоответчики - тоже своего рода роботы, только предельно жёстко запрограммированные. Роботы же представляют собой универсальный способ расширения функциональности сервера.

В PigMail+PigProxy роботы выступают в роли локальных получателей, поэтому отправлять им сообщения могут и внешние отправители - следовательно, робот должен тщательно проверять права своих корреспондентов, чтобы случайно не разгласить секретную информацию только для внутреннего пользования.

Подобно обычным локальным получателям и спискам рассылки, роботы могут быть общедоступные и закрытые.

Робот может быть временно выключен - тогда использовать его не сможет никто. Существует также возможность сделать робота "невидимым". Это связано с особенностями реализации - дело в том, что роботы обрабатываются сразу вслед за алиасами и списками рассылки, поэтому робот может "закрыть" реально существующий локальный адрес - например, для временной переадресации поступающей почты на несколько последовательно перебираемых адресов. Если такую переадресацию периодически требуется то включать, то отключать, режим невидимости робота очень пригодится - это гораздо удобнее, чем удалять робота, а потом создавать заново.

В отличие от стандартной конфигурации Eserv/3, здесь все роботы являются самодостаточными - при их срабатывании дальнейшая обработка адреса робота-получателя прерывается (на остальных адресатов того же письма, сколько бы их ни было и какому бы количестве роботов письмо ни было направлено, это не распространяется - разумеется, если не предусмотрено программой самого робота). Поэтому любые стан-

дартные действия (даже простая доставка письма в назначенный роботу почтовый ящик) должны быть явно описаны в алгоритме самого робота.

По своей реализации роботы делятся на два типа - внешние приложения и встроенные (в виде либо интерпретируемых файлов правил, либо дополнительных модулей расширений) правила сервера. Необходимо учесть, что выполнение особо сложного встроенного правила (если не принять специальных мер) может сильно задержать доставку письма другим получателям, если таковые имеются. Поэтому предпочтительным вариантом подключения "самодельных" роботов является использование внешних приложений - тем более что такие приложения можно создавать с использованием любого языка программирования.

Одно и то же письмо может быть адресовано любому количеству роботов. Конфликтов при этом не возникнет, поскольку каждый робот получает для обработки собственную рабочую копию письма. Копия создаётся в каталоге для размещения временных файлов, поэтому в хорошо настроенной системе (когда этот каталог регулярно автоматически освобождается от устаревших файлов) робот может даже не заботиться об удалении ненужной копии. Внешнему приложению имя файла рабочей копии (и другие необходимые сведения) передаются через командную строку запуска. Встроенный робот выполняется в контексте сервера, поэтому имеет непосредственный доступ ко всем необходимым переменным.

Роботы обслуживаются специальным плагином **robots**, загрузкой которого при старте сервера можно управлять с помощью специального параметра конфигурационного файла PigMail2.ini. Этот же параметр позволяет временно отключать использование роботов в случае возникновения проблем.

## *Перенаправление*

Хотя корпоративный почтовый сервер (в отличие от почтового сервера Интернет-провайдера) не предназначен для обслуживания "чужих" почтовых доменов, тем не менее, такая возможность на всякий случай предусмотрена. На этапе окончательной доставки письма за пределы локального домена проверяется специальный список, в котором адресам внешних получателей сопоставлены имена либо IP-адреса SMTP-серверов, назначенных принимать почту, адресованную таким получателям. В результате письмо вместо "свободной" пересылки (обычно основанной на данных серверов DNS) направляется по жёстко запрограммированному маршруту. Такая возможность, помимо собственно обслуживания почтовых доменов, размещённых на других почтовых серверах, позволяет обходить ошибки конфигурации DNS.

## *Очереди доставки и планировщик*

Очередь доставки представляет собой каталог, в который помещаются письма, предназначенные для отправки за пределы сервера. В самом минимальном варианте есть одна общая очередь, письма из которой доставляются "свободным" образом - агент отправки для каждого домена назначения получает у сервера DNS реквизиты почтового сервера, на который следует доставить письмо, и соединяется с этим сервером напрямую. Письма, перенаправленные по фиксированному маршруту, помещаются в отдельные очереди - по одному каталогу на каждый маршрут.

Начальная настройка почтового сервера предусматривает немедленную отправку письма. Каждый раз, как письмо помещается в каталог очереди доставки, запускается агент smtpsend3 или smtpsend4, просматривающий эту конкретную очередь и доставляющий все хранящиеся в ней письма. Если доставка прошла успешно, этого достаточно. Однако если сервер получателя недоступен или по каким-то причинам отказывается принимать письмо, но при этом не настаивает на немедленном возврате, письмо остаётся в "подвешенном" состоянии. Следующая попытка отправки состоится тогда и только тогда, когда в эту же очередь будет помещено ещё одно письмо. Сколько времени пройдёт до этого момента, не возьмётся оценить ни один ясновидец. Для того, чтобы письмо не "зависло" на неопределённое время, требуется периодически просматривать все существующие очереди доставки и при наличии в них писем инициировать сеанс доставки. Эта задача возложена на так называемый планировщик.

Конечно, до функциональности полноразмерных планировщиков уровня nnCron этой службе далеко, но от неё многого и не требуется. С заданной в настройках сервера периодичностью планировщик анализирует каталоги очередей доставки. Первой анализируется общая очередь. Затем планировщик по списку перенаправления просматривает очереди всех определённых в списке маршрутов. Если в какой-либо очереди обнаруживается недоставленное письмо, запускается агент доставки с указанием настроек, соответствующих параметрам очереди. Планировщик обслуживается специальным плагином **scheduler**, загрузкой которого при старте сервера можно управлять с помощью специального параметра конфигурационного файла PigMail2.ini.

Если письмо не удаётся доставить в течение достаточно длительного времени (обычно измеряемого несколькими часами), агент перемещает его в каталог так называемой очереди отложенной доставки. Структура этой очереди подобна структуре основной, она тоже подразделяется на общую очередь и очереди фиксированных маршрутов. Её обработка также возложена на планировщик, различие лишь в том, что очередь отложенной доставки проверяется существенно реже, как правило, раз в несколько часов.

Если письмо так и не удалось доставить - либо вышел отведённый для этого срок, либо сервер-получатель отказал в приёме сообщения жёстко и безапелляционно, - отправителя следует известить о неудаче. Для этого агент создаёт письмо-извещение по заранее настроенному шаблону. Остаётся доставить его по назначению. Поскольку агент работает как изолированное приложение и не в состоянии обработать все

сложные правила доставки письма в локальный ящик, к тому же в зависимости от настроек сервера отправитель может оказаться и внешним, выбран простой и безотказный вариант. Извещение помещается в особую очередь внутренней доставки с фиксированным маршрутом, указывающим на локально работающий SMTP-сервер. Запись для такого маршрута присутствует в примере управляющего списка перенаправления, удалять её оттуда не рекомендуется. Из этой очереди внутренней доставки письмо может быть доставлено по назначению только с помощью планировщика, немедленный запуск сеанса доставки при помещении туда письма в текущей версии не предусмотрен.

При выборе маршрута для внутренней доставки следует обратить внимание на выбор IP-адреса для обращения к SMTP-серверу. Поскольку клиент (агент доставки) и сервер работают на одной машине, сервер "увидит" агента под тем же адресом, который будет использован агентом для обращения к серверу. С одной стороны, это должен быть адрес по возможности из доверенного диапазона, чтобы максимально облегчить прохождение письма, исключив ненужные проверки политик и спам-фильтрацию. Первое, что приходит в голову - использовать стандартный адрес внутреннего замыкания 127.0.0.1, он же localhost. Однако, если спамерам удаётся нащупать дыру в настройках прокси-сервера, они первым делом начинают использовать именно этот адрес. Поэтому в целях безопасности в PigMail+PigProxy жёстко запрещён доступ со всех адресов этого диапазона - от 127.0.0.1 до 127.255.255.255. По этой же причине нежелательно (хотя и менее опасно) использование IP-адреса сетевого интерфейса, предназначенного для связи с локальной сетью. К использованию предлагается особо изощрённый вариант. Необходимо выбрать для внутреннего употребления один секретный IP-адрес (например, 127.5.33.198) и записать его в список доверенных сетей для обхода запрета. Затем этот же адрес записывается в нужную строку списка перенаправления. Также следует изменить настройки агента отправки, чтобы письмо-извещение формировалось в каталоге, соответствующем новым настройкам очереди внутренней доставки.

Вместо связки из планировщика и внешнего агента можно использовать расширенный сервис доставки исходящей почты, незатейливо названный SmtpSend. Он обслуживается плагином **smtpsend**, загрузкой которого при старте сервера можно управлять с помощью специального параметра конфигурационного файла PigMail2.ini. Сервис сочетает в себе функции планировщика и агента доставки. Кроме того, он имеет большое количество настроечных параметров, позволяющих более гибко подстраивать его под капризы окружающей среды. А поскольку сервис работает прямо в контексте SMTP-сервера, он может доставлять письма-предупреждения и письма-возвраты непосредственно в почтовые ящики отправителей, без использования маршрута внутренней доставки. Что, впрочем, нисколько не мешает использовать этот маршрут для нужд других сторонних служб.

Сервис SmtpSend использует три очереди доставки. Работа начинается с первичной очереди - именно туда SMTP-сервер помещает письма, предназначенные для отправки наружу. Для обеспечения практической синхронности отправки обработка этой очереди запускается каждый раз, как туда помещается хоть одно письмо. Для каждого письма, помещённого в первичную очередь, сервис предпринимает всего одну попытку доставки. Если письмо с первого раза доставить не удалось, оно перемещается в очередь повторной доставки. Обработка этой очереди запускается с интервалом в несколько минут. В очереди повторной доставки письмо может находиться несколько часов. Если за это время письмо доставить не удалось, оно перемещается в очередь отложенной доставки, при этом для отправителя генерируется письмо-предупреждение, сообщающее о возникших проблемах. Очередь отложенной доставки - самая медленная. Её обработка производится раз в несколько часов. Письма в этой очереди хранятся несколько суток. Если доставка не удалась и за это время, письмо возвращается отправителю.

Если письмо адресовано нескольким получателям, то отправитель может получить несколько писем-возвратов. Они генерируются каждый раз, когда выясняется невозможность доставки исходного письма хотя бы одному адресату.

Начиная с версии 2.2, в состав PigMail+PigProxy входит сервис локальной (внутренней) доставки, работающий в обход протокола SMTP. Его основное назначение - доставка по назначению переклассифицированных писем. Как правило, адресаты у таких писем локальные, но в некоторых случаях возможна отправка исходящей почты. Сервис также может использоваться для работы с унаследованными приложениями, не умеющими отправлять письма по протоколу SMTP, но обученными формировать файлы писем в формате Eserv. Сервис использует свою очередь - это может быть каталог очереди внутренней доставки, исторически присутствующий в иерархии очередей, но ничто не мешает назначить любой другой каталог. Сервис локальной доставки можно использовать независимо от способа доставки исходящей почты, необходимо только иметь в виду, что при отсутствии планировщика своевременную реакцию на появление письма в очереди может обеспечить только этот сервис.

## *Спам-контроль*

Поскольку количество мусорной почты проявляет устойчивую тенденцию к росту, спам-фильтры следует признать неотъемлемой и весьма существенной частью почтового сервера. В этой конфигурации предлагается на выбор две системы спам-контроля. Одна из них - это статистический анализатор **POPfile**, обладающий к тому же немалыми способностями к обучению. Первоначально он разрабатывался в качестве фильтра-посредника между почтовой программой и POP-сервером, отсюда и название. Последние версии, кроме того, позволяют использовать для общения с ним другой механизм, поэтому появилась возможность

состыковать его с SMTP-сервером. Пока что он достаточно сложен в установке и настройке, однако после запуска о его существовании можно забыть и вспоминать лишь время от времени только затем, чтобы переклассифицировать очередное письмо. Кстати, по своим возможностям POPfile существенно превосходит обычные спам-фильтры, поскольку позволяет не только "отделять мух от котлет", но и сортировать почту по любому количеству произвольных категорий. В стандартной конфигурации Eserv/3 для его работы требуется также web-сервер - при отнесении письма к категории спама отправителю передаётся (в качестве отрицательного ответа на команду протокола SMTP) web-ссылка, позволяющая ему "протолкнуть" ошибочно классифицированное письмо. PigMail+PigProxy тоже предоставляет такую возможность, но позволяет обойтись и без предоставления этой услуги, если развёртывание публичного web-сервера по какой-либо причине невозможно. Кроме этого, переклассификацию может проводить и получатель письма, используя возможности IMAP-сервера - это делается простым перемещением письма из одной IMAP-папки в другую, благо в текущей реализации сообщение, определённое как спам, всё равно может быть доставлено получателю, только при этом помещается не в папку входящих сообщений, а в папку для спама.

Ближайший родственник POPfile статистический анализатор **SpamProtexx** (разработка компании **Agava**) построен на тех же принципах и обладает тем же набором возможностей. По сравнению с POPfile у него один плюс - лёгкость установки - и два минуса - во-первых, это платный компонент, а во-вторых, он не обучен премудростям сложной классификации и работает в рамках двочной логики: либо спам, либо нет.

Ещё один статистический анализатор **LibSD** разработан компанией **Extravalent**, выпустившей в свет POPfile. Собственно, он и представляет собой упрощённую версию последнего, по функциональности близкую к SpamProtexx. Впрочем, у него есть своя изюминка - возможность проверки обнаруженных в письмах ссылок на сайты по онлайновым чёрным спискам - Spam URI Realtime Blocklists или SURBL. В отличие от IP-ориентированных списков Realtime Blackhole List (RBL), SURBL содержит сведения о сайтах, которые рекламируются в спамерских сообщениях. Поскольку значительное число спам-писем (и фишерских писем в частности) призывают посетить какой-либо сайт, и сайтов этих меньше, чем IP-адресов отправителей спама, то SURBL может работать более эффективно, чем RBL - фильтровать до 80 - 90% спама при ложных срабатываниях не выше 0.001 - 0.05%. Надо сказать, что на самом деле этот процент ложных срабатываний достаточно высок - выше, чем у CBL RBL, например. Риск ложных срабатываний в SURBL вызван ещё и тем, что в спам-письмах может намеренно "рекламироваться" и невиновный в спаме сайт. У спам-ловушек, поставляющих ссылки в список, нет надёжного способа их различения, кроме выяснения даты регистрации домена (спам-сайты обычно "молодые") и сверки с белым списком. Если у Вас свежезарегистрированный домен и злые конкуренты, то они легко с помощью спамеров смогут отправить URL вашего нового сайта в SURBL, заказав спам, в котором рекламируется Ваш сайт. Аналогично могут пострадать и Ваши партнёры. Поэтому использовать проверку с помощью SURBL следует с осторожностью.

PigMail+PigProxy позволяет настраивать реакцию сервера на обнаружение спама. Письмо может быть как доставлено получателю, так и перемещено в специальную папку - в этом случае переклассификацию ошибочно задержанных писем будет выполнять администратор сервера. Можно также выбрать форму ответа отправителю - либо, как и в стандартной конфигурации, будет передаваться web-ссылка, либо некий условный идентификатор сообщения и предложение написать администратору. Таким образом, наличие специально настроенного web-сервера не обязательно.

В качестве альтернативного варианта имеется упрощённый контент-фильтр. Его гораздо проще запустить, и он не требует ни обязательного использования web-сервера, ни подключения по протоколу IMAP, зато нуждается в постоянном ручном сопровождении в виде пополнения многочисленных списков. К тому же при его использовании письма, отнесённые к разряду спама, вместо доставки по адресу перемещаются в специальную карантинную папку (хотя в качестве таковой можно указать и папку спама кого-либо из получателей). Поэтому для крупных организаций POPfile, SpamProtexx и LibSD подходят больше.

Ещё один анализатор содержимого - **MContent** (разработка Андрея Матвеева) - прямого отношения к фильтрации спама вроде бы не имеет. Его задача - потрошить письма различными способами: анализировать и изменять содержимое заголовков, извлекать вложенные файлы, удалять нежелательные вложения, добавлять необходимые; при желании можно все вложения перепаковать любимым архиватором и собрать письмо практически заново. Но и эти способности можно поставить на службу целям защиты - с помощью Mcontent несложно организовать блокировку писем с нежелательными типами вложений, если возникнет такая необходимость.

Если все вышеперечисленные системы основаны на анализе содержимого письма (то есть, его необходимо полностью принять, заплатив за соответствующий объём сетевого трафика - хорошо ещё, что спамеры по собственным техническим причинам не шлют больших писем), то модуль поддержки **Sender Policy Framework** позволяет эффективно блокировать приём письма. Кроме собственно SPF, он использует также **MS Caller ID** - эти две различные технологии решают одну задачу: на основании сопоставления электронного адреса отправителя (который передаётся командой протокола SMTP) и IP-адреса подключения делают заключение, соответствует ли одно другому, то есть, действительно ли почтовый домен отправителя располагается именно там, откуда пришло письмо, или же адрес подделан. Основанием для принятия решения служат записанные в параметрах почтового домена политики - правила, определяющие допустимые сочетания почтовых и IP-адресов. В случае подделки письмо можно с почти чистой совестью отклонять не глядя - профессиональные спамеры (как и находящиеся в активном обращении почтовые черви) поголовно используют поддельные адреса. "Почти" - поскольку существует некоторое количество благонамеренных

"поддельщиков", использующих адреса бесплатных почтовых систем при отправке почты с "домашних" почтовых серверов, да и вообще фильтров без ложных срабатываний не бывает. Ситуацию можно поправить путём определения собственных локальных политик, дополняющих или переопределяющих (полностью либо частично) "большую политику". А чтобы исключить попадание под раздачу "своих" отправителей, проверка не производится, если клиент находится на самом почтовом сервере (например, письмо отправляется сценарием web-сервера), подключился из локальной сети или правильно авторизовался.

Новая технология **Yahoo Domain Keys** представляет собой некую комбинацию систем анализа содержимого и онлайновой проверки допустимости. Её суть состоит в том, что в заголовок каждого письма почтовый сервер отправителя включает электронную подпись. Ключ-сертификат, на основании которого сгенерирована эта подпись, публикуется на сервере DNS среди другой информации о домене отправителя, поэтому почтовый сервер получателя всегда имеет возможность проверить достоверность подписи. Несмотря на относительную молодость технологии, применяется она с размахом. Уже сейчас цифровой подписью заверяются все исходящие письма таких могучих почтовых систем, как Google Mail и Yahoo Mail, а это триста миллионов сообщений в день только по статистике последней. Основной и неустранимый недостаток у такой методы один: чтобы проверить подпись, письмо надо принять.

К системе спам-контроля можно также отнести чёрные и белые списки отправителей - как по IP-адресам, так и по почтовым, и по именам узлов, сообщаемым в командах приветствия, а также автоматические проверки существования и доступности почтовых доменов и поиск в онлайновых чёрных списках.

Среди локальных получателей рекомендуется выделить специальный адрес для жалоб (обычно это **abuse@**). Письмам, направленным на этот адрес, позволяется обходить некоторые ограничения - например, чёрный список отправителей, такие письма даже не всегда пропускаются через спам-фильтр. Это специально предоставленная отправителям возможность пожаловаться на необоснованную блокировку адреса или чрезмерную придирчивость спам-фильтра.

Спам-фильтры обслуживаются специальными плагинами - соответственно **popfile**, **spamprotexx**, **contentfilter**, **mcontent**, **spf**, **lsp** и **ydk**, загрузкой которых при старте сервера можно управлять с помощью специальных параметров конфигурационного файла PigMail2.ini. Эти же параметры позволяют временно отключать спам-фильтры в случае возникновения проблем.

## *Управление спамом*

Одна из приятных изюминок POPfile, SpamProtexx и LibSD состоит в чрезвычайной лёгкости подстройки под изменяющуюся ситуацию. Никого не волнует, насколько сложные процессы происходят внутри фильтра - вся подстройка заключается в изменении классификации выбранного письма. При этом для пользователей PigMail+PigProxy/2 процедура переклассификации упрощена до предела. Неудачливым отправителям, в отношении которых спам-фильтр принял неверное решение, достаточно обратиться по web-ссылке, которую сообщил в своём отрицательном ответе SMTP-сервер. Получатели получают в свои руки несколько другой, но не менее простой инструмент.

Письма, классифицированные как спам, доставляются в почтовый ящик получателя, но не в стандартную папку **INBOX**, а в специальную папку. В текущей версии таких папок может быть как минимум три: **spam** (основная папка), **spam-ambiguous** (в эту папку попадают письма, в оценке которых не сошлись одновременно работающие POPfile, SpamProtexx и LibSD) и **spam-virus** (сюда попадают письма, пропущенные антивирусом, но классифицированные противоспамными фильтрами как вирусы - при условии, что отлов вирусов с помощью антиспама не предусмотрен настройками). Имена папок соответствуют названиям классов, под нож попадают письма, получившие класс, название которого начинается с подстроки **spam**. Такого счастья удостаиваются получатели, имеющие привилегии "администратора спама". Получатели, не наделённые такими привилегиями, но имеющие право переклассификации спама, получают весь спам, за исключением вирусов, в одну папку **spam**. Если получатель не обладает необходимой квалификацией либо вообще не принадлежит к локальным (это может быть несуществующий локальный получатель - в том числе из неописанного локального домена, внешний адресат, получатель, принадлежащий перенаправленному домену), проблемное письмо доставляется в ящик специального администратора спама, тоже в папку для спама. Исключение из этого правила делается для почтовых роботов - до них спам вообще не доходит. Для каждого из описанных в конфигурации почтовых доменов расположение такого ящика можно задать индивидуально; кроме того, имеется почтовый ящик спам-администратора по умолчанию.

Переклассификацию можно выполнять путём перемещения писем между различными папками IMAP. Всё, что требуется - это подключение к POP/IMAP-серверу по протоколу IMAP и наличие некоторого опыта. Перемещение письма в папку **spam** из любой другой приводит к запуску процедуры переклассификации письма в категорию спама. Перемещение письма в специальную папку **not_spam** запускает процедуру обратной переклассификации - из спама в категорию "чистых". Имена таких специальных папок IMAP, равно как и назначенные для них специальные действия, задаются в специальном управляющем списке и могут быть достаточно произвольно изменены.

Спам-администратору доступны те же операции по переклассификации почты, что и обычным пользователям. Кроме того, он может инициировать повторную отправку писем получателям - на этот раз в обход спам-фильтров, - по желанию совместив эту операцию с переклассификацией. Естественно, переотправка возможна только в отношении писем, перенаправленных спам-администратору по результатам фильтрации, а не полученных им обычным образом - перечень получателей сохраняется только в перенаправлен-

ных письмах. Переотправка инициируется также перемещением письма в особую папку. Сервер, интерпретируя команду, перемещает письмо в каталог очереди внутренней доставки, где его обязательно обнаружит правильно настроенный работающий планировщик и передаст на повторную обработку SMTP-серверу.

### *Совместная работа POPfile, SpamProtexx и LibSD*

Различные спам-фильтры могут использоваться совместно. Если упрощённый фильтр содержания действует без оглядки на "конкурентов", то совместная работа POPfile, SpamProtexx и LibSD - как втроём, так и любой пары - имеет свои особенности. Считается, что в силу исторических причин POPfile работает дольше и уже достаточно обучен, поэтому может выступать в роли наставника для менее опытных коллег - если классы писем, определённые фильтрами, не совпадают, SpamProtexx и LibSD проходят принудительную переклассификацию такого письма. Аналогичным образом в качестве наставника для LibSD может выступать SpamProtexx. Обучение может производиться как полностью автоматически, так и в ручном режиме. В последнем случае (к нему относится, в частности, ситуация, когда фильтр-наставник не может определить классификацию) письма копируются в специальный каталог **ambiguous**. Рекомендуется разместить этот каталог как одну из папок в почтовом ящике главного спам-администратора. Письма раскладываются в нём по подкаталогам в соответствии с полученной ими классификацией - имена подкаталогов совпадают с названиями классов. Таким образом, спам-администратор легко определяет текущую классификацию и может выступить в роли арбитра, определив письмо в положенный ему класс. Однако перепосылка писем, попавших в **ambiguous**, в текущей версии возможна только из подкаталога **spam** - в остальные подкаталоги они копируются без указания получателей и предназначены только для возможной переклассификации.

## *Загрузка почты из внешних POP-ящиков*

Помимо обычного режима почтового сервера - приём и выдача почтовых сообщений по запросам клиентов, - PigMail+PigProxy/2 способен получать и распределять почту, хранящуюся на других почтовых серверах. Для этого используется специальная служба-плагин **Pop2Smtp**, входящая в состав стандартной конфигурации. В полном соответствии с названием служба регулярно опрашивает заданные в настройках почтовые ящики, загружает из них сообщения по протоколу POP3 и пересылает эти сообщения на заданные в настройках почтовые серверы уже по протоколу SMTP - то есть, является модулем-соединителем. Обычно в качестве сервера-получателя выступает собственный SMTP-сервер, однако ничто не мешает указать любой другой сервер назначения. Такая особенность реализации позволяет выстраивать довольно замысловатые схемы доставки почты.

Альтернативный загрузчик **Pop3Recv** (позаимствовавший у Pop2Smtp значительную часть программного кода) из всех SMTP-серверов знает только один - тот, в связке с которым он работает, - да и вообще передаёт принятые письма на доставку в обход протокола, по внутренним каналам. Этим он напоминает одноимённого агента из состава Eserv/2. Похожи в этом случае и правила доставки - отправитель считается неавторизованным и не имеющим права на отсылку почты за пределы локального домена, поэтому загруженные письма доставляются только локальным получателям; "завернуть" принятое по протоколу POP3 письмо наружу возможно только явным образом, с помощью перенаправления или списка рассылки. К этому ограничению можно относиться по-разному, но в типичных конфигурациях это скорее достоинство, упрощающее настройку сервера. Из прочих отличий от Pop2Smtp имеет смысл отметить большее число индивидуальных настроек обслуживаемых ящиков и ведение полноценных журналов - в том числе и статистических, пригодных для обработки существующими пакетами без их переделки.

Однако в каждой бочке мёда водятся свои минусы. В соответствии со стандартом, у сообщений, попавших в почтовый ящик (то есть, дошедших по назначению), нет "конверта". Пока письмо путешествует от сервера к серверу, "конверт", содержащий адреса отправителя и получателя, существует и передаётся командами протокола SMTP. Но как только письмо достигает конечной точки, эта информация отбрасывается. Разумеется, любой почтовый сервер, как промежуточный, так и конечный, имеет право записать эту информацию в служебные заголовки (шапку) письма - но он точно так же имеет полное право ничего такого не записывать. Более того, нет никакого стандарта, определяющего формат записи такой информации. А то, что записывает в служебные поля письма сформировавшая его программа, вовсе не обязано совпадать с параметрами "конверта". И если подделкой адреса отправителя обычно балуются спамеры и почтовые черви, то реальный адрес получателя может быть скрыт за безличным именем списка рассылки - PigMail+PigProxy/2 тоже умеет действовать подобным образом. Поэтому действует следующее правило - если из шапки письма не удалось извлечь ни одного приемлемого адреса получателя, используется сопоставленный опрашиваемому почтовому ящику адрес по умолчанию. Если же, несмотря на все ухищрения, сервер назначения отказался принимать письмо, есть возможность не оставлять его в ящике, а сохранить у себя до лучших времён - доставляться по назначению оно, конечно, будет уже не автоматически, а с помощью администратора сервера.

## *Антивирусы*

Антивирусы тоже выполняют функцию специфической фильтрации содержимого писем, и тоже превратились в неотъемлемый компонент почтовых систем. На сегодня acSMTP поддерживает работу с тремя анти-

вирусами (впрочем, в природе иногда встречаются раритетные сборки без поддержки антивируса вообще) - это **KAV** производства **Лаборатории Касперского**, **Dr.Web**, продукт компании **Доктор Веб**, и **ClamAV**, один из немногих пока антивирусов, разрабатываемых в открытых кодах. Использовать два и более антивируса одновременно пока не получится, как и переключать их "на лету"; используемый антивирус выбирается при запуске сервера. Помимо основной функции - выявления в проходящей почте вредоносных кодов - антивирусные модули также умеют выполнять автоматическую загрузку обновлений вирусных баз из Интернета или со специального сервера обновлений, устроенного в локальной сети.

При обнаружении заражённого или подозрительного письма SMTP-сервер отвечает клиенту отказом в приёме письма с соответствующим случаю пояснительным текстом, а само письмо перемещает в специальный каталог. Поскольку, в отличие от спама, обнаружение вируса требует быстрой реакции, имеется возможность сформировать и направить автоматические извещения как адресатам заражённого письма, так и администратору сервера. Извещения можно отсылать не на всякий вирусный чих, а только в критических случаях, когда опасность исходит от своих. К сожалению, хитрость вирусописателей не позволяет однозначно отделить агнцев от козлищ. Конечно, если отправитель находится в локальной сети, проблем нет, но, по условиям задачи, существуют и внешние пользователи. Проверка электронного адреса отправителя помогает далеко не всегда - современный червяк с равной лёгкостью воспользуется чужим адресом, пробиваясь от удалённого собственного пользователя, или же подставит локальный адрес в попытке прорваться ICANN знает откуда. Но в редких (будем надеяться) случаях честной рассылки заражённых макровирусами прайс-листов или докладных записок - спасёт.

Если антивирус по собственным внутренним причинам вместо проверки письма вывалился в ошибку, письмо перемещается в специальный карантинный каталог. При этом также могут быть отосланы извещения - как адресатам непроверенного письма, так и администратору сервера. Поскольку этот случай однозначно критический, никакой дополнительной фильтрации не предполагается.

Web-страницы наряду с почтой также представляют собой способ массового распространения вредоносных кодов, благо количество дыр в защите браузеров (особенно Internet Explorer) с течением времени только возастает, поэтому антивирусная фильтрация HTTP-трафика приобретает всё большую актуальность. Eproxy поддерживает работу с **KAV** и **Dr.Web**. Особенности устройства последнего, к сожалению, не позволяют организовать проверку потока непосредственно в памяти, поэтому "паучок" ограничивается проверкой файлов в кэше прокси-сервера. Как и почтовый сервер, Eproxy не позволяет ни менять выбранный антивирус "на лету", ни задействовать оба антивируса одновременно.

Никаких настроек реакции антивируса на обнаружение опасности для прокси-сервера не предусмотрено. Выбора нет - если вредоносный код обнаружен, его надлежит блокировать по пути, чтобы он не достался клиенту. Браузер в этом случае получает имя обнаруженного "зверя", которое и отображает при удачном стечении обстоятельств (когда проверяемый объект имеет текстовый формат).

Антивирусная защита обслуживается целой системой плагинов, главный из которых - **antivirus**. Загрузкой этих плагинов при старте сервера можно управлять с помощью специальных параметров конфигурационного файла PigMail2.ini. Эти же параметры позволяют временно отключать антивирусную защиту (чего вообще-то делать очень не рекомендуется) в случае возникновения проблем.

## *Управление трафиком*[*]

Ограничитель трафика TrafC обеспечивает гибкое управление трафиком - позволяет выделить приоритетным приложениям (или пользователям) достаточную полосу пропускания даже в условиях перегрузки канала (придержав при этом менее приоритетные приложения), позволяет организовать что-то вроде корпоративной биллинговой системы, выделив приложениям или пользователям квоты на использование трафика - заданный объём в течение заданного периода времени. Эти задачи решаются путём регулирования трёх характеристик проходящего трафика: приоритет, средняя скорость и суммарный объём. Основными элементами управления TrafC являются так называемые каналы, которые подразделяются на Band-каналы, выделяющие внутри физического канала ограниченную полосу пропускания (bandwith), и Quota-каналы, задающие общий объём трафика (quota), проходящий через них за определённый период времени.

Band-каналы ограничивают верхнее значение средней скорости. Для этих каналов задаётся пропускная способность в CPS (то есть, столько-то байт в секунду). Band-каналы имеют приоритетные очереди, поэтому в них возможно обслуживание запросов в порядке приоритета. Это означает, что каждый запрос будет ожидать, пока в очереди есть более приоритетный запрос. Приоритетные очереди дают возможность вне конкуренции обслуживать каких-то клиентов (например, почтовых агентов или администратора). Каждому сеансу (каждому подключившемуся клиенту) можно выставить свой приоритет. Значения приоритета используется в очередях Band-каналов. При этом сегменты более приоритетного трафика проходят через канал вперед сегментов менее приоритетного трафика. Приоритетные очереди совместно с виртуальными каналами позволяют очень гибко распределять имеющийся канал связи (полосу пропускания). Они дают возможность гарантировать заданную пропускную способность для части трафика, сравнимую с резервированием части физического канала. При резервировании выделенный канал (или часть канала) не может использоваться иначе, чем под целевой трафик, независимо от наличия этого трафика. Виртуальные каналы

[*] *Основу этого подраздела составляет авторское описание принципа работы TrafC, включённое в состав web-интерфейса Eserv*

позволяют использовать не востребованную часть физического канала под любой другой имеющийся трафик (возможно, также с учётом приоритетов). Использовать наивысший приоритет имеет смысл для постоянного (синхронного) трафика, которому нужна неизменная пропускная способность независимо от пульсаций асинхронного трафика.

Quota-каналы обеспечивают выполнение квот (норм, допусков, ограничений) на объём проходящего через них трафика. Эти каналы подсчитают объём информации. Если период канала не закончился, а его квота исчерпалась, то канал закрывается, и передача данных через него невозможна, пока не закончится период. Для этих каналов задается квота на объём и период времени - например, 10 МБ в неделю.

TrafC может для управления выделять часть трафика в пространстве и во времени. Минимальной частью в пространстве является трафик одного сеанса. Минимальной частью во времени является трафик одного HTTP-запроса или одного соединения. При этом размер сегмента дискретизации сравним с размером IP-пакета. Для выделения части общего трафика используются правила. На основе этих правил для каждой выделенной части трафика определяется приоритет и набор виртуальных каналов, через которые будет пропускаться этот трафик. Таким образом, весь трафик распределяется по виртуальным каналам. Динамические характеристики трафика каждого сеанса будут определяться его приоритетом, набором виртуальных каналов, через которые он проходит, а также параметрами и загруженностью этих каналов. Другими словами, характеристики трафика каждого сеанса будут определяться самым тонким местом в наборе каналов - каналом, в котором удельная на каждый сеанс пропускная способность (с учётом приоритетов) наименьшая.

## *Динамическая генерация каналов*

Выделение пользователям прокси-сервера индивидуальных каналов - типичная корпоративная политика управления трафиком. При этом пользователи обычно разделяются на группы, и для каждой группы устанавливаются одинаковые для всех членов ограничения. Когда пользователей много, описывать каждый личный канал хотя и посильно, но затратно по времени. Для таких ситуаций предусмотрена динамическая генерация каналов на основе классов или шаблонов.

Класс каналов - это особое описание канала, строка в общем списке каналов. Непосредственно канал с именем класса при запуске сервера не создаётся, он используется при работе. Если при обработке запроса пользователю назначается канал, основанный на классе, сервер находит в списке описание канала и на лету создаёт канал с характеристиками, соответствующими шаблону. При повторном обращении сервер находит уже созданный канал и работает с ним обычным образом.

Обращение к каналу, основанному на классе, выглядит почти привычно для тех, кто знаком с основами объектно-ориентированного программирования, классами и наследованием. Имя канала в этом случае записывается в виде **класс::имя**, где **класс** - ссылка по имени на описание класса каналов в списке, а **имя** - это собственно и есть имя вновь назначаемого канала. Пусть, например, в системе имеется описание класса Quota-каналов **Q10W** (пусть это означает 10 мегабайт в неделю), а при обработке запроса встречается назначение канала вида **Q10W::{LUserEmail}_Q10W**. Это означает, что на основе данного шаблона каждому авторизованному пользователю будет назначен индивидуальный канал с именем, основанном на полном имени учётной записи пользователя (что определяется макросом **{LUserEmail}**). Поскольку имена каналов регистрозависимы, а имена учётных записей и доменов - нет, выбран макрос, автоматически приводящий имя учётной записи к нижнему регистру. В принципе, можно приводить и к верхнему; собственно регистр значения не имеет, важно единообразие.

## *Именованные наборы каналов*

В PigMail+PigProxy реализован ещё один механизм, позволяющий несколько упростить управление трафиком. Если некоторый набор каналов используется достаточно часто при различных условиях, его можно сохранить в особом списке под специальным именем и в дальнейшем обращаться к нему по этому имени. Иными словами, за таким именем скрывается составной канал - например, сочетание Band- и Qouta-каналов. Чтобы отличить именованный набор от обычного канала, обращение к набору при назначении каналов записывается в виде **::имя**, где **имя** собственно и является именем набора.

Именованный набор не может быть использован в качестве класса, но сам может содержать обращения к динамически создаваемым каналам. Возможны ссылки и на другие именованные наборы каналов, но такими рекурсивными определениями лучше не увлекаться: это ведёт к увеличению нагрузки на сервер, а в случае ошибок - к зацикливанию.

# Установка и конфигурация

## *Состав*

В состав дистрибутива PigMail+PigProxy входят следующие компоненты:

- HTTP-сервер. Это единственный обязательный компонент для любого варианта установки, поскольку именно он обеспечивает работу web-интерфейса. Кроме того, HTTP-сервер может быть использован и по прямому назначению, для обслуживания корпоративных web-сайтов.
- FTP-сервер. Его назначение - обслуживание файлового хранилища, доступного по протоколу FTP.
- SMTP-сервер. Обеспечивает приём входящей почты и доставку исходящей почты по протоколу SMTP. Также может собирать входящую почту из внешних ящиков по протоколу POP3.
- POP/IMAP-сервер. Обеспечивает доступ почтовых клиентов к обслуживаемым почтовым ящикам по протоколам POP3 и IMAP4.
- Прокси-сервер. Обеспечивает связь локальной и глобальной сетей по протоколам HTTP, FTP и Socks. Также может поддерживать работу почтовых клиентов с внешними почтовыми ящиками по протоколу POP3. Может поддерживать прямое отображение портов TCP и UDP.
- Антивирусное ядро Dr.Web. Может использоваться SMTP-сервером и HTTP-прокси для проверки трафика. В бесплатном варианте имеет ряд серьёзных ограничений. Полная версия приобретается отдельно. В состав дистрибутива включены только исполняемые файлы модулей проверки и загрузки обновлений. Вирусные базы в комплект поставки не входят, их перед запуском антивируса необходимо загрузить отдельно с сервера производителя антивируса.
- Антивирусное ядро KAV. Может использоваться SMTP-сервером и HTTP-прокси для проверки трафика. Бесплатного варианта использования не имеет, приобретается отдельно. В дистрибутив включены две версии антивирусного ядра KAV - KAVSS (версия 4) и KAVE (версия 5). В состав дистрибутива включены только исполняемые файлы модулей проверки и загрузки обновлений. Вирусные базы в комплект поставки не входят, их перед запуском антивируса необходимо загрузить отдельно с сервера производителя антивируса.
- Ядро спам-фильтра SpamProtexx. Устанавливается вместе с SMTP-сервером и может использоваться для отсечения нежелательной почты. Бесплатного варианта использования не имеет, приобретается отдельно. В состав дистрибутива включены только исполняемые файлы спам-фильтра. Базы в комплект поставки не входят, их перед запуском SpamProtexx необходимо загрузить отдельно с сервера **www.eserv.ru**.
- Ядро спам-фильтра LibSD. Устанавливается вместе с SMTP-сервером и может использоваться для отсечения нежелательной почты. Бесплатного варианта использования не имеет, приобретается отдельно. В состав дистрибутива включены только исполняемые файлы спам-фильтра. Базы в комплект поставки не входят, их перед запуском LibSD необходимо загрузить отдельно с сервера **www.eserv.ru**.
- Ядро контент-анализатора MContent. Устанавливается вместе с SMTP-сервером и может использоваться для сложной автоматической обработки проходящей почты. В бесплатном варианте имеет ряд серьёзных ограничений. Полная версия приобретается отдельно.
- Ограничитель трафика TrafC. Устанавливается вместе с прокси-сервером и может использоваться для ограничения полосы пропускания и общего объёма трафика в зависимости от различных условий. В бесплатном варианте имеет ряд серьёзных ограничений. Полная версия приобретается отдельно.
- Статистическая программа Estat32. Используется для анализа работы PigMail+PigProxy. В состав дистрибутива включена бесплатная версия программы, имеющая ряд ограничений. Полная версия приобретается и устанавливается отдельно.
- Статистическая программа Elog. Используется для анализа работы PigMail+PigProxy. Для работы программы должна быть установлена поддержка языка сценариев Perl.
- Вспомогательные программы Eping и Etrace. Используются для проверки доступности удалённых сетевых узлов. Для их работы должна быть установлена поддержка языка сценариев Perl.
- Поддержка языка сценариев ForthScript.

В комплект поставки не входят:

- Антивирус ClamAV.
- Спам-фильтр POPfile.
- Подсистема ведения статистики в базе данных MStat.
- Поддержка языка сценариев Perl.
- Поддержка языка сценариев PHP.
- Поддержка языка сценариев Python.
- Поддержка языка сценариев Parser.
- Поддержка других языков сценариев.

Эти компоненты при необходимости следует загрузить и установить отдельно, указав затем в настройках PigMail+PigProxy пути их размещения.

## Установка

PigMail+PigProxy версии 2 представляет собой самодостаточную сборку и снабжён программой-установщиком. Поэтому ни первоначальная установка, ни обновление с более ранней версии, при условии, что эта более ранняя версия тоже 2 и отличается только цифрами после первой точки, не должна представлять сложности. Установщик всё сделает сам, разве что при первоначальной установке задаст несколько несложных вопросов.

### Обновление предыдущей версии PigMail+PigProxy/2

Обновления версии установкой поверх - штатный режим, предусмотренный программой-установщиком. Все индивидуальные настройки и данные при этом сохраняются. Возможно добавление новых элементов настройки и удаление устаревших. Установщик допускает даже установку поверх актуальной версии - для восстановления повреждённой конфигурации, для доустановки нужных, но не установленных ранее компонентов или для удаления компонентов ненужных. Он даже не обидится, если Вы забудете остановить службы PigMail+PigProxy (что, разумеется, будет предложено на первом же шаге), сам остановит работающие службы и после обновления запустит их заново. Одним словом, откиньтесь в кресле и получайте удовольствие.

### Полуавтоматическое обновление с PigMail+PigProxy/1

Если у Вас установлен PigMail+PigProxy версии 1, обновить эту установку до версии 2 в один шаг не получится. Возможных вариантов настройки слишком много, и совершенно не обязательно, что установщик справится с преобразованием без ошибок. Вероятность ошибок возрастает, если Вы задумали обновить не самую последнюю из версий PigMail+PigProxy/1. Поэтому рекомендуется сначала обновить имеющуюся установку до актуальной версии традиционным способом (вручную) и только после этого приступать к переходу на новую версию.

Независимо от степени новизны обновляемой версии установщик с задачей сам не справится. Он свято следует принципу "не навреди" и при обнаружении признаков существования "старшего брата" предлагает только пробную установку куда-нибудь в отдельный каталог, напрочь отказываясь устанавливать службы, чтобы не нарушить работу уже существующего приложения. Установщику придётся помочь.

1. Выполните пробную установку PigMail+PigProxy в отдельный каталог рядом с рабочей установкой. Согласитесь на предложение установщика выполнить импорт настроек и данных из существующей установки версии 1.
2. Запустите HTTP-сервер новой установки (сервер рабочей установки придётся остановить) и с помощью web-интерфейса проверьте, насколько успешно прошёл импорт настроек. Проверьте ВСЕ пути к каталогам и файлам конфигурации и данных, которые в настройках PigMail+PigProxy/1 были заданы явно, в том числе (и особенно) в управляющих списках. Исправьте ошибки установщика.
3. Убедитесь, что все рабочие данные - содержимое почтовых ящиков, обученные базы антиспама и прочее содержимое каталога **DATA** - успешно и полностью скопированы в новую установку. Обратите особое внимание на публикации - сайты HTTP и FTP, - заданные в списках виртуальных каталогов соответствующих серверов. Содержимое этих каталогов НЕ копируется: установщик полагает, что они либо располагаются в стандартном каталоге, определённом для публикаций, и потому скопированы вместе с ним, либо находятся вне иерархии каталогов PigMail+PigProxy, и, следовательно, двигать их незачем. Если эти предположения неверны, исправьте ситуацию.
4. Тщательно проверив результаты импорта и убедившись в отсутствии ошибок, полностью удалите Eserv/3 с помощью штатной программы. В памяти системы не должно остаться никаких следов - ни установленных служб, ни более формальных отметок.
5. Снова запустите установщик PigMail+PigProxy, выберите режим изменения конфигурации и установите службы.

Если все шаги выполнены аккуратно, и при этом ни одно животное не пострадало, то после запуска серверов они заработают в новой конфигурации.

### Ручное обновление с PigMail+PigProxy/1

Если Ваши настройки в части расположения каталогов и файлов настроек и данных радикально отличаются от принятых по умолчанию, установщик может наделать слишком много ошибок при импорте. Вероятность ошибок возрастает, если Вы задумали обновить не самую последнюю из версий PigMail+PigProxy/1. Поэтому рекомендуется сначала обновить имеющуюся установку до актуальной версии традиционным способом (вручную) и только после этого приступать к переходу на новую версию. Если Вы опасаетесь проблем с вышеописанным полуавтоматическим переходом (или уже имели возможность наблюдать большое количество таких проблем), выполните обновление вручную.

Здесь установщик сам не справится. Он свято следует принципу "не навреди" и при обнаружении признаков существования "старшего брата" предлагает только пробную установку куда-нибудь в отдельный каталог, напрочь отказываясь устанавливать службы, чтобы не нарушить работу уже существующего приложения. Установщику придётся помочь.

1. Сохраните все отредактированные Вами управляющие списки, конфигурационный файл **Eserv3.ini** и другие данные конфигурации - всё, что обычно хранится в каталоге **CONF**.
2. Сохраните все рабочие данные - содержимое почтовых ящиков, обученные базы антиспама и прочее содержимое каталога **DATA**.
3. С помощью штатной программы полностью удалите Eserv/3. В памяти системы не должно остаться никаких следов - ни установленных служб, ни более формальных отметок.
4. Выполните установку PigMail+PigProxy. Об ответах на вопросы установщика можете особо не задумываться, они в конечном итоге нигде не сохранятся.
5. Скопируйте сохранённый конфигурационный файл **Eserv3.ini** в каталог установки PigMail+PigProxy под именем **PigMail2.ini**, перезаписав имеющийся там файл.
6. Откройте только что скопированный файл в Блокноте и отредактируйте два параметра в секции **[Dirs]**:
   6.1. **Conf**. По идее, этот параметр не нуждается в редактировании - либо Вы его оставили в первоначальном состоянии, либо изменили сознательно. Просто проверьте, на какой каталог он указывает. Если хотите изменить расположение каталога, то сейчас самое время.
   6.2. **PigMailConf**. Скорее всего, его значение не совпадает со значением параметра **Conf**. Если Вы намеревались собрать все данные конфигурации вместе, то сейчас самое время поменять настройки.
7. Теперь, когда Вы определились с расположением данных конфигурации, поместите сохранённые настроечные данные на определённое для них место.
8. Скопируйте в надлежащие места сохранённые рабочие данные.
9. Проверьте целостность системы управляющих списков и шаблонов с помощью специального инструмента администратора - он допускает возможность автономного запуска с помощью командного файла **checklists.bat** в каталоге **CONF** или **CONF.orig**. Протокол работы программы будет отображён на экране в окне Блокнота. Язык протокола - английский (**en**) или русский (**ru**) - можно указать в качестве параметра запуска командного файла, воспользовавшись окном командной строки. Программа способна воссоздавать отсутствующие списки. По возможности для этого используются образцы списков из каталога **CONF.orig**, а если подходящий файл не обнаруживается, то программа создаёт пустой список. Кроме того, она умеет преобразовывать списки из старого формата в новый. Однако, делает она это, исходя из собственных среднестатистических представлений, поэтому результат преобразования следует тщательно проверить и при необходимости внести исправления.

Если все шаги выполнены аккуратно, и при этом ни одно животное не пострадало, то после запуска серверов они заработают в новой конфигурации.

## *Обновление со стандартной конфигурации Eserv/3*

Здесь установщик сам не справится. Он свято следует принципу "не навреди" и при обнаружении признаков существования "старшего брата" предлагает только пробную установку куда-нибудь в отдельный каталог, напрочь отказываясь устанавливать службы, чтобы не нарушить работу уже существующего приложения. Установщику придётся помочь.

1. Выполните пробную установку PigMail+PigProxy в отдельный каталог и внимательно изучите его содержимое (см. раздел **Структура каталогов**). Это поможет Вам понять различие между двумя конфигурациями и правильно перенести данные.
2. Сохраните все отредактированные Вами управляющие списки, конфигурационный файл **Eserv3.ini** и другие данные конфигурации - всё, что обычно хранится в каталоге **CONF**.
3. Сохраните все рабочие данные - содержимое почтовых ящиков, обученные базы антиспама и прочее содержимое каталога **DATA**.
4. С помощью штатной программы полностью удалите Eserv/3. В памяти системы не должно остаться никаких следов - ни установленных служб, ни более формальных отметок.
5. Выполните чистовую установку PigMail+PigProxy. Об ответах на вопросы установщика можете особо не задумываться, они в конечном итоге нигде не сохранятся.
6. Скопируйте сохранённый конфигурационный файл **Eserv3.ini** в каталог установки PigMail+PigProxy под именем **PigMail2.ini**, перезаписав имеющийся там файл.
7. Откройте только что скопированный файл в Блокноте и отредактируйте два параметра в секции **[Dirs]**:
   7.1. **Conf**. По идее, этот параметр не нуждается в редактировании - либо Вы его оставили в первоначальном состоянии, либо изменили сознательно. Просто проверьте, на какой каталог он указывает. Если хотите изменить расположение каталога, то сейчас самое время.
   7.2. **PigMailConf**. Этого параметра там нет. Создайте его с тем же значением, что и у параметра **Conf**.
8. Теперь, когда Вы определились с расположением данных конфигурации, поместите сохранённые настроечные данные на определённое для них место. Обратите внимание существующую при настройках по умолчанию на разницу в расположении каталогов и отдельных файлов.
9. Скопируйте в надлежащие места сохранённые рабочие данные. Обратите внимание существующую при настройках по умолчанию на разницу в расположении каталогов данных.
10. Проверьте целостность системы управляющих списков и шаблонов с помощью специального инструмента администратора - он допускает возможность автономного запуска с помощью командного файла **checklists.bat** в каталоге **CONF** или **CONF.orig**. Протокол работы программы будет отображён на экра-

не в окне Блокнота. Язык протокола - английский (**en**) или русский (**ru**) - можно указать в качестве параметра запуска командного файла, воспользовавшись окном командной строки. Программа способна воссоздавать отсутствующие списки. По возможности для этого используются образцы списков из каталога **CONF.orig**, а если подходящий файл не обнаруживается, то программа создаёт пустой список. Кроме того, она умеет преобразовывать списки из старого формата в новый. Однако, делает она это, исходя из собственных среднестатистических представлений, поэтому результат преобразования следует тщательно проверить и при необходимости внести исправления.

11. Заполните списки и шаблоны в соответствии с Вашими потребностями (см. разделы **Назначение и формат управляющих списков** и **Шаблоны**, а также **Вопросы и ответы**). Также дополните Ваш конфигурационный файл PigMail2.ini в каталоге установки недостающими индивидуальными параметрами, переопределяющими стандартные настройки (см. раздел **Параметры файла настроек PigMail2.orig.ini**). Хотя этот шаг можно слегка отложить и выполнить с помощью web-интерфейса.

Если все шаги выполнены аккуратно, и при этом ни одно животное не пострадало, то после запуска серверов они заработают в новой конфигурации.

## *Настройка и управление*

Настройка и управление PigMail+PigProxy могут выполняться различными способами. Для запуска, остановки и перезапуска служб можно использовать стандартные средства Windows - ярлыки главного меню, командные файлы, расположенные в каталогах служб, апплет консоли управления, утилиты командной строки **net** и **sc**. Для изменения настроек достаточно стандартного Блокнота или его продвинутых аналогов (см. разделы **Параметры файла настроек PigMail2.orig.ini**, **Назначение и формат управляющих списков** и **Шаблоны**). Управляющие списки можно также редактировать с помощью электронных таблиц Microsoft Excel и OpenOffice.org Calc. Этот способ наиболее предпочтителен для списков большого объёма (пятьсот строк и более). В остальных же случаях удобнее всего использовать web-интерфейс, по умолчанию доступный на портах 3140 (незащищённый HTTP) и 3143 (защищённый HTTP).

## Структура каталогов

| | |
|---|---|
| \ | "Корневой" каталог. Здесь располагаются основной файл настроек **PigMail2.orig.ini** и пользовательский файл настроек **PigMail2.ini**. |
| **acFTP** | Основной каталог FTP-сервера. |
| **conf** | Каталог основной конфигурации FTP-сервера. Здесь располагаются файлы правил и модулей расширения (плагинов). |
| **ftp** | Каталог конфигурации собственно FTP-сервера. |
| **plugins** | Каталог расположения плагинов FTP-сервера. |
| **acl** | Поддержка списков управления доступом к FTP-серверу. При желании может быть отключена для экономии памяти и повышения быстродействия. |
| **plugins** | Каталог размещения общих плагинов FTP-сервера. |
| **pigmail.myconf** | Описание необходимых для работы расширений FTP-сервера. |
| **acIMAP** | Основной каталог IMAP/POP-сервера. |
| **conf** | Каталог основной конфигурации IMAP/POP-сервера. Здесь располагаются файлы правил и модулей расширения (плагинов). |
| **imap** | Каталог конфигурации собственно MAP-сервера для работы по незащищённому соединению. |
| **imaps** | Каталог конфигурации собственно MAP-сервера для работы по защищённому соединению. |
| **plugins** | Каталог размещения общих плагинов IMAP/POP-сервера. |
| **pigmail.myconf** | Описание необходимых для работы расширений IMAP/POP-сервера. |
| **pop** | Каталог конфигурации собственно POP-сервера для работы по незащищённому соединению. |
| **plugins** | Каталог расположения плагинов POP-сервера. |
| **callback** | Специальные расширения протокола POP3, предназначенные для поддержки монитора почтовых ящиков **Piafi MailKnocker**. |
| **pops** | Каталог конфигурации собственно POP-сервера для работы по незащищённому соединению. |
| **acSMTP** | Основной каталог SMTP-сервера. |
| **conf** | Каталог основной конфигурации SMTP-сервера. Здесь располагаются файлы правил и модулей расширения (плагинов). |
| **plugins** | Каталог расположения "общих" плагинов SMTP-сервера. |
| **localdelivery** | Поддержка сервиса локальной доставки почты. |
| **pigmail.myconf** | Описание необходимых для работы расширений SMTP-сервера. |
| **pop2smtp** | Стандартный загрузчик внешней POP-почты Pop2Smtp. |
| **pop3recv** | Альтернативный стандартному загрузчик внешней POP-почты Pop3Recv. |
| **smtpsend** | Поддержка расширенного сервиса доставки исходящей почты SmtpSend. |
| **smtp** | Каталог конфигурации SMTP-сервера. |
| **customrules** | В этом каталоге рекомендуется размещать собственные правила обработки почты. Этот каталог изначально пуст и не перезаписывается при установке обновлений. |
| **MContent.samples** | В этом каталоге размещены примеры правил для контент-анализатора Mcontent. |

| | |
|---|---|
| **delivery** | В этом каталоге расположены файлы правил доставки почты. |
| **filters** | В этом каталоге расположены файлы правил фильтрации почты. |
| **headers** | В этом каталоге расположены файлы правил обработки заголовков писем. |
| **plugins** | Каталог расположения плагинов SMTP-сервера. |
| **alerter** | Поддержка формирования административных оповещений о не доставленной по различным причинам почте. При желании может быть безболезненно отключена для экономии памяти и повышения быстродействия. |
| **antivirus** | Антивирусная проверка проходящей почты. Может быть при желании отключена для экономии памяти и повышения быстродействия. |
| **clamav** | Антивирусная проверка почты антивирусом ClamAV. |
| **drweb** | Антивирусная проверка почты антивирусом Dr.Web. |
| **kav** | Антивирусная проверка почты антивирусом KAV версии 4 (KAVSS). |
| **kav5** | Антивирусная проверка почты антивирусом KAV версии 5 (KAVE). |
| **autoresponders** | Поддержка автоответчиков. При желании может быть безболезненно отключена для экономии памяти и повышения быстродействия. |
| **callback** | Специальные расширения протокола SMTP, предназначенные для поддержки монитора почтовых ящиков **Piafi MailKnocker**. |
| **contentfilter** | Спам-фильтр (альтернативный по отношению к POPfile/SpamProtexx/LibSD). При желании может быть безболезненно отключён для экономии памяти и повышения быстродействия. |
| **email_validator** | Плагин, выполняющий проверку адреса получателя на целевом сервере. |
| **headers** | Вспомогательный плагин, обеспечивающий расширенную поддержку заголовочных полей письма. Используется упрощённым фильтром содержания, автоответчиком, обработчиком "магических слов" и встроенными почтовыми роботами. |
| **lsp** | Поддержка локальных политик для отправителя. Может быть при желании отключена для экономии памяти и повышения быстродействия. |
| **magicwodrs** | Поддержка дополнительной маршрутизации почты с использованием "магических слов" в полях шапки письма. При желании может быть безболезненно отключена для экономии памяти и повышения быстродействия. |
| **maillists** | Поддержка списков рассылки. При желании может быть безболезненно отключена для экономии памяти и повышения быстродействия. |
| **notifier** | Поддержка извещений о поступлении входящей почты. При желании может быть безболезненно отключена для экономии памяти и повышения быстродействия. |
| **paser** | Вспомогательный плагин, обеспечивающий разбор письма, принятого с использованием блочного метода передачи BDAT, когда анализ содержимого во время приёма невозможен. |
| **popdupcheck** | Вспомогательный плагин, обеспечивающий удаление дубликатов спам-почты при совместной работе внешнего загрузчика POP-почты (Pop3Recv или Pop2Smtp) и спам-фильтров - POPfile, SpamProtexx, LibSD и упрощённого контент-фильтра. |
| **quota** | Поддержка квот на общий объём и количество писем в локальных почтовых ящиках. При желании может быть безболезненно отключена для экономии памяти и повышения быстродействия. |

| | |
|---|---|
| **rbl** | Поддержка фильтрации по IP-адресу отправителя с использованием списка блокирующих сервисов. При желании может быть отключена для экономии памяти и повышения быстродействия. |
| **robots** | Поддержка почтовых роботов. При желании может быть безболезненно отключена для экономии памяти и повышения быстродействия. |
| **scheduler** | Планировщик запуска агента отправки исходящей почты. Не используется при включённой поддержке расширенного сервиса доставки исходящей почты SmtpSend. |
| **spf** | Поддержка Sender Policy Framework. |
| **tarpit** | Дополнительные расширения. |
| **ydk** | Поддержка Yahoo Domain Keys. |
| **robots** | В этом каталоге рекомендуется размещать файлы правил встроенных почтовых роботов. Изначально здесь располагается простой пример такого робота, а также несколько готовых к применению роботов, описание которых приведено в приложении 3. |
| **DomainLister** | В этом каталоге располагаются файлы правил робота, выполняющего функции динамического общедоменного списка рассылки. |
| **ListEmail** | В этом каталоге располагаются файлы правил робота, выполняющего внесение заданных адресов в список доверенных либо запрещённых отправителей. |
| **ListMailSender** | В этом каталоге располагаются файлы правил робота на основе контент-анализатора MContent, выполняющего внесение адресов отправителей передаваемых ему писем в список доверенных либо запрещённых отправителей. |
| **MailClassify** | В этом каталоге располагаются файлы правил робота на основе контент-анализатора MContent, выполняющего переклассификацию писем в спам-анализаторах POPfile, SpamProtexx и LibSD. |
| **mcontent** | В этом каталоге располагаются файлы правил робота-фильтра на основе контент-анализатора MContent, обрабатывающего все проходящие письма. |
| **acWEB** | Основной каталог HTTP-сервера. |
| **conf** | Каталог основной конфигурации HTTP-сервера. Здесь располагаются файлы правил и модулей расширения (плагинов). |
| **http** | Каталог конфигурации собственно HTTP-сервера. |
| **plugins** | Каталог расположения плагинов HTTP-сервера. |
| **acl** | Поддержка списков управления доступом к HTTP-серверу. При желании может быть отключена для экономии памяти и повышения быстродействия. |
| **day_dialer** | Поддержка работы с модемом - дозвон, перезвон при обрыве связи, отключение. |
| **fs** | Поддержка встроенных (выполняющихся непосредственно в контексте сервера) сценариев. |
| **impersonation** | Поддержка имперсонализации сценариев. При желании может быть отключена для экономии памяти и повышения быстродействия. |
| **list_dir** | Поддержка вывода оглавления каталога. |
| **multiport** | Поддержка работы на произвольном количестве портов. При желании может быть отключена для экономии памяти и повышения быстродействия. |
| **ssi** | Поддержка Server Side Includes (SSI). |
| **plugins** | Каталог расположения "общих" плагинов HTTP-сервера. |

| | |
|---|---|
| **pigmail.myconf** | Описание необходимых для работы расширений HTTP-сервера. |
| **antivirus** | Каталог для размещения исполняемых файлов антивирусных "движков". Там же могут располагаться и вирусные базы, если нет причины использовать для этого другой каталог. |
| **clamav** | Каталог для размещения файлов ядра антивируса ClamAV. Сам антивирус в комплект поставки не входит, его надо устанавливать отдельно. |
| **drweb** | Каталог для размещения файлов ядра антивируса Dr.Web. Здесь же по умолчанию размещаются вирусные базы антивируса. Сами базы в комплект поставки не входят, их надо загрузить отдельно - например, с помощью штатного загрузчика обновлений. |
| **kav** | Каталог для размещения файлов ядра антивируса KAV версии 4 (KAVSS). |
| **data** | Каталог для размещения вирусных баз антивируса KAV. Сами базы в комплект поставки не входят, их надо загрузить отдельно - например, с помощью штатного загрузчика обновлений. |
| **kav5** | Каталог для размещения файлов ядра антивируса KAV версии 5 (KAVE). |
| **cert** | Каталог для размещения сертификатов. Здесь располагаются как сертификаты, играющие роль ключей активации компонентов, так и (в соответствии с настройками по умолчанию) сертификаты, обеспечивающие работу защищённых соединений. |
| **CommonPlugins** | Базовый каталог правил и плагинов, общих для всех серверов. |
| **plugins** | Каталог расположения плагинов, общих для всех серверов. |
| **access_codes** | Дополнительное расширение - коды прав доступа и методы работы с ними, общие для FTP- и HTTP-сервера. Используются плагином acl. |
| **auth** | Описание специфических процедур авторизации пользователя для различных типов источника авторизации. |
| **auth_e2** | Описание процедуры авторизации по списку пользователей Eserv/2. |
| **auth_md5** | Описание процедуры авторизации по списку пользователей Eserv/3. |
| **auth_md5plain** | Описание процедуры авторизации по объединённому списку пользователей Eserv/3. |
| **auth_nt** | Описание процедуры авторизации по списку домена Active Directory. |
| **auth_odbc** | Описание процедуры авторизации по базе данных. |
| **auth_cache** | Ускоритель авторизации. Запоминает реквизиты успешно авторизовавшихся пользователей и сведения о членстве пользователей в группах. |
| **auth_lib** | Дополнительные расширения для поддержки различных методов авторизации. |
| **cache_ini** | Дополнительное расширение - кэширование параметров конфигурационного файла PigMail2.ini на время активности подключения. |
| **cache_log_str** | Дополнительное расширение - кэширование списка форматных строк журналов. |
| **console** | Дополнительное расширение - работа сервера с активным консольным окном. Обычно применяется для отладки и для использования требует ручного редактирования правил. |
| **dial** | Поддержка автоматического модемного дозвона при необходимости. |
| **firewall** | Поддержка межсетевого экрана. |
| **flagmon** | Монитор флагов. |
| **geo_ip** | Определение географического положения (с точностью до региона) клиента по IP-адресу. |

| | |
|---|---|
| **groups_ext** | Поддержка расширенной (кросс-доменной) группировки пользователей. |
| **ids_memo** | Поддержка блокиратора атак. Плагин обеспечивает хранение информации о событиях, могущих быть признаками атаки. |
| **include_url** | Поддержка загрузки контента с внешних серверов. |
| **mailroll** | Дополнительное расширение - почтовый реестр. Хранение истории переписки позволяет автоматически регулировать уровень подозрительности почтовых фильтров. |
| **match_ext** | Дополнительное расширение - расширенная функция сравнения строки с шаблоном, поддерживающая большое количество образцов. |
| **mlog_db** | Дополнительное расширение - поддержка сохранения журналов работы в базе данных. |
| **mlogc** | Поддержка мультижурнальности - запись журналов в файлы с произвольными именами и в несколько журналов разного формата одновременно, а также поддержка уровней журнала. |
| **mstat.pigmail** | Дополнительные функции поддержки подсистемы ведения статистики в базе данных MStat. Расширение, обеспечивающее основные функции, необходимо устанавливать отдельно. |
| **pigmail** | Описание необходимых для работы расширений, общих для всех серверов. |
| **popfile** | Поддержка спам-фильтра POPfile. |
| **proc_list** | Дополнительное расширение - доступ к списку активных процессов Windows. |
| **ras_list** | Дополнительное расширение - доступ к списку модемных и VPN соединений. |
| **rconsole** | Поддержка дистанционного наблюдения за текущей работой сервера по протоколу telnet. |
| **sd** | Поддержка спам-фильтра LibSD. |
| **snmp** | Поддержка агента SNMP. |
| **spamprotexx** | Поддержка спам-фильтра SpamProtexx. |
| **ssl** | Поддержка работы по защищённому соединению. |
| **syslog** | Поддержка записи файла журнала через отдельную программу, работающую по протоколу syslog. |
| **tcp_list** | Дополнительное расширение - доступ к списку активных соединений TCP/IP. |
| **CONF** | Это каталог **рабочей** конфигурации, в котором располагаются управляющие списки и шаблоны. |
| **lists** | Каталог для размещения общих для системы управляющих списков. |
| **antispam** | Каталог для размещения общих управляющих списков спам-фильтров. |
| **ftp** | Каталог для размещения управляющих списков FTP-сервера. |
| **http** | Каталог для размещения управляющих списков HTTP-сервера. |
| **imap** | Каталог для размещения управляющих списков IMAP-сервера. |
| **mstat** | Каталог для размещения управляющих списков сборщика статистики MStat. |
| **pop** | Каталог для размещения управляющих списков POP-сервера. |
| **pop2smtp** | Каталог для размещения управляющих списков загрузчика внешней POP-почты Pop2Smtp. |
| **pop3recv** | Каталог для размещения управляющих списков загрузчика внешней POP-почты Pop3Recv. |

| | |
|---|---|
| **proxy** | Каталог для размещения управляющих списков прокси-сервера. |
| **ftpp** | Каталог для размещения управляющих списков FTP-прокси. |
| **user-acl** | Каталог для размещения списков управления доступом к FTP-прокси. |
| **httpp** | Каталог для размещения управляющих списков HTTP-прокси. |
| **user-acl** | Каталог для размещения списков управления доступом к HTTP-прокси. |
| **pop3p** | Каталог для размещения управляющих списков POP3-прокси. |
| **socks** | Каталог для размещения управляющих списков Socks-прокси. |
| **user-acl** | Каталог для размещения списков управления доступом к Socks-прокси. |
| **tcpmap** | Каталог для размещения управляющих списков отображения портов TCP. |
| **trafc** | Каталог для размещения управляющих списков ограничителя трафика TrafC. |
| **udpmap** | Каталог для размещения управляющих списков отображения портов UDP. |
| **smtp** | Каталог для размещения управляющих списков SMTP-сервера. |
| **autoresponders** | Каталог для размещения вспомогательных списков автоответчиков. |
| **filters** | Каталог для размещения списков фильтрации содержимого писем. |
| **maillists** | Каталог для размещения списков рассылки. |
| **restricted** | Каталог для размещения списков ограниченного доступа ("серых" списков). |
| **smtpsend** | Каталог для размещения управляющих списков расширенного сервиса доставки исходящей почты SmtpSend. |
| **pub** | Каталог по умолчанию для публикации данных. |
| **ftproot** | Используемый по умолчанию корневой каталог FTP-сайта. |
| **guest_area** | Образец гостевого каталога - виртуального корня для анонимных подключений. |
| **secret** | Образец секретного каталога, доступного только особо доверенным пользователям. |
| **wwwroot** | Используемый по умолчанию корневой каталог web-сайта. |
| **admin** | Образец каталога, закрытого паролем. |
| **img** | Каталог с используемыми сайтом изображениями. |
| **readme** | Здесь располагаются описания форматов всех управляющих списков. |
| **templates** | Каталог для размещения общих для системы шаблонов. |
| **ftp** | Каталог для размещения шаблонов, используемых FTP-сервером. |
| **http** | Каталог для размещения шаблонов, используемых HTTP-сервером. |
| **en** | Каталог для размещения шаблонов ответов HTTP-сервера на английском языке. |
| **ru** | Каталог для размещения шаблонов ответов HTTP-сервера на русском языке. |
| **imap** | Каталог для размещения шаблонов, используемых IMAP-сервером. |
| **pop** | Каталог для размещения шаблонов, используемых POP-сервером. |
| **proxy** | Каталог для размещения шаблонов, используемых прокси-сервером. |
| **ftpp** | Каталог для размещения шаблонов, используемых FTP-прокси. |
| **httpp** | Каталог для размещения шаблонов, используемых HTTP-прокси. |

| | |
|---|---|
| **en** | Каталог для размещения шаблонов ответов HTTP-прокси на английском языке. |
| **errors** | Каталог для размещения шаблонов с расшифровками системных ошибок WinSock. |
| **en** | Каталог для размещения шаблонов с расшифровками системных ошибок WinSock на английском языке. |
| **ru** | Каталог для размещения шаблонов с расшифровками системных ошибок WinSock на русском языке. |
| **ru** | Каталог для размещения шаблонов ответов HTTP-прокси на русском языке. |
| **pop3p** | Каталог для размещения шаблонов, используемых POP3-прокси. |
| **smtp** | Каталог для размещения шаблонов, используемых SMTP-сервером. |
| **smtpsend** | Каталог для размещения шаблонов, используемых расширенным сервисом доставки исходящей почты SmtpSend. |
| **CONF.orig** | Это **образец** каталога **CONF** рабочей конфигурации, в котором располагаются управляющие списки и шаблоны. Его не рекомендуется использовать для работы непосредственно - для этого существует каталог **CONF**, а данный каталог лучше оставить в качестве образца. |
| **lists** | Каталог для размещения общих для системы управляющих списков. |
| **antispam** | Каталог для размещения общих управляющих списков спам-фильтров. |
| **ftp** | Каталог для размещения управляющих списков FTP-сервера. |
| **http** | Каталог для размещения управляющих списков HTTP-сервера. |
| **imap** | Каталог для размещения управляющих списков IMAP-сервера. |
| **mstat** | Каталог для размещения управляющих списков сборщика статистики MStat. |
| **pop** | Каталог для размещения управляющих списков POP-сервера. |
| **pop2smtp** | Каталог для размещения управляющих списков загрузчика внешней POP-почты Pop2Smtp. |
| **pop3recv** | Каталог для размещения управляющих списков загрузчика внешней POP-почты Pop3Recv. |
| **proxy** | Каталог для размещения управляющих списков прокси-сервера. |
| **ftpp** | Каталог для размещения управляющих списков FTP-прокси. |
| **user-acl** | Каталог для размещения списков управления доступом к FTP-прокси. |
| **httpp** | Каталог для размещения управляющих списков HTTP-прокси. |
| **user-acl** | Каталог для размещения списков управления доступом к HTTP-прокси. |
| **pop3p** | Каталог для размещения управляющих списков POP3-прокси. |
| **socks** | Каталог для размещения управляющих списков Socks-прокси. |
| **user-acl** | Каталог для размещения списков управления доступом к Socks-прокси. |
| **tcpmap** | Каталог для размещения управляющих списков отображения портов TCP. |
| **trafc** | Каталог для размещения управляющих списков ограничителя трафика TrafC. |
| **udpmap** | Каталог для размещения управляющих списков отображения портов UDP. |
| **smtp** | Каталог для размещения управляющих списков SMTP-сервера. |
| **autoresponders** | Каталог для размещения вспомогательных списков автоответчиков. |

| | |
|---|---|
| **filters** | Каталог для размещения списков фильтрации содержимого писем. |
| **maillists** | Каталог для размещения списков рассылки. |
| **restricted** | Каталог для размещения списков ограниченного доступа ("серых" списков). |
| **smtpsend** | Каталог для размещения управляющих списков расширенного сервиса доставки исходящей почты SmtpSend. |
| **pub** | Каталог по умолчанию для публикации данных. |
| **ftproot** | Используемый по умолчанию корневой каталог FTP-сайта. |
| **guest_area** | Образец гостевого каталога - виртуального корня для анонимных подключений. |
| **secret** | Образец секретного каталога, доступного только особо доверенным пользователям. |
| **wwwroot** | Используемый по умолчанию корневой каталог web-сайта. |
| **admin** | Образец каталога, закрытого паролем. |
| **img** | Каталог с используемыми сайтом изображениями. |
| **readme** | Здесь располагаются описания форматов всех управляющих списков. |
| **templates** | Каталог для размещения общих для системы шаблонов. |
| **ftp** | Каталог для размещения шаблонов, используемых FTP-сервером. |
| **http** | Каталог для размещения шаблонов, используемых HTTP-сервером. |
| **en** | Каталог для размещения шаблонов ответов HTTP-сервера на английском языке. |
| **ru** | Каталог для размещения шаблонов ответов HTTP-сервера на русском языке. |
| **imap** | Каталог для размещения шаблонов, используемых IMAP-сервером. |
| **pop** | Каталог для размещения шаблонов, используемых POP-сервером. |
| **proxy** | Каталог для размещения шаблонов, используемых прокси-сервером. |
| **ftpp** | Каталог для размещения шаблонов, используемых FTP-прокси. |
| **httpp** | Каталог для размещения шаблонов, используемых HTTP-прокси. |
| **en** | Каталог для размещения шаблонов ответов HTTP-прокси на английском языке. |
| **errors** | Каталог для размещения шаблонов с расшифровками системных ошибок WinSock. |
| **en** | Каталог для размещения шаблонов с расшифровками системных ошибок WinSock на английском языке. |
| **ru** | Каталог для размещения шаблонов с расшифровками системных ошибок WinSock на русском языке. |
| **ru** | Каталог для размещения шаблонов ответов HTTP-прокси на русском языке. |
| **pop3p** | Каталог для размещения шаблонов, используемых POP3-прокси. |
| **smtp** | Каталог для размещения шаблонов, используемых SMTP-сервером. |
| **smtpsend** | Каталог для размещения шаблонов, используемых расширенным сервисом доставки исходящей почты SmtpSend. |
| **DATA** | Каталог размещения данных. Большей частью это устаревающая информация, подлежащая либо удалению, либо переносу в архив. |
| **cache** | Каталог размещения кэша HTTP-прокси. |

| | |
|---|---|
| **DB** | Базовый каталог для размещения различных баз данных, используемых при работе серверов. |
| **smtp** | Каталог для размещения баз данных, используемых при работе SMTP-сервера. |
| **flags** | Базовый рабочий каталог монитора флагов. |
| **proxy** | Рабочий каталог монитора флагов для прокси-сервера. |
| **log** | Каталог размещения оперативных журналов работы серверов. |
| **mail** | Каталог для работы с почтой. |
| **abuse** | В этот каталог в некоторых случаях помещается почта, направленная специальному (abuse) получателю отправителем из чёрного списка. |
| **antispam** | В этом каталоге размещаются рабочие файлы спам-фильтров - и POP-file, и SpamProtexx, и LibSD, и упрощённого фильтра содержания, - подлежащие длительному хранению, - в частности, перечень Message-ID загруженных писем. |
| **sd** | В этом каталоге размещаются базы данных спам-фильтра LibSD. Сами базы в комплект поставки не входят, их надо загрузить отдельно. |
| **spamprotexx** | В этом каталоге размещаются базы данных спам-фильтра SpamProtexx. Сами базы в комплект поставки не входят, их надо загрузить отдельно. |
| **archive** | В этот каталог помещаются архивные копии проходящих через сервер писем. |
| **bounce** | В этот каталог помещается почта, отправленная автоответчику, если такую почту разрешено принимать. |
| **forward** | Этот каталог используется для передачи писем, пришедших локальным получателям, на обработку в другую почтовую систему (в ситуации, когда PigMail+PigProxy/2 работает только на приём почты, а почтовые ящики обслуживаются другим программным пакетом) либо специфическому обработчику наподобие неинтегрированной версии контент-анализатора **MContent**. |
| **in** | Каталог для размещения почтовых ящиков пользователей. |
| **unlisted** | Специальный почтовый ящик, предлагаемый пользователю IMAP/POP-сервера, ящик которого на сервере не обнаружен. |
| **INBOX** | Папка "Входящие". |
| **infected** | В этот каталог перемещаются письма, в которых был обнаружен вредоносный программный код. |
| **loop** | В этот каталог помещаются письма, признанные зациклившимися, то есть, содержащие в шапке ненормально большое количество заголовков Received:. |
| **mail_att_files** | Этот каталог предназначен для размещения вложенных файлов, извлекаемых из писем контент-анализатором **MContent**. |
| **malformed** | В этот каталог перемещаются искажённые письма, в которых обнаружены ошибки формата. |
| **nonreadable** | В этот каталог перемещаются письма, признанные нечитаемыми (изначально - содержащие китайскую кодировку). |
| **out** | Каталог общей очереди доставки исходящей почты. Отсюда её забирает агент отправки или сервис SmtpSend. |
| **127.0.0.10** | Пример базового каталога очереди внутренней доставки. |

| | |
|---|---|
| **25** | Пример рабочего каталога очереди внутренней доставки. Сюда агент отправки помещает письма-возвраты, сюда же перемещаются для повторной доставки переклассифицированные спам-администратором письма. Если используется планировщик (плагин scheduler) или расширенный сервис SmtpSend, то этот каталог регулярно просматривается, и находящиеся в нём письма пересылаются на SMTP-сервер. |
| **overquoted** | В этот каталог перемещаются письма, размер которых превысил установленные ограничения. |
| **pop3recv** | В этом каталоге размещаются рабочие файлы загрузчика внешней POP-почты Pop3Recv, подлежащие длительному хранению, - в частности, перечень Message-ID загруженных писем. |
| **quarantined** | Каталог "карантина". В него перемещаются письма, поступившие с некоторых адресов из чёрного списка. |
| **retry** | Каталог очереди отложенной доставки. Сюда перемещаются письма, которые не удалось доставить в течение заранее заданного срока. Дальнейшие попытки доставки таких писем будут предприниматься существенно реже. |
| **spam** | В этот каталог перемещаются письма, не прошедшие спам-фильтрацию. |
| **spool** | Рабочий каталог для обработки почты. |
| **try** | Каталог очереди повторной доставки. Сюда сервис SmtpSend перемещает письма, которые не удалось доставить с первого раза. |
| **unchecked** | В этот каталог перемещаются письма, антивирусная проверка которых не состоялась из-за внутренней ошибки антивируса. |
| **undelivered** | В этот каталог перемещаются письма, которые по каким-либо причинам не могут быть никуда доставлены. |
| **stat** | Каталог для размещения статистических журналов сервера. |
| **advsoft** | Каталог для размещения статистических журналов в формате программ **ProxyInspector** и **MailDetective** производства компании **AdvSoft**. |
| **elog** | Каталог для размещения статистических журналов в формате программы **Elog**, разработанной **Игорем Панасенко** из компании **ЛЭНК**. |
| **estat** | Каталог для размещения статистических журналов в формате программы **Estat32**, разработанной **Андреем Волковым** из **EPE Labs**. |
| **maillog** | Каталог для размещения статистических журналов в собственном текстовом формате. |
| **temp** | Каталог для размещения временных файлов (изначально - журналов работы агентов отправки исходящей почты). |
| **Docs** | Каталог, содержащий настоящую документацию в HTML-формате. |
| **en** | HTML-документация на английском языке. |
| **ru** | HTML-документация на русском языке. |
| **Elog** | Основной каталог статистической программы Elog. |
| **cgi-bin** | В этом каталоге размещаются исполняемые на HTTP-сервере сценарии Elog. |
| **lib** | В этом каталоге размещаются используемые программой библиотеки общего назначения. |
| **docs** | Каталог, содержащий описание программы. |
| **ini** | Каталог с файлами настроек программы. |
| **locale** | Каталог с файлами локализации программы. |
| **static** | В этом каталоге размещаются статические компоненты Elog. |

| | |
|---|---|
| **ePing** | Каталог, в котором располагаются вспомогательные утилиты ePing и eTrace. |
| **Eproxy** | Основной каталог прокси-сервера. |
| **conf** | Каталог основной конфигурации прокси-сервера. Здесь располагаются файлы правил и модулей расширения (плагинов). |
| **ftp-proxy** | Каталог конфигурации FTP-прокси. |
| **plugins** | Каталог расположения плагинов FTP-прокси. |
| **acl** | Поддержка списков управления доступом к FTP-прокси. При желании может быть отключена для экономии памяти и повышения быстродействия. |
| **http-proxy** | Каталог конфигурации HTTP-прокси. |
| **plugins** | Каталог расположения плагинов HTTP-прокси. |
| **acl** | Поддержка списков управления доступом к HTTP-прокси. При желании может быть отключена для экономии памяти и повышения быстродействия. |
| **alias** | Поддержка алиасов - специальных коротких обозначений для наиболее часто посещаемых web-ресурсов. При желании может быть безболезненно отключена для экономии памяти и повышения быстродействия. |
| **antivirus** | Антивирусная проверка HTTP-трафика. Может быть при желании отключена для экономии памяти и повышения быстродействия. |
| **drweb** | Антивирусная проверка HTTP-трафика антивирусом Dr.Web. В силу ограничений антивирусного ядра проверка проходящего трафика "на лету" не поддерживается, антивирус проверяет только файлы, попадающие в кэш HTTP-прокси. |
| **kav** | Антивирусная проверка HTTP-трафика антивирусом KAV версии 4 (KAVSS). |
| **kav5** | Антивирусная проверка HTTP-трафика антивирусом KAV версии 5 (KAVE). |
| **auth** | Вспомогательный плагин поддержки HTTP-авторизации. Используется списками управления доступом к HTTP-прокси. |
| **cache** | Поддержка кэширования трафика. При желании может быть отключена для экономии памяти. |
| **hierarchy** | Поддержка каскадного включения прокси-серверов. |
| **redirect** | Поддержка перенаправления, позволяющая при обращении браузера к одному web-ресурсу направить его на другой. При желании может быть безболезненно отключена для экономии памяти и повышения быстродействия. |
| **spylog** | Поддержка выборочного подробного отслеживания пользовательских запросов. Предназначена в помощь разработчикам web-приложений и сотрудникам служб собственной безопасности. В остальных случаях может быть безболезненно отключена для экономии памяти и повышения быстродействия. |
| **plugins** | Каталог расположения "общих" плагинов прокси-сервера. |
| **acl** | Вспомогательный плагин поддержки списков доступа. |
| **http-map** | Поддержка так называемого HTTP-отображения. |
| **monitoring** | Поддержка удалённого наблюдения за работой прокси-сервера через web-браузер. Наблюдателю передаётся содержимое главного журнала прокси-сервера. |
| **pigmail.myconf** | Описание необходимых для работы конфигурации расширений прокси-сервера. |

| | |
|---|---|
| **pop3proxy** | Поддержка POP3-прокси. При желании и отсутствии необходимости может быть безболезненно отключена для экономии памяти. |
| **tcpmap** | Поддержка отображения портов TCP. При желании и отсутствии необходимости может быть безболезненно отключена для экономии памяти. |
| **TrafC** | Поддержка управления трафиком. |
| **udpmap** | Поддержка отображения портов UDP. При желании и отсутствии необходимости может быть безболезненно отключена для экономии памяти. |
| **socks** | Каталог конфигурации Socks-прокси. |
| **plugins** | Каталог расположения плагинов Socks-прокси. |
| **acl** | Поддержка списков управления доступом к Socks-прокси. При желании может быть отключена для экономии памяти и повышения быстродействия. |
| **hierarchy** | Поддержка каскадного включения прокси-серверов. |
| **ext** | В этом каталоге размещаются сторонние библиотеки, используемые для расширения возможностей PigMail+PigProxy. |
| **robots** | В этом каталоге рекомендуется размещать файлы внешних почтовых роботов. |
| **script** | Каталог, содержащий сценарии поддержки и другие компоненты web-интерфейса и обработчик сценариев ForthScript. |
| **control** | Базовый каталог для размещения HTML-страниц и статических компонентов web-интерфейса. |
| **wwwroot.pigmail** | В этом каталоге размещаются HTML-страницы и статические компоненты web-интерфейса, используемые в PigMail+PigProxy. |
| **fs** | В этом каталоге располагаются исполняемые файлы обработчика сценариев ForthScript. |
| **fs.pigmail** | Сценарии и компоненты web-интерфейса, используемые в PigMail+PigProxy. |
| **en** | Шаблоны и текстовые ресурсы web-интерфейса на английском языке. |
| **lists** | Управляющие списки, используемые web-интерфейсом. |
| **ru** | Шаблоны и текстовые ресурсы web-интерфейса на русском языке. |
| **scripts** | Сценарии на языках Форт и SQL, используемые web-интерфейсом. |
| **utils** | В этом каталоге размещаются вспомогательные утилиты и агенты PigMail+PigProxy. |

# Параметры файла настроек PigMail2.orig.ini

Файл настроек используется для управления поведением сервера. Параметры файла настроек считываются файлами правил и плагинами по мере необходимости. Доступ к параметрам осуществляется посредством специальных слов вида **ИмяСекции[ИмяПараметра]**. Все считанные параметры представляют собой текстовые строки, для получения числовых значений необходимо выполнять преобразование. Если параметр содержит оператор подстановки значения **{}**, подстановка выполняется в процессе считывания на основании текущих значений.

Формат записи значений подчиняется типовым правилам записи текстовых строк. Если значение не содержит пробелов, оно может быть записано как есть. При наличии пробелов строка обязательно заключается в двойные кавычки **"**. Если в строку необходимо вставить символ кавычки, то во избежание неоднозначности его следует заменять макроподстановкой **{"}** - два апострофа в фигурных скобках. Для бесконфликтной вставки символа левой фигурной скобки **{** можно использовать макроподстановку **{S'{'}**.

Правая колонка таблицы содержит следующие условные обозначения:

**!** - параметр обязательно должен быть явно определён в PigMail2.ini
**!*** - параметр настоятельно рекомендуется явно определить в PigMail2.ini
***** - параметр рекомендуется явно определить в PigMail2.ini
**+** - параметр не рекомендуется явно определять в PigMail2.ini
**&** - параметр особым образом обрабатывается при запуске сервера
$ - параметр запоминается (кэшируется) сервером в момент подключения клиента на время соединения с клиентом, это кэширование не может быть отменено
**?** - параметр кэшируется сервером в памяти на время соединения с клиентом; это кэширование может быть отменено

## *Секция Server - общие параметры сервера*

| | | |
|---|---|---|
| **HostName** | Имя сервера в глобальной сети. Начальное значение - **{SERVER_NAME}**, использующее имя, автоматически определённое при запуске сервера. К сожалению, имя не всегда определяется правильно, поэтому его можно задать явно, например, **HostName=mail.mycompany.ru**. | * ? |
| **DefaultDomain** | Домен по умолчанию. Именно это значение запрашивает установщик PigMail+PigProxy при первоначальной установке. Напрямую оно нигде не используется, а служит начальным значением для определения почтового домена по умолчанию и домена авторизации по умолчанию. Начальное значение - **{Server[HostName]}**. | ! |
| **DefaultMailDomain** | Почтовый домен по умолчанию. В PigMail+PigProxy предусмотрены отдельные понятия почтового домена и домена авторизации. Начальное значение **{Server[DefaultDomain]}** (позволяющее уменьшить количество вопросов при установке) рекомендуется заменить на имя своего основного почтового домена. | !* |
| **ExternIP** | Внешний (доступный из интернета) IP-адрес сервера. В большинстве случаев он определяется автоматически, поэтому можно не заполнять. Пример: **ExternIP=194.87.0.50**. | & |
| **Certificate** | Имя файла формата PEM, содержащего закрытый ключ и сертификаты, используемые при организации защищённого (SSL) соединения сервера с клиентом. Начальное значение - **..\cert\server.pem**. | |

| | | |
|---|---|---|
| **SslVerifyClient** | Определяет режим проверки подлинности сертификатов клиентской стороны при установлении защищённого соединения. Задаётся либо числовым кодом, либо символьным обозначением:<br>**SSL_VERIFY:NONE** - сертификат клиента не запрашивается (числовое значение 0);<br>**SSL_VERIFY:STANDARD** - сертификат клиента запрашивается, но соединение устанавливается и при отсутствии сертификата; при переустановке соединения сертификат запрашивается повторно (числовое значение 1);<br>**SSL_VERIFY:FORCE** - сертификат клиента запрашивается, при его отсутствии соединение не устанавливается; при переустановке соединения сертификат запрашивается повторно (числовое значение 3);<br>**SSL_VERIFY:ONCE** - сертификат клиента запрашивается, но соединение устанавливается и при отсутствии сертификата; при переустановке соединения сертификат повторно не запрашивается (числовое значение 5);<br>**SSL_VERIFY:ONCE_FORCE** - сертификат клиента запрашивается, при его отсутствии соединение не устанавливается; при переустановке соединения сертификат повторно не запрашивается (числовое значение 7).<br>Начальное значение - **SSL_VERIFY:NONE**, то есть, клиентские сертификаты принимаются без проверки. | * |
| **AdminEmail** | Почтовый адрес администратора сервера. Может использоваться в шаблонах сообщений об ошибках, в почтовых извещениях и т.п. Начальное значение - **postmaster@{Server[DefaultMailDomain]}**. | ! |
| **AdminName** | Имя (звание, титул) администратора сервера. Обычно подставляется в заголовки автоматически формируемых писем в поле адреса или в качестве подписи. Начальное значение - **Postmaster**. | ! |
| **SiteName** | Название обслуживаемого сервером web-сайта. Это параметр настройки HTTP-сервера, который может использоваться в различном контексте, в том числе и в автоответах почтового сервера. Начальное значение - **"This Site"**. | |
| **SiteUrl** | Ссылка (URL) для доступа к обслуживаемому сервером web-сайту. Это параметр настройки HTTP-сервера, который может использоваться в различном контексте, в том числе и в автоответах почтового сервера. Начальное значение - **http://{Server[HostName]}/**. | |
| **SafeMode** | Если службы PigMail+PigProxy вдруг начинают сбоить и писать в журналы многочисленные сообщения про EXCEPTION, то виной этому может быть интенсивная работа с динамической памятью. Установка этому параметру ненулевого значения и перезапуск служб отключает оптимизацию динамической памяти и за счёт некоторого роста максимального объёма служб позволяет повысить устойчивость их работы. Начальное значение - **0**. | & |
| **InteractiveMode** | Определяет способ реакции сервера на ряд серьёзных ошибок, которые могут обнаружиться во время запуска - например, на попытку повторного открытия порта TCP. При любом ненулевом значении этого параметра сервер при обнаружении такой ошибки выводит на экран диалоговое окно, позволяющее прервать запуск либо продолжить работу. Если значение нулевое, запуск прерывается, а информация об ошибке записывается в журнал. Начальное значение - **0**. | & |
| **LockIntruders** | Определяет, использовать ли блокировку атак. Признаком атаки считается частое повторение различных нежелательных событий - таких, как ошибки авторизации. Если частота следования таких событий для какого-либо IP-адреса клиентского подключения превышает установленную в настройках величину, то этот адрес заносится в список запрещённых сетей. IP-адреса, находящиеся в списках локальных или доверенных сетей, блокировке не подвергаются. Если при запуске сервера этот параметр имеет любое ненулевое значение, подключается плагин **ids_memo**, обеспечивающий хранение и накопление информации о нежелательных событиях. После этого параметр может использоваться для временного отключения блокировки атак, если его работа будет создавать какие-либо проблемы. Начальное значение - **0**, блокировка атак не используется. | * |

| | | |
|---|---|---|
| **IdsMemoDB** | Файл базы данных, в которой блокиратор атак хранит и накапливает информацию о нежелательных событиях. Начальное значение - **{Dirs[DB]}\IdsMemo.db3**. | & |
| **AuthFailCount** | Пороговое значение числа ошибок авторизации. Если количество неудачных попыток авторизации за определённый временной интервал на одном из серверов для одного и того же IP-адреса клиентского подключения превышает заданную этим параметром величину, это считается атакой - со всеми вытекающими отрицательными последствиями для соответствующего клиента. Начальное значение - **5**. | * |
| **AuthFailPeriod** | Период подсчёта ошибок авторизации. Если количество неудачных попыток авторизации за определённый этим параметром временной интервал на одном из серверов для одного и того же IP-адреса клиентского подключения превышает заданную величину, это считается атакой - со всеми вытекающими отрицательными последствиями для соответствующего клиента. Длительность периода задаётся в минутах. Начальное значение - **10**. | * |
| **UseTarpit** | Указывает, использовать ли при выдаче отказов клиенту Tarpit - "липучку". В этом случае отрицательные ответы искусственно задерживаются, что уменьшает нагрузку на сеть. Начальное значение - **1**, то есть, использовать. | * |
| **TarpitInterval** | Если задано использование "липучки", то этот параметр задаёт длительность задержки в секундах. Начальное значение - **10**. | * |
| **LogLevel** | Задаёт уровень детализации оперативного журнала. Параметр может принимать значения от 1 до 9. Чем выше уровень, тем больше подробностей пишется в журнал. Для совместимости с ранними версиями, в которых уровень детализации не задавался, нулевое значение соответствует максимальному уровню детализации. Начальное значение - **6**. | * |
| **LogToIntDb** | Определяет, вести ли журнал во внутренней базе данных формата SQLite3. Если при запуске сервера этот параметр имеет любое ненулевое значение, создаётся база данных, в которую в процессе работы сервера записывается дополнительная информация. Начальное значение - **0**. | * & |
| **LogToEStat** | Определяет, ведёт ли сервер статистику в формате программы **Estat32**, разработанной **Андреем Волковым** из **EPE Labs** для обработки статистических журналов Eserv/2. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **1**. | * |
| **LogToAdvSoft** | Определяет, ведёт ли сервер статистику в формате программ **ProxyInspector** и **MailDetective** производства компании **AdvSoft**. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **1**. | * |
| **LogToElog** | Определяет, ведёт ли сервер статистику в формате программы **Elog**, разработанной **Игорем Панасенко** из компании **ЛЭНК** для обработки статистических журналов Eserv/3. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **1**. | * |
| **LogToMaillog** | Определяет, ведёт ли сервер статистику в собственном текстовом формате. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **1**. | * |

| | | |
|---|---|---|
| **LogToMStat** | Определяет, используется ли подсистема ведения статистики в базе данных MStat, разработанная Андреем Матвеевым. Этот сборщик статистики имеет немалое преимущество перед текстовыми журналами, позволяя хранить и эффективно обрабатывать статистическую информацию за большие периоды времени, измеряемые годами. Но для его работы необходима установка дополнительного приложения - СУБД одного из поддерживаемых сборщиком типов. Если указано любое ненулевое число, статистика в базе данных ведётся. Начальное значение - **0**. | * |

## *Секция Dirs - расположение каталогов настроек и данных*

| | | |
|---|---|---|
| **Data** | Расположение базового каталога данных. Путь задаётся относительно EXE-файлов серверов, для которых "корневой" каталог является родительским. Поэтому начальное значение - **..\DATA**. | |
| **Mail** | Расположение базового каталога почтовых данных. Начальное значение - **{Dirs[Data]}\mail**. Здесь располагаются почтовые ящики пользователей и специальные каталоги для работы с почтой (см. раздел **Структура каталогов**). | |
| **Cache** | Расположение файлового кэша HTTP-прокси-сервера. Начальное значение - **{Dirs[Data]}\cache**. | |
| **TrafC** | Расположение каталога хранимых данных ограничителя трафика **TrafC**. В текущей версии PigMail+PigProxy ограничение трафика реализовано только в составе прокси-сервера. Начальное значение - **{Dirs[Data]}\trafc**. | |
| **Temp** | Расположение каталога для временных файлов. Начальное значение - **{Dirs[Data]}\temp**. Здесь накапливаются промежуточные файлы, а также файлы журналов, которые по некоторым причинам не являются "ротируемыми" (собираемыми в один файл в соответствии с датой), - например, журналы работы агентов отправки исходящей почты smtpsend, smtpsend3 и smtpsend4. | ? |
| **Logs** | Расположение каталога оперативных журналов сервера. Начальное значение - **{Dirs[Data]}\log**. Текущая версия PigMail+PigProxy позволяет расположить журналы каждого сервера в отдельном каталоге - это определяется в параметрах настройки серверов. Начальная настройка определяет для оперативных журналов один общий каталог, что не должно представлять большой сложности, поскольку все журналы различаются именами файлов. | |
| **Stat** | Расположение каталога статистики сервера. Начальное значение - **{Dirs[Data]}\stat**. | |
| **EStat** | Расположение каталога статистических журналов формата **Estat32**. Начальное значение - **{Dirs[Stat]}\estat\log**. | ? |
| **AdvSoft** | Расположение каталога статистических журналов формата **ProxiInspector** и **MailDetective**. Начальное значение - **{Dirs[Stat]}\advsoft**. | ? |
| **Elog** | Расположение каталога статистических журналов формата **Elog**. Начальное значение - **{Dirs[Stat]}\elog**. | ? |
| **Maillog** | Расположение каталога статистических журналов собственного текстового формата. Начальное значение - **{Dirs[Stat]}\maillog**. | ? |
| **TrafCStat** | Расположение каталога статистических журналов ограничителя трафика **TrafC**. В текущей версии PigMail+PigProxy ограничение трафика реализовано только в составе прокси-сервера. Начальное значение - **{Dirs[Stat]}\trafc**. | |
| **Flags** | Расположение базового рабочего каталога монитора флагов. Монитор флагов представляет собой вспомогательный сервис, обслуживающий ряд расширений PigMail+PigProxy, в частности, ограничитель трафика **TrafC**. Монитор отслеживает появление в рабочем каталоге так называемых флаг-файлов и в зависимости от их наименования и содержимого инициирует выполнение различных действий. Некоторые администраторские функции web-интерфейса, в частности, управление квотами, используют возможности монитора флагов. Начальное значение - **{Dirs[Data]}\flags**. | |

| | | |
|---|---|---|
| **DB** | Расположение базового каталога для размещения различных баз данных, используемых при работе серверов. Примером такой базы является почтовый реестр MailRoll. Начальное значение - **{Dirs[Data]}\DB**. | |
| **PigMailConf** | Расположение базового каталога управляющих файлов расширенной конфигурации PigMail+PigProxy версии 1. В настройках по умолчанию этот параметр не используется, но присутствует на случай, если унаследованные пользовательские настройки содержат явную ссылку на него. Для правильной работы проверки целостности управляющих списков параметр в базовом конфигурационном файле **PigMail2.orig.ini** должен содержать ссылку на каталог с образцами списков. Путь задаётся относительно EXE-файлов серверов, для которых "корневой" каталог является родительским. Поэтому начальное значение - **..\CONF.orig**. Файл пользовательских настроек **PigMail2.ini**, создающийся при первоначальной установке, изначально содержит другое значение этого параметра - **..\CONF**. | ! |
| **Conf** | Расположение базового каталога управляющих файлов стандартной конфигурации. Для правильной работы проверки целостности управляющих списков параметр в базовом конфигурационном файле **PigMail2.orig.ini** должен содержать ссылку на каталог с образцами списков. Путь задаётся относительно EXE-файлов серверов, для которых "корневой" каталог является родительским. Поэтому начальное значение - **..\CONF.orig**. Файл пользовательских настроек **PigMail2.ini**, создающийся при первоначальной установке, изначально содержит другое значение этого параметра - **..\CONF**. | ! |
| **Lists** | Расположение базового каталога управляющих списков сервера. Этот параметр имеет глобальное действие - он влияет на большинство настроек PigMail+PigProxy. Определять его явно в пользовательском файле настроек **PigMail2.ini** настоятельно не рекомендуется - если только Вы не выстраиваете свою собственную раскладку каталогов. Начальное значение - **{Dirs[Conf]}\lists**. Подробно списки рассмотрены в разделе **Назначение и формат управляющих списков**. | + |
| **Templates** | Расположение базового каталога используемых сервером шаблонов. Определять этот параметр явно в пользовательском файле настроек **PigMail2.ini** настоятельно не рекомендуется - если только Вы не выстраиваете свою собственную раскладку каталогов. Начальное значение - **{Dirs[Conf]}\templates**. Подробно шаблоны рассмотрены в разделе **Шаблоны**. | + |
| **Pub** | Расположение базового каталога данных HTTP- и FTP-сервера. Определять этот параметр явно в пользовательском файле настроек **PigMail2.ini** настоятельно не рекомендуется - если только Вы не выстраиваете свою собственную раскладку каталогов. Начальное значение - **{Dirs[Conf]}\pub**. | + |
| **CommonPlugins** | Расположение базового каталога правил и плагинов, общих для всех серверов. Определять этот параметр явно в пользовательском файле настроек **PigMail2.ini** настоятельно не рекомендуется - если только Вы не выстраиваете свою собственную раскладку каталогов. Путь задаётся относительно EXE-файлов серверов, для которых "корневой" каталог является родительским. Поэтому начальное значение - **..\CommonPlugins**. | + |

## *Секция Lists - общие управляющие списки сервера*

| | | |
|---|---|---|
| **LocalDomains** | Файл со списком доменов, для которых SMTP-сервер будет принимать приходящую извне почту. Остальных получателей будет отвергать, если отправитель не относится к "своим". Этот же список (в нарушение принципа разделения почтовых доменов и доменов авторизации - возможно, в будущем это нарушение будет устранено) используется для определения способов авторизации в домене. В этой конфигурации функции списка локальных доменов урезаны - он используется только для определения общих параметров домена и выявления несуществующего получателя, в основном же используется отдельный список локальных пользователей. Начальное значение - **{Dirs[Lists]}\LocalDomains.txt**. | ? |
| **LocalNetworks** | Файл со списком локальных сетей, обслуживаемых сервером. Почта, поступающая с этих IP-адресов, будет отправляться наружу, если получатели не являются локальными пользователями. Начальное значение - **{Dirs[Lists]}\LocalNetworks.txt**. | ? |

| | | |
|---|---|---|
| **DomainIP** | Файл со списком IP-адресов, назначенных сетевым интерфейсам компьютера. Если адрес интерфейса, к которому подключилась клиентская программа, присутствует в этом списке, то домен авторизации по умолчанию (если клиент при авторизации не указал свой домен) назначается на основании содержимого списка. В противном случае используется заданный в следующей секции глобальный домен авторизации. Этот же список используется для выбора параметров защищённого (SSL) соединения сервера с клиентом - используемого сертификата сервера и режима проверки подлинности сертификатов клиентской стороны. Начальное значение - **{Dirs[Lists]}\DomainIP.txt**. | |
| **IpMacAuth** | Файл со списком, устанавливающим соответствие пары адресов - IP и MAC (media access control address - уникальный аппаратный идентификатор сетевого адаптера, имеющий длину 6 байтов) - и именем учётной записи (логином) пользователя. Этот список позволяет выполнять автоматическую авторизацию пользователя в тех случаях, когда это по каким-либо причинам невозможно или нежелательно делать явно, а надёжность авторизации по спискам локальных и доверенных сетей оставляет желать лучшего. Начальное значение - **{Dirs[Lists]}\IpMacAuth.txt**. | |
| **UserMailBoxes** | Файл со списком, сопоставляющим данные авторизации пользователя с адресом его почтового ящика. Поскольку они не тождественны (наилучшая политика безопасности состоит как раз в том, чтобы имя учётной записи - логин - не совпадало с именем почтового ящика), POP/IMAP-сервер при авторизации должен каким-то образом получить дополнительную информацию о пользователе. Если используется авторизация по списку пользователей формата Eserv/3 или по базе данных, это несложно - адреса электронной почты легко доступны. При авторизации по списку пользователей формата Eserv/2 или домена Active Directory эта информация либо отсутствует вообще, либо (в текущей версии) недоступна. Тогда в качестве источника информации выступает дополнительный список. Начальное значение - **{Dirs[Lists]}\UserMailBoxes.txt**. | |
| **Db3Log** | Файл базы данных формата SQLite3, в который записываются дополнительные журналы, если это разрешено настройками сервера. Начальное значение - **{Dirs[Logs]}\log.db3**. | |

## *Секция AUTH - настройка авторизации*

| | | |
|---|---|---|
| **DefaultAuthDomain** | Домен авторизации по умолчанию. Будет использоваться ТОЛЬКО в том случае, когда при авторизации не задаётся домен. В PigMail+PigProxy предусмотрены отдельные понятия почтового домена и домена авторизации. Начальное значение **{Server[DefaultDomain]}** (позволяющее уменьшить количество вопросов при установке) рекомендуется заменить на имя своего основного домена авторизации. | !* |
| **AuthSources** | Файл со списком настройки разных способов авторизации для разных источников. По имени домена в списке локальных доменов находится имя источника авторизации, далее по имени источника определяется СПОСОБ авторизации (домен Active Directory, файл со списком, база данных и т.д.) и параметры этого способа авторизации для конкретного источника - имя домена, или параметры доступа к БД и SQL запрос, или URL сервера, и т.д. Начальное значение - **{Dirs[Lists]}\AuthSources.txt**. | ? |
| **AuthPlugins** | Каталог, в котором располагаются общие процедуры авторизации. В качестве стандарта принято его расположение в подкаталоге **plugins** каталога **CommonPlugins**. В любом случае Вам необходимо указать реальное расположение этих процедур. Начальное значение - **{Dirs[CommonPlugins]}\plugins\auth**. | |
| **UserList** | Файл со списком пользователей формата Eserv/3. Используется, если выбран способ авторизации по списку с паролями, зашифрованными по алгоритму MD5 (**MD5File**). Начальное значение - **{Dirs[Lists]}\UserList-{Domain}.txt**, то есть, имя файла списка изменяется в соответствии с текущим доменом авторизации. | |

| | | |
|---|---|---|
| **GroupList** | Файл со списком группировки пользователей формата Eserv/3. Используется, если выбран способ авторизации по списку с паролями, зашифрованными по алгоритму MD5 (**MD5File**). Начальное значение - **{Dirs[Lists]}\GroupsList-{Domain}.txt**, то есть, имя файла списка изменяется в соответствии с текущим доменом авторизации. | |
| **PlainUserList** | Файл со списком пользователей формата Eserv/3. Используется, если выбран способ авторизации по объединённому списку с паролями, зашифрованными по алгоритму MD5 (**MD5PlainFile**). Начальное значение - **{Dirs[Lists]}\PlainUserList.txt**. | |
| **PlainGroupList** | Файл со списком группировки пользователей формата Eserv/3. Используется, если выбран способ авторизации по объединённому списку с паролями, зашифрованными по алгоритму MD5 (**MD5PlainFile**). Начальное значение - **{Dirs[Lists]}\PlainGroupsrList.txt**. Использование общего списка для различных доменов (одного способа авторизации) позволяет задействовать кросс-доменную группировку - в этом случае в группу могут входить пользователи из разных доменов. | |
| **Eserv2Userlist** | Файл со списком пользователей, извлечённым из Eserv.ini версии Eserv/2.x. Можно не тратить время на извлечение и использовать INI-файл в оригинальном виде - система предусматривает и такой вариант. Используется, если выбран способ авторизации по такому списку (**AuthFile**). Начальное значение - **{Dirs[Lists]}\E2UserBase.txt**. В принципе, имя файла также может включать в себя имя текущего домена. Однако пользоваться этим списком не слишком удобно, поскольку в него невозможно включить дополнительные параметры. | |
| **Eserv2Grouplist** | Файл со списком группировки пользователей, извлечённым из Eserv.ini версии Eserv/2.x. Можно не тратить время на извлечение и использовать INI-файл в оригинальном виде - система предусматривает и такой вариант. Может быть использован тот же файл, что и для списка пользователей, благо формат Eserv.ini это позволяет. Используется, если выбран способ авторизации по такому списку (**AuthFile**). Начальное значение - **{Dirs[Lists]}\E2UserBase.txt**. В принципе, имя файла также может включать в себя имя текущего домена. | |
| **NTdomain** | Имя домена Active Directory или локального компьютера под управлением Windows линейки NT, по списку пользователей которого выполняется авторизация пользователей, если выбран соответствующий способ авторизации (**NtLogon**). Начальное значение - **myntdomain**. | |
| **DefaultAuthSource** | Имя источника авторизации из списка источников авторизации. Используется, если выбран способ авторизации в соответствии с параметрами источника авторизации (**AuthSource**). Начальное значение - **Eserv3**, что в соответствии с изначальным содержимым списка источников авторизации соответствует авторизации по списку с MD5-паролями. | |
| **AuthMethod** | Способ авторизации по умолчанию. Используется ТОЛЬКО в том случае, когда не найден источник авторизации, соответствующий текущему домену (в списке источников авторизации) или заданный домен не найден в списке локальных доменов. Настройка способа содержится в файлах правил **(my)conf\{AUTH[AuthMethod]}.rules.txt** конкретного сервера либо в одноимённых файлах правил общего для всех серверов каталога **CommonPlugins**. Возможные значения параметра:<br>**AuthFile** - авторизация по списку пользователей Eserv/2 (**Eserv2Userlist**);<br>**NtLogon** - авторизация по пользователям Windows NT - по списку домена Active Directory или локального компьютера (**NTdomain**);<br>**MD5File** - авторизация по списку с MD5-паролями (**UserList**);<br>**MD5PlainFile** - авторизация по объединённому списку с MD5-паролями (**PlainUserList**);<br>**AuthSource** - авторизация по источнику с именем, заданном в **DefaultAuthSource**.<br>Начальное значение - **MD5File**. | |

| | | |
|---|---|---|
| **NtlmpersonateLogon** | Авторизация пользователя в домене Active Directory может быть выполнена двумя различными способами. В первом варианте только проверяется наличие пользователя и правильность его пароля. Во втором варианте сервер после авторизации переключается в контекст безопасности пользователя. С одной стороны это удобно, поскольку обеспечивает серверу доступ к пользовательской информации, которая иначе может быть недоступна. С другой стороны, пользователь при этом должен быть наделён правами в каталоге установки PigMail+PigProxy - это право чтения файлов в самом каталоге и всех его подкаталогах и право изменения в каталоге DATA и всех его подкаталогах. В ряде случаев могут потребоваться дополнительные привилегии. Этот параметр позволяет выбирать способ авторизации в домене Active Directory. Поскольку в PigMail+PigProxy в настоящее время отсутствуют какие-либо функции, требующие работы в контексте безопасности авторизовавшегося пользователя, то начальное значение параметра - **0**. | * |
| **UseExtendedGroups** | Указывает, использовать ли расширенную (кросс-доменную) группировку пользователей. Если при запуске сервера этот параметр имеет любое ненулевое значение, то загружается специальный плагин **groups_ext**. Начальное значение - **0**. | * |
| **ExtendedGroupList** | Файл с расширенным списком группировки пользователей. Этот список позволяет использовать кросс-доменную группировку пользователей наподобие принятой в Active Directory, когда пользователь может входить в группу, принадлежащую другому (но доверенному) домену. Расширенная группировка поддерживается специальным плагином **groups_ext**, проверяющим также группы, определённые на уровне соответствующих источников авторизации. Однако существование заданных в этом списке групп не проверяется, что позволяет создавать группы, не только не существующие в реальности, но и принадлежащие несуществующим доменам авторизации. Неизвестно, насколько может быть полезен такой побочный эффект, но он существует. Начальное значение - **{Dirs[Lists]}\ExtendedGroupsList.txt**. | |
| **RejectNonexistentDomains** | Указывает, отвергать ли попытки авторизации, если домен авторизации не описан в настройках сервера. Если домен авторизации пользователя не найден в списке локальных доменов или же отсутствует в списке назначенный домену источник авторизации, то обычно делается попытка использовать метод авторизации по умолчанию. Этот приём позволяет поддерживать неопределённо большое множество однотипных доменов без необходимости явного их описания. Если такая возможность не требуется, достаточно задать этом параметру любое ненулевое значение. Начальное значение - **0**. | * |
| **MaxAuthAttempts** | Максимально допустимое число попыток протокольной (не по IP/MAC-адресу) авторизации в одной сессии. Применяется для сессий-ориентированных протоколов: POP3, IMAP, SMTP, FTP (в том числе FTP-прокси) и Socks. Определяет, сколько неудачных попыток авторизации допускается в течение одной сессии. Если это число превышено, подключение считается атакой и разрывается. Если значение нулевое, то ограничения на число попыток подбора пароля отсутствуют. Начальное значение - **3**. | * |

## *Секция SMTP - параметры настройки SMTP-сервера*

| | | |
|---|---|---|
| **DefaultMailDomain** | Почтовый домен по умолчанию для SMTP-сервера - переопределяет соответствующий параметр из секции **Server**. Начальное значение **{Server[DefaultMailDomain]}** может быть переопределено требуемым образом. | ? |
| **AdminEmail** | Почтовый адрес администратора SMTP-сервера. Может использоваться в шаблонах сообщений об ошибках, в почтовых извещениях и т.п. Начальное значение **{Server[AdminEmail]}** может быть переопределено требуемым образом. | ? |

| | | |
|---|---|---|
| **AdminName** | Имя (звание, титул) администратора SMTP-сервера. Обычно подставляется в заголовки автоматически формируемых писем в поле адреса или в качестве подписи. Начальное значение **{Server[AdminName]}** может быть переопределено требуемым образом. | |
| **AbuseEmail** | Специальный почтовый адрес для отсылки жалоб на работу почтового сервера. Этот адрес подставляется в ответы сервера в случае отклонения приёма письма на основании чёрных списков. На этот адрес могут отправить письмо даже отправители, заблокированные чёрным списком, кроме самых отъявленных хулиганов. Начальное значение - **abuse@{SMTP[DefaultMailDomain]}**. | ? |
| **BounceEmail** | Адрес "отскока" или "вышибала". Чтобы исключить переписку между почтовыми роботами, этот адрес подставляется в качестве обратного при формировании глобального автоответа о доставке (если таковой был запрошен в поступившем письме). Направленные на этот адрес письма обычно отвергаются. Путём изменения настроек можно разрешить серверу принимать такие письма, но отвечать на них он ни в коем случае не будет. Начальное значение - **bounce@{SMTP[DefaultMailDomain]}**. | ? |
| **DefaultAuthDomain** | Домен авторизации по умолчанию для SMTP-сервера. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[DefaultAuthDomain]}**. | $ |
| **DomainIP** | Файл со списком IP-адресов, назначенных сетевым интерфейсам компьютера. Переопределяет соответствующий параметр из секции **Lists**. Начальное значение - **{Lists[DomainIP]}**. | ? |
| **UserList** | Файл со списком пользователей формата Eserv/3 для SMTP-сервера. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[UserList]}**. | |
| **GroupList** | Файл со списком группировки пользователей формата Eserv/3 для SMTP-сервера. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[GroupList]}**. | |
| **PlainUserList** | Файл с объединённым списком пользователей формата Eserv/3 для SMTP-сервера. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[PlainUserList]}**. | ? |
| **PlainGroupList** | Файл со списком группировки пользователей формата Eserv/3 для SMTP-сервера. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[PlainGroupList]}**. | ? |
| **Eserv2Userlist** | Файл со списком пользователей SMTP-сервера, извлечённым из Eserv.ini версии Eserv/2.x. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[Eserv2Userlist]}**. | |
| **Eserv2Grouplist** | Файл со списком группировки пользователей SMTP-сервера, извлечённым из Eserv.ini версии Eserv/2.x. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[Eserv2Grouplist]}**. | |
| **NTdomain** | Имя домена Active Directory или локального компьютера под управлением Windows линейки NT, по списку пользователей которого выполняется авторизация пользователей SMTP-сервера, если выбран соответствующий способ авторизации (**NtLogon**). Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[NTdomain]}**. | ? |

| | | |
|---|---|---|
| **DefaultAuthSource** | Имя источника авторизации на SMTP-сервере из списка источников авторизации. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[DefaultAuthSource]}**. | ? |
| **AuthMethod** | Способ авторизации на SMTP-сервере по умолчанию. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[AuthMethod]}**. | ? |
| **NtImpersonateLogon** | Определяет, требуется ли переключение в контекст безопасности пользователя при авторизации в домене Active Directory. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[NtImpersonateLogon]}**. | |
| **UseExtendedGroups** | Указывает, использовать ли расширенную (кросс-доменную) группировку пользователей. Переопределяет соответствующий параметр из секции **AUTH**. Если при запуске сервера этот параметр имеет любое ненулевое значение, то загружается специальный плагин **groups_ext**. Начальное значение - **{AUTH[UseExtendedGroups]}**. | * & |
| **ExtendedGroupList** | Файл с расширенным списком группировки пользователей для SMTP-сервера. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[ExtendedGroupList]}**. | ? |
| **RejectNonexistentDomains** | Указывает, отвергать ли попытки авторизации, если домен авторизации не описан в настройках сервера. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[RejectNonexistentDomains]}**. | ? |
| **MaxAuthAttempts** | Максимально допустимое число попыток протокольной (не по IP/MAC-адресу) авторизации в одной сессии. Определяет, сколько неудачных попыток авторизации допускается в течение одной сессии. Если это число превышено, подключение считается атакой и разрывается. Если значение нулевое, то ограничения на число попыток подбора пароля отсутствуют. Начальное значение - **{AUTH[MaxAuthAttempts]}**. | ? |
| **CacheIni** | Для ускорения анализа адресов и локальной доставки писем SMTP-сервер может кэшировать в оперативной памяти ряд параметров конфигурационного файла. Кэширование производится только на время почтовой сессии - от подключения клиента до его отсоединения - и не влияет на параллельные сессии. Если кэширование создаёт проблемы, его можно отключить, установив этот параметр в ноль и перезапустив SMTP-сервер. Начальное значение - **1**. | * & |
| **Active** | Определяет, активен ли SMTP-сервер. Если значение нулевое, то все попытки подключения отвергаются с кодом 4xx, что означает предложение повторить попытку позже. Если указано любое ненулевое число, сервер принимает подключения. Начальное значение - **1**. | |
| **Port** | Порт, на котором работает SMTP-сервер. Начальное значение стандартное - **25**. | & |
| **SslPort** | Порт, на котором SMTP-сервер принимает подключения по защищённому соединению. Начальное значение - **465**. | & |
| **NetworkInterface** | Адрес сетевого интерфейса, слушаемого сервером. Начальное значение - пустая строка; это означает, что сервер слушает все интерфейсы. | & |
| **SslNetworkInterface** | Адрес сетевого интерфейса, слушаемого сервером для приёма подключений по защищённому соединению. Начальное значение - пустая строка; это означает, что сервер слушает все интерфейсы. | & |

| | | |
|---|---|---|
| **Certificate** | Имя файла формата PEM, содержащего закрытый ключ и сертификаты, используемые при организации защищённого (SSL) соединения сервера с клиентом. Переопределяет соответствующий параметр из секции **Server**. Начальное значение - **{Server[Certificate]}**. | $ |
| **SslVerifyClient** | Определяет режим проверки подлинности сертификатов клиентской стороны при установлении защищённого соединения. Переопределяет соответствующий параметр из секции **Server**. Начальное значение - **{Server[SslVerifyClient]}**. | $ |
| **UsePreferredDns** | Для выполнения различных проверок SMTP-сервер обращается к серверу DNS, запрашивая необходимую информацию. Обычно он успешно справляется с выбором необходимого сервера, ориентируясь по настройкам сетевых интерфейсов. Если же сервер ошибается, его можно поправить, задав этому параметру любое ненулевое значение. В этом случае SMTP-сервер будет использовать в качестве основного DNS-сервер, заданный параметром **DNSServer**. Начальное значение - **0**. | * |
| **DNSServer** | Этот параметр задаёт имя или IP-адрес основного сервера DNS, который будет использоваться SMTP-сервером при включённом флаге **UsePreferredDns**. Если для доставки исходящей почты используется агент smtpsend3 или smtpsend4, то ему для корректной работы тоже может потребоваться указать имя или адрес сервера DNS, посредством которого он будет получать необходимую информацию. Начальное значение **192.168.0.1** следует заменить на имя или адрес реально используемого сервера DNS. | *<br>$<br># |
| **MaxMessageSize** | Максимально допустимый размер письма. Это значение сообщается в ответ на SMTP-команду EHLO и действует для всех "чужих" отправителей (для "своих" ограничения устанавливаются динамически и более изощрённым способом). Размер письма задаётся в байтах. Начальное значение - **10485760** (10 МБ). Если указать нулевое значение, размер письма ограничиваться не будет. | *<br>$ |
| **MaxOutboundMessageSize** | Максимально допустимый размер письма, отправляемого из локального домена "чужим" получателям. Это ограничение налагается в дополнение к параметрам, заданным в списках локальных и доверенных сетей, а также в списке локальных пользователей. Размер письма задаётся в байтах. Начальное значение - **3145728** (3 МБ). Если указать нулевое значение, размер письма дополнительно ограничиваться не будет. | *<br>$ |
| **MailBombThreshold** | Предельный размер письма, при превышении которого письмо считается почтовой бомбой. Меры пресечения в отношении бомб применяются более жёсткие, чем в отношении просто больших писем: почтовые бомбы не сохраняются для последующего анализа и не передаются в ящик администратора, кроме того, отправитель почтовой бомбы имеет все шансы попасть в чёрные списки отправителей (если автоматическое занесение в какой-либо чёрный список разрешено параметром **MaxMessageSizeAutoblacklist**). Пороговый размер почтовой бомбы проверяется только тогда, когда письмо не прошло первичный контроль размера. То есть, в зависимости от групповых и персональных настроек, отправители могут успешно посылать письма, формально подходящие под определение почтовой бомбы. Начальное значение - **104857600** (100 МБ). Если указать нулевое значение, бомбы обрабатываться не будут. | *<br>? |
| **MaxRcptNumber** | Максимально допустимое число адресатов для письма. Противоспамная мера, не действующая на администраторов. Список рассылки независимо от объёма считается за одного получателя. Начальное значение - **20**. | ? |

| | | |
|---|---|---|
| **MaxMsgsNumber** | Максимально допустимое число писем за одну сессию. Тоже противоспамная мера, не действующая на администраторов. Начальное значение - **10**. | ? |
| **MsgsNumberThreshold** | Мир не идеален, и в нём встречаются отправители, не понимающие вежливый отказ принять адрес отправителя. В число таких "упёртых" отправителей входят не только спамерские программы, но и вполне законопослушные почтовые клиенты, например, Microsoft Office Outlook 2007 - он в таких случаях просто зацикливается, многократно пытаясь отправить одно и то же письмо. Этот параметр определяет число попыток (включая успешные) отправки письма, после которого сервер принудительно разрывает соединение с клиентом. Начальное значение - **20**. | ? |
| **MaxConnections** | Максимально допустимое число одновременных подключений к серверу. Позволяет противостоять пиковым нагрузкам и целенаправленным попыткам завалить сервер путём неумеренного потребления всех ресурсов компьютера. Начальное значение - **25**. | & |
| **MaxConnectionsFromIP** | Максимально допустимое число одновременных подключений к серверу с одного IP-адреса. Противоспамная мера, распространяющаяся на всех отправителей, поскольку ограничение включается ещё до любой попытки распознавания отправителя. В текущей версии эта настройка не поддерживается и зарезервирована на будущее. Начальное значение - **10**. | & |
| **MaxReceivedCnt** | Максимально допустимое количество заголовков **Received:** в шапке письма. Если их слишком много, это с очень большой вероятностью означает зацикливание письма. Такие письма во избежание неприятностей изымаются из оборота. Начальное значение - **20**. Если указать нулевое значение, то контроль числа заголовков отключается. | *<br>? |
| **RejectLoopbackedMail** | Определяет, как надлежит поступить с зациклившимся письмом. Если параметр имеет ненулевое значение, то отправителю сервер отвечает отказом в приёме, а принятое письмо удаляется. Если значение параметра нулевое, сервер подтверждает приём письма, но само письмо при этом перемещается в особый карантинный каталог для последующего его анализа администратором. Начальное значение - **0**. | *<br>? |
| **Timeout** | Время бездействия, задаваемое в миллисекундах, по истечении которого сервер прекращает соединение с клиентом. Это вынужденная мера, предотвращающая утечку ресурсов при плохой связи - как правило, тайм-аут срабатывает, когда соединение уже фактически разорвано, но серверу неоткуда получить извещение об этом. Начальное значение - **60000**, что соответствует 10 минутам. | $ |
| **AllowOutboundMail** | Указывает, разрешена ли отправка почты за пределы локального домена. Это настройка по умолчанию, она может быть изменена в зависимости от настроек сети, из которой подключился отправитель, и адреса отправителя. Начальное значение - **1**, то есть, отправка исходящей почты разрешена. | *<br>$ |
| **RequireAuthForAllMail** | Указывает, требовать или нет SMTP-авторизацию для всех почтовых сессий. Установка этого параметра (задание любого ненулевого значения) закрывает SMTP-сервер для доступа извне и блокирует получение любой почты, поступающей из-за пределов локального домена. Начальное значение - **0**, то есть, сервер открыт для приёма почты извне. | *<br>? |

| | | |
|---|---|---|
| **RequireAuthForOutboundMail** | Указывает, требовать или нет SMTP-авторизацию для отправки почты за пределы локального домена. Используется для усиления ограничений, которые в противном случае будут основываться только на IP-адресах из списков локальных и доверенных сетей. Установка этого флага (задание любого ненулевого значения) включает проверку определённых в списке локальных пользователей дополнительных параметров отправителей. Начальное значение - **1**, то есть, явная авторизация необходима. | * ? |
| **RequireAuthForHiddenMail** | Указывает, требовать или нет SMTP-авторизацию для отправки почты скрытым получателям локального домена. Если этот флаг не установлен (задано нулевое значение), скрытому получателю может отправлять почту любой отправитель, указавший правильный обратный адрес. Начальное значение - **1**, то есть, явная авторизация необходима. | * ? |
| **RequireAuthForLocalSenders** | Указывает, требовать или нет SMTP-авторизацию для отправителей из локального домена. Если этот флаг не установлен (задано нулевое значение), авторизация может потребоваться (в соответствии с вышеперечисленными параметрами) для отправки почты за пределы локального домена и на секретные адреса локального домена, входящая же почта для несекретных получателей проходит без авторизации независимо от адреса отправителя (если не задано драконовское требование поголовной обязательной авторизации). Установка флага означает, что локальные отправители обязаны авторизоваться, прежде чем вообще получат право отправлять письма куда-либо. Это хоть как-то спасает от подделки адресов отправителей, применяемой в массовом порядке спамерами и почтовыми червями. Начальное значение - **0**, авторизация для локальных отправителей не является обязательной. | * ? |
| **RequireSslForLocalSenders** | Указывает, требовать ли от пользователей локальных доменов обязательного подключения по защищённому соединению (SSL). Если этот флаг установлен (задано любое ненулевое значение), то обратные адреса, принадлежащие локальным доменам, принимаются только при наличии защищённого соединения, иначе отвергаются. Подобно предыдущему параметру, спасает от подделки адресов отправителей, применяемой в массовом порядке спамерами и почтовыми червями. К тому же положительно сказывается на безопасности общения клиента с сервером. Начальное значение - **0**, защищённое соединение для локальных отправителей не является обязательным. | * ? |
| **RequireLocalDomainsFromLocalUsers** | Указывает, требовать ли от локальных клиентов использовать в качестве обратных адреса только из списка локальных почтовых ящиков. Локальными клиентами считаются отправители, подключившиеся из локальной или доверенной сети, а также отправители, авторизованные любым способом - явно либо на основании IP-адреса или сочетания IP и MAC-адресов. Если параметр имеет любое ненулевое значение, выполняется дополнительная проверка обратного адреса для такого класса отправителей. В противном случае проверка не выполняется - правда, отсылать письма наружу такие своевольные отправители всё равно не смогут. На администраторов действие этого ограничения не распространяется. Начальное значение - **0**. | * ? |

| | | |
|---|---|---|
| **AllowAdminAuth** | Определяет условия, при которых при авторизации пользователя возможно назначение администраторских прав. В отличие от рядовых пользователей, администратор имеет право применять любой обратный адрес, а в ряде случаев ему дозволяется отсылать письма адресатам из списка запрещённых получателей. Возможные значения:<br>**Always** - для назначения администраторских прав дополнительных условий нет;<br>**Local** - права администратора могут быть назначены только пользователям, подключившимся из локальной сети;<br>**Ssl** - права администратора могут быть назначены только пользователям, подключившимся с использованием защищённого соединения (SSL);<br>**Both** - права администратора могут быть назначены только пользователям, подключившимся из локальной сети с использованием защищённого соединения (SSL);<br>**Either** - права администратора могут быть назначены только пользователям, подключившимся из локальной сети либо с использованием защищённого соединения (SSL);<br>**Never** - права администратора не могут быть назначены ни при каких условиях.<br>Слово-значение можно сократить вплоть до единственного первого символа, регистр значения не имеет. Начальное значение - **Either**. | * |
| **UseChunking** | Указывает, использовать ли специальное расширение протокола SMTP - возможность блочного приёма письма по команде BDAT. В ряде случаев передача письма несколькими мелкими порциями может повысить устойчивость приёма, в ряде других случаев некорректные настройки маршрутизаторов могут заблокировать приём. Поскольку письмо может быть произвольным образом разбито на фрагменты, его невозможно проанализировать в время приёма. Если при запуске сервера параметр имеет ненулевое значение, подключается дополнительный плагин **parser**, предназначенный для анализа заголовков писем, принятых блочным методом. В дальнейшем использование расширения при возникновении проблем может быть отключено динамически. Начальное значение - **0**, расширение не используется. | * & ? |
| **UseStartTLS** | Указывает, использовать ли специальное расширение протокола SMTP - возможность динамического переключения в режим защищённого соединения. Само по себе защищённое соединение с шифрованием данных есть вещь полезная, но в ряде случаев его применение может привести к блокировке приёма. Начальное значение - **0**, расширение не используется. | * ? |
| **UsePipelining** | Указывает, использовать ли специальное расширение протокола SMTP - конвейерный, он же пакетный, режим передачи данных. В этом режиме клиент передаёт команды и данные, не ожидая ответов сервера, что, несомненно, ускоряет передачу. Однако при возникновении нештатной ситуации (например, при отсутствии адресата) передаваемый в общем потоке текст письма будет интерпретирован как команды. Начальное значение - **0**, расширение не используется. | |

| | | |
|---|---|---|
| **UseAutoLogon** | Указывает, использовать или нет автоматическую авторизацию отправителя. Если есть программы, отсылающие письма, но не умеющие авторизоваться на SMTP-сервере, а для отправки почты обязательна авторизация, таких специфических отправителей можно авторизовать автоматически. Начальное значение - **0**, то есть, автоматическая авторизация не используется. | *<br>? |
| **UseMailingLists** | Указывает, использовать или нет списки рассылки. Списки рассылки обслуживаются отдельным плагином **maillists** - он загружается, если при старте SMTP-сервера параметр имеет ненулевое значение. Если соответствующий плагин не загружен, то списки рассылки не используются независимо от значения этого флага; при загруженном плагине параметр позволяет временно запретить использование списков в случае возникновения проблем. Начальное значение - **1**, то есть, списки рассылки используются. | *<br>&<br>? |
| **UseAutoresponders** | Указывает, использовать или нет автоответчики. Автоответчики обслуживаются отдельным плагином **autoresponders** - он загружается, если при старте SMTP-сервера параметр имеет ненулевое значение. Если соответствующий плагин не загружен, то автоответчики не используются независимо от значения этого флага; при загруженном плагине параметр позволяет временно запретить использование автоответчиков в случае возникновения проблем. Начальное значение - **1**, то есть, автоответчики используются. | *<br>&<br>? |
| **UseNotifiers** | Указывает, использовать или нет извещения о поступлении входящей почты в локальный почтовый ящик. В качестве извещения используется короткое электронное письмо, отсылаемое на особый адрес - обычно это адрес SMS-шлюза или почтового сервиса оператора мобильной связи, в результате чего извещение поступает на сотовый телефон. Сервис извещений обслуживается отдельным плагином **notifier** - он загружается, если при старте SMTP-сервера параметр имеет ненулевое значение. Если соответствующий плагин не загружен, то извещения не используются независимо от значения этого флага; при загруженном плагине параметр позволяет временно запретить использование извещений в случае возникновения проблем. Начальное значение - **0**. | *<br>&<br>? |
| **UseRobots** | Указывает, использовать или нет почтовые роботы. Почтовые роботы обслуживаются отдельным плагином **robots** - он загружается, если при старте SMTP-сервера параметр имеет ненулевое значение. Если соответствующий плагин не загружен, то роботы не используются независимо от значения этого флага; при загруженном плагине параметр позволяет временно запретить использование роботов в случае возникновения проблем. Начальное значение - **0**, то есть, роботы не используются. | *<br>&<br>? |
| **UseGrayLists** | Указывает, использовать или нет так называемые "серые" списки отправителей и получателей. С помощью "серых" списков можно настраивать избирательную маршрутизацию почты - например, защищать почтовые ящики специальных роботов от спама. Начальное значение - **0**, то есть, "серые" списки не используются. | *<br>? |

| | | |
|---|---|---|
| **AcceptNotListedLocalDomains** | Указывает, принимать ли почту, если запись в DNS, указывающая на почтовый сервер для домена получателя, приводит на наш сервер, но такого домена в списке локальных доменов нет. Это возможно в следующих случаях:<br>1. PigMail+PigProxy не до конца настроен, администратор ещё не заполнил список;<br>2. ошибка администратора чужого DNS при настройке MX-записей его домена;<br>3. злой умысел администратора чужого DNS;<br>4. сбой программы отправителя.<br>Если возможен первый случай, приём такой почты надо разрешить, установив любое ненулевое значение. Начальное значение - **0**, то есть, приём такой "подозрительной" почты запрещён. | *<br>? |
| **VerifyDomainsInDns** | Указывает, проверять ли существование и правильность внешнего почтового домена. Обычно такие проверки хорошо защищают как от грубых ошибок в адресах, так и от намеренных подделок, однако при сложных конфигурациях сети могут осложнять работу. Начальное значение - **1**, то есть, существование и правильность домена проверяются. | *<br>? |

| | | |
|---|---|---|
| **DomainVerificationLevel** | Задаёт уровень дотошности, с которой SMTP-сервер проверяет корректность почтового домена. Помимо стандартной формальной проверки существования самого домена и наличия у него хотя бы одной записи MX (определяющей SMTP-сервер домена) или A (задающей IP-адрес узла сети, олицетворяющего домен), можно выполнить ряд дополнительных проверок. Параметр представляет собой строку символов-флагов, задающих выполняемые проверки:<br>**L** - проверка, не указывает ли одна из MX-записей домена на наш локальный компьютер (то есть, не сопоставлен ли ей IP-адрес из диапазона 127.0.0.0 - 127.255.255.255). Если такая ситуация имеет место быть, это означает три возможных варианта: либо это ошибка администратора домена, либо домен "припаркован", то есть, реально не задействован нынешним владельцем, либо это намеренный спамерский трюк, чтобы не получать ответов. В любом случае отправка письма по такому адресу, скорее всего, невозможна - письмо никуда не уйдёт;<br>**F** - проверка, не указывает ли одна из MX-записей домена на специальный адрес (0.0.0.0 или 255.255.255.255), а также не указывает ли она случайно на адрес, принадлежащий немаршрутизируемому диапазону адресов, выделенному для локальных сетей (таких диапазонов три: 10.0.0.0 - 10.255.255.255, 172.16.0.0 - 172.31.255.255 и 192.168.0.0 - 192.168.255.255) или на стандартный адрес локального компьютера 127.0.0.1. Здесь возможны те же самые три варианта. Отправка письма в такой некорректно настроенный домен также невозможна;<br>**H** - проверка, не указывает ли собственно домен (A-запись, также именуемая "хост") на наш локальный компьютер (то есть, не сопоставлен ли ей IP-адрес из диапазона 127.0.0.0 - 127.255.255.255). Если такая ситуация имеет место быть, это означает три возможных варианта: либо это ошибка администратора домена, либо домен "припаркован", то есть, реально не задействован нынешним владельцем, либо это намеренный спамерский трюк, чтобы не получать ответов. В любом случае отправка письма по такому адресу, скорее всего, невозможна - письмо никуда не уйдёт;<br>**K** - проверка, не указывает ли собственно домен (A-запись, также именуемая "хост") на специальный адрес (0.0.0.0 или 255.255.255.255), а также не указывает ли она случайно на адрес, принадлежащий немаршрутизируемому диапазону адресов, выделенному для локальных сетей (таких диапазонов три: 10.0.0.0 - 10.255.255.255, 172.16.0.0 - 172.31.255.255 и 192.168.0.0 - 192.168.255.255) или на стандартный адрес локального компьютера 127.0.0.1. Здесь возможны те же самые три варианта. Отправка письма в такой некорректно настроенный домен также невозможна.<br>Прочие символы игнорируются - эту особенность можно использовать для полной отмены дополнительных проверок. Начальное значение - **L**. | *<br>? |

| | | |
|---|---|---|
| **EmptySenderQuarantined** | Определяет, при каких условиях письма с пустым адресом отправителя должны приниматься в карантин. Пустой адрес обычно используется почтовыми серверами при отправке служебных сообщений - например, о невозможности доставки письма получателю или наоборот, об успешной доставке. По умолчанию такие письма принимаются обычным образом с некоторой оглядкой на ранее выполненные проверки IP-адреса подключения и имени клиентского узла: если они сочтены недоверенными, то письмо будет принято в карантин. Однако при включённой поддержке локальных или глобальных (Sender Policy Framework) политик можно направить письмо в карантин также в зависимости от результата проверки этих политик. Параметр представляет собой строку символов-флагов, задающих условия для такого перенаправления:<br>**L** (Local) - отправитель локальный (IP-адрес принадлежит локальной сети или самому серверу), поэтому политики не проверялись, - в текущей версии смысла не имеет, поскольку использование пустого адреса отправителя в локальной сети запрещено;<br>**K** (Known) - отправитель известен, поскольку успешно авторизовался на сервере;<br>**W** (Whitelist) - по результатам проверки локальных политик отправитель признан особо доверенным (код политики **WL**);<br>**M** (Match) - по результатам проверки локальных политик адрес отправителя признан действительным (код политики **AM**);<br>**P** (Pass) - по результатам проверки глобальных политик адрес отправителя признан действительным;<br>**N** (None) - проверка глобальных политик не выявила никакой информации в отношении отправителя;<br>**E** (Error) - проверка глобальных политик не удалась из-за ошибки при получении информации;<br>**U** (Unknown) - проверка глобальных политик не дала однозначный результат;<br>**T** (neuTral) - по результатам проверки локальных политик отправитель признан крайне подозрительным и подлежащим дополнительной проверке по глобальным политикам с отказом при уровне недостоверности NEUTRAL (код политики **NE**);<br>**R** (neutRal) - по результатам проверки глобальных политик отправитель признан незначительно нарушающим правила (уровень недостоверности NEUTRAL);<br>**O** (sOftfail) - по результатам проверки локальных политик отправитель признан подозрительным и подлежащим дополнительной проверке по глобальным политикам с отказом при уровне недостоверности SOFTFAIL (код политики **SF**);<br>**S** (Softfail) - по результатам проверки глобальных политик отправитель признан нарушающим правила (уровень недостоверности SOFTFAIL);<br>**F** (Fail) - по результатам проверки локальных политик отправитель признан обычным и подлежащим дополнительной проверке по глобальным политикам с отказом при уровне недостоверности FAIL (код политики **FA**);<br>**#** - условие срабатывает, если проверка политик (и локальных, и глобальных) отключена;<br>**A** (Always) - условие срабатывает всегда, в том числе при полностью отключённой проверке политик.<br>Прочие символы игнорируются. Начальное значение - **TROS**. | *<br>? |

| | | |
|---|---|---|
| **EmptySenderNoSpam** | Определяет, при каких условиях письма с пустым адресом отправителя должны быть избавлены от проверки спам-фильтрами. Как и предыдущий параметр, он используется при включённой поддержке локальных или глобальных политик и позволяет изменить режим по умолчанию, при котором письма с пустым адресом отправителя всегда обрабатываются спам-фильтрами. Параметр представляет собой строку символов-флагов, задающих условия для исключения:<br>**L** (Local) - отправитель локальный (IP-адрес принадлежит локальной сети или самому серверу), поэтому политики не проверялись, - в текущей версии смысла не имеет, поскольку использование пустого адреса отправителя в локальной сети запрещено;<br>**K** (Known) - отправитель известен, поскольку успешно авторизовался на сервере;<br>**W** (Whitelist) - по результатам проверки локальных политик отправитель признан особо доверенным (код политики **WL**; спам-фильтр уже отключён, так что этот флаг в данном случае большого смысла не имеет);<br>**M** (Match) - по результатам проверки локальных политик адрес отправителя признан действительным (код политики **AM**);<br>**P** (Pass) - по результатам проверки глобальных политик адрес отправителя признан действительным;<br>**N** (None) - проверка глобальных политик не выявила никакой информации в отношении отправителя;<br>**E** (Error) - проверка глобальных политик не удалась из-за ошибки при получении информации;<br>**U** (Unknown) - проверка глобальных политик не дала однозначный результат;<br>**T** (neuTral) - по результатам проверки локальных политик отправитель признан крайне подозрительным и подлежащим дополнительной проверке по глобальным политикам с отказом при уровне недостоверности NEUTRAL (код политики **NE**);<br>**R** (neutRal) - по результатам проверки глобальных политик отправитель признан незначительно нарушающим правила (уровень недостоверности NEUTRAL);<br>**O** (sOftfail) - по результатам проверки локальных политик отправитель признан подозрительным и подлежащим дополнительной проверке по глобальным политикам с отказом при уровне недостоверности SOFTFAIL (код политики **SF**);<br>**S** (Softfail) - по результатам проверки глобальных политик отправитель признан нарушающим правила (уровень недостоверности SOFTFAIL);<br>**F** (Fail) - по результатам проверки локальных политик отправитель признан обычным и подлежащим дополнительной проверке по глобальным политикам с отказом при уровне недостоверности FAIL (код политики **FA**);<br>**#** - условие срабатывает, если проверка политик (и локальных, и глобальных) отключена;<br>**A** (Always) - условие срабатывает всегда, в том числе при полностью отключённой проверке политик.<br>Прочие символы игнорируются. Начальное значение - **WMP**. | *<br>? |

| | | |
|---|---|---|
| **AcceptNonExistentUsers** | Указывает, принимать ли почту для несуществующих пользователей существующего локального домена. Если список пользователей домена ещё не заполнен либо домен имеет специфическое назначение, в результате чего составить такой список не представляется возможным, приём такой почты необходимо разрешить, задав любое ненулевое значение. Это глобальный флаг, в параметрах каждого домена в отдельности также имеется соответствующий флаг. Почта принимается, если установлены оба флага. Начальное значение - **0**, то есть, приём почты для несуществующих пользователей запрещён. | * ? |
| **CreateNonExistentUsersBoxes** | Если приём почты для несуществующих пользователей разрешён, то обрабатывать её можно различными способами. Можно либо автоматически создавать для таких пользователей почтовые ящики, либо переправлять на другой адрес, либо просто складировать в специальный каталог, чтобы администратор время от времени заглядывал туда и принимал необходимые меры. Этот флаг указывает, создавать ли почтовые ящики несуществующих пользователей автоматически. Это глобальный флаг, в параметрах каждого домена в отдельности также имеется соответствующий флаг. Ящики несуществующих пользователей создаются, если установлены оба флага. Начальное значение - **0**, то есть, автоматическое создание почтовых ящиков запрещено. | * ? |
| **KeepNonExistentUsersUndelivered** | Если приём почты для несуществующих пользователей разрешён, но автоматическое создание почтовых ящиков запрещено либо глобально, либо в параметрах домена, то остаются ещё два варианта обработки. Можно либо переправлять почту на другой адрес, либо просто складировать в специальный каталог, чтобы администратор время от времени заглядывал туда и принимал необходимые меры. Этот флаг указывает, помещать ли принятую для несуществующего пользователя почту в такой каталог. Это глобальный флаг, в параметрах каждого домена в отдельности также имеется соответствующий флаг. Почта помещается в специальный каталог, если установлены оба флага. Начальное значение - **1**, то есть, разбор такой почты оставлен на усмотрение администратора. | * ? |
| **ForwardNonExistentUsersTo** | Если создавать почтовые ящики для несуществующих пользователей запрещено, но и складировать такие письма в специальный каталог нежелательно, можно использовать переадресацию. Этот параметр задаёт глобальный адрес для перенаправления почты. В параметрах каждого домена также может быть задан адрес для перенаправления почты, в этом случае он имеет приоритет. Если не задан ни один адрес, почта помещается в специальный каталог для недоставленных писем. Начальное значение - **{SMTP[AdminEmail]}**. | * ? |
| **AcceptBounce** | Указывает, принимать ли почту, поступившую на адрес "отскока". В обычном режиме сервер отклоняет письмо под предлогом отсутствия получателя. Установка этого флага путём задания любого ненулевого значения позволяет превратить "вышибалу" в "пылесос" - сервер принимает письма на адрес "отскока" и помещает их в отдельный каталог, не формируя автоответов. Это глобальный флаг, в параметрах каждого домена в отдельности также имеется соответствующий флаг. Почта на адрес "отскока" принимается, если установлены оба флага. Начальное значение - **0**, то есть, почта на адрес "отскока" не принимается. | * ? |

| | | |
|---|---|---|
| **MultiSite** | Указывает, обрабатывать ли адреса отправителей и получателей в режиме многосерверного домена. В этом режиме предполагается, что сервер локально обслуживает лишь часть почтовых ящиков одного или нескольких доменов, отсутствующие почтовые ящики могут располагаться на других серверах, которые должны быть указаны в списке перенаправления почты. Это глобальный флаг, в параметрах каждого домена в отдельности также имеется соответствующий флаг. Домен считается многосерверным, если установлены оба флага. Начальное значение - **0**, то есть, многосерверные домены не обслуживаются. | * ? |
| **RelayMultiSite** | По умолчанию отправители, приписанные к многосерверному домену и отсутствующие в списке локальных почтовых ящиков, имеют право посылать только входящую почту, адресованную исключительно на существующие локальные адреса. Однако возможна ситуация, когда PigMail+PigProxy исполняет обязанности шлюза: сервер, реально обслуживающий почтовые ящики домена, не имеет прямого выхода в интернет и переправляет все исходящие письма через PigMail+PigProxy. Такой режим возможен, если одновременно установлен этот глобальный флаг и соответствующий флаг в параметрах домена, а отправитель успешно прошёл авторизацию - либо протокольную, либо на основании IP (или IP+MAC) адреса, либо автоматическую. Начальное значение - **0**, то есть, режим шлюза для многосерверных доменов запрещён. | * ? |
| **PopMultiSite** | Указывает, принимать ли почту для нелокальных адресатов многосерверного домена, если приём выполняется загрузчиком внешней POP-почты Pop3Recv. По умолчанию предполагается, что пользователи других серверов получат предназначенную им почту другими путями. Однако, если PigMail+PigProxy исполняет обязанности шлюза или есть иная необходимость, приём таких писем следует разрешить, для чего необходимо установить не только этот глобальный флаг, но и соответствующий флаг в параметрах домена. Начальное значение - **0**. | * ? |
| **ValidateMultisiteRcpts** | Указывает, проверять ли на целевом сервере адреса нелокальных получателей, относящиеся к многосерверному домену. По умолчанию сервер принимает такие адреса без дополнительной проверки, что в случае ошибки отправителя (или злостной уловки спамера) непременно повлечёт за собой неудачную попытку доставки письма по назначению и отправку письма-отскока. Проверка позволяет этого избежать. Однако, если связь с целевым сервером плохая, проверка может выполняться долго, что приведёт к отключению отправителя по тайм-ауту. Проверку выполняет специальный плагин **email_validator**, который загружается, если при запуске сервера этот параметр имеет любое ненулевое значение. Плагин имитирует работу расширенного сервиса доставки исходящей почты SmtpSend и пользуется его настройками, даже если сам сервис не активирован. Начальное значение - **0**, проверка на целевом сервере не используется. | * & ? |

| | | |
|---|---|---|
| **ValidateForwardedRcpts** | Указывает, проверять ли на целевом сервере адреса нелокальных получателей, относящиеся к обслуживаемому сервером "чужому" домену. По умолчанию сервер принимает такие адреса без дополнительной проверки, что в случае ошибки отправителя (или злостной уловки спамера) непременно повлечёт за собой неудачную попытку доставки письма по назначению и отправку письма-отскока. Проверка позволяет этого избежать. Однако, если связь с целевым сервером плохая, проверка может выполняться долго, что приведёт к отключению отправителя по тайм-ауту. Проверку выполняет специальный плагин **email_validator**, который загружается, если при запуске сервера этот параметр имеет любое ненулевое значение. Плагин имитирует работу расширенного сервиса доставки исходящей почты SmtpSend и пользуется его настройками, даже если сам сервис не активирован. Начальное значение - **0**, проверка на целевом сервере не используется. | * & ? |
| **ValidateExternRcpts** | Указывает, проверять ли на целевом сервере адреса нелокальных получателей, соответствующие обычной исходящей почте. По умолчанию сервер проверяет только существование и корректность настроек почтового домена, а сами адреса принимает без дополнительной проверки, что в случае ошибки отправителя непременно повлечёт за собой неудачную попытку доставки письма по назначению и отправку письма-отскока. Проверка позволяет этого избежать. Однако, если связь с целевым сервером плохая, проверка может выполняться долго, что приведёт к отключению отправителя по тайм-ауту. Проверку выполняет специальный плагин **email_validator**, который загружается, если при запуске сервера этот параметр имеет любое ненулевое значение. Плагин имитирует работу расширенного сервиса доставки исходящей почты SmtpSend и пользуется его настройками, даже если сам сервис не активирован. Начальное значение - **0**, проверка на целевом сервере не используется. | * & ? |
| **MailBoxes** | Расположение базового каталога почтовых ящиков. В этом каталоге располагаются почтовые ящики всех пользователей. Начальное значение - **{Dirs[Mail]}\in**. | |
| **DefaultDomainMailBoxes** | Расположение каталога почтовых ящиков домена по умолчанию, задаваемого параметром **DefaultMailDomain**. Если этот домен по каким-либо причинам не занесён в список локальных доменов, почта, отправленная пользователям этого домена, всё равно будет принята и помещена в указанный каталог. Начальное значение - **{SMTP[MailBoxes]}\{SMTP[DefaultMailDomain]}**. | ? |
| **Out** | Расположение каталога первичной очереди доставки исходящей почты. Все письма, адресованные за пределы локального домена, помещаются в этот каталог и в дальнейшем обрабатываются агентом либо сервисом доставки. Начальное значение - **{Dirs[Mail]}\out**. | ? |
| **Retry** | Расположение каталога очереди отложенной доставки исходящей почты. Если письмо не удаётся доставить по назначению в течение заданного времени, подсистема доставки перемещает его в этот каталог. Попытки доставки попавших сюда писем тоже предпринимаются, но существенно реже, что снижает нагрузку на каналы связи и серверы-адресаты. Начальное значение - **{Dirs[Mail]}\retry**. | ? |
| **Spool** | Расположение рабочего каталога SMTP-сервера. Здесь создаются временные файлы принимаемых писем. Начальное значение - **{Dirs[Mail]}\spool**. | ? |

| | | |
|---|---|---|
| **Local** | Расположение каталога очереди локальной (внутренней) доставки. Исторически это один из подкаталогов в каталоге первичной очереди доставки исходящей почты, соответствующий фиксированному маршруту, указывающему на локальный SMTP-сервер. При использовании сервиса локальной доставки его расположение можно указать достаточно произвольно. Начальное значение - **{SMTP[Out]}\127.0.0.10\25**. | ? |
| **InfectedDir** | Расположение каталога для хранения писем, содержащих вирусы или подозрительные объекты. Поскольку эти письма всё равно уже приняты, они, несмотря на отрицательный ответ отправителю, не удаляются, а остаются для последующего анализа администратором. Начальное значение - **{Dirs[Mail]}\infected**. | |
| **Infected** | Шаблон пути для помещения в карантин писем, содержащих вирусы или подозрительные объекты. Письма не обязательно сваливать в одну кучу - можно автоматически раскладывать их "по полочкам", используя различные характеристики письма (например, адрес отправителя или имя вируса). Начальное значение - **{SMTP[InfectedDir]}**. | |
| **Unchecked** | Расположение каталога для хранения писем, антивирусная проверка которых не состоялась из-за внутренней ошибки антивируса. Поскольку причина ошибки заранее неизвестна, письма остаются для последующего анализа администратором. Начальное значение - **{Dirs[Mail]}\unchecked**. | |
| **SpamDir** | Расположение каталога для хранения писем, не прошедших спам-фильтрацию. Поскольку эти письма всё равно уже приняты, они, несмотря на отрицательный ответ отправителю, не удаляются, а остаются для последующего анализа администратором. Начальное значение - **{Dirs[Mail]}\spam**. | |
| **Spam** | Шаблон пути для размещения хранимых копий писем, не прошедших спам-фильтрацию. Письма не обязательно сваливать в одну кучу - можно автоматически раскладывать их "по полочкам", используя различные характеристики письма (например, адрес отправителя). Начальное значение - **{SMTP[SpamDir]}**. | |
| **Reclassify** | Каталог для хранения писем, прошедших переклассификацию POPfile, SpamProtexx или LibSD по инициативе отправителя. Начальное значение - **{Dirs[Mail]}\reclassify**. | |
| **Ambiguous** | Каталог для хранения писем, которые не были однозначно классифицированы спам-фильтрами POPfile, SpamProtexx и LibSD. Такие письма классифицируются вручную спам-администратором для дообучения фильтров. Начальное значение - **{SMTP[SpamAdmin]}\ambiguous**. | |
| **Quarantined** | Расположение каталога для хранения писем, принятых в карантин (писем, отправители которых попали в чёрный список). Начальное значение - **{Dirs[Mail]}\quarantined**. | |
| **Overquoted** | Расположение каталога для хранения писем, превысивших ограничения на максимально допустимый размер. Поскольку эти письма всё равно уже приняты, они, несмотря на отрицательный ответ отправителю, не удаляются, а остаются для последующего анализа администратором. Начальное значение - **{Dirs[Mail]}\overquoted**. | |
| **Nonreadable** | Расположение каталога для хранения "нечитаемых" писем (в изначальном варианте это письма с китайской кодировкой текста). Поскольку эти письма всё равно уже приняты, они, несмотря на отрицательный ответ отправителю, не удаляются, а остаются для последующего анализа администратором. Начальное значение - **{Dirs[Mail]}\nonreadable**. | |

| | | |
|---|---|---|
| **Malformed** | Расположение каталога для хранения искажённых писем, в которых были обнаружены ошибки формата. В текущей версии такими считаются письма с пустыми (но объявленными в шапке) заголовками Message-ID либо с заголовками Message-ID, начинающихся с символа **<**, но не заканчивающиеся символом **>** или же содержащие только последовательность **<>**. Такие идентификаторы писем обычно встречаются в оборванных спамерских посланиях. Они сбивают с толку различные обработчики почты, в том числе некоторые клиентские антивирусы, которые могут заблокировать доступ к почтовому ящику. Подобные письма лучше оставить для ручной обработки. Начальное значение - **{Dirs[Mail]}\malformed**. | |
| **Undelivered** | Расположение каталога для хранения недоставленных писем. Это могут быть письма для несуществующих локальных пользователей, если есть установка не доставлять такие письма, а также письма, для которых не нашлось получателей (например, из-за ошибок в настройке). Начальное значение - **{Dirs[Mail]}\undelivered**. | |
| **Abuse** | Расположение каталога для хранения писем-жалоб. Сюда в отдельных случаях перемещаются письма от адресатов, попавших в чёрный список, направленные на специальный адрес. Обычно сервер предпринимает меры по доставке любой корреспонденции в почтовый ящик такого адресата, но при невозможности доставки может поместить письмо в этот каталог. Начальное значение - **{Dirs[Mail]}\abuse**. | |
| **Bounce** | Расположение каталога для хранения писем, принятых на адрес "отскока". Поскольку эти письма всё равно уже приняты, они не удаляются, а остаются для последующего анализа администратором. Начальное значение - **{Dirs[Mail]}\bounce**. | |
| **Loop** | Расположение каталога для хранения зациклившихся писем - таких, у которых число заголовков Received: превышает установленный лимит. Поскольку эти письма всё равно уже приняты, разумнее сохранить их для последующего анализа администратором. Начальное значение - **{Dirs[Mail]}\loop**. | |
| **SpamAdmin** | Каталог, в котором располагаются почтовые папки "администратора спама". Это специальный пользователь, назначенный просматривать письма, задержанные спам-фильтрами POPfile, SpamProtexx и LibSD и по этой причине не доставленные получателям - вместо этого они попадают к "администратору спама", который при необходимости может выполнить их переклассификацию. В параметрах каждого домена также может быть задан каталог "администратора спама", в этом случае он имеет приоритет. Начальное значение - **{SMTP[DefaultDomainMailBoxes]}\spamadmin**. | ? |
| **DB** | Расположение каталога для размещения используемых SMTP-сервером баз данных, таких, как почтовый реестр MailRoll. Начальное значение - **{Dirs[DB]}\smtp**. | |
| **Lists** | Расположение каталога со списками настройки SMTP-сервера. Начальное значение - **{Dirs[Lists]}\smtp**. | |
| **Templates** | Расположение каталога с шаблонами ответов и служебных писем SMTP-сервера. Начальное значение - **{Dirs[Templates]}\smtp**. | ? |
| **Filters** | Расположение каталога со списками фильтрации содержания. Начальное значение - **{SMTP[Lists]}\filters**. | |
| **MailingLists** | Расположение каталога со списками рассылки. Начальное значение - **{SMTP[Lists]}\maillists**. | |

| | | |
|---|---|---|
| **Restricted** | Расположение каталога со списками ограничения доступа для отправителей и получателей, они же "серые" списки. Начальное значение - **{SMTP[Lists]}\restricted**. | |
| **Autoresponders** | Расположение каталога со вспомогательными списками автоответчиков. Начальное значение - **{SMTP[Lists]}\autoresponders**. | |
| **Logs** | Расположение каталога оперативных журналов SMTP-сервера. Начальное значение - **{Dirs[Logs]}**. | $ |
| **LocalDomainUsers** | Файл со списком локальных почтовых ящиков. Здесь задаются особые права каждого пользователя по части отправки и получения почты. Начальное значение - **{SMTP[Lists]}\LocalDomainUsers.txt**. | ? |
| **ACL** | Список прав пользователей, назначаемых по данным авторизации на SMTP-сервере. Здесь можно задать начальные права пользователя по части отправки почты; в дальнейшем они могут быть изменены по данным списка локальных почтовых ящиков. Начальное значение - **{SMTP[Lists]}\ACL.txt**. | |
| **IpBlackList** | Список IP-адресов и подсетей, которым запрещено обращаться к SMTP-серверу. Начальное значение - **{SMTP[Lists]}\IpBlackList.txt**. | ? |
| **LocalNetworks** | Список локальных сетей, обслуживаемых SMTP-сервером. Переопределяет соответствующий параметр из секции **Lists**. Начальное значение - **{Lists[LocalNetworks]}**. | ? |
| **IpWhiteList** | Список доверенных IP-адресов или сетей, которые обслуживаются этим SMTP-сервером, то есть, которым позволено отправлять через него почту на внешние домены, а не только на локальные. Этот список ДОПОЛНЯЕТ список локальных сетей. В нём могут быть не локальные сети, а, например, особые внешние IP-адреса. Начальное значение - **{SMTP[Lists]}\IpWhiteList.txt**. | ? |
| **IpMacAuth** | Файл со списком, устанавливающим соответствие между IP и MAC адресами клиентского компьютера и именем учётной записи пользователя. Переопределяет соответствующий параметр из секции **Lists**. Начальное значение - **{Lists[IpMacAuth]}**. | |
| **HeloBlackList** | Список запрещённых имён клиентских компьютеров, сообщаемых в командах HELO и EHLO. Это ещё один рубеж защиты от нежелательного трафика, сгенерированного вирусами и спамерами, научившимися подделывать обратные адреса, но пока не освоившими искусство подделки имён узлов. Начальное значение - **{SMTP[Lists]}\HeloBlackList.txt**. | |
| **ToEmailAliases** | Список алиасов - псевдонимов, вместо которых подставляются реальные адреса ПОЛУЧАТЕЛЕЙ. На адреса отправителей алиасы не действуют. В отличие от стандартной конфигурации, здесь задаются только алиасы - если в соответствии с приведённым в стандартной конфигурации примером задать список рассылки, это приведёт к ошибкам в работе сервера. Списки рассылки обрабатываются отдельно. Начальное значение - **{SMTP[Lists]}\ToEmailAliases.txt**. | ? |
| **ToEmailWhiteList** | Список адресов получателей, почта для которых принимается в любом случае, независимо от других условий (кроме одного - отправителю должно быть разрешено воспользоваться услугами сервера) и настроек. Начальное значение - **{SMTP[Lists]}\ToEmailWhiteList.txt**. | ? |

| | | |
|---|---|---|
| **ToEmailBlackList** | Список адресов, почта для которых НЕ принимается в любом случае, независимо от других условий и настроек. Единственное исключение - отправитель является администратором, которому разрешено обходить это ограничение. Начальное значение - **{SMTP[Lists]}\ToEmailBlackList.txt**. | ? |
| **ToEmailMailLists** | Список адресов, являющихся списками рассылки. В PigMail+PigProxy обработка рассылок более изощрённая, чем в стандартной конфигурации, хотя до полного сервиса с автоматизацией и модерированием не дотягивает. Начальное значение - **{SMTP[Lists]}\ToEmailMailLists.txt**. | ? |
| **ToEmailDNDList** | Этот список можно условно назвать списком нерассылки. В нём перечислены адреса, по которым приходящие по рассылке письма доставляться не должны. Если некий сотрудник, занесённый в десяток списков внутренней рассылки, уходит в отпуск, проще занести его адрес в один список запрета, нежели исключать из всех списков, а затем восстанавливать. Этот список действует только на списки рассылки; письма, поступающие непосредственно на адрес (в том числе и по переадресации), будут доставляться. Начальное значение - **{SMTP[MailingLists]}\--DND--.txt**. | ? |
| **ToEmailNotify** | Список локальных почтовых ящиков, владельцев которых следует немедленно извещать о поступлении новой почты. Извещение не генерируется, если сервер посчитал входящее письмо спамом, а также если почтовый ящик получателя отсутствует в списке локальных почтовых ящиков (например, в случае автоматического создания неописанного ящика в локальном домене). Начальное значение - **{SMTP[Lists]}\ToEmailNotify.txt**. | ? |
| **ToEmailRobots** | Список адресов, на которых функционируют почтовые роботы. Обращение к этим адресам возможно только явное (в том числе посредством алиасов), получателями рассылок роботы быть не могут. Начальное значение - **{SMTP[Lists]}\ToEmailRobots.txt**. | ? |
| **FromEmailAliasesTo** | Иногда возникает необходимость выбирать получателя письма в зависимости от адреса отправителя, а вовсе не в соответствии с передаваемыми клиентом адресами получателей. Этот список устанавливает соответствие между отправителем и требуемым получателем. Если требуется доставить письмо нескольким адресатам, то качестве получателя можно указать список рассылки. Начальное значение - **{SMTP[Lists]}\FromEmailAliasesTo.txt**. | ? |
| **FromEmailNeedAuthList** | Список "подозрительных" или критических адресов, для отправки писем с которых обязательно требуется SMTP-авторизация (или IP-авторизация по спискам локальных и доверенных сетей, если не установлено требование обязательной SMTP-авторизации) с заданным именем. Начальное значение - **{SMTP[Lists]}\FromEmailNeedAuthList.txt**. | |
| **FromEmailWhiteList** | Список адресов, почта от которых принимается в любом случае, независимо от других условий (кроме одного - отправитель должен указать допустимый адрес получателя) и настроек. Список также содержит дополнительные параметры, позволяющие выключать спам-фильтрацию для конкретного отправителя. Начальное значение - **{SMTP[Lists]}\FromEmailWhiteList.txt**. | ? |
| **FromEmailBlackList** | Список адресов, почта от которых НЕ принимается в любом случае, независимо от других условий и настроек. Жёсткостью отказа можно управлять - от приёма в карантин до запрета даже на подачу жалобы. Начальное значение - **{SMTP[Lists]}\FromEmailBlackList.txt**. | ? |

| | | |
|---|---|---|
| **FromEmailAutoLogon** | Список адресов, которые надо авторизовать автоматически. Используется в ситуации, когда для отправки почты требуется SMTP-авторизация, а отправитель не умеет её выполнять и изменить его поведение не представляется возможным. Начальное значение - **{SMTP[Lists]}\FromEmailAutoLogon.txt**. | ? |
| **AutoReply** | Список адресов, на которых работают автоответчики. Автоответ генерируется только в ответ на явное обращение по адресу (в том числе посредством алиаса). При доставке письма через список рассылки автоответы не формируются. Начальное значение - **{SMTP[Lists]}\AutoReply.txt**. | ? |
| **NoAutoReplyTo** | Список адресов, КОТОРЫМ не слать автоответы - обычно это списки рассылки, которые в случае автоответа могут из списка рассылки автоматически исключить, или завяжется переписка роботов. Начальное значение - **{SMTP[Lists]}\NoAutoReplyTo.txt**. | ? |
| **EmailSmtpForward** | Список адресов и SMTP-серверов, куда надлежит переправлять почту для этих получателей. Используется в случаях, если почтовый сервер обслуживает "чужие" домены и должен пересылать почту этих доменов на другой SMTP-сервер, не пользуясь MX-маршрутизацией. Используется также в качестве управляющего файла планировщика для доставки писем-возвратов от агентов отправки smtpsend3 и smtpsend4. Начальное значение - **{SMTP[Lists]}\EmailSmtpForward.txt**. | ? |
| **SpecialSenders** | Список "неправильных" адресов отправителей. Такими неправильными адресами обычно представляются программы автоматической доставки почты, например, Fetchmail, smtpsend3 или smtpsend4. В списке задаются такие адреса и указывается, с каких IP-адресов разрешено их использование. Начальное значение - **{SMTP[Lists]}\SpecialSenders.txt**. | ? |
| **RestrictedEmails** | Список получателей, которым разрешено принимать почту от ограниченного круга отправителей. От каких именно отправителей - указывается в отдельном списке. Такими получателями могут быть и локальные почтовые ящики, и внешние получатели, и списки рассылки, и роботы - но не алиасы; их перечень обрабатывается раньше. Если получатель обнаруживается в этом списке, а отправитель не входит в список разрешённых для данного получателя, то сервер отвергает письмоНачальное значение - **{SMTP[Lists]}\RestrictedEmails.txt**. | ? |
| **RestrictedFromEmails** | Список отправителей, которым разрешено отправлять почту ограниченному кругу получателей. Каким именно получателям - указывается в отдельном списке. В качестве получателей могут выступать и локальные почтовые ящики, и внешние получатели, и списки рассылки, и роботы - но не алиасы; их перечень обрабатывается раньше. Если отправитель обнаруживается в этом списке, а получатель не входит в список разрешённых для данного отправителя, то сервер отвергает письмо. Начальное значение - **{SMTP[Lists]}\RestrictedFromEmails.txt**. | ? |

| | | |
|---|---|---|
| **IpInHelo** | Как показывает практика, спамеры довольно часто применяют нехитрую уловку, используя в командах HELO и EHLO вместо имени узла его IP-адрес. Заносить все возможные (или все замеченные в рассылке спама) IP-адреса в чёрный список нереально. Зато известно, что честные отправители этим практически не страдают - то есть, если предъявленное имя узла совпадает с его IP-адресом, мы с очень большой вероятностью имеем дело со спамом. В текущей версии проверяется не совпадение имени узла с IP-адресом, а его формальная корректность - некорректным считается имя, состоящее только из цифр, точек, минусов и квадратных скобок. Этот параметр определяет, что надлежит делать при обнаружении такой ситуации. Возможные значения:<br>**Ignore** - ничего не делать, пусть представляются как хотят;<br>**Quarantine** - установить режим приёма писем в карантин;<br>**Reject** - отвергать письма, если ни отправитель не попадает в список доверенных, ни получатель не является специальным (не имеет статуса Abuse);<br>**Abort** - отвечать отказом и немедленно отключаться.<br>Слово-значение можно сократить вплоть до единственного первого символа, регистр значения не имеет. Начальное значение - **Reject**. | *<br>? |
| **UseMapsRbl** | Указывает, использовать ли фильтрацию по IP-адресу отправителя с использованием сервиса MAPS (**http://mail-abuse.org/**). Это платный сервис, его услуги доступны только подписчикам. Начальное значение - **0**, то есть, не используется. | * |
| **UseRBLList** | Указывает, использовать ли фильтрацию по IP-адресу отправителя с использованием списка блокирующих сервисов. Работу со списком выполняет специальный плагин - он загружается, если при старте SMTP-сервера параметр имеет ненулевое значение. В этом случае предыдущий параметр игнорируется - если требуется фильтрация с использованием MAPS, ссылка на соответствующий сервис просто включается в список. Если плагин не загружен или параметр имеет нулевое значение, фильтрация выполняется только с использованием одной явно указанной службы. Начальное значение - **1**, то есть, список блокировочных систем используется. | * |
| **RBLSystemList** | Список используемых блокировочных сервисов, используемых, если установлен предыдущий параметр. Начальное значение - **{SMTP[Lists]}\RBLSystemList.txt**. | |
| **RBLWhiteList** | По умолчанию фильтрация по IP-адресу не выполняется, если IP-адрес клиента находится в списке локальных, доверенных или, напротив, запрещённых сетей (в этом случае явно заданные локальные настройки перекрывают действие глобальных фильтров), а также принадлежит одному из зарезервированных диапазонов, выделенных для локальных сетей (эти адреса не могут принадлежать Интернету, поэтому в глобальные фильтры не вносятся). Кроме того, есть возможность исключить фильтрацию отдельных подсетей или конкретных IP-адресов, указав их в специальном списке надёжных сетей, расположение которого задаётся этим параметром. Начальное значение - **{SMTP[Lists]}\RBLWhiteList.txt**. | |

| | | |
|---|---|---|
| **LockIntruders** | Определяет, использовать ли блокировку атак. Признаком атаки считается частое повторение различных нежелательных событий - таких, как ошибки авторизации. Если частота следования таких событий для какого-либо IP-адреса клиентского подключения превышает установленную в настройках величину, то этот адрес заносится в список запрещённых сетей. IP-адреса, находящиеся в списках локальных или доверенных сетей, блокировке не подвергаются. Если при запуске сервера этот параметр имеет любое ненулевое значение, подключается плагин **ids_memo**, обеспечивающий хранение и накопление информации о нежелательных событиях. После этого параметр может использоваться для временного отключения блокировки атак, если его работа будет создавать какие-либо проблемы. Начальное значение - **{Server[LockIntruders]}**. | * ? |
| **AuthFailCount** | Пороговое значение числа ошибок авторизации. Если количество неудачных попыток авторизации за определённый временной интервал для одного и того же IP-адреса клиентского подключения превышает заданную этим параметром величину, это считается атакой - со всеми вытекающими отрицательными последствиями для соответствующего клиента. Начальное значение - **{Server[AuthFailCount]}**. | * ? |
| **AuthFailPeriod** | Период подсчёта ошибок авторизации. Если количество неудачных попыток авторизации за определённый этим параметром временной интервал для одного и того же IP-адреса клиентского подключения превышает заданную величину, это считается атакой - со всеми вытекающими отрицательными последствиями для соответствующего клиента. Длительность периода задаётся в минутах. Начальное значение - **{Server[AuthFailPeriod]}**. | * ? |
| **UsePerformanceTuning** | Определяет, применять ли собственное нестандартное значение следующего параметра тонкой настройки производительности или же оставить заданное в коде сервера значение по умолчанию. Если сервер успешно справляется с нагрузкой, эти настройки лучше оставить как есть. Если при запуске сервера этот параметр имеет ненулевое значение, вместо значений по умолчанию применяются собственные нестандартные значения. Начальное значение - **0**. | & |
| **ListenQLen** | Задаёт максимальную длину очереди запросов на подключение к серверу. Чем больше очередь, тем вероятнее, что клиент, пусть даже после длительного ожидания, будет обслужен, а не получит от ворот поворот. Однако для обслуживания большой очереди требуется пропорциональное количество ресурсов сервера. Начальное значение соответствует значению по умолчанию - **1000**. | & |
| **WriteSocketRetryDelay** | Определяет величину задержки отслеживания событий при записи в основной сокет. Чем меньше значение этого параметра, тем оперативнее сервер реагирует на изменение состояния сокета, но, одновременно, тем больше потребление процессорного времени. Величина задержки задаётся в миллисекундах. Начальное значение соответствует значению по умолчанию - **200**. | & |
| **UseTarpit** | Указывает, использовать ли при общении с нежелательными отправителями Tarpit - "липучку". В этом случае отрицательные ответы искусственно задерживаются, что уменьшает нагрузку на сеть. Начальное значение - **{Server[UseTarpit]}**. | * ? |
| **TarpitInterval** | Если задано использование "липучки", то этот параметр задаёт длительность задержки в секундах. Начальное значение - **{Server[TarpitInterval]}**. | * ? |

| | | |
|---|---|---|
| **KeepAbuseUndelivered** | PigMail+PigProxy позволяет указать особых получателей (так называемых abuse-адресатов, как правило, это администраторы почтового сервера), написать которым могут отправители, обычно попадающие под действие различных чёрных списков. Этим адресатам также доставляются письма, заблокированные фильтрами содержания. По умолчанию эти письма доставляются непосредственно в почтовые ящики таких адресатов. Если мусор в почтовых ящиках раздражает, можно путём установки любого ненулевого значения этого параметра определить для сервера режим хранения таких писем в особом каталоге. Начальное значение - **0**. | * ? |
| **PassOverquotedToAbuse** | Указывает, можно ли доставлять письма, размер которых превышает установленные ограничения, в почтовый ящик специального (abuse) получателя. Если задано любое ненулевое значение и abuse-получатель присутствует в списке адресатов, то письмо будет помещено в его ящик (а при невозможности - в специальный каталог). В противном случае письмо, нарушающее ограничение, будет, в соответствии с другими настройками, либо удалено, либо перемещено в специальный каталог для последующего рассмотрения администратором. Начальное значение - **0**. | * ? |
| **DeleteOverquoted** | Если письмо излишне большого объёма не было доставлено специальному получателю, случившемуся среди его адресатов, то его можно либо переместить в отдельный каталог, где его однажды обнаружит администратор, либо, если на диске не слишком много места, просто удалить. Любое ненулевое значение этого параметра означает, что письма, выходящие за рамки дозволенного размера, удаляются немедленно. Начальное значение - **0**, что предполагает перемещение писем в отдельный каталог для последующего анализа администратором. | * ? |
| **DeleteMalformed** | Определяет, сохранять для ручной обработки или же незамедлительно удалять искажённые письма, в которых были обнаружены ошибки формата. В текущей версии такими считаются письма с пустыми (но объявленными в шапке) заголовками Message-ID либо с заголовками Message-ID, начинающихся с символа **<**, но не заканчивающиеся символом **>** или же содержащие только последовательность **<>**. Такие идентификаторы писем обычно встречаются в оборванных спамерских посланиях. Они сбивают с толку различные обработчики почты, в том числе некоторые клиентские антивирусы, которые могут заблокировать доступ к почтовому ящику. Любое ненулевое значение этого параметра означает, что письма с нарушениями формата удаляются немедленно. Начальное значение - **0**, что предполагает перемещение писем в отдельный каталог для последующего анализа администратором. | * ? |

| | | |
|---|---|---|
| **MaxMessageSizeAutoblacklist** | Задаёт режим автоматической блокировки отправителей почтовых бомб - писем, превышающих ограничения на максимально допустимый размер. Параметр представляет собой строку символов-флагов, определяющих способ автоблокировки:<br>**I** - IP-адрес отправителя заносится в список запрещённых сетей;<br>**H** - имя компьютера-отправителя, переданное в команде HELO, заносится в список запрещённых имён клиентских узлов;<br>**M** - адрес отправителя заносится в список запрещённых отправителей;<br>**D** - почтовый домен отправителя заносится в список запрещённых отправителей;<br>**A** - эквивалентно **IDH**;<br>**1** - эквивалентно **IDH**, используется для совместимости обозначений.<br>Флаги **M** и **D** являются взаимоисключающими, причём **M** имеет приоритет. Прочие символы игнорируются - эту особенность можно использовать для полной отмены автоблокировки. Эту возможность вообще следует использовать с большой осторожностью и пристально следить за результатами деятельности робота - особым интеллектом он не отличается, поэтому способен невзначай заблокировать любого VIP-клиента. Для снижения вероятности ошибок при автоблокировке проверяются не только пополняемые запрещающие списки, но и парные к ним разрешающие - если отправитель обнаружен в разрешающем списке, соответствующая блокировка не выполняется. Никогда не блокируются отправители, подключившиеся из локальной сети, и отправители писем, доставляемых из внешних POP-ящиков посредством загрузчика Pop3Recv. Начальное значение - **0**, автоблокировка не применяется. | *<br>? |

| | | |
|---|---|---|
| **MalformedAutoblacklist** | Задаёт режим автоматической блокировки отправителей искажённых писем, в которых были обнаружены ошибки формата. В текущей версии такими считаются письма с пустыми (но объявленными в шапке) заголовками Message-ID либо с заголовками Message-ID, начинающихся с символа **<**, но не заканчивающиеся символом **>** или же содержащие только последовательность **<>**. Такие идентификаторы писем обычно встречаются в оборванных спамерских посланиях. Они сбивают с толку различные обработчики почты, в том числе некоторые клиентские антивирусы, которые могут заблокировать доступ к почтовому ящику. Параметр представляет собой строку символов-флагов, определяющих способ автоблокировки:<br>**I** - IP-адрес отправителя заносится в список запрещённых сетей;<br>**H** - имя компьютера-отправителя, переданное в команде HELO, заносится в список запрещённых имён клиентских узлов;<br>**M** - адрес отправителя заносится в список запрещённых отправителей;<br>**D** - почтовый домен отправителя заносится в список запрещённых отправителей;<br>**A** - эквивалентно **IDH**;<br>**1** - эквивалентно **IDH**, используется для совместимости обозначений.<br>Флаги **M** и **D** являются взаимоисключающими, причём **M** имеет приоритет. Прочие символы игнорируются - эту особенность можно использовать для полной отмены автоблокировки. Эту возможность вообще следует использовать с большой осторожностью и пристально следить за результатами деятельности робота - особым интеллектом он не отличается, поэтому способен невзначай заблокировать любого VIP-клиента. Для снижения вероятности ошибок при автоблокировке проверяются не только пополняемые запрещающие списки, но и парные к ним разрешающие - если отправитель обнаружен в разрешающем списке, соответствующая блокировка не выполняется. Никогда не блокируются отправители, подключившиеся из локальной сети, и отправители писем, доставляемых из внешних POP-ящиков посредством загрузчика Pop3Recv. Начальное значение - **0**, автоблокировка не применяется. | *<br>? |

| | | |
|---|---|---|
| **SpamAutoblacklist** | Задаёт режим автоматической блокировки отправителей спама. Параметр представляет собой строку символов-флагов, определяющих способ автоблокировки:<br>**I** - IP-адрес отправителя заносится в список запрещённых сетей;<br>**H** - имя компьютера-отправителя, переданное в команде HELO, заносится в список запрещённых имён клиентских узлов;<br>**M** - адрес отправителя заносится в список запрещённых отправителей;<br>**D** - почтовый домен отправителя заносится в список запрещённых отправителей;<br>**A** - эквивалентно **IDH**;<br>**1** - эквивалентно **IDH**, используется для совместимости обозначений.<br>Флаги **M** и **D** являются взаимоисключающими, причём **M** имеет приоритет. Прочие символы игнорируются - эту особенность можно использовать для полной отмены автоблокировки. Эту возможность вообще следует использовать с большой осторожностью и пристально следить за результатами деятельности робота - особым интеллектом он не отличается, поэтому способен невзначай заблокировать любого VIP-клиента. Для снижения вероятности ошибок при автоблокировке проверяются не только пополняемые запрещающие списки, но и парные к ним разрешающие - если отправитель обнаружен в разрешающем списке, соответствующая блокировка не выполняется. Никогда не блокируются отправители, подключившиеся из локальной сети, и отправители писем, доставляемых из внешних POP-ящиков посредством загрузчика Pop3Recv. В силу параноидальных наклонностей робота начальное значение - **0** (автоблокировка отключена), однако в качестве примера имеется также закомментированный вариант со значением **HD**, адресованный любителям "острых ощущений". | *<br>? |

| | | |
|---|---|---|
| **VirusAutoblacklist** | Задаёт режим автоматической блокировки отправителей компьютерных вирусов, почтовых червей, троянских коней и прочей подобной гадости. Параметр представляет собой строку символов-флагов, определяющих способ автоблокировки:<br>**I** - IP-адрес отправителя заносится в список запрещённых сетей;<br>**H** - имя компьютера-отправителя, переданное в команде HELO, заносится в список запрещённых имён клиентских узлов;<br>**M** - адрес отправителя заносится в список запрещённых отправителей;<br>**D** - почтовый домен отправителя заносится в список запрещённых отправителей;<br>**A** - эквивалентно **IDH**;<br>**1** - эквивалентно **IDH**, используется для совместимости обозначений.<br>Флаги **M** и **D** являются взаимоисключающими, причём **M** имеет приоритет. Прочие символы игнорируются - эту особенность можно использовать для полной отмены автоблокировки. Эту возможность вообще следует использовать с большой осторожностью и пристально следить за результатами деятельности робота - особым интеллектом он не отличается, поэтому способен невзначай заблокировать любого VIP-клиента. Для снижения вероятности ошибок при автоблокировке проверяются не только пополняемые запрещающие списки, но и парные к ним разрешающие - если отправитель обнаружен в разрешающем списке, соответствующая блокировка не выполняется. Никогда не блокируются отправители, подключившиеся из локальной сети, и отправители писем, доставляемых из внешних POP-ящиков посредством загрузчика Pop3Recv. В силу параноидальных наклонностей робота начальное значение - **0** (автоблокировка отключена), однако в качестве примера имеется также закомментированный вариант со значением **I**, адресованный любителям "острых ощущений". | * ? |

| | | |
|---|---|---|
| **AutoComplementBlacklists** | Задаёт режим автоматического взаимодополнения запрещающих списков. Механизм взаимодополнения основан на простом эмпирическом правиле - у приходящего спама, как правило, все три идентификатора (IP-адрес, имя узла и адрес отправителя) являются кандидатами на занесение в чёрные списки. Следовательно, определив спамера по одному идентификатору, на оставшиеся два тоже можно достаточно смело ставить блок. Параметр представляет собой строку символов-флагов, определяющих способ автоблокировки:<br>**I** - IP-адрес отправителя заносится в список запрещённых сетей;<br>**H** - имя компьютера-отправителя, переданное в команде HELO, заносится в список запрещённых имён клиентских узлов;<br>**M** - адрес отправителя заносится в список запрещённых отправителей;<br>**D** - почтовый домен отправителя заносится в список запрещённых отправителей;<br>**A** - эквивалентно **IDH**;<br>**1** - эквивалентно **IDH**, используется для совместимости обозначений.<br>Флаги **M** и **D** являются взаимоисключающими, причём **M** имеет приоритет. Прочие символы игнорируются - эту особенность можно использовать для полной отмены автоблокировки. Эту возможность вообще следует использовать с большой осторожностью и пристально следить за результатами деятельности робота - особым интеллектом он не отличается, поэтому способен невзначай заблокировать любого VIP-клиента. Для снижения вероятности ошибок при автоблокировке проверяются не только пополняемые запрещающие списки, но и парные к ним разрешающие - если отправитель обнаружен в разрешающем списке, соответствующая блокировка не выполняется. Никогда не блокируются отправители, подключившиеся из локальной сети, и отправители писем, доставляемых из внешних POP-ящиков посредством загрузчика Pop3Recv. Блокировка не выполняется и в том случае, когда по результатам проверок включился режим приёма в карантин. В силу параноидальных наклонностей робота начальное значение - **0** (автодополнение отключено), однако в качестве примера имеется также закомментированный вариант со значением **HD**, адресованный любителям "острых ощущений". | * ? |
| **UsePopFile** | Указывает, использовать ли байесовый классификатор/фильтр почты POPfile. Для использования POPfile должен быть загружен соответствующий плагин - он загружается, если при старте SMTP-сервера параметр имеет ненулевое значение. Начальное значение - **0**, то есть, не используется. | * & $ |
| **UseSpamProtexx** | Указывает, использовать ли байесовый классификатор/фильтр почты SpamProtexx. Для использования SpamProtexx должен быть загружен соответствующий плагин - он загружается, если при старте SMTP-сервера параметр имеет ненулевое значение. Начальное значение - **0**, то есть, не используется. | * & $ |
| **UseSD** | Указывает, использовать ли байесовый классификатор/фильтр почты LibSD. Для использования LibSD должен быть загружен соответствующий плагин - он загружается, если при старте SMTP-сервера параметр имеет ненулевое значение. Начальное значение - **0**, то есть, не используется. | * & $ |

| | | |
|---|---|---|
| **UseContentFilter** | Указывает, использовать ли упрощённый фильтр содержания. В отличие от POPfile, этот фильтр проще в установке, но требует ручного сопровождения. Если используется POPfile, SpamProtexx и/или LibSD, то дополнительная фильтрация не нужна. Для упрощённой фильтрации по содержимому должен быть загружен плагин **contentfilter** - он загружается, если при старте SMTP-сервера параметр имеет ненулевое значение. Начальное значение - **0**, то есть, не используется. | *<br>&<br>$ |
| **UseContentTypeFilter** | Указывает, использовать ли проверку по списку недопустимых типов содержимого. Эта проверка работает аналогично упрощённому фильтру содержания, но независимо от него и с использованием отдельного списка шаблонов недопустимых данных. Начальное значение - **1**. | *<br>$ |
| **BlackListContentType** | Список шаблонов отвергаемых SMTP-сервером типов содержимого (**Content-Type**), применяемый, если установлен флаг **UseContentTypeFilter**. Изначально он содержит признаки китайской кодировки текста. В PigMail с этим списком сверяется не только поле **Content-Type**, но и поле **Subject**. Начальное значение - **{SMTP[Filters]}\BlackListContentType.txt**. | ? |
| **CheckMailFormat** | Указывает, выполнять ли проверку правильности формата писем. Если этот параметр имеет любое ненулевое значение, то сервер проверяет формат ряда критических (не столько для самого сервера, сколько для почтовых клиентов и антивирусов) полей в шапке письма, а также отсеивает пустые письма. Пустыми считаются письма, в шапке которых отсутствуют поля From:, To:, Subject: и Message-ID:. Начальное значение - **0**. | ? |
| **GenerateMissedHeaders** | Указывает, воссоздавать ли при доставке писем опущенные отправителем поля шапки Date: и Message-ID:. Подобной "забывчивостью" обычно страдают самодельные роботы, обслуживающие сайты и автоматизированные информационные системы. На работу почтового сервера отсутствие этих полей практически не влияет, а вот почтовый клиент или антивирус могут в этом случае повести себя неадекватно. Начальное значение - **0**. | ? |
| **Headers** | Список заголовочных полей письма, сохраняемых для последующей обработки различными фильтрами содержания. Такими обработчиками могут быть упрощённый фильтр содержания, обработчик "магических слов", автоответчик, встроенный почтовый робот. Начальное значение - **{SMTP[Lists]}\Headers.txt**. | ? |
| **UseMagicWords** | Указывает, использовать ли обработку "магических слов" в заголовочных полях письма. Эта обработка выполняется плагином **magicwords**, который загружается, если при старте SMTP-сервера параметр имеет ненулевое значение. Начальное значение - **1**, то есть, выполняется дополнительный анализ полей шапки письма. | *<br>&<br>? |
| **MagicWords** | Список сочетаний "магических" слов, сопоставленных адресам получателей. Если в заголовочных полях письма присутствует сочетание заданных слов, в список получателей письма добавляется ещё один адрес. Начальное значение - **{SMTP[Lists]}\MagicWords.txt**. | ? |
| **UseAntivirus** | Указывает, использовать ли антивирус. Если этот флаг установлен при запуске SMTP-сервера, то загружаются соответствующие плагины, после этого антивирусную проверку можно отключать и включать динамически. Начальное значение - **0**, то есть, антивирус не используется. | *<br>&<br>$ |

| | | |
|---|---|---|
| **Antivirus** | Указывает, какой именно антивирус использовать. В настоящее время можно выбирать между DrWeb (**http://www.drweb.-com/**), KAV либо KAV5 (**http://www.kaspersky.ru/**) и ClamAV (**http://www.clamav.net/**). Переключение активного антивируса "на лету" не предусмотрено, выбор производится при запуске SMTP-сервера. Начальное значение - **DrWEB**. | * & |
| **DeleteInfectedFile** | Указывает, сохранять ли файл заражённого вирусом письма для последующего анализа. Если параметр имеет нулевое значение, письмо перемещается в специальный каталог. Начальное значение - **0**. | * ? |
| **SendVirusNotify** | Указывает, посылать ли получателю вируса уведомление о том, что вирус к нему не допущен или письмо задержано по причине сбоя антивируса. В случае обнаружения вируса отправитель получит уведомление от своего почтового сервера или непосредственно от почтового клиента, поскольку SMTP-сервер при обнаружении вируса отвечает кодом ошибки 5xx. По статистике, почти все заражённые письма сгенерированы почтовыми червями, не несут никакой полезной информации и не являются ожидаемыми. Поэтому лучше получателям нервы извещениями не трепать. Начальное значение - **0**, то есть, получатели не информируются. | * ? |
| **SendAdminVirusNotify** | Указывает, формировать ли извещение для администратора сервера об отлове вируса и сбое в работе антивируса. Это, в общем-то, рекомендуемый вариант, тем более что потенциальные жертвы вируса никаких извещений по умолчанию не получают, - администратор затем и существует, чтобы держать ситуацию под контролем. Начальное значение - **1**, то есть, извещение формируется. | * ? |
| **NotifyLocalsOnly** | Если рассылка извещений о выявлении вируса включена хотя бы одним из двух вышеописанных параметров, то поток извещений о выявлении вируса можно существенно уменьшить. При ненулевом значении этого параметра извещения - как для получателей, так и для администратора - формируются только при условии, что отправитель находится в локальной сети либо представился адресом локального пользователя. Извещения о сбоях в работе антивируса формируются в любом случае. Начальное значение - **0**, отправитель не проверяется. | * ? |
| **OnVirusGeneralNotification** | Если адресат заражённого письма получает уведомление о несостоявшейся атаке, то оно генерируется на основании шаблона, задаваемого этим параметром. Начальное значение - **{SMTP[Templates]}\OnVirus.pat.txt**. | ? |
| **OnVErrorGeneralNotification** | Если адресат извещается о сбоях в работе антивируса, то уведомление генерируется на основании шаблона, задаваемого этим параметром. Начальное значение - **{SMTP[Templates]}\OnVError.pat.txt**. | ? |
| **AdminVirusNotifyEmail** | Адрес для извещения администратора сервера об отлове вируса. Начальное значение - **{SMTP[AdminEmail]}**. | * ? |
| **OnVirusAdminNotification** | Если администратор получает извещения о поимке вируса, то они генерируются на основании шаблона, задаваемого этим параметром. Начальное значение - **{SMTP[Templates]}\OnVirusAdmin.pat.txt**. | ? |
| **OnVErrorAdminNotification** | Если администратор получает извещения о сбоях в работе антивируса, то они генерируются на основании шаблона, задаваемого этим параметром. Начальное значение - **{SMTP[Templates]}\OnVErrorAdmin.pat.txt**. | ? |

| | | |
|---|---|---|
| **AntivirusDaemonEmail** | Обратный адрес демона-антивируса, подставляемый во все письма-извещения. Начальное значение - **antivir@{SMTP[DefaultMailDomain]}**. | * ? |
| **InfectedFileNameAddOns** | Файл специального списка субшаблонов - вставок, используемых при формировании писем-извещений для указания имени файла, в котором сохранено заражённое письмо, либо для информирования о том, что письмо в соответствии с настройками сервера незамедлительно удалено. Начальное значение - **{SMTP[Lists]}\InfectedFileNameAddOns.txt**. | ? |
| **UsePop2Smtp** | Указывает, использовать ли загрузчик внешней POP-почты **Pop2Smtp**. Начальное значение - **0**, то есть, загрузчик не используется. | * & |
| **Pop2SmtpDebug** | Если загрузчик внешней POP-почты Pop2Smtp используется, то этот параметр управляет отладочным выводом загрузчика. Начальное значение - **0**, то есть, отладочный вывод не используется. | * & |
| **SendReturnReceipts** | Указывает, обрабатывать ли запросы подтверждения о доставке писем (**Return-Receipt-To**). Лучше, если это будет решать сам получатель письма. Начальное значение - **0**, то есть, автоматическое подтверждение доставки не формируется. | * ? |
| **ReturnReceiptsNotification** | Если автоматическое подтверждение о доставке формируется, то оно генерируется на основании шаблона, задаваемого этим параметром. Начальное значение - **{SMTP[Templates]}\ReturnReceipt.pat.txt**. | ? |
| **DontDeliverOutboundMail** | По умолчанию (в типичной конфигурации) SMTP-сервер сам занимается доставкой исходящей почты. Однако в специфических конфигурациях, когда вся поступающая почта отдаётся для дальнейшей обработки и доставки в другую почтовую систему, это ни к чему. В лучшем случае дело закончится неудачными запусками агента отправки, в худшем - бесследным "уходом" писем в неизвестном направлении. Ненулевое значение этого параметра блокирует поползновения SMTP-сервера самостоятельно отослать исходящее письмо. Эта настройка влияет только на отправку писем, помещённых в каталог общей очереди доставки исходящих писем, определяемый параметром **Out**. Доставка перенаправленной почты блокируется индивидуально для каждого целевого сервера путём редактирования списка перенаправлений. Начальное значение - **0**. | * ? |
| **UseSmtpSend** | Указывает, использовать ли расширенный сервис доставки исходящей почты. Работа этого сервиса обеспечивается плагином **smtpsend**, который загружается, если при запуске сервера этот параметр имеет любое ненулевое значение. Выбор использования расширенного сервиса отключает использование исторического способа доставки с использованием агентов и планировщика. Начальное значение - **0**. | * & |
| **UseLocalDelivery** | Указывает, использовать ли сервис локальной доставки. Работа этого сервиса обеспечивается плагином **localdelivery**, который загружается, если при запуске сервера этот параметр имеет любое ненулевое значение. Сервис локальной доставки может работать как совместно с исторической связкой агентов и планировщика, так и с расширенным сервисом доставки исходящей почты. В последнем случае его использование настоятельно рекомендуется, поэтому начальное значение - **{SMTP[UseSmtpSend]}**. | & |

| | | |
|---|---|---|
| **SmtpSend** | Путь к приложению, играющему роль агента доставки исходящей почты. Начальное значение - **"..\utils\smtpsend4.exe -ll {SMTP[LogLine]}"**. | * |
| **LogLine** | Номер форматной строки, реализующей вывод агента smtpsend4 в статистический журнал. Возможные значения:<br>**2907** - вывод в статистический журнал формата Elog;<br>**2979** - вывод в статистический журнал собственного текстового формата.<br>К сожалению, вести одновременную запись в несколько различных журналов невозможно. Начальное значение - **2907**. | * |
| **ReturnFromEmail** | Задаёт почтовый адрес, от имени которого агент smtpsend3 или smtpsend4 генерирует письмо-возврат. Начальное значение - **{SMTP[AdminEmail]}**. | *<br>? |
| **ReturnPath** | Задаёт путь к каталогу очереди внутренней доставки, в который агент smtpsend3 или smtpsend4 помещает сгенерированное письмо-возврат. Начальное значение - **{SMTP[Local]}**. | * |
| **Return** | Если используется агент smtpsend3 или smtpsend4, то ему можно указать путь для размещения писем-возвратов, генерируемых в случае невозможности доставки почты, а также адрес, от имени которого генерируется это письмо. Начальное значение - **"-rd {SMTP[ReturnPath]} -ra {SMTP[ReturnFromEmail]}"**. | * |
| **OutForward** | Задаёт путь к каталогу очереди доставки маршрута, в котором агент ищет перенаправленные письма, подлежащие отправке на заданный почтовый сервер. Этот параметр вычисляется при обработке списка перенаправлений для каждой строки списка. Начальное значение - **{SMTP[Out]}\{FIELD2}\ {FIELD3}**. | |
| **RetryForward** | Задаёт путь к каталогу очереди отложенной доставки маршрута, в котором агент ищет перенаправленные письма, подлежащие отправке на заданный почтовый сервер. Этот параметр вычисляется при обработке списка перенаправлений для каждой строки списка. Начальное значение - **{SMTP[Retry]}\{FIELD2}\{FIELD3}**. | |
| **SendMailApp** | Полная командная строка запуска агента доставки, содержащая все необходимые параметры для доставки писем из общей очереди доставки. Начальное значение - **"{SMTP[SmtpSend]} -dc -dw -ld -r 1 -rh 4 -helo {Server[HostName]} -s {SMTP[DNSServer]} -o {Dirs[Temp]}\smtpsend-{RANDOM-ID}.log -f {SMTP[Out]}\ -rf {SMTP[Retry]} {SMTP[Return]}"**. | * |
| **SendMailAppRetry** | Полная командная строка запуска агента доставки, содержащая все необходимые параметры для доставки залежавшихся писем из очереди отложенной доставки. Начальное значение - **"{SMTP[SmtpSend]} -dc -dw -ld -r 1 -rh 0 -helo {Server[HostName]} -s {SMTP[DNSServer]} -o {Dirs[Temp]}\smtpsend-{RANDOM-ID}.log -f {SMTP[Retry]}\ {SMTP[Return]}"**. | * |
| **SendMailAppForward** | Полная командная строка агента доставки, содержащая все необходимые параметры для доставки перенаправленной почты на конкретный SMTP-сервер без использования авторизации. Начальное значение - **"{SMTP[SmtpSend]} -dc -dw -ld -r 1 -rh 4 -helo {Server[HostName]} -sm {FIELD2} -p {FIELD3} -o {Dirs[Temp]}\smtpsend-{RANDOM-ID}.log -f {SMTP[OutForward]}\ -rf {SMTP[RetryForward]} {SMTP[Return]}"**. | * |

| | | |
|---|---|---|
| **SendMailAppForwardRetry** | Полная командная строка агента доставки, содержащая все необходимые параметры для повторной доставки залежавшейся перенаправленной почты на конкретный SMTP-сервер без использования авторизации. Начальное значение - **"{SMTP[SmtpSend]} -dc -dw -ld -r 1 -rh 0 -helo {Server[HostName]} -sm {FIELD2} -p {FIELD3} -o {Dirs[Temp]}\smtpsend-{RANDOM-ID}.log -f {SMTP[RetryForward]}\ {SMTP[Return]}"**. | * |
| **SendMailAppForwardAS** | Полная командная строка агента доставки, содержащая все необходимые параметры для доставки перенаправленной почты на конкретный SMTP-сервер с использованием SMTP-авторизации. Начальное значение - **"{SMTP[SmtpSend]} -dc -dw -ld -r 1 -rh 4 -helo {Server[HostName]} -sm {FIELD2} -p {FIELD3} -u {FIELD4} -w {FIELD5} -o {Dirs[Temp]}\smtpsend-{RANDOM-ID}.log -f {SMTP[OutForward]}\ -rf {SMTP[RetryForward]} {SMTP[Return]}"**. | * |
| **SendMailAppForwardASRetry** | Полная командная строка агента доставки, содержащая все необходимые параметры для повторной доставки залежавшейся перенаправленной почты на конкретный SMTP-сервер с использованием SMTP-авторизации. Начальное значение - **"{SMTP[SmtpSend]} -dc -dw -ld -r 1 -rh 0 -helo {Server[HostName]} -sm {FIELD2} -p {FIELD3} -u {FIELD4} -w {FIELD5} -o {Dirs[Temp]}\smtpsend-{RANDOM-ID}.log -f {SMTP[RetryForward]}\ {SMTP[Return]}"**. | * |
| **SynchronousSend** | Указывает, использовать ли синхронную отправку исходящей почты. Обычно отправкой ведает планировщик - плагин **scheduler**, регулярно проверяющий наличие исходящих писем и при необходимости запускающий агента отправки. В синхронном режиме агент также запускается при каждом помещении письма в папку исходящей почты. Если плагин **scheduler** не загружен (что не рекомендуется, поскольку при этом часть функций просто перестаёт работать), используется синхронная отправка независимо от значения параметра. Начальное значение - **1**, то есть, синхронные запуски агента производятся при каждом помещении письма в очередь отправки. | * ? |
| **UseScheduler** | Указывает, использовать ли планировщик. Для загрузки плагина **scheduler** при запуске сервера следует указать любое ненулевое значение. Начальное значение - **1**, то есть, предполагается использование планировщика. | * & |
| **SerializeSend** | Указывает, использовать ли в планировщике "сериализацию" запусков агента. Если задано любое ненулевое значение, планировщик при каждом запуске агента отправки ожидает окончания его работы. В противном случае при работе на медленных каналах есть реальный риск съедания как ресурсов системы, так и полосы пропускания канала большим количеством одновременно работающих копий агента. Начальное значение - **1**. | * ? |
| **SchedulerPause** | Длительность основного цикла планировщика, задаваемая в миллисекундах. Минимально допустимое значение составляет 1000 (одну секунду). Начальное значение - **300000**, что соответствует пяти минутам. | * |
| **SchedulerRetryPause** | Задаваемая в миллисекундах длительность цикла планировщика, ответственного за повторную отправку залежавшейся почты. Минимально допустимое значение составляет 1000 (одну секунду). Начальное значение - **7200000**, что соответствует двум часам. | * |

| | | |
|---|---|---|
| **DenyLocalPartCharacters** | Строка символов, которые запрещены в имени почтового ящика (часть адреса слева от разделителя **@**, называемая также локальной) и имени почтового домена. При обнаружении такого символа в адресе отправителя либо получателя адрес будет отвергнут. Начальное значение - **" !$%&'()*,/:;<>?@[\]^`\|~{"}"**. Сочетание **{"}** (два апострофа в фигурных скобках) - это макрос, обозначающий символ двойной кавычки **"**, который не может быть указан явно, чтобы не вызвать конфликта с ограничителями строки. | ? |
| **MaxEmailLength** | Максимально допустимая длина адреса. Слишком длинный адрес является либо признаком атаки, либо порождением генератора адресов, применяемого при рассылке спама, поэтому имеет смысл отсекать такие попытки в самом начале. Начальное значение - **64**. | ? |
| **LogLevel** | Задаёт уровень детализации оперативного журнала SMTP-сервера. Параметр может принимать значения от 1 до 9. Чем выше уровень, тем больше подробностей пишется в журнал. Для совместимости с ранними версиями, в которых уровень детализации не задавался, нулевое значение соответствует максимальному уровню детализации. Начальное значение - **{Server[LogLevel]}**. | $ |
| **LogAVEvents** | Указывает, вести ли дополнительный оперативный журнал работы антивируса. Если параметр имеет любое ненулевое значение, создаётся дополнительный журнал, в который записываются результаты антивирусной проверки принятых писем. Начальное значение - **1**. | * ? |
| **LogAVOkEvents** | Если ведётся дополнительный оперативный журнал работы антивируса, то этот параметр указывает, записывать ли в него информацию о письмах, в которых вредоносный код не обнаружен. Запись ведётся при любом ненулевом значении. Начальное значение - **0**. | * ? |
| **LogToEStat** | Определяет, ведёт ли сервер статистику в формате программы **Estat32**, разработанной **Андреем Волковым** из **EPE Labs** для обработки статистических журналов Eserv/2. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{Server[LogToEStat]}**. | $ |
| **LogToAdvSoft** | Определяет, ведёт ли сервер статистику в формате программ **ProxyInspector** и **MailDetective** производства компании **AdvSoft**. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{Server[LogToAdvSoft]}**. | $ |
| **LogToElog** | Определяет, ведёт ли сервер статистику в формате программы **Elog**, разработанной **Игорем Панасенко** из компании **ЛЭНК** для обработки статистических журналов Eserv/3. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{Server[LogToElog]}**. | $ |

| | | |
|---|---|---|
| **LogToMaillog** | Определяет, ведёт ли сервер статистику в собственном текстовом формате. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{Server[LogToMaillog]}**. | $ |
| **LogToMStat** | Определяет, используется ли подсистема ведения статистики в базе данных MStat, разработанная Андреем Матвеевым. Этот сборщик статистики имеет немалое преимущество перед текстовыми журналами, позволяя хранить и эффективно обрабатывать статистическую информацию за большие периоды времени, измеряемые годами. Но для его работы необходима установка дополнительного приложения - СУБД одного из поддерживаемых сборщиком типов. Если при запуске сервера указано любое ненулевое число, загружается специальный плагин **mstat**. В дальнейшем при возникновении проблем сбор статистики в базе данных можно временно отключить, установив нулевое значение. Начальное значение - **{Server[LogToMStat]}**. | $<br>& |
| **LogMessageBody** | Если плагин **contentfilter** (упрощённый фильтр содержания) не используется, SMTP-сервер использует определённое в стандартной конфигурации правило обработки тела письма. Будучи активированным, стандартное правило выполняет запись тела письма в основной журнал сервера, что приводит как к замедлению обработки почты, так и к повышенному расходу дискового пространства. Если этому параметру присвоить нулевое значение, то запись тела письма в журнал блокируется. Начальное значение - **0**. | *<br>& |
| **LogDataErrors** | Определяет, записывать ли в журнал ошибок информацию о сбоях во время приёма писем. Обычно эти сбои связаны с разрывами связи между сервером и клиентом, происходящими по причинам, устранить которые администратор принимающей стороны не в силах. Поэтому запись этих ошибок можно заблокировать, чтобы не пугаться понапрасну. Однако попутно блокируется запись информации о других возможных ошибках. Это могут сбои при записи данных на диск, связанные, например, с недостатком места. Если задать параметру любое ненулевое значение, информация о сбоях будет записываться в журнал ошибок. Начальное значение - **0**. | *<br>? |
| **UseMcontent** | Определяет, использовать ли контент-анализатор **MContent**. Этот анализатор, выполненный в виде отдельного плагина **mcontent**, позволяет выполнять над письмами практически любые операции - извлекать из них вложенные файлы, удалять нежелательные вложения, добавлять и удалять заголовки. В зависимости от наличия тех или иных заголовков или вложений можно определить дальнейшую судьбу сообщения. Самая впечатляющая возможность - сжать все вложения архиватором и поместить их обратно в письмо, заместив исходные. Для загрузки плагина при запуске сервера следует указать любое ненулевое значение; при загруженном плагине флаг позволяет динамически включать или отключать контент-анализатор. Начальное значение - **0**. | *<br>&<br>? |

| | | |
|---|---|---|
| **UseLsp** | Определяет, использовать ли локальные политики для отправителя. Собственные локальные политики позволяют дополнить или переопределить правила выявления подделанных обратных адресов, используемые Sender Policy Framework. Локальные политики могут применяться и самостоятельно, если использование SPF по каким-либо причинам невозможно. Поддержка работы с локальными политиками выполнена в виде отдельного плагина **lsp**, который загружается, если при старте SMTP-сервера этот параметр имеет ненулевое значение. В дальнейшем при необходимости использование локальных политик можно временно отключить, задав нулевое значение. Начальное значение - **0**. | * & ? |
| **LocalSenderPolicy** | Список локальных политик для отправителя, используемых, если установлен предыдущий параметр. Начальное значение - **{SMTP[Lists]}\LocalSenderPolicy.txt**. | ? |
| **UseSpf** | Определяет, использовать ли Sender Policy Framework. Эта мощная технология позволяет на основании сопоставления переданного в команде протокола электронного адреса отправителя с IP-адресом подключения выявлять факт подделки обратного адреса - этим обычно грешат спамеры и почтовые черви. Поддержка работы с Sender Policy Framework выполнена в виде отдельного плагина **spf**, который загружается, если при старте SMTP-сервера этот параметр имеет ненулевое значение. В дальнейшем при необходимости использование этой технологии можно временно отключить, задав нулевое значение. Начальное значение - **0**. | * & ? |
| **UseMailRoll** | Определяет, использовать ли почтовый реестр MailRoll. В базу данных почтового реестра записывается статистика переписки между различными отправителями и получателями. На основании этих данных сервер может более благосклонно относиться к отправителям, с которыми у пользователей сервера происходит достаточно интенсивная переписка. Поддержка почтового реестра реализована в виде отдельного плагина **mailroll**, который загружается, если при старте SMTP-сервера этот параметр имеет ненулевое значение. В дальнейшем при необходимости использование почтового реестра можно временно отключить, задав нулевое значение. Начальное значение - **0**. | * & ? |
| **MailRollDebug** | Управляет отладочным выводом плагина поддержки почтового реестра. Начальное значение - **0**. | * & |
| **MailRollDB** | Файл базы данных почтового реестра. Это база данных формата SQLite3. Начальное значение - **{SMTP[DB]}\mailroll.db3**. | & |

| | | |
|---|---|---|
| **MailRollPolicy** | Политика использования и обновления информации почтового реестра. Этот параметр используется при включённой поддержке локальных или глобальных политик и позволяет регулировать уровень доверия к отправителю в зависимости от степени достоверности его адреса. Параметр представляет собой строку символов-флагов, задающих условия для использования:<br>**L** (Local) - отправитель локальный (IP-адрес принадлежит локальной сети или самому серверу), поэтому политики не проверялись;<br>**K** (Known) - отправитель известен, поскольку успешно авторизовался на сервере; на самом деле статистика переписки для успешно авторизованных отправителей заносится в базу реестра независимо от наличия этого флага;<br>**W** (Whitelist) - по результатам проверки локальных политик отправитель признан особо доверенным (код политики **WL**);<br>**M** (Match) - по результатам проверки локальных политик адрес отправителя признан действительным (код политики **AM**);<br>**P** (Pass) - по результатам проверки глобальных политик адрес отправителя признан действительным;<br>**N** (None) - проверка глобальных политик не выявила никакой информации в отношении отправителя;<br>**E** (Error) - проверка глобальных политик не удалась из-за ошибки при получении информации;<br>**U** (Unknown) - проверка глобальных политик не дала однозначный результат;<br>**T** (neuTral) - по результатам проверки локальных политик отправитель признан крайне подозрительным и подлежащим дополнительной проверке по глобальным политикам с отказом при уровне недостоверности NEUTRAL (код политики **NE**);<br>**R** (neutRal) - по результатам проверки глобальных политик отправитель признан незначительно нарушающим правила (уровень недостоверности NEUTRAL);<br>**O** (sOftfail) - по результатам проверки локальных политик отправитель признан подозрительным и подлежащим дополнительной проверке по глобальным политикам с отказом при уровне недостоверности SOFTFAIL (код политики **SF**);<br>**S** (Softfail) - по результатам проверки глобальных политик отправитель признан нарушающим правила (уровень недостоверности SOFTFAIL);<br>**F** (Fail) - по результатам проверки локальных политик отправитель признан обычным и подлежащим дополнительной проверке по глобальным политикам с отказом при уровне недостоверности FAIL (код политики **FA**);<br>**#** - условие срабатывает, если проверка политик (и локальных, и глобальных) отключена;<br>**A** (Always) - условие срабатывает всегда, в том числе при полностью отключённой проверке политик.<br>Прочие символы игнорируются. Начальное значение - **#PMWNEUF**. | * ? |
| **MailRollWhiteListThreshold** | Определяет пороговое количество зарегистрированных в базе почтового реестра писем данному отправителю (неважно, с каких адресов), при превышении которого отправитель будет считаться доверенным - как если бы этот адрес находился в соответствующем списке. Начальное значение - **1**. | * $ |

| | | |
|---|---|---|
| **MailRollInboundThreshold** | Определяет пороговое количество зарегистрированных в базе почтового реестра писем от данного отправителя данному получателю, при превышении которого переписка может считаться систематической. Чтобы она действительно считалась таковой, должно также выполняться аналогичное условие для ответных писем (от получателя к отправителю). Участники систематической переписки считаются особо доверенными, отправляемые ими письма не проверяются спам-фильтрами. Начальное значение - **5**. | * $ |
| **MailRollOutboundThreshold** | Определяет пороговое количество зарегистрированных в базе почтового реестра писем от данного получателя данному отправителю, при превышении которого переписка может считаться систематической. Чтобы она действительно считалась таковой, должно также выполняться аналогичное условие для прямых писем (от отправителя к получателю). Участники систематической переписки считаются особо доверенными, отправляемые ими письма не проверяются спам-фильтрами. Начальное значение - **3**. | * $ |
| **UseAlerter** | Определяет, задействовать ли механизм административных оповещений о недоставке почты. Если этот механизм включён, то администратор сервера будет извещаться специальным электронным письмом о каждом случае отказа отправителю, включая отсеивание уже принятого письма фильтрами содержания. Поддержка административных оповещений выполнена в виде отдельного плагина **alerter**, который загружается, если при старте SMTP-сервера этот параметр имеет ненулевое значение. В дальнейшем при возникновении проблем административные оповещения можно временно отключить, задав нулевое значение. Начальное значение - **0**. | * & $ |
| **OnAlertNotification** | Задаёт шаблон, на основании которого генерируется письмо-оповещение. Начальное значение - **{SMTP[Templates]}\OnAlertNotification.pat.txt**. | ? |
| **OnAlertNotifyFrom** | Адрес отправителя, от имени которого посылаются оповещения. Начальное значение - **{SMTP[AdminEmail]}**. | ? |
| **OnAlertNotifyTo** | Адрес администратора-получателя. Если необходимо доставлять оповещения нескольким адресатам, следует указать адрес списка рассылки. Начальное значение - **{SMTP[AdminEmail]}**. | ? |
| **UseYdk** | Определяет, использовать ли механизм подписи Yahoo Domain Keys. Этот механизм использует сертификаты, публикуемые с помощью DNS-серверов. Обратившись к серверу, хранящему записи домена отправителя, можно проверить правильность подписи и её соответствие сертификату домена, обеспечив таким образом достаточно надёжную защиту от подделки адреса отправителя. Со временем, если эта технология распространится повсеместно, уже сам факт отсутствия подписи будет порождать определённые подозрения. Поддержка Yahoo Domain Keys выполнена в виде отдельного плагина **ydk**, который загружается, если при старте SMTP-сервера этот параметр имеет ненулевое значение. В дальнейшем при необходимости использование этой технологии можно временно отключить, задав нулевое значение. Начальное значение - **0**. | * & ? |

| | | |
|---|---|---|
| **UseQuotas** | Определяет, использовать ли квоты на общий объём и количество писем в локальных почтовых ящиках. Если квоты используются и заданы, то в случае их превышения адрес соответствующего локального получателя будет отвергнут сервером. Если письмо отправлено в список рассылки, в котором состоит чрезмерно распухший ящик, письмо просто не будет доставлено беспечному адресату. В отличие от стандартной конфигурации, проверяются параметры всего почтового ящика, а не одной папки INBOX. Поддержка квот выполнена в виде отдельного плагина **quota**, который загружается, если при старте SMTP-сервера этот параметр имеет ненулевое значение. В дальнейшем при необходимости использование квот можно временно запретить, задав нулевое значение. Начальное значение - **0**. | * & ? |
| **DefaultSizeQuota** | Задаёт квоту на объём почтового ящика по умолчанию. Это значение используется, если почтовый ящик адресата отсутствует в списке локальных почтовых ящиков. Объём задаётся в мегабайтах. Нулевое значение отключает проверку объёма. Начальное значение - **0**. | * ? |
| **DefaultFilesQuota** | Задаёт квоту на количество писем в почтовом ящике по умолчанию. Это значение используется, если почтовый ящик адресата отсутствует в списке локальных почтовых ящиков. Нулевое значение отключает проверку количества писем. Начальное значение - **0**. | * ? |
| **QuotaExceedNotify** | Определяет, извещать ли получателей о факте превышения квоты. Если этот параметр имеет любое ненулевое значение, то при первом обнаружении переполнения в почтовый ящик помещается специальное письмо-уведомление. Начальное значение - **0**. | * ? |
| **QuotaExceedNotification** | Если извещение о превышении квоты формируется, то оно генерируется на основании шаблона, задаваемого этим параметром. Начальное значение - **{SMTP[Templates]}\QuotaExceeded.pat.txt**. | ? |
| **UsePop3Recv** | Определяет, использовать ли альтернативный стандартному Pop2Smtp загрузчик внешней POP-почты Pop3Recv. Загрузчик реализован в виде специального плагина **pop3recv**, который загружается, если при старте SMTP-сервера этот параметр имеет ненулевое значение. В дальнейшем загрузчик можно временно отключить, задав нулевое значение. Начальное значение - **0**, загрузчик не используется. | * & |
| **ForwardLocalMail** | Модульная архитектура Eserv/3 позволяет произвольным образом выбирать работающие службы. Что активно используется - встречаются конфигурации, в которых из почтовых служб задействован только SMTP-сервер, а локальные почтовые ящики располагаются в совершенно другом месте и обслуживаются другой почтовой системой. Этот параметр позволяет выбирать, будет ли работать SMTP-сервер в типовой конфигурации либо же почта, адресованная локальным получателям, вместо раскладки по соответствующим ящикам будет перемещаться в специальный каталог, откуда её каким-то образом будет забирать целевая почтовая система. Ненулевое значение параметра задаёт такой режим работы с передачей локальной почты вовне. Начальное значение - **0**. | * ? |
| **ForwardLocalSpam** | Совместно с параметром **ForwardLocalMail** определяет, передаются ли на обработку в стороннюю почтовую систему письма, отсеянные фильтром POPfile, SpamProtexx или LibSD. Перенаправление спама выполняется, если оба параметра имеют ненулевое значение. Начальное значение - **0**; спам помещается в ящики локальных спам-администраторов. | * ? |

| | | |
|---|---|---|
| **ForwardDir** | Если локальная почта передаётся сторонней почтовой системе, то этот параметр определяет расположение каталога передачи. Начальное значение - **{Dirs[Mail]}\forward**. | ? |
| **ArchiveLocalMail** | Определяет, вести ли архив почты, доставляемой локальным получателям. Начальное значение - **0**, то есть, архив не ведётся. | * ? |
| **ArchiveDir** | Если доставляемая в почтовые ящики локальных пользователей почта помещается в архив, то этот параметр определяет расположение архивного каталога. Сам каталог может быть расположен где угодно, в том числе он может быть и папкой любого локального почтового ящика. Начальное значение - **{Dirs[Mail]}\archive**. | |
| **ArchiveLocalSendersMail** | Определяет, вести ли архив почты, посылаемой локальными отправителями - независимо от того, является ли она исходящей или предназначена локальным же получателям. Начальное значение - **0**, то есть, архив не ведётся. | * ? |
| **LocalSendersArchiveDir** | Если отсылаемая локальными отправителями почта помещается в архив, то этот параметр определяет расположение архивного каталога. Письма помещаются в архив в том виде, в каком они были отправлены, без изменений, вносимых контент-анализатором MContent. При этом в файле письма сохраняется список всех получателей - тоже в исходном виде, без подстановки псевдонимов и раскрытия списков рассылки. Сам каталог может быть расположен где угодно, в том числе он может быть и папкой любого локального почтового ящика. Начальное значение - **{SMTP[ArchiveDir]}**, то есть, по умолчанию ведётся (если ведётся) один общий архив. | |
| **ArchiveOutboundMail** | Определяет, вести ли архив почты, отправляемой за пределы локального домена (исходящей). Начальное значение - **0**, то есть, архив не ведётся. | * ? |
| **OutboundArchiveDir** | В отличие от стандартной конфигурации, помещение исходящей почты в архив достигается не пересылкой по специальному адресу, а копированием файла письма в заданный этим параметром каталог. При этом в файле письма сохраняется список внешних получателей. Сам каталог может быть расположен где угодно, в том числе он может быть и папкой любого локального почтового ящика. Начальное значение - **{SMTP[ArchiveDir]}**, то есть, по умолчанию ведётся (если ведётся) один общий архив. | |
| **ArchiveForwardedMail** | Определяет, вести ли архив перенаправленной почты. Это может быть почта для внешних получателей многосерверного домена либо транзитная почта для обслуживаемого сервером "чужого" домена. Начальное значение - **0**, то есть, архив не ведётся. | * ? |
| **ForwardedArchiveDir** | Если перенаправляемая почта сохраняется в архиве, то этот параметр определяет расположение архивного каталога. Сам каталог может быть расположен где угодно, в том числе он может быть и папкой любого локального почтового ящика. Начальное значение - **{SMTP[ArchiveDir]}**, то есть, по умолчанию ведётся (если ведётся) один общий архив. | |
| **ArchiveListedOnly** | Определяет, вести ли архив всех проходящих через сервер писем (разумеется, в зависимости от настроек, заданных для соответствующей категории) или имеющих отношение только к особо перечисленным отправителям или адресатам. Начальное значение - **0**, то есть, архивируются (если разрешено) все письма. | * ? |

| | | |
|---|---|---|
| **ArchiveRecipients** | Список адресатов с особым режимом архивации предназначенных им писем. В этом списке задаются особые архивные каталоги для таких адресатов. Кроме того, в режиме архивации всех писем этот список можно использовать для исключения некоторых адресатов - предназначенные им письма не будут помещаться в архив. Начальное значение - **{SMTP[Lists]}\ArchiveRecipients.txt**. | ? |
| **ArchiveSenders** | Список отправителей с особым режимом архивации отправляемых ими писем. В этом списке задаются особые архивные каталоги для таких отправителей. Кроме того, в режиме архивации всех писем этот список можно использовать для исключения некоторых отправителей - посылаемые ими письма не будут помещаться в архив. Начальное значение - **{SMTP[Lists]}\ArchiveSenders.txt**. | ? |

## *Секция Pop2Smtp - параметры настройки загрузчика внешней POP-почты Pop2Smtp*

| | | |
|---|---|---|
| **Boxes** | Файл со списком опрашиваемых внешних почтовых ящиков и соответствующих им SMTP-серверов. Начальное значение - **{Dirs[Conf]}\lists\pop2smtp\Boxes.txt**. | |
| **PollInterval** | Интервал опроса почтовых ящиков, задаваемый в минутах. Начальное значение - **10**. | * & |
| **PollSchedule** | Задаёт нестандартное условие, при выполнении которого происходит опрос почтовых ящиков. Если такое условие задано, то его истинность проверяется раз в минуту, наподобие правил в планировщике Eserv/2. Таким образом можно выполнять опрос почтовых ящиков не регулярно (вряд ли стоит своих денег трафик, набегающий от постоянных обращений к внешнему POP-серверу в ночное время), а в зависимости от ситуации - хотя бы от времени суток. У этого параметра есть специфическое свойство - условие непременно и обязательно честно проверяется каждый раз, а вот его формулировка считывается из конфигурационного файла единожды, при запуске сервера. Поэтому для изменения условия сервер придётся перезапускать. Начальное значение - пустая строка, условие не задано. | & |
| **SaveRejected** | Указывает, сохранять ли для последующего анализа письма, отвергнутые SMTP-сервером. Начальное значение - **0**, то есть, такие письма отбрасываются. | * |
| **FileName** | Если отвергнутые письма сохраняются, то этот параметр задаёт путь и шаблон для формирования имени файла, в котором будет сохраняться письмо. Начальное значение - **{SMTP[Undelivered]}\pop2smtp-{RANDOM-ID}.eml**. | |
| **DeleteRejected** | Указывает, удалять ли из почтового ящика письма, которые не были штатно, без ошибок, перенаправлены на SMTP-сервер и не были сохранены для последующего анализа. Этот параметр позволяет ценой возможной потери важной информации избежать переполнения ящика при возникновении каких-либо проблем. Начальное значение - **0**, то есть, удаляются только письма, которые удалось прочитать. | * |

| | | |
|---|---|---|
| **DupCheck** | Поскольку хранящиеся в почтовом ящике письма не содержат (а если и содержат, то неизвестно, в каком виде) информации об истинном адресате, её приходится извлекать из заголовка письма, в котором может содержаться множество адресов, в том числе там могут быть упомянуты сразу несколько локальных получателей. Обычно это означает, что для каждого из этих получателей имеется отдельная копия письма. Поскольку список адресатов воссоздаётся заново, каждый адресат получит столько копий письма, сколько существует самих локальных адресатов. К тому же особенности реализации рассылок электронной почты и сами по себе довольно часто приводят к дублированию. Разрядить ситуацию призван этот параметр, указывающий, удалять ли дубликаты писем непосредственно на внешнем почтовом сервере. Дубликаты определяются по уникальному идентификатору письма, хранящемуся в заголовочном поле **Message-ID**. Если при анализе заголовка письма выясняется, что такой идентификатор уже встречался, то письмо считается уже загруженным и оставляется в ящике без обработки. Однако в случае некорректного повторного использования идентификатора (этим грешат некоторые почтовые серверы, использующие в автоответах Message-ID исходного сообщения, а также некоторые почтовые клиенты, присваивающие один и тот же идентификатор всем фрагментам автоматически разбитого на части большого сообщения) такие действия могут привести к потере данных. Поэтому начальное значение - **0**, удаление дубликатов выключено. | * |
| **Pop3Log** | Определяет, выводить ли в специальный отладочный журнал передаваемые внешнему POP-серверу команды и ответы сервера. Начальное значение - **1**, отладочный журнал ведётся. | * |
| **SmtpLog** | Определяет, выводить ли в специальный отладочный журнал передаваемые SMTP-серверу команды и ответы сервера. Начальное значение - **1**, отладочный журнал ведётся. | * |
| **AllowExternRcpt** | Определяет, разрешено ли отправлять принятую загрузчиком почту наружу. Эту возможность следует использовать с осторожностью - только если загрузчик доставляет почту на внешний сетевой интерфейс SMTP-сервера (то есть, работает как обычный внешний отправитель) и только в случае особой необходимости. В противном случае есть опасность зацикливания почты, когда уже принятые письма отправляются наружу в тот самый внешний ящик, откуда были только что загружены. Начальное значение - **0**, отправка наружу запрещена. | * |

## *Секция Pop3Recv - параметры настройки загрузчика внешней POP-почты Pop3Recv*

| | | |
|---|---|---|
| **Certificate** | Имя файла формата PEM, содержащего закрытый ключ и сертификаты, используемые при организации защищённого (SSL) соединения с целевым сервером. Начальное значение - **{SMTP[Certificate]}**. | ? |
| **SslVerifyServer** | Определяет режим проверки подлинности сертификатов целевого сервера при установлении защищённого соединения. Задаётся либо числовым кодом, либо символьным обозначением:<br>**SSL_VERIFY:IGNORE** - сертификат целевого сервера проверяется, но соединение устанавливается независимо от результата проверки, при этом клиентский сертификат серверу не предъявляется (числовое значение -1);<br>**SSL_VERIFY:NONE** - сертификат целевого сервера проверяется, но соединение устанавливается независимо от результата проверки (числовое значение 0);<br>**SSL_VERIFY:STANDARD** - сертификат целевого сервера проверяется, при отрицательном результате проверки соединение незамедлительно разрывается (числовое значение 1).<br>Начальное значение - **SSL_VERIFY:NONE**, то есть, сертификаты целевых серверов принимаются вне зависимости от результата их проверки. | * ? |
| **Lists** | Расположение каталога со списками настройки загрузчика. Начальное значение - **{Dirs[Lists]}\pop3recv**. | |
| **Boxes** | Файл со списком опрашиваемых внешних почтовых ящиков. Начальное значение - **{Pop3Recv[Lists]}\Boxes.txt**. | |

| | | |
|---|---|---|
| **Headers** | Файл со списком заголовочных полей письма, из которых извлекаются адреса отправителей и получателей. Начальное значение - **{Pop3Recv[Lists]}\Headers.txt**. | ? |
| **Pop3RecvDB** | Файл рабочей базы данных загрузчика. Здесь хранятся идентификаторы обработанных писем (если активировано удаление дубликатов) и моменты последних опросов внешних ящиков. Это база данных формата SQLite3. Начальное значение - **{SMTP[DB]}\pop3recv.db3**. | & |
| **PollInterval** | Интервал опроса почтовых ящиков, задаваемый в минутах. Начальное значение - **10**. | * |
| **PollSchedule** | Задаёт нестандартное условие, при выполнении которого происходит опрос почтовых ящиков. Если такое условие задано, то его истинность проверяется раз в минуту, наподобие правил в планировщике Eserv/2. Таким образом можно выполнять опрос почтовых ящиков не регулярно (вряд ли стоит своих денег трафик, набегающий от постоянных обращений к внешнему POP-серверу в ночное время), а в зависимости от ситуации - хотя бы от времени суток. Начальное значение - пустая строка, условие не задано. | |
| **FileName** | Если отвергнутые письма сохраняются (это определяется соответствующим полем списка почтовых ящиков), то в списке также задаётся путь и шаблон для формирования имени файла, в котором будет сохраняться письмо. Если по каким-либо причинам шаблон в списке не задан, то в качестве шаблона по умолчанию используется этот параметр. Начальное значение - **{SMTP[Undelivered]}\pop3recv-{RANDOM-ID}.eml**. | |
| **Debug** | Указывает, использовать или нет отладочный вывод загрузчика. Начальное значение - **0**, то есть, отладочный вывод не используется (в большинстве случаев вполне достаточно обычного оперативного журнала). | & |
| **DupCheck** | Поскольку хранящиеся в почтовом ящике письма не содержат (а если и содержат, то неизвестно, в каком виде) информации об истинном адресате, её приходится извлекать из заголовка письма, в котором может содержаться множество адресов, в том числе там могут быть упомянуты сразу несколько локальных получателей. Обычно это означает, что для каждого из этих получателей имеется отдельная копия письма. Поскольку список адресатов воссоздаётся заново, каждый адресат получит столько копий письма, сколько существует самих локальных адресатов. К тому же особенности реализации рассылок электронной почты и сами по себе довольно часто приводят к дублированию. Разрядить ситуацию призван этот параметр, указывающий, удалять ли дубликаты писем непосредственно на внешнем почтовом сервере. Дубликаты определяются по уникальному идентификатору письма, хранящемуся в заголовочном поле **Message-ID**. Если при анализе заголовка письма выясняется, что такой идентификатор уже встречался, то письмо считается уже загруженным и при установке соответствующего флага в списке почтовых ящиков удаляется без загрузки. Однако в случае некорректного повторного использования идентификатора (этим грешат некоторые почтовые серверы, использующие в автоответах Message-ID исходного сообщения, а также некоторые почтовые клиенты, присваивающие один и тот же идентификатор всем фрагментам автоматически разбитого на части большого сообщения) такие действия могут привести к потере данных. Поэтому начальное значение - **0**, удаление дубликатов выключено. | ? |
| **MessageIdList** | Файл со списком идентификаторов обработанных писем. На самом деле список теперь хранится в базе данных, а эта унаследованная от предыдущих версий настройка позволяет импортировать в базу ранее накопленную информацию. Импорт выполняется один раз при создании базы данных, в дальнейшем список не используется. Начальное значение - **{Dirs[Mail]}\pop3recv\pop3msgids.txt**. | |
| **UseAlerter** | Определяет, задействовать ли механизм административных оповещений о недоставке почты. Если этот механизм включён, то администратор сервера будет извещаться специальным электронным письмом о каждом случае отказа в приёме письма, включая отсеивание уже принятого письма фильтрами содержания. Поддержка административных оповещений выполнена в виде отдельного плагина **alerter**, который загружается, если при старте SMTP-сервера этот параметр имеет ненулевое значение. В дальнейшем при возникновении проблем административные оповещения можно временно отключить, задав нулевое значение. Начальное значение - **{SMTP[UseAlerter]}**. | * & $ |

| | | |
|---|---|---|
| **OnAlertNotification** | Задаёт шаблон, на основании которого генерируется письмо-оповещение. Начальное значение - **{SMTP[OnAlertNotification]}**. | ? |
| **OnAlertNotifyFrom** | Адрес отправителя, от имени которого посылаются оповещения. Начальное значение - **{SMTP[OnAlertNotifyFrom]}**. | ? |
| **OnAlertNotifyTo** | Адрес администратора-получателя. Если необходимо доставлять оповещения нескольким адресатам, следует указать адрес списка рассылки. Начальное значение - **{SMTP[OnAlertNotifyTo]}**. | ? |
| **MaxMessageSize** | Максимально допустимый размер письма. Если в параметрах почтового ящика не указано индивидуальное ограничение, то используется это глобальное значение. Оно действует для всех "чужих" отправителей (для "своих" ограничения устанавливаются динамически и более изощрённым способом). Для отключения контроля за размером писем достаточно задать нулевое значение. Размер письма задаётся в байтах. Начальное значение - **{SMTP[MaxMessageSize]}**. | ? |
| **Timeout** | Время бездействия, задаваемое в миллисекундах, по истечении которого загрузчик прекращает соединение с POP-сервером. Это вынужденная мера, предотвращающая утечку ресурсов при плохой связи - как правило, тайм-аут срабатывает, когда соединение уже фактически разорвано, но загрузчику неоткуда получить извещение об этом. Начальное значение - **60000**, что соответствует 10 минутам. | $ |
| **Logs** | Расположение каталога оперативных журналов загрузчика. Поскольку загрузчик является компонентом SMTP-сервера, то начальное значение - **{SMTP[Logs]}**. | $ |
| **LogLevel** | Задаёт уровень детализации оперативного журнала загрузчика. Параметр может принимать значения от 1 до 9. Чем выше уровень, тем больше подробностей пишется в журнал. Для совместимости с ранними версиями, в которых уровень детализации не задавался, нулевое значение соответствует максимальному уровню детализации. Начальное значение - **{SMTP[LogLevel]}**. | $ |
| **LogToEStat** | Определяет, ведёт ли загрузчик статистику в формате программы **Estat32**, разработанной **Андреем Волковым** из **EPE Labs** для обработки статистических журналов Eserv/2. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{SMTP[LogToEStat]}**. | $ |
| **LogToAdvSoft** | Определяет, ведёт ли загрузчик статистику в формате программ **ProxyInspector** и **MailDetective** производства компании **AdvSoft**. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{SMTP[LogToAdvSoft]}**. | $ |
| **LogToElog** | Определяет, ведёт ли загрузчик статистику в формате программы **Elog**, разработанной **Игорем Панасенко** из компании **ЛЭНК** для обработки статистических журналов Eserv/3. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{SMTP[LogToElog]}**. | $ |
| **LogToMaillog** | Определяет, ведёт ли загрузчик статистику в собственном текстовом формате. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{SMTP[LogToMaillog]}**. | $ |

| | | |
|---|---|---|
| **LogToMStat** | Определяет, используется ли подсистема ведения статистики в базе данных MStat, разработанная Андреем Матвеевым. Этот сборщик статистики имеет немалое преимущество перед текстовыми журналами, позволяя хранить и эффективно обрабатывать статистическую информацию за большие периоды времени, измеряемые годами. Но для его работы необходима установка дополнительного приложения - СУБД одного из поддерживаемых сборщиком типов. Если при запуске сервера указано любое ненулевое число, загружается специальный плагин **mstat**. В дальнейшем при возникновении проблем сбор статистики в базе данных можно временно отключить, установив нулевое значение. Начальное значение - **{SMTP[LogToMStat]}**. | $<br>& |

## *Секция SmtpSend - параметры настройки расширенного сервиса доставки исходящей почты SmtpSend*

| | | |
|---|---|---|
| **Certificate** | Имя файла формата PEM, содержащего закрытый ключ и сертификаты, используемые при организации защищённого (SSL) соединения с целевым сервером. Начальное значение - **{SMTP[Certificate]}**. | ? |
| **SslVerifyServer** | Определяет режим проверки подлинности сертификатов целевого сервера при установлении защищённого соединения. Задаётся либо числовым кодом, либо символьным обозначением:<br>**SSL_VERIFY:IGNORE** - сертификат целевого сервера проверяется, но соединение устанавливается независимо от результата проверки, при этом клиентский сертификат серверу не предъявляется (числовое значение -1);<br>**SSL_VERIFY:NONE** - сертификат целевого сервера проверяется, но соединение устанавливается независимо от результата проверки (числовое значение 0);<br>**SSL_VERIFY:STANDARD** - сертификат целевого сервера проверяется, при отрицательном результате проверки соединение незамедлительно разрывается (числовое значение 1).<br>Начальное значение - **SSL_VERIFY:NONE**, то есть, сертификаты целевых серверов принимаются вне зависимости от результата их проверки. | *<br>? |
| **Lists** | Расположение каталога со списками настройки сервиса. Начальное значение - **{Dirs[Lists]}\smtpsend**. | |
| **Templates** | Расположение каталога с шаблонами служебных писем сервиса. Начальное значение - **{Dirs[Templates]}\smtpsend**. | |
| **Try** | Расположение каталога очереди повторной доставки. В этот каталог перемещаются письма, которые не удалось доставить с первого раза. Попытки доставки писем, находящихся в очереди повторной доставки, производятся довольно часто (с интервалом в несколько минут, определяемым параметром **SchedulerTryPause**), но в течение относительно короткого периода (единицы часов), определяемого параметром **RetryHours**. Если письмо так и осталось недоставленным, оно перемещается в каталог очереди отложенной доставки. Начальное значение - **{Dirs[Mail]}\try**. | $ |
| **Retry** | Расположение каталога очереди отложенной доставки. В этот каталог перемещаются письма, которые не удалось доставить в течение нескольких часов. При этом отправитель извещается о возникшей проблеме специальным письмом. Чтобы не перегружать каналы связи, попытки доставки писем, попавших в эту очередь, производятся раз в несколько часов - этот интервал определяется параметром **SchedulerRetryPause**. Предельный срок нахождения писем в этой очереди, задаваемый параметром **RetryDays**, составляет несколько дней. Если в течение этого срока письмо всё ещё не доставлено адресату, отправитель извещается о невозможности доставки, а исходное письмо удаляется. Начальное значение - **{Dirs[Mail]}\retry**. | $ |
| **Malformed** | Расположение каталога для хранения искажённых писем, в которых были обнаружены ошибки формата. Применительно к сервису доставки исходящей почты таковыми считаются письма с некорректным форматом имени файла, не содержащим адреса отправителя, а также письма без списка адресатов. Начальное значение - **{SMTP[Malformed]}**. | |

| | | |
|---|---|---|
| **Debug** | Указывает, использовать или нет отладочный вывод сервиса. Начальное значение - **0**, то есть, отладочный вывод не используется (в большинстве случаев вполне достаточно обычного оперативного журнала). | & |
| **Timeout** | Время бездействия, задаваемое в миллисекундах, по истечении которого сервис прекращает соединение с целевым SMTP-сервером. Это вынужденная мера, предотвращающая утечку ресурсов при плохой связи - как правило, тайм-аут срабатывает, когда соединение уже фактически разорвано, но сервису неоткуда получить извещение об этом. Начальное значение - **600000**, что соответствует 10 минутам. | $ |
| **SynchronousSend** | Признак синхронной отправки почты. Если при запуске сервера и во время работы этот параметр имеет любое ненулевое значение, то отправка запускается при каждом попадании письма в каталог очереди исходящей почты, определяемый параметром **SMTP[Out]**. Если значение параметра нулевое, каталог исходящей очереди просматривается с тем же интервалом, что и каталог очереди повторной доставки. Начальное значение - **1**. | *<br>? |
| **SchedulerTryPause** | Длительность цикла проверки очереди повторной доставки, задаваемая в миллисекундах. Минимально допустимое значение составляет 60000 (одну минуту). Начальное значение - **300000**, что соответствует пяти минутам. | * |
| **SchedulerRetryPause** | Длительность цикла проверки очереди отложенной доставки, задаваемая в миллисекундах. Минимально допустимое значение составляет 600000 (десять минут). Начальное значение - **7200000**, что соответствует двум часам. | * |
| **SendDelay** | Длительность паузы между отправками серверу-адресату очередной порции данных, задаваемая в миллисекундах. Позволяет снизить нагрузку как на процессор, так и на каналы связи. Если значение нулевое, пауза отсутствует. Начальное значение - **0**. | *<br>$ |
| **RetryDays** | Указывает, в течение какого количества суток продолжать попытки доставки письма, находящегося в очереди отложенной доставки. Начальное значение - **2**. | *<br>? |
| **RetryHours** | Указывает, в течение какого количества часов продолжать попытки доставки письма, находящегося в очереди повторной доставки. Начальное значение - **2**. | *<br>? |
| **GroupDelivery** | Задаёт режим групповой доставки. В этом режиме сервис для уменьшения нагрузки отправляет одну копию письма нескольким получателям. Для писем из очередей фиксированных маршрутов единственная копия отправляется сразу всем адресатам - целевой сервер сам должен доставить необходимое число копий по назначению. Для писем из очередей со "свободной" доставкой адресаты группируются по почтовым доменам, для каждой группы отправляется отдельная копия. Если значение параметра нулевое, используется режим индивидуальной доставки - отправляется отдельная копия письма для каждого адресата. Начальное значение - **0**. | *<br>$ |
| **AllowEmptySender** | Указывает, разрешена ли отправка исходящей почты с пустым обратным адресом. По стандарту протокола SMTP этот адрес предназначен для доставки автоизвещений, формируемых почтовыми серверами. Подобным образом пытаются вести себя некоторые почтовые клиенты. Тем не менее, рекомендуется избегать использования пустого обратного адреса. Начальное значение - **1**. | *<br>? |
| **EmptySenderAlias** | Задаёт замену для пустого обратного адреса в случае, когда его использование запрещено. Начальное значение - **{SMTP[BounceEmail]}**. | *<br>? |
| **FromEmailAliases** | Список подмены адресов отправителей. Если есть существенная необходимость, можно одного отправителя выдать за другого, выполнив подмену адреса на основании этого списка. Начальное значение - **{SmtpSend[Lists]}\FromEmailAliases.txt**. | ? |

| | | |
|---|---|---|
| **RcptReturnMode** | Список управления режимами возврата недоставленных писем отправителям. Дело в том, что различные почтовые системы могут иметь различные представления о правилах хорошего тона. Одни либерально относятся к множественным попыткам доставить письмо по несуществующему адресу, зато не озадачиваются согласованием списков пользователей основного и резервного серверов. Другие (как, например, Yahoo! или Google Mail) активно используют технологию грейлистинга (отправителю несколько раз предлагается "зайти в следующий раз", прежде чем сервер соизволит принять письмо к рассмотрению) и крайне болезненно реагируют на слишком настойчивых отправителей, не воспринимающих сообщение об отсутствии адресата. С помощью этого списка можно выбрать режим, наиболее соответствующий нравам почтового сервера получателя. Начальное значение - **{SmtpSend[Lists]}\RcptReturnMode.txt**. | ? |
| **DefaultReturnMode** | Режим возврата недоставленных писем, используемый по умолчанию, когда его не удаётся определить на основании списка. Режим задаётся двухсимвольным кодом и может быть одним из следующих:<br>**RO** (Reject Only) - возврат выполняется, если все испробованные почтовые серверы категорически отвергли адрес получателя, выдав ответ с кодом 5xx. Это наиболее агрессивный и, как ни странно, наиболее применимый режим;<br>**WR** (Was Rejected) - возврат выполняется, если из испробованных почтовых серверов хотя бы один категорически отверг адрес получателя, выдав ответ с кодом 5xx. Этот режим наилучшим образом подходит для почтовых систем типа Yahoo! или Google Mail, где списки пользователей на серверах согласованы, зато механизм грейлистинга постоянно ставит препоны в виде временных отказов с кодом 4xx;<br>**AE** (Any Error) - возврат выполняется, если доставка не удалась ни на один из испробованных почтовых серверов. При этом неважно, был отказ категорическим (с кодом 5xx), временным (4xx) или имели место технические проблемы, например, отсутствие связи с сервером. Этот режим предназначен для очень особых случаев.<br>Начальное значение - **RO**. | *<br>? |
| **DirectDelivery** | Определяет, использовать ли прямую доставку писем на сервер получателя. Прямая доставка - обычный режим работы для почтовых серверов. Этот режим используется, если параметр имеет любое ненулевое значение. Однако, если Ваш сервер надёжно упрятан в недрах локальной сети, прямой выход наружу из которой запрещён, единственным вариантом для Вас будет отправка исходящей почты через транзитный сервер провайдера. В этом случае параметру следует задать нулевое значение. Начальное значение - **1**. | *<br>? |
| **UseAltRelays** | Определяет, использовать ли в режиме прямой доставки дополнительные серверы. Если доставка не удалась ни на один из серверов, назначенных почтовому домену получателя, сервис пробует отправить письмо через дополнительные серверы. Как правило, это транзитные серверы провайдера. Этот режим включается, если параметр имеет любое ненулевое значение. Если прямая доставка не используется, то отправка всегда выполняется через дополнительные серверы. Начальное значение - **0**. | *<br>? |
| **AltRelayList** | Список дополнительных транзитных серверов, используемых при невозможности или запрете прямой доставки писем. Начальное значение - **{SmtpSend[Lists]}\AltRelayList.txt**. | ? |
| **TargetAuthList** | Список параметров авторизации на почтовых серверах адресатов. Прямая доставка авторизации, как правило, не требует (чужие списки пользователей, по идее, представляют тайну не хуже государственной). А вот транзитный сервер провайдера вполне может потребовать подтверждения прав на проталкивание через него исходящих писем. По этому списку на основании сочетания адреса отправителя и имени почтового сервера можно определить требуемые реквизиты авторизации. Начальное значение - **{SmtpSend[Lists]}\TargetAuthList.txt**. | ? |

| | | |
|---|---|---|
| **TransferSecurityList** | Список требуемых параметров безопасности передачи писем. Обычно передача выполняется открытым текстом, и это нормально, учитывая полное отсутствие тайны электронной переписки. Однако бывают ситуации, когда передачу необходимо защитить от прослушивания. По этому списку на основании адреса отправителя, адреса получателя и имени почтового сервера можно определить необходимый уровень безопасности при передаче письма, а также указать особые параметры настройки защищённого соединения - клиентский сертификат и режим проверки подлинности сертификата сервера. Начальное значение - **{SmtpSend[Lists]}\TransferSecurityList.txt**. | ? |
| **HeloIP** | Список выбора имени узла для команды HELO или EHLO. Каждый почтовый сервер имеет свои предпочтения относительно этого имени. Кто-то требует обязательного соответствия имени и IP-адреса, кто-то по IP-адресу отыскивает имя в обратной зоне DNS и сравнивает с переданным в команде, кого-то категорически не устраивает честное, но сконструированное на основе IP-адреса шаблонное имя вида host-www-xxx-yyy-zzz.pppoe.provider.com. К тому же сам сервер-отправитель может иметь несколько IP-адресов, которым сопоставлены разные имена. Этот список позволяет решить проблему выбора. Кроме того, он позволяет в особых случаях переопределить ранее заданные параметры настройки защищённого соединения - клиентский сертификат и режим проверки подлинности сертификата сервера. Начальное значение - **{SmtpSend[Lists]}\HeloIP.txt**. | ? |
| **DefaultHeloHost** | Имя узла, назначаемое по умолчанию, когда его не удаётся определить по списку. Начальное значение - **{Server[HostName]}**. | * ? |
| **NoAutoReplyTo** | Список отправителей, которым не следует формировать и доставлять письма-возвраты и письма-предупреждения. Как правило, это специальные адреса - "вышибалы" и почтовые роботы. Они всё равно не в состоянии понять смысл послания и правильно на него отреагировать. Начальное значение - **{SmtpSend[Lists]}\NoAutoReplyTo.txt**. | ? |
| **ReturnFromEmail** | Почтовый адрес, от имени которого сервис генерирует письмо-возврат. Начальное значение - **{SMTP[AdminEmail]}**. | * ? |
| **ReturnNotification** | Шаблон письма-возврата, генерируемого при полной невозможности доставить письмо хотя бы одному адресату. В этом письме перечисляются причины недоставки, и, как правило, к нему прилагается исходное письмо. Начальное значение - **{SmtpSend[Templates]}\ReturnNotification.pat.txt**. | ? |
| **RetryNotification** | Шаблон письма-предупреждения, генерируемого при перемещении исходного письма в очередь отложенной доставки. Начальное значение - **{SmtpSend[Templates]}\RetryNotification.pat.txt**. | ? |
| **Logs** | Расположение каталога оперативных журналов сервиса. Начальное значение - **{SMTP[Logs]}**. | $ |
| **LogLevel** | Задаёт уровень детализации оперативного журнала сервиса. Параметр может принимать значения от 1 до 9. Чем выше уровень, тем больше подробностей пишется в журнал. Для совместимости с ранними версиями, в которых уровень детализации не задавался, нулевое значение соответствует максимальному уровню детализации. Начальное значение - **{SMTP[LogLevel]}**. | $ |
| **LogToEStat** | Определяет, ведёт ли сервис статистику в формате программы **Estat32**, разработанной **Андреем Волковым** из **EPE Labs** для обработки статистических журналов Eserv/2. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{SMTP[LogToEStat]}**. | $ |
| **LogToAdvSoft** | Определяет, ведёт ли сервис статистику в формате программ **ProxyInspector** и **MailDetective** производства компании **AdvSoft**. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{SMTP[LogToAdvSoft]}**. | $ |

| | | |
|---|---|---|
| **LogToElog** | Определяет, ведёт ли сервис статистику в формате программы **Elog**, разработанной **Игорем Панасенко** из компании **ЛЭНК** для обработки статистических журналов Eserv/3. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{SMTP[LogToElog]}**. | $ |
| **LogToMaillog** | Определяет, ведёт ли сервис статистику в собственном текстовом формате. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{SMTP[LogToMaillog]}**. | $ |
| **LogToMStat** | Определяет, используется ли подсистема ведения статистики в базе данных MStat, разработанная Андреем Матвеевым. Этот сборщик статистики имеет немалое преимущество перед текстовыми журналами, позволяя хранить и эффективно обрабатывать статистическую информацию за большие периоды времени, измеряемые годами. Но для его работы необходима установка дополнительного приложения - СУБД одного из поддерживаемых сборщиком типов. Если при запуске сервера указано любое ненулевое число, загружается специальный плагин **mstat**. В дальнейшем при возникновении проблем сбор статистики в базе данных можно временно отключить, установив нулевое значение. Начальное значение - **{SMTP[LogToMStat]}**. | $<br>& |

## *Секция LocalDelivery - параметры настройки сервиса локальной доставки*

| | | |
|---|---|---|
| **Malformed** | Расположение каталога для хранения искажённых писем, в которых были обнаружены ошибки формата. Применительно к сервису локальной доставки таковыми считаются письма с некорректным форматом имени файла, не содержащим адреса отправителя, а также письма без списка адресатов. Начальное значение - **{SMTP[Malformed]}**. | |
| **Undelivered** | Расположение каталога для хранения недоставленных писем. Применительно к сервису локальной доставки к таковым относятся письма, адрес отправителя у которых не прошёл проверку на допустимость, а также письма, часть адресатов для которых была отвергнута, даже если части адресатов письмо было доставлено. Также это могут быть письма для несуществующих локальных пользователей, если есть установка не доставлять такие письма, а также письма, для которых в итоге не нашлось получателей (например, из-за ошибок в настройке). Начальное значение - **{SMTP[Undelivered]}**. | |
| **MaxMessageSize** | Максимально допустимый размер письма. Это значение действует для всех "чужих" отправителей (для "своих" ограничения устанавливаются динамически и более изощрённым способом). Размер письма задаётся в байтах. Начальное значение - **{SMTP[MaxMessageSize]}**. Если указать нулевое значение, размер письма ограничиваться не будет. | *<br>$ |
| **MaxOutboundMessageSize** | Максимально допустимый размер письма, отправляемого из локального домена "чужим" получателям. Это ограничение налагается в дополнение к параметрам, заданным в списках локальных и доверенных сетей, а также в списке локальных пользователей. Размер письма задаётся в байтах. Начальное значение - **{SMTP[MaxOutboundMessageSize]}**. Если указать нулевое значение, размер письма дополнительно ограничиваться не будет. | *<br>$ |
| **AllowOutboundMail** | Указывает, разрешена ли сервису отправка почты за пределы локального домена. Обычно этого не требуется, поскольку основное назначение сервиса - внутренняя доставка переклассифицированной почты. Однако это может потребоваться, если сервис также обеспечивает обслуживание программ-роботов, общающихся с внешними адресатами. Начальное значение - **0**, отправка исходящей почты запрещена. | *<br>$ |

| | | |
|---|---|---|
| **UseAlerter** | Определяет, задействовать ли механизм административных оповещений о недоставке почты. Если этот механизм включён, то администратор сервера будет извещаться специальным электронным письмом о каждом случае отказа в приёме письма, включая отсеивание уже принятого письма фильтрами содержания. Поддержка административных оповещений выполнена в виде отдельного плагина **alerter**, который загружается, если при старте SMTP-сервера этот параметр имеет ненулевое значение. В дальнейшем при возникновении проблем административные оповещения можно временно отключить, задав нулевое значение. Начальное значение - **{SMTP[UseAlerter]}**. | * & $ |
| **OnAlertNotification** | Задаёт шаблон, на основании которого генерируется письмо-оповещение. Начальное значение - **{SMTP[OnAlertNotification]}**. | ? |
| **OnAlertNotifyFrom** | Адрес отправителя, от имени которого посылаются оповещения. Начальное значение - **{SMTP[OnAlertNotifyFrom]}**. | ? |
| **OnAlertNotifyTo** | Адрес администратора-получателя. Если необходимо доставлять оповещения нескольким адресатам, следует указать адрес списка рассылки. Начальное значение - **{SMTP[OnAlertNotifyTo]}**. | ? |
| **Logs** | Расположение каталога оперативных журналов сервиса. Начальное значение - **{SMTP[Logs]}**. | $ |
| **LogLevel** | Задаёт уровень детализации оперативного журнала сервиса. Параметр может принимать значения от 1 до 9. Чем выше уровень, тем больше подробностей пишется в журнал. Для совместимости с ранними версиями, в которых уровень детализации не задавался, нулевое значение соответствует максимальному уровню детализации. Начальное значение - **{SMTP[LogLevel]}**. | $ |
| **LogToEStat** | Определяет, ведёт ли сервис статистику в формате программы **Estat32**, разработанной **Андреем Волковым** из **EPE Labs** для обработки статистических журналов Eserv/2. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{SMTP[LogToEStat]}**. | $ |
| **LogToAdvSoft** | Определяет, ведёт ли сервис статистику в формате программ **ProxyInspector** и **MailDetective** производства компании **AdvSoft**. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{SMTP[LogToAdvSoft]}**. | $ |
| **LogToElog** | Определяет, ведёт ли сервис статистику в формате программы **Elog**, разработанной **Игорем Панасенко** из компании **ЛЭНК** для обработки статистических журналов Eserv/3. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{SMTP[LogToElog]}**. | $ |
| **LogToMaillog** | Определяет, ведёт ли сервис статистику в собственном текстовом формате. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{SMTP[LogToMaillog]}**. | $ |

| | | |
|---|---|---|
| **LogToMStat** | Определяет, используется ли подсистема ведения статистики в базе данных MStat, разработанная Андреем Матвеевым. Этот сборщик статистики имеет немалое преимущество перед текстовыми журналами, позволяя хранить и эффективно обрабатывать статистическую информацию за большие периоды времени, измеряемые годами. Но для его работы необходима установка дополнительного приложения - СУБД одного из поддерживаемых сборщиком типов. Если при запуске сервера указано любое ненулевое число, загружается специальный плагин **mstat**. В дальнейшем при возникновении проблем сбор статистики в базе данных можно временно отключить, установив нулевое значение. Начальное значение - **{SMTP[LogToMStat]}**. | $<br>& |

## *Секция Antispam - общие параметры настройки противоспамных фильтров*

| | | |
|---|---|---|
| **Lists** | Расположение каталога с общими списками настройки фильтров. Начальное значение - **{Dirs[Lists]}\antispam**. | |
| **Data** | Расположение каталога, в котором хранятся рабочие данные спам-фильтров. Начальное значение - **{Dirs[Mail]}\antispam**. | |
| **ResendDir** | Расположение каталога, в который для повторной доставки помещаются письма, переклассифицированные "администратором спама" из мусорных в "добропорядочные". Начальное значение - **{SMTP[Local]}**, что соответствует каталогу очереди внутренней доставки SMTP-сервера. | !*<br>? |
| **MaxMessageSize** | Письма большого объёма проверяются классифицирующими фильтрами типа POPfile, SpamProtexx или LibSD достаточно долго. Между тем, по статистике, спамеры предпочитают слишком большие письма не слать. Этот параметр позволяет задать предельный размер писем (в байтах), передаваемых на проверку спам-фильтру. Размер письма задаётся в байтах. Начальное значение - **100000**. Указание нулевого значения отменяет действие ограничения на размер. | *<br>? |
| **IpWhiteList** | Это ещё один список доверенных сетей - дополнительный по отношению к спискам локальных и доверенных сетей SMTP-сервера в целом. Доверие к этим IP-адресам не настолько велико, чтобы считать находящихся там отправителей "своими", но известно, что спам из этих сетей не приходит. Начальное значение - **{Antispam[Lists]}\IpWhiteList.txt**. | |
| **FromEmailWhiteList** | Это ещё один список доверенных отправителей - дополнительный по отношению к списку доверенных отправителей SMTP-сервера в целом. Доверие к этим адресам не настолько велико, чтобы включить их в основной "белый" список, но известно, что спам с этих адресов не приходит. Начальное значение - **{Antispam[Lists]}\FromEmailWhiteList.txt**. | ? |
| **ToEmailWhiteList** | Это список особых получателей. Если все получатели письма состоят в этом списке, то письмо не будет подвергаться спам-фильтрации, в противном случае решение об отмене проверки будет приниматься исходя из других условий. Начальное значение - **{Antispam[Lists]}\ToEmailWhiteList.txt**. | ? |
| **CheckAuthorizedSenders** | Если есть уверенность в благонадёжности своих пользователей, можно отправляемую ими почту вывести из-под контроля спам-фильтра. Нулевое значение этого параметра означает, что письма от правильно авторизованных отправителей не подвергаются проверке на спам, что несколько ускоряет отправку писем локальными пользователями. Начальное значение - **0**, то есть, к "своим" отправителям сервер относится более лояльно. | *<br>? |
| **TrainingMode** | Ненулевое значение этого параметра означает, что спам-фильтр работает в режиме обучения. В этом режиме при обнаружении в письме признаков спама отправитель не получает отказ в приёме, а анализ письма не прерывается. Однако доставка такого письма происходит только в локальные почтовые ящики спам-администраторов. Начальное значение - **0**. | *<br>? |

| | | |
|---|---|---|
| **DupCheck** | Когда почта помимо более привычного для почтового сервера "самотёка" по протоколу SMTP доставляется ещё и из внешних POP-ящиков (посредством загрузчика **Pop2Smtp** или **Pop3Recv**), довольно часто случается самопроизвольное размножение писем. И если дублирование полезной информации пережить можно (временами это даже полезно), то многочисленные копии одного и того же спам-письма есть явление совершенно нежелательное. Если этот параметр имеет ненулевое значение, то такие лишние копии будут незамедлительно удаляться. Дубликаты определяются по уникальному идентификатору письма, хранящемуся в заголовочном поле **Message-ID**. Если при анализе заголовка спам-письма выясняется, что такой идентификатор уже встречался, письмо удаляется без копирования куда-либо. Это правило действует только в отношении писем, загруженных из внешних POP-ящиков. Письма-дубликаты, поступившие по протоколу SMTP, не удаляются. Это связано с тем, что абсолютно точное распознавание спама невозможно, а повторение уникального идентификатора может быть вызвано некорректными настройками партнёрской системы рассылки или ошибками в почтовом клиенте. Начальное значение - **0**, то есть, дубликаты спам-писем обрабатываются обычным образом. | * ? |
| **MessageIdList** | Файл со списком идентификаторов обработанных писем. На самом деле список теперь хранится в базе данных, а эта унаследованная от предыдущих версий настройка позволяет импортировать в базу ранее накопленную информацию. Импорт выполняется один раз при создании базы данных, в дальнейшем список не используется. Начальное значение - **{Antispam[Data]}\antispammsgids.txt**. | |
| **MessageIdDB** | Если удаление дубликатов писем активировано, то список идентификаторов обработанных писем хранится в базе данных формата SQLite3. Её имя и расположение определяется этим параметром. Начальное значение - **{Antispam[Data]}\antispammsgids.db3**. | & |
| **DeliverAnyway** | Определяет режим обработки писем, классифицированных как спам. Если параметр имеет нулевое значение, письмо перемещается в общий каталог для хранения спама. Если среди адресатов письма был специальный (**abuse**), то письмо также доставляется в его почтовый ящик; до остальных получателей спам не доходит. Если значение параметра ненулевое, спам доставляется в локальные почтовые ящики всех получателей, имеющих квалификацию спам-администратора. В случае доставки спам-почта помещается в специальную папку **spam**, доступную по протоколу IMAP. Начальное значение - **1**, то есть, доставка спама выполняется по второй схеме. | * ? |
| **ShowReclassificationUrl** | Этот параметр определяет форму ответа сервера отправителю в случае классификации письма как мусорного. В стандартной конфигурации предполагается, что почтовый сервер работает в составе полного комплекта серверов Eserv/3, при этом запущен и должным образом настроен общедоступный web-сервер. Среди служебных сценариев сервера имеется сценарий ручной принудительной переклассификации ошибочно распознанных писем. Если параметр имеет любое ненулевое значение, в ответ сервера подставляется web-ссылка, обращение к которой активизирует этот сценарий. Если общедоступный web-сервер отсутствует, параметру следует присвоить нулевое значение - тогда в ответ сервера будет подставляться обычное предложение пожаловаться администратору на некорректную работу фильтра. Начальное значение - **1**, то есть, предполагается работа совместно с web-сервером. | * ? |
| **ServerName** | Если в ответах сервера приводится ссылка на web-страницу переклассификации писем, можно задать имя web-сервера, на котором располагается эта страница. Начальное значение - **{Server[HostName]}**. | ? |
| **ServerPort** | Порт, на котором работает web-сервер, выполняющий переклассификацию. Поскольку предполагается, что это собственный web-сервер на базе PigMail+PigProxy, то начальное значение - **{HTTP[Port]}**. | ? |

| | | |
|---|---|---|
| **ResendOnWebRC** | Определяет, выполнять ли автоматическую повторную доставку письма, переклассифицированного отправителем с использованием web-интерфейса. Если параметр имеет любое ненулевое значение, переклассифицированные письма будут автоматически доставляться адресату с учётом новой классификации - в папку INBOX. Если значение нулевое, то доставку инициирует только спам-администратор, вручную перемещая письмо в надлежащую IMAP-папку. Начальное значение - **1**. | * |
| **CleanAmbiguousOnWebRC** | Определяет, удалять ли копию письма из каталога хранения неоднозначно классифицированных писем, если письмо было переклассифицировано отправителем с использованием web-интерфейса. Если параметр имеет любое ненулевое значение, копии писем будут удаляться, чтобы администратор случайно, по недосмотру, не переклассифицировал их неверным образом. Если значение нулевое, копии остаются в неприкосновенности на усмотрение администратора. Начальное значение - **0**. | * |
| **CopyUnclassifiedToTrainer** | Плохо обученный спам-фильтр может испытывать затруднения с отнесением писем к той или иной категории. В таком случае ему можно помочь, задав ненулевое значение этого параметра. Тогда письма, с которыми фильтр не справился, будут дополнительно копироваться в почтовый ящик "тренера" - точнее, в специальный каталог для хранения неоднозначно классифицированных писем. Начальное значение - **0**. | * ? |
| **DetectViruses** | Помимо собственно спама, используемые противоспамные фильтры способны определять также и вирусные письма. Этот параметр определяет, обрабатывать ли письма, классифицированные как заражённые вирусами, особым образом. Если он имеет ненулевое значение, обработка выполняется по правилам антивирусной фильтрации - с перемещением письма в специальный каталог и формированием писем-извещений. В противном случае письмо обрабатывается как обычный спам - правда, ему присваивается особый класс, определяющий, что это не просто спам. Начальное значение - **1**. | * ? |
| **OnVirusGeneralNotification** | Если адресат заражённого письма получает уведомление о несостоявшейся вирусной атаке, отбитой противоспамными фильтрами, то оно генерируется на основании шаблона, задаваемого этим параметром. Начальное значение - **{SMTP[Templates]}\OnSpamVirus.pat.txt**. | ? |
| **OnVirusAdminNotification** | Если администратор получает извещения о распознавании противоспамными фильтрами вируса, то они генерируются на основании шаблона, задаваемого этим параметром,. Начальное значение - **{SMTP[Templates]}\OnSpamVirusAdmin.pat.txt**. | ? |
| **SmtpServer** | Библиотеки классификаторов SpamProtexx и LibSD интегрированы в SMTP-сервер, который использует их постоянно. IMAP и HTTP-сервер при переклассификации писем должны обращаться к SMTP-серверу с запросами и получать от него ответы. Этот параметр задаёт имя или IP-адрес SMTP-сервера. Наилучшим вариантом представляется использование "секретного" локального адреса, зарезервированного для различных внутренних целей. Поэтому начальное значение - **127.0.0.10**, соответствующее адресу, указанному в примерах списков и других начальных настройках. | * ? |
| **SmtpPort** | Задаёт номер порта, по которому IMAP и HTTP-сервер будут обращаться к SMTP-серверу. Начальное значение - **{SMTP[Port]}**. | * ? |

## *Секция AntispamPopFile - параметры настройки противоспамного фильтра POPfile*

| | | |
|---|---|---|
| **Port** | Задаёт номер порта, на котором работает XMLRPC-интерфейс POPfile. Начальное значение - **8081**. | * & |
| **Debug** | Указывает, использовать или нет отладочный вывод модуля связи с сервером POPfile. Начальное значение - **1**, то есть, в журнал SMTP-сервера выводится отладочная информация. | * |

| | | |
|---|---|---|
| **NotSpamBucket** | Указывает, в какое "ведро" (согласно текущей русификации POPfile; в оригинале эта сущность называется *bucket*, а по смыслу представляет собой группу классификации) следует помещать письмо при перемещении его в IMAP-каталог **not_spam**. Начальное значение - **clear**. | & |
| **ShowColorized** | Определяет, показывать ли отправителю, переклассифицирующему через web-интерфейс своё ошибочно задержанное письмо, его текущую раскраску - визуализацию распределения различных слов письма по классам. Раскраска показывается, если параметр имеет любое ненулевое значение. Начальное значение - **0**. | |
| **Dir** | Каталог, в котором размещаются файлы сервера POPfile. Начальное значение - **{ModuleDirName}..\PopFile**. | |
| **CommandLine** | Командная строка, используемая для запуска сервера POPfile. Начальное значение - **"{AntispamPopFile[Dir]}\wperl.exe popfile.pl"**, но, поскольку **wperl.exe** суть компонент ещё одной системы - языка программирования Perl, - и располагаться он может совершенно отдельно от POPfile, рекомендуется переопределить эту команду в конфигурационном файле PigMail2.ini в соответствии с Вашими настройками Perl. | * |
| **StartupTimeout** | Предельное время ожидания запуска POPfile - от момента собственно запуска до получения доступа к XMLRPC-интерфейсу приложения. Время задаётся в секундах. Начальное значение - **60**. | & |
| **InitTimeout** | Предельное время ожидания завершения инициализации POPfile после получения доступа к XMLRPC-интерфейсу приложения. Время задаётся в секундах. Начальное значение - **60**. | & |

## *Секция AntispamSpamProtexx - параметры настройки противоспамного фильтра SpamProtexx*

| | | |
|---|---|---|
| **Dir** | Каталог, в котором размещаются базы данных SpamProtexx. Начальное значение - **{Antispam[Data]}\spamprotexx**. | |
| **MainDb** | Задаёт имя и расположение основной базы данных классификатора. Начальное значение - **{AntispamSpamProtexx[Dir]}\Storage.esp**. | |
| **LearnDb** | Задаёт имя и расположение базы данных периода обучения. Начальное значение - **{AntispamSpamProtexx[Dir]}\Relearn.esp**. | |
| **PopFileTrainer** | Если SpamProtexx работает совместно с POPfile, последний на правах более опытного может выступить в качестве "тренера" для SpamProtexx. В режиме тандема, если SpamProtexx затрудняется классифицировать письмо, а POPfile выполнил классификацию, принимается точка зрения POPfile, и для SpamProtexx выполняется принудительная классификация письма. Для включения режима следует задать любое ненулевое значение. Начальное значение - **1**. | * ? |
| **AutoTraining** | Совместно с предыдущим параметром задаёт режим автообучения. В этом режиме дообучение SpamProtexx и принудительная классификация писем выполняются не только при неопределённых результатах классификации, но и при любом расхождении с POPfile. Для включения режима следует задать любое ненулевое значение. Начальное значение - **0**. | * ? |
| **PopFileGuru** | Обычно при разногласиях между POPfile и SpamProtexx, если оба уверены каждый в своём мнении, письму назначается специальная категория **ambiguous**. Если этот параметр имеет любое ненулевое значение, в таких случаях к письму применяется классификация, определённая POPfile. Если одновременно активен и классификатор LibSD, для него POPfile также должен иметь статус гуру. Начальное значение - **0**. | * ? |

## *Секция AntispamSD - параметры настройки противоспамного фильтра Extravalent LibSD*

| | | |
|---|---|---|
| **Dir** | Каталог, в котором размещается база данных LibSD. Начальное значение - **{Antispam[Data]}\sd**. | |
| **Db** | Задаёт имя и расположение базы данных классификатора. Начальное значение - **{AntispamSD[Dir]}\corpus**. | |

| | | |
|---|---|---|
| **UseSURBL** | Хитрая изюминка LibSD заключается в его умении проверять обнаруженные в письмах ссылки на сайты по онлайновым чёрным спискам - Spam URI Realtime Blocklists или SURBL, - привлекая таким образом на свою сторону немалые силы мирового антиспамерского сообщества. Если при старте сервера этот параметр имеет ненулевое значение, это умение будет использовано при анализе поступающих писем. Начальное значение - **0**. | *<br>& |
| **PopFileTrainer** | Если LibSD работает совместно с POPfile, последний на правах более опытного может выступить в качестве "тренера" для LibSD. В режиме тандема, если LibSD затрудняется классифицировать письмо, а POPfile выполнил классификацию, принимается точка зрения POPfile, и для LibSD выполняется принудительная классификация письма. Для включения режима следует задать любое ненулевое значение. Начальное значение - **1**. | *<br>? |
| **SpamProtexxTrainer** | Если LibSD работает совместно со SpamProtexx, последний на правах более опытного может выступить в качестве "тренера" для LibSD. В режиме тандема, если LibSD затрудняется классифицировать письмо, а SpamProtexx выполнил классификацию, принимается точка зрения SpamProtexx, и для LibSD выполняется принудительная классификация письма. Если одновременно в качестве учителя назначен POPfile, то его мнение имеет больший вес. Для включения режима следует задать любое ненулевое значение. Начальное значение - **1**. | *<br>? |
| **AutoTraining** | Совместно с предыдущими параметрами задаёт режим автообучения. В этом режиме дообучение LibSD и принудительная классификация писем выполняются не только при неопределённых результатах классификации, но и при любом расхождении с фильтром-учителем. Для включения режима следует задать любое ненулевое значение. Начальное значение - **0**. | *<br>? |
| **PopFileGuru** | Обычно при разногласиях между POPfile и LibSD, если оба уверены каждый в своём мнении, письму назначается специальная категория **ambiguous**. Если этот параметр имеет любое ненулевое значение, в таких случаях к письму применяется классификация, определённая POPfile. Если одновременно активен и классификатор SpamProtexx, для него POPfile также должен иметь статус гуру. Начальное значение - **0**. | *<br>? |
| **SpamProtexxGuru** | Обычно при разногласиях между SpamProtexx и LibSD, если оба уверены каждый в своём мнении, письму назначается специальная категория **ambiguous**. Если этот параметр имеет любое ненулевое значение, в таких случаях к письму применяется классификация, определённая SpamProtexx. Этот режим возможен только при отключённом классификаторе POPfile. Начальное значение - **0**. | *<br>? |

## *Секция ContentFilter - параметры настройки упрощённого фильтра содержания*

| | | |
|---|---|---|
| **UseBodyFilter** | Если разрешено использование упрощённого фильтра содержания, то фильтр можно наложить не только на заголовки, но и на тело письма - однако это может существенно замедлить приём почты. Этот параметр указывает, использовать ли фильтр по телу письма. Начальное значение - **1**, то есть, использовать. | *<br>? |
| **BodyLineCount** | Для ускорения ухода почты тело письма можно анализировать не полностью, а только заданное количество строк. Если указать ноль, это означает отсутствие ограничения - тело письма будет проанализировано полностью. Начальное значение - **250**. | *<br>? |
| **BodyLineQuant** | Проверка тела письма - достаточно ресурсоёмкий процесс. Этот параметр определяет число строк, проверяемых фильтром "на одном дыхании". По окончании каждой такой порции фильтр делает небольшую паузу. Это замедляет процесс приёма письма, зато выделяет процессорное время для работы других служб Eserv или обработки других писем. Нулевая величина означает отсутствие пауз и практически монопольный захват процессора на время проверки письма. Начальное значение - **50**. | *<br>? |

| | | |
|---|---|---|
| **BodyCheckPause** | Длительность паузы в миллисекундах. Нулевая величина означает отсутствие пауз и практически монопольный захват процессора на время проверки письма. Начальное значение - **50**. | * ? |
| **BlackListBody** | Список шаблонов запрещённого содержимого тела письма. Если разрешена фильтрация по телу письма, то с этим списком сравнивается каждая строка тела письма. В отличие от полей заголовка, раскодирование строк не производится. Начальное значение - **{SMTP[Filters]}\BlackListBody.txt**. | ? |
| **FiltersList** | Основной управляющий список упрощённого фильтра содержания. В этом списке перечислены проверяемые заголовочные поля письма (из тех, что запоминаются в соответствии со списком, определённым параметром **SMTP[Headers]**) и соответствующие им списки шаблонов запрещённого содержимого. Начальное значение - **{SMTP[Filters]}\FiltersList.txt**. | ? |

## *Секция MContent - параметры настройки контент-анализатора MContent*

| | | |
|---|---|---|
| **AttSaveDir** | Если используется контент-анализатор **MContent**, ему необходимо указать каталог для сохранения вложенных в письма файлов. Этот параметр задаёт базовый путь к общему каталогу сохранения. Начальное значение - **{Dirs[Mail]}\mail_att_files**. | |
| **AttSaveExtraPath** | Этот параметр задаёт дополнительный путь к подкаталогу сохранения вложений, если их требуется как-то разделять в зависимости от адресов отправителя и получателя или по каким-то другим условиям. Начальное значение - **"{PIG.MAILFROM GetDomainFromEmail}\{PIG.MAILFROM GetUserFromEmail}"**. | |
| **AttSavePath** | Этот параметр задаёт полный путь к подкаталогу для штатного сохранения вложенных файлов. Начальное значение - **{Mcontent[AttSaveDir]}\saved\ {MContent[AttSaveExtraPath]}**. | |
| **LoadFailed** | Если **MContent** не может загрузить письмо для анализа, он копирует его в специальный каталог. В дальнейшем эту копию и сопроводительную информацию можно будет переслать разработчику для анализа ситуации. Начальное значение - **{MContent[AttSaveDir]}\failed\{RANDOM-ID}.eml**. | |
| **DefaultCharset** | Для правильного добавления MIME-фрагментов в письмо требуется указать используемый в каждом фрагменте набор символов. Этот параметр задаёт наиболее вероятное значение, используемое по умолчанию. Начальное значение - **"koi8-r"**, соответствующее настройкам по умолчанию, принятым в большинстве распространённых в России почтовых программ. | |
| **DefTextEncoding** | Кроме набора символов для правильного добавления MIME-фрагментов в письмо необходимо знать ещё и способ кодирования содержимого. Этот параметр задаёт наиболее вероятное значение, используемое по умолчанию. Начальное значение - **"NoEncoding"**, означающее отсутствие какого-либо кодирования вообще: текст передаётся "как есть". | |
| **Pass1** | Определяет, использовать ли общую для всех получателей процедуру обработки письма контент-анализатором. Если параметр имеет любое ненулевое значение, письмо подвергается обработке непосредственно после завершения приёма; результат этой обработки будет доступен всем получателям письма. Начальное значение - **1**. | * ? |
| **Pass2** | Определяет, использовать ли индивидуальную, специфическую для каждого получателя, процедуру обработки письма контент-анализатором. Если параметр имеет любое ненулевое значение, письмо подвергается обработке на этапе доставки конечному получателю. Такой подход позволяет задавать для каждого получателя свои специфические правила обработки. Начальное значение - **0**. | * ? |

| | | |
|---|---|---|
| **Archiver** | Контент-анализатор может помимо всего прочего "облагородить" проходящее сообщение посредством сжатия вложенных файлов. Этот параметр задаёт путь к исполняемому файлу "любимого" архиватора. В принципе, ничто не мешает использовать несколько архиваторов на разные случаи жизни, но в этом случае придётся для каждого из них написать десяток строк кода собственных правил, а сжатие вложения "любимым" архиватором уже реализовано в самом контент-анализаторе. Начальное значение - **"C:\PROGRA~1\WinRAR\RAR.exe"**. | |
| **ArchiverSwitches** | Задаёт строку команд и ключей, определяющих режим архивации. Начальное значение - **"a -m5 -df -inul"**. | |
| **ArchiverExt** | Определяет расширение имени для файла архива. Начальное значение - **".rar"**. | |
| **ArchiverCommand** | Определяет общий формат командной строки архиватора - взаимное расположение имён файлов и строки команд и ключей. Начальное значение - **"{Mcontent[ArchiverSwitches]} {"}{McontentArchiveTo}{"} {"}{McontentArchiveFrom}{"}"**. | |
| **KeepSubjectUnchanged** | Включённый в поставку файл правил общего анализа письма предусматривает добавление в тему письма (поле **Subject:**) информации о классификации письма спам-фильтрами POPfile, SpamProtexx и LibSD. Примерно в половине случаев эта в общем-то полезная возможность оказывается невостребованной, а иногда и создаёт проблемы (например, если среди получателей писем попадаются роботы, управляемые командами в теме письма). Задав любое ненулевое значение параметра, можно предотвратить модификацию темы. Начальное значение - **0**. | * ? |

## *Секция YahooDomainKeys - параметры настройки модуля поддержки Yahoo Domain Keys*

| | | |
|---|---|---|
| **SignMail** | Определяет, подписывать ли исходящую почту по спецификации Yahoo Domain Keys. Под исходящей почтой в данном случае следует понимать всякое письмо, покидающее пределы сервера (включая перенаправления для "чужих" адресатов и для отсутствующих адресатов многосерверного домена) и отправленное с использованием обратного адреса, принадлежащего одному из локальных почтовых доменов. Если письмо уже содержит подпись Yahoo Domain Keys, то повторно оно не подписывается. Если значение ненулевое, в заголовок письма добавляется электронная подпись. Начальное значение - **1**. | * ? |
| **SigningKey** | Если SMTP-сервер подписывает исходящую почту, то этот параметр задаёт расположение сертификата, закрытый ключ которого используется для формирования подписи. Сертификат формата PFX должен быть без пароля и содержать 384-битный закрытый RSA-ключ. Соответствующий ему открытый ключ должен быть опубликован в DNS домена отправителя. Начальное значение - **..\cert\{FromDomain}_ydk.pfx**; в соответствии с ним каждому локальному почтовому домену должен соответствовать свой сертификат. | |
| **VerifySignatures** | Определяет, проверять ли наличие и достоверность электронной подписи во входящей почте. Если значение ненулевое, то подпись проверяется. Поскольку подписывание ещё не стало правилом хорошего тона, то к отсутствию подписи в письме сервер пока относится благосклонно. Начальное значение - **1**. | * ? |
| **Selector** | Задаёт поддомен самого нижнего уровня в специально сконструированном доменном имени вида **{selector}._domainkeys.ваш.домен**. Именно в параметрах этого домена записан открытый ключ, используемый для верификации YDK-подписи. Открытый ключ должен соответствовать закрытому ключу, который хранится в сертификате, задаваемом параметром **SigningKey**. Начальное значение - **pigmail**. | ? |

| | | |
|---|---|---|
| **Canon** | Задаёт метод преобразования (Canonicalization) письма перед подписыванием. Действующий стандарт **YDK-base01** предусматривает два метода - **simple** и **nofws**. Начальное значение - **simple**. | ? |
| **SkipOnDisabledAntispam** | Позволяет динамически (для одного письма) отключить проверку электронной подписи, если отправитель по результатам анализа белых списков и локальных политик признан настолько надёжным, что спам-фильтр для него отключён. Начальное значение - **0**, то есть, подпись проверяется всегда. | * ? |

## *Секция POP - параметры настройки POP-сервера*

| | | |
|---|---|---|
| **DefaultMailDomain** | Почтовый домен по умолчанию для POP-сервера - переопределяет соответствующий параметр из секции **Server**. Начальное значение **{SMTP[DefaultMailDomain]}** может быть переопределено требуемым образом. | |
| **DefaultAuthDomain** | Домен авторизации по умолчанию для POP-сервера. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{SMTP[DefaultAuthDomain]}**. | $ |
| **DomainIP** | Файл со списком IP-адресов, назначенных сетевым интерфейсам компьютера. Переопределяет соответствующий параметр из секции **Lists**. Начальное значение - **{SMTP[DomainIP]}**. | |
| **UserMailBoxes** | Файл со списком, сопоставляющим данные авторизации пользователя с адресом его почтового ящика. Переопределяет соответствующий параметр из секции **Lists**. Начальное значение - **{Lists[UserMailBoxes]}**. | |
| **UserList** | Файл со списком пользователей формата Eserv/3 для POP-сервера. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{SMTP[UserList]}**. | |
| **GroupList** | Файл со списком группировки пользователей формата Eserv/3 для POP-сервера. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{SMTP[GroupList]}**. | |
| **PlainUserList** | Файл с объединённым списком пользователей формата Eserv/3 для POP-сервера. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{SMTP[PlainUserList]}**. | |
| **PlainGroupList** | Файл со списком группировки пользователей формата Eserv/3 для POP-сервера. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{SMTP[PlainGroupList]}**. | |
| **Eserv2Userlist** | Файл со списком пользователей POP-сервера, извлечённым из Eserv.ini версии Eserv/2.x. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{SMTP[Eserv2Userlist]}**. | |
| **Eserv2Grouplist** | Файл со списком группировки пользователей POP-сервера, извлечённым из Eserv.ini версии Eserv/2.x. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{SMTP[Eserv2-Grouplist]}**. | |
| **NTdomain** | Имя домена Active Directory или локального компьютера под управлением Windows линейки NT, по списку пользователей которого выполняется авторизация пользователей POP-сервера, если выбран соответствующий способ авторизации (**NtLogon**). Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{SMTP[NTdomain]}**. | |
| **DefaultAuthSource** | Имя источника авторизации на POP-сервере из списка источников авторизации. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{SMTP[DefaultAuthSource]}**. | |
| **AuthMethod** | Способ авторизации на POP-сервере по умолчанию. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{SMTP[AuthMethod]}**. | |

| | | |
|---|---|---|
| **NtlmpersonateLogon** | Определяет, требуется ли переключение в контекст безопасности пользователя при авторизации в домене Active Directory. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{SMTP[NtlmpersonateLogon]}**. | |
| **ExtendedGroupList** | Файл с расширенным списком группировки пользователей для POP-сервера. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{SMTP[ExtendedGroupList]}**. | |
| **RejectNonexistentDomains** | Указывает, отвергать ли попытки авторизации, если домен авторизации не описан в настройках сервера. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{SMTP[RejectNonexistentDomains]}**. | |
| **MaxAuthAttempts** | Максимально допустимое число попыток авторизации в одной сессии. Определяет, сколько неудачных попыток авторизации допускается в течение одной сессии. Если это число превышено, подключение считается атакой и разрывается. Если значение нулевое, то ограничения на число попыток подбора пароля отсутствуют. Начальное значение - **{SMTP[MaxAuthAttempts]}**. | |
| **Active** | Определяет, активен ли POP-сервер. Если значение нулевое, то все попытки подключения отвергаются с сообщением, что сервер временно не работает. Если указано любое ненулевое число, сервер принимает подключения. Начальное значение - **1**. | |
| **Port** | Порт, на котором работает POP-сервер. Начальное значение стандартное - **110**. | & |
| **SslPort** | Порт, на котором POP-сервер принимает подключения по защищённому соединению. Начальное значение - **995**. | & |
| **NetworkInterface** | Адрес сетевого интерфейса, слушаемого сервером. Начальное значение - пустая строка; это означает, что сервер слушает все интерфейсы. | & |
| **SslNetworkInterface** | Адрес сетевого интерфейса, слушаемого сервером для приёма подключений по защищённому соединению. Начальное значение - пустая строка; это означает, что сервер слушает все интерфейсы. | & |
| **Certificate** | Имя файла формата PEM, содержащего закрытый ключ и сертификаты, используемые при организации защищённого (SSL) соединения сервера с клиентом. Переопределяет соответствующий параметр из секции **Server**. Начальное значение - **{Server[Certificate]}**. | $ |
| **SslVerifyClient** | Определяет режим проверки подлинности сертификатов клиентской стороны при установлении защищённого соединения. Переопределяет соответствующий параметр из секции **Server**. Начальное значение - **{Server[SslVerifyClient]}**. | $ |
| **RequireSsl** | Определяет, требовать ли от пользователей обязательного подключения по защищённому соединению (SSL). Если этот флаг установлен (задано любое ненулевое значение), все попытки авторизации без предварительной инициализации защищённого соединения будут отвергаться. Начальное значение - **0**. | * |
| **Timeout** | Время бездействия, задаваемое в миллисекундах, по истечении которого сервер прекращает соединение с клиентом. Это вынужденная мера, предотвращающая утечку ресурсов при плохой связи - как правило, тайм-аут срабатывает, когда соединение уже фактически разорвано, но серверу неоткуда получить извещение об этом. Начальное значение - **60000**, что соответствует 10 минутам. | $ |
| **DelayAfterCommand** | Этот параметр позволяет искусственно замедлять работу POP-сервера в тех случаях, когда почтовые клиенты по каким-либо причинам не успевают адекватно принять ими же самими запрошенные данные. Параметр задаёт длительность паузы между получением сервером команды и началом выдачи ответа. Длительность задаётся в миллисекундах. Начальное значение - **100**. | * $ |

| | | |
|---|---|---|
| **PopListDelay** | Этот параметр позволяет искусственно замедлять работу POP-сервера в тех случаях, когда почтовые клиенты по каким-либо причинам не успевают адекватно принять ими же самими запрошенные данные. Параметр задаёт длительность паузы между передачей строк в ответ на команду LIST. Длительность задаётся в миллисекундах. Обычно достаточно 15 - 20 миллисекунд, чтобы подвисающие при получении списка писем клиенты пришли в норму. Начальное значение - **0**. | * $ |
| **Lists** | Расположение каталога со списками настройки POP-сервера. Начальное значение - **{Dirs[Lists]}\pop**. | |
| **Templates** | Расположение каталога с шаблонами ответов POP-сервера. Начальное значение - **{Dirs[Templates]}\pop**. | |
| **DefaultDomainMailBoxes** | Расположение каталога почтовых ящиков домена по умолчанию, задаваемого параметром **DefaultMailDomain**. Если этот домен по каким-либо причинам не занесён в список локальных доменов, почтовые ящики пользователей этого домена всё равно будут доступны. Начальное значение - **{SMTP[DefaultDomainMailBoxes]}**. | |
| **Unlisted** | Расположение почтового ящика "отсутствующего" пользователя. Если в результате ошибки в настройке пользователь успешно авторизовался, но информацию о расположении его почтового ящика найти не удаётся, сервер подключит пользователя к этому вечно пустому ящику. Начальное значение - **{SMTP[MailBoxes]}\unlisted**. | |
| **Logs** | Расположение каталога оперативных журналов POP-сервера. Начальное значение - **{Dirs[Logs]}**. | $ |
| **ACL** | Список прав пользователей, назначаемых по данным авторизации на POP-сервере. Начальное значение - **{POP[Lists]}\ACL.txt**. | |
| **SpecialFolders** | Список особых пользователей (с указанием домена авторизации - **логин@домен**), которым в качестве почтового ящика назначаются особые каталоги - вплоть до полной иерархии почтовых каталогов. Начальное значение - **{IMAP[SpecialFolders]}**. | |
| **IpBlackList** | Список IP-адресов и подсетей, которым запрещено обращаться к POP-серверу. Начальное значение - **{POP[Lists]}\IpBlackList.txt**. | |
| **LocalNetworks** | Список локальных сетей, обслуживаемых POP-сервером. Переопределяет соответствующий параметр из секции **Lists**. Начальное значение - **{SMTP[LocalNetworks]}**. | |
| **IpWhiteList** | Список доверенных IP-адресов или сетей, которые обслуживаются этим POP-сервером, то есть, которым позволено читать почту сервера. Этот список ДОПОЛНЯЕТ список локальных сетей. В нём могут быть не локальные сети, а, например, особые внешние IP-адреса. Начальное значение - **{POP[Lists]}\IpWhiteList.txt**. | |
| **ExpungeAlways** | В соответствии со стандартом протокола POP3 письма, запрошенные почтовым клиентом к удалению, не удаляются с сервера немедленно - их физическое удаление происходит только при корректном завершении сеанса связи между клиентом и сервером. Часть почтовых клиентов (в частности, Outlook Express) даже запрашивает удаление писем пачками - после того, как примет с сервера всю почту. Однако если связь плохая и часто прерывается, такая постановка дела создаёт проблемы. "Продвинутые" почтовые клиенты (например, TheBat!), отдают команду на удаление письма сразу после того, как оно было успешно принято. Остаётся "научить" POP-сервер физически удалять запрошенные к удалению письма не только при корректном завершении сеанса, но и при аварийном разрыве связи. Если этот параметр имеет любое ненулевое значение, POP-сервер выполняет ревизию почтового ящика и удаление ненужных писем при любом завершении сеанса, что идёт вразрез со стандартом, но иногда более соответствует реалиям. Начальное значение - **0**. | * |

| | | |
|---|---|---|
| **UseCallback** | Определяет, используются ли почтовым сервером специальные расширения протокола, предназначенные для поддержки монитора почтовых ящиков **Piafi MailKnocker**. Применение расширений позволяет не использовать регулярный опрос состояния ящиков (как это сделано в большинстве других мониторов - включая и сам MailKnocker при работе в "стандартном" режиме), а оперативно уведомлять о поступлении почты в момент помещения письма в почтовый ящик. Любое ненулевое значение включает использование расширений. Начальное значение - **0**. | * |
| **MsgIdDupCheck** | Управляет отображением дубликатов писем. Дубликаты определяются по одинаковому содержимому заголовка **Message-ID**. Если задано любое ненулевое значение, почтовый клиент получает информацию только об одном из дублирующихся писем. Начальное значение - **0**, то есть, контроль дубликатов не производится, отображаются все письма. | * $ |
| **LockIntruders** | Определяет, использовать ли блокировку атак. Признаком атаки считается частое повторение различных нежелательных событий - таких, как ошибки авторизации. Если частота следования таких событий для какого-либо IP-адреса клиентского подключения превышает установленную в настройках величину, то этот адрес заносится в список запрещённых сетей. IP-адреса, находящиеся в списках локальных или доверенных сетей, блокировке не подвергаются. Если при запуске сервера этот параметр имеет любое ненулевое значение, подключается плагин **ids_memo**, обеспечивающий хранение и накопление информации о нежелательных событиях. После этого параметр может использоваться для временного отключения блокировки атак, если его работа будет создавать какие-либо проблемы. Начальное значение - **{Server[LockIntruders]}**. | |
| **AuthFailCount** | Пороговое значение числа ошибок авторизации. Если количество неудачных попыток авторизации за определённый временной интервал для одного и того же IP-адреса клиентского подключения превышает заданную этим параметром величину, это считается атакой - со всеми вытекающими отрицательными последствиями для соответствующего клиента. Начальное значение - **{Server[AuthFailCount]}**. | |
| **AuthFailPeriod** | Период подсчёта ошибок авторизации. Если количество неудачных попыток авторизации за определённый этим параметром временной интервал для одного и того же IP-адреса клиентского подключения превышает заданную величину, это считается атакой - со всеми вытекающими отрицательными последствиями для соответствующего клиента. Длительность периода задаётся в минутах. Начальное значение - **{Server[AuthFailPeriod]}**. | |
| **UseTarpit** | Указывает, использовать ли при выдаче отказов клиенту Tarpit - "липучку". В этом случае отрицательные ответы искусственно задерживаются, что уменьшает нагрузку на сеть. Начальное значение - **{Server[UseTarpit]}**. | |
| **TarpitInterval** | Если задано использование "липучки", то этот параметр задаёт длительность задержки в секундах. Начальное значение - **{Server[TarpitInterval]}**. | |
| **LogLevel** | Задаёт уровень детализации оперативного журнала POP-сервера. Параметр может принимать значения от 1 до 9. Чем выше уровень, тем больше подробностей пишется в журнал. Для совместимости с ранними версиями, в которых уровень детализации не задавался, нулевое значение соответствует максимальному уровню детализации. Начальное значение - **{Server[LogLevel]}**. | $ |

| | | |
|---|---|---|
| **LogToEStat** | Определяет, ведёт ли сервер статистику в формате программы **Estat32**, разработанной **Андреем Волковым** из **EPE Labs** для обработки статистических журналов Eserv/2. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{SMTP[LogToEStat]}**. | $ |
| **LogToAdvSoft** | Определяет, ведёт ли сервер статистику в формате программ **ProxyInspector** и **MailDetective** производства компании **AdvSoft**. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{SMTP[LogToAdvSoft]}**. | $ |
| **LogToElog** | Определяет, ведёт ли сервер статистику в формате программы **Elog**, разработанной **Игорем Панасенко** из компании **ЛЭНК** для обработки статистических журналов Eserv/3. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{SMTP[LogToElog]}**. | $ |
| **LogToMaillog** | Определяет, ведёт ли сервер статистику в собственном текстовом формате. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{SMTP[LogToMaillog]}**. | $ |
| **LogToMStat** | Определяет, используется ли подсистема ведения статистики в базе данных MStat, разработанная Андреем Матвеевым. Этот сборщик статистики имеет немалое преимущество перед текстовыми журналами, позволяя хранить и эффективно обрабатывать статистическую информацию за большие периоды времени, измеряемые годами. Но для его работы необходима установка дополнительного приложения - СУБД одного из поддерживаемых сборщиком типов. Если при запуске сервера указано любое ненулевое число, загружается специальный плагин **mstat**. В дальнейшем при возникновении проблем сбор статистики в базе данных можно временно отключить, установив нулевое значение. Начальное значение - **{SMTP[LogToMStat]}**. | $<br>& |

## *Секция IMAP - параметры настройки IMAP-сервера*

| | | |
|---|---|---|
| **DefaultMailDomain** | Почтовый домен по умолчанию для IMAP-сервера - переопределяет соответствующий параметр из секции **Server**. Начальное значение **{SMTP[DefaultMailDomain]}** может быть переопределено требуемым образом. | |
| **DefaultAuthDomain** | Домен авторизации по умолчанию для IMAP-сервера. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{SMTP[DefaultAuthDomain]}**. | $ |
| **DomainIP** | Файл со списком IP-адресов, назначенных сетевым интерфейсам компьютера. Переопределяет соответствующий параметр из секции **Lists**. Начальное значение - **{SMTP[DomainIP]}**. | |
| **UserMailBoxes** | Файл со списком, сопоставляющим данные авторизации пользователя с адресом его почтового ящика. Переопределяет соответствующий параметр из секции **Lists**. Начальное значение - **{Lists[UserMailBoxes]}**. | |

| | | |
|---|---|---|
| **UserList** | Файл со списком пользователей формата Eserv/3 для IMAP-сервера. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{SMTP[UserList]}**. | |
| **GroupList** | Файл со списком группировки пользователей формата Eserv/3 для IMAP-сервера. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{SMTP[GroupList]}**. | |
| **PlainUserList** | Файл с объединённым списком пользователей формата Eserv/3 для IMAP-сервера. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{SMTP[PlainUserList]}**. | |
| **PlainGroupList** | Файл со списком группировки пользователей формата Eserv/3 для IMAP-сервера. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{SMTP[PlainGroupList]}**. | |
| **Eserv2Userlist** | Файл со списком пользователей IMAP-сервера, извлечённым из Eserv.ini версии Eserv/2.x. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{SMTP[Eserv2Userlist]}**. | |
| **Eserv2Grouplist** | Файл со списком группировки пользователей IMAP-сервера, извлечённым из Eserv.ini версии Eserv/2.x. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{SMTP[Eserv2-Grouplist]}**. | |
| **NTdomain** | Имя домена Active Directory или локального компьютера под управлением Windows линейки NT, по списку пользователей которого выполняется авторизация пользователей IMAP-сервера, если выбран соответствующий способ авторизации (**NtLogon**). Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{SMTP[NTdomain]}**. | |
| **DefaultAuthSource** | Имя источника авторизации на IMAP-сервере из списка источников авторизации. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{SMTP[DefaultAuthSource]}**. | |
| **AuthMethod** | Способ авторизации на IMAP-сервере по умолчанию. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{SMTP[AuthMethod]}**. | |
| **NtImpersonateLogon** | Определяет, требуется ли переключение в контекст безопасности пользователя при авторизации в домене Active Directory. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{SMTP[NtImpersonateLogon]}**. | |
| **UseExtendedGroups** | Указывает, использовать ли расширенную (кросс-доменную) группировку пользователей. Переопределяет соответствующий параметр из секции **AUTH**. Если при запуске сервера этот параметр имеет любое ненулевое значение, то загружается специальный плагин **groups_ext**. Начальное значение - **{SMTP[UseExtendedGroups]}**. | * & |
| **ExtendedGroupList** | Файл с расширенным списком группировки пользователей для IMAP-сервера. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{SMTP[ExtendedGroupList]}**. | |
| **RejectNonexistentDomains** | Указывает, отвергать ли попытки авторизации, если домен авторизации не описан в настройках сервера. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{SMTP[RejectNonexistentDomains]}**. | |
| **MaxAuthAttempts** | Максимально допустимое число попыток авторизации в одной сессии. Определяет, сколько неудачных попыток авторизации допускается в течение одной сессии. Если это число превышено, подключение считается атакой и разрывается. Если значение нулевое, то ограничения на число попыток подбора пароля отсутствуют. Начальное значение - **{SMTP[MaxAuthAttempts]}**. | ? |

| | | |
|---|---|---|
| **CacheIni** | Для ускорения анализа запросов IMAP-сервер может кэшировать в оперативной памяти ряд параметров конфигурационного файла. Кэширование производится только на время сессии - от подключения клиента до его отсоединения - и не влияет на параллельные сессии. Если кэширование создаёт проблемы, его можно отключить, установив этот параметр в ноль и перезапустив IMAP-сервер. Начальное значение - **1**. | * & |
| **Active** | Определяет, активен ли IMAP-сервер. Если значение нулевое, то все попытки подключения отвергаются с сообщением, что сервер временно не работает. Если указано любое ненулевое число, сервер принимает подключения. Начальное значение - **1**. | |
| **Port** | Порт, на котором работает IMAP-сервер. Начальное значение стандартное - **143**. | & |
| **SslPort** | Порт, на котором IMAP-сервер принимает подключения по защищённому соединению. Начальное значение - **993**. | & |
| **NetworkInterface** | Адрес сетевого интерфейса, слушаемого сервером. Начальное значение - пустая строка; это означает, что сервер слушает все интерфейсы. | & |
| **SslNetworkInterface** | Адрес сетевого интерфейса, слушаемого сервером для приёма подключений по защищённому соединению. Начальное значение - пустая строка; это означает, что сервер слушает все интерфейсы. | & |
| **Certificate** | Имя файла формата PEM, содержащего закрытый ключ и сертификаты, используемые при организации защищённого (SSL) соединения сервера с клиентом. Переопределяет соответствующий параметр из секции **Server**. Начальное значение - **{Server[Certificate]}**. | $ |
| **SslVerifyClient** | Определяет режим проверки подлинности сертификатов клиентской стороны при установлении защищённого соединения. Переопределяет соответствующий параметр из секции **Server**. Начальное значение - **{Server[SslVerifyClient]}**. | $ |
| **RequireSsl** | Определяет, требовать ли от пользователей обязательного подключения по защищённому соединению (SSL). Если этот флаг установлен (задано любое ненулевое значение), все попытки авторизации без предварительной инициализации защищённого соединения будут отвергаться. Начальное значение - **0**. | * |
| **Timeout** | Время бездействия, задаваемое в миллисекундах, по истечении которого сервер прекращает соединение с клиентом. Это вынужденная мера, предотвращающая утечку ресурсов при плохой связи - как правило, тайм-аут срабатывает, когда соединение уже фактически разорвано, но серверу неоткуда получить извещение об этом. Начальное значение - **1800000**, что соответствует получасу: подключение по протоколу IMAP не "одноразовое", и длительные периоды бездействия клиента могут иметь вполне законное происхождение. | $ |
| **DelayAfterCommand** | Этот параметр позволяет искусственно замедлять работу IMAP-сервера в тех случаях, когда почтовые клиенты по каким-либо причинам не успевают адекватно принять ими же самими запрошенные данные. Параметр задаёт длительность паузы между получением сервером команды и началом выдачи ответа. Длительность задаётся в миллисекундах. Начальное значение - **100**. | * $ |
| **FetchDelay** | Этот параметр позволяет искусственно замедлять работу IMAP-сервера в тех случаях, когда почтовые клиенты по каким-либо причинам не успевают адекватно принять ими же самими запрошенные данные. Параметр задаёт длительность паузы между передачей строк в ответ на команду FETCH. Длительность задаётся в миллисекундах. Обычно достаточно 15 - 20 миллисекунд, чтобы подвисающие при получении списка писем клиенты пришли в норму. Начальное значение - **0**. | * $ |
| **MaxConnections** | Максимально допустимое число одновременных подключений к серверу. Позволяет противостоять пиковым нагрузкам и целенаправленным попыткам завалить сервер путём неумеренного потребления всех ресурсов компьютера. Начальное значение - **25**. | & |

| | | |
|---|---|---|
| **MaxConnectionsFromIP** | Максимально допустимое число одновременных подключений к серверу с одного IP-адреса. В текущей версии эта настройка не поддерживается и зарезервирована на будущее. Начальное значение - **10**. | & |
| **Lists** | Расположение каталога со списками настройки IMAP-сервера. Начальное значение - **{Dirs[Lists]}\imap**. | |
| **Templates** | Расположение каталога с шаблонами ответов IMAP-сервера. Начальное значение - **{Dirs[Templates]}\imap**. | |
| **DefaultDomainMailBoxes** | Расположение каталога почтовых ящиков домена по умолчанию, задаваемого параметром **DefaultMailDomain**. Если этот домен по каким-либо причинам не занесён в список локальных доменов, почтовые ящики пользователей этого домена всё равно будут доступны. ЭНачальное значение - **{SMTP[DefaultDomainMailBoxes]}**. | |
| **Unlisted** | Расположение почтового ящика "отсутствующего" пользователя. Если в результате ошибки в настройке пользователь успешно авторизовался, но информацию о расположении его почтового ящика найти не удаётся, сервер подключит пользователя к этому вечно пустому ящику. Начальное значение - **{SMTP[MailBoxes]}\unlisted**. | |
| **Logs** | Расположение каталога оперативных журналов IMAP-сервера. Начальное значение - **{Dirs[Logs]}**. | $ |
| **ACL** | Список прав пользователей, назначаемых по данным авторизации на IMAP-сервере. Начальное значение - **{IMAP[Lists]}\ACL.txt**. | |
| **SpecialFolders** | Список особых пользователей (с указанием домена авторизации - **логин@домен**), которым в качестве почтового ящика назначаются особые каталоги - вплоть до полной иерархии почтовых каталогов. Начальное значение - **{IMAP[Lists]}\SpecialFolders.txt**. | |
| **IpBlackList** | Список IP-адресов и подсетей, которым запрещено обращаться к IMAP-серверу. Начальное значение - **{IMAP[Lists]}\IpBlackList.txt**. | ? |
| **LocalNetworks** | Список локальных сетей, обслуживаемых IMAP-сервером. Переопределяет соответствующий параметр из секции **Lists**. Начальное значение - **{SMTP[LocalNetworks]}**. | ? |
| **IpWhiteList** | Список доверенных IP-адресов или сетей, которые обслуживаются этим IMAP-сервером, то есть, которым позволено читать почту сервера. Этот список ДОПОЛНЯЕТ список локальных сетей. В нём могут быть не локальные сети, а, например, особые внешние IP-адреса. Начальное значение - **{IMAP[Lists]}\IpWhiteList.txt**. | ? |
| **ImapFolderActions** | Список специальных действий, назначенных некоторым папкам IMAP. Действия (это может быть переклассификация письма с помощью POPfile, SpamProtexx или LibSD, переотправка письма получателям) выполняются над каждым письмом, перемещаемым в эти папки. Начальное значение - **{IMAP[Lists]}\ImapFolderActions.txt**. | ? |
| **UsePerformanceTuning** | Определяет, применять ли собственные нестандартные значения двух перечисленных ниже параметров тонкой настройки производительности или же оставить заданные в коде сервера значения по умолчанию. Если сервер успешно справляется с нагрузкой, эти настройки лучше оставить как есть. Если при запуске сервера этот параметр имеет ненулевое значение, вместо значений по умолчанию применяются собственные нестандартные значения. Начальное значение - **0**. | & |
| **PacketSize** | Задаёт размер пакета для передачи файлов. Чем больше размер пакета, тем выше производительность сервера на этапе передачи клиенту результатов обработки запроса. Однако это справедливо только при надёжных каналах связи. Если связь плохая, большой размер пакета приведёт к частым сбоям и снижению производительности. Размер пакета задаётся в байтах. Начальное значение соответствует значению по умолчанию - **65000**. | & |

| | | |
|---|---|---|
| **ListenQLen** | Задаёт максимальную длину очереди запросов на подключение к серверу. Чем больше очередь, тем вероятнее, что клиент, пусть даже после длительного ожидания, будет обслужен, а не получит от ворот поворот. Однако для обслуживания большой очереди требуется пропорциональное количество ресурсов сервера. Начальное значение соответствует значению по умолчанию - **1000**. | & |
| **WriteSocketRetryDelay** | Определяет величину задержки отслеживания событий при записи в основной сокет. Чем меньше значение этого параметра, тем оперативнее сервер реагирует на изменение состояния сокета, но, одновременно, тем больше потребление процессорного времени. Величина задержки задаётся в миллисекундах. Начальное значение соответствует значению по умолчанию - **200**. | & |
| **MsgIdDupCheck** | Управляет отображением дубликатов писем. Дубликаты определяются по одинаковому содержимому заголовка **Message-ID**. Если задано любое ненулевое значение, почтовый клиент получает информацию только об одном из дублирующихся писем. Начальное значение - **0**, то есть, контроль дубликатов не производится, отображаются все письма. | * $ |
| **Debug** | Управляет выводом в журнал отладочной информации о командах протокола IMAP и ответах сервера. Начальное значение - **0**, то есть, отладочная информация не выводится. | $ |
| **LockIntruders** | Определяет, использовать ли блокировку атак. Признаком атаки считается частое повторение различных нежелательных событий - таких, как ошибки авторизации. Если частота следования таких событий для какого-либо IP-адреса клиентского подключения превышает установленную в настройках величину, то этот адрес заносится в список запрещённых сетей. IP-адреса, находящиеся в списках локальных или доверенных сетей, блокировке не подвергаются. Если при запуске сервера этот параметр имеет любое ненулевое значение, подключается плагин **ids_memo**, обеспечивающий хранение и накопление информации о нежелательных событиях. После этого параметр может использоваться для временного отключения блокировки атак, если его работа будет создавать какие-либо проблемы. Начальное значение - **{Server[LockIntruders]}**. | * ? |
| **AuthFailCount** | Пороговое значение числа ошибок авторизации. Если количество неудачных попыток авторизации за определённый временной интервал для одного и того же IP-адреса клиентского подключения превышает заданную этим параметром величину, это считается атакой - со всеми вытекающими отрицательными последствиями для соответствующего клиента. Начальное значение - **{Server[AuthFailCount]}**. | * ? |
| **AuthFailPeriod** | Период подсчёта ошибок авторизации. Если количество неудачных попыток авторизации за определённый этим параметром временной интервал для одного и того же IP-адреса клиентского подключения превышает заданную величину, это считается атакой - со всеми вытекающими отрицательными последствиями для соответствующего клиента. Длительность периода задаётся в минутах. Начальное значение - **{Server[AuthFailPeriod]}**. | * ? |
| **UseTarpit** | Указывает, использовать ли при выдаче отказов клиенту Tarpit - "липучку". В этом случае отрицательные ответы искусственно задерживаются, что уменьшает нагрузку на сеть. Начальное значение - **{Server[UseTarpit]}**. | * ? |
| **TarpitInterval** | Если задано использование "липучки", то этот параметр задаёт длительность задержки в секундах. Начальное значение - **{Server[TarpitInterval]}**. | * ? |

| | | |
|---|---|---|
| **LogLevel** | Задаёт уровень детализации оперативного журнала IMAP-сервера. Параметр может принимать значения от 1 до 9. Чем выше уровень, тем больше подробностей пишется в журнал. Для совместимости с ранними версиями, в которых уровень детализации не задавался, нулевое значение соответствует максимальному уровню детализации. Начальное значение - **{Server[LogLevel]}**. | $ |
| **LogToEStat** | Определяет, ведёт ли сервер статистику в формате программы **Estat32**, разработанной **Андреем Волковым** из **EPE Labs** для обработки статистических журналов Eserv/2. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{SMTP[LogToEStat]}**. | $ |
| **LogToAdvSoft** | Определяет, ведёт ли сервер статистику в формате программ **ProxyInspector** и **MailDetective** производства компании **AdvSoft**. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{SMTP[LogToAdvSoft]}**. | $ |
| **LogToElog** | Определяет, ведёт ли сервер статистику в формате программы **Elog**, разработанной **Игорем Панасенко** из компании **ЛЭНК** для обработки статистических журналов Eserv/3. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{SMTP[LogToElog]}**. | $ |
| **LogToMaillog** | Определяет, ведёт ли сервер статистику в собственном текстовом формате. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{SMTP[LogToMaillog]}**. | $ |
| **LogToMStat** | Определяет, используется ли подсистема ведения статистики в базе данных MStat, разработанная Андреем Матвеевым. Этот сборщик статистики имеет немалое преимущество перед текстовыми журналами, позволяя хранить и эффективно обрабатывать статистическую информацию за большие периоды времени, измеряемые годами. Но для его работы необходима установка дополнительного приложения - СУБД одного из поддерживаемых сборщиком типов. Если при запуске сервера указано любое ненулевое число, загружается специальный плагин **mstat**. В дальнейшем при возникновении проблем сбор статистики в базе данных можно временно отключить, установив нулевое значение. Начальное значение - **{SMTP[LogToMStat]}**. | $<br>& |

## *Секция PROXY - общие параметры настройки прокси-сервера*

| | | |
|---|---|---|
| **DefaultAuthDomain** | Домен авторизации по умолчанию для прокси-сервера. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[DefaultAuthDomain]}**. | |
| **DomainIP** | Файл со списком IP-адресов, назначенных сетевым интерфейсам компьютера. Переопределяет соответствующий параметр из секции **Lists**. Начальное значение - **{Lists[DomainIP]}**. | |
| **UserList** | Файл со списком пользователей формата Eserv/3 для прокси-сервера. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[UserList]}**. | |

| | | |
|---|---|---|
| **GroupList** | Файл со списком группировки пользователей формата Eserv/3 для прокси-сервера. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[GroupList]}**. | |
| **PlainUserList** | Файл с объединённым списком пользователей формата Eserv/3 для прокси-сервера. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[PlainUserList]}**. | |
| **PlainGroupList** | Файл со списком группировки пользователей формата Eserv/3 для прокси-сервера. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[PlainGroupList]}**. | |
| **Eserv2Userlist** | Файл со списком пользователей прокси-сервера, извлечённым из Eserv.ini версии Eserv/2.x. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[Eserv2Userlist]}**. | |
| **Eserv2Grouplist** | Файл со списком группировки пользователей прокси-сервера, извлечённым из Eserv.ini версии Eserv/2.x. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[Eserv2-Grouplist]}**. | |
| **NTdomain** | Имя домена Active Directory или локального компьютера под управлением Windows линейки NT, по списку пользователей которого выполняется авторизация пользователей прокси-сервера, если выбран соответствующий способ авторизации (**NtLogon**). Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[NTdomain]}**. | |
| **DefaultAuthSource** | Имя источника авторизации на прокси-сервера из списка источников авторизации. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[DefaultAuthSource]}**. | |
| **AuthMethod** | Способ авторизации на прокси-сервера по умолчанию. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[AuthMethod]}**. | |
| **NtImpersonateLogon** | Определяет, требуется ли переключение в контекст безопасности пользователя при авторизации в домене Active Directory. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[NtImpersonateLogon]}**. | |
| **UseExtendedGroups** | Указывает, использовать ли расширенную (кросс-доменную) группировку пользователей. Переопределяет соответствующий параметр из секции **AUTH**. Если при запуске сервера этот параметр имеет любое ненулевое значение, то загружается специальный плагин **groups_ext**. Начальное значение - **{AUTH[UseExtendedGroups]}**. | & |
| **ExtendedGroupList** | Файл с расширенным списком группировки пользователей для прокси-сервера. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[ExtendedGroupList]}**. | |
| **RejectNonexistentDomains** | Указывает, отвергать ли попытки авторизации, если домен авторизации не описан в настройках сервера. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[RejectNonexist-entDomains]}**. | |
| **MaxAuthAttempts** | Максимально допустимое число попыток протокольной (не по IP/MAC-адресу) авторизации в одной сессии FTP- или Socks-прокси. Определяет, сколько неудачных попыток авторизации допускается в течение одной сессии. Если это число превышено, подключение считается атакой и разрывается. Если значение нулевое, то ограничения на число попыток подбора пароля отсутствуют. Начальное значение - **{AUTH[MaxAuthAttempts]}**. | |
| **CacheIni** | Для ускорения обработки запросов прокси-сервер может кэшировать в оперативной памяти ряд параметров конфигурационного файла. Кэширование производится только на время сессии - от подключения клиента до его отсоединения - и не влияет на параллельные сессии. Если кэширование создаёт проблемы, его можно отключить, установив этот параметр в ноль и перезапустив прокси-сервер. Начальное значение - **1**. | * & |

| | | |
|---|---|---|
| **CacheAuth** | Для ускорения обработки запросов прокси-сервер может кэшировать в оперативной памяти реквизиты успешно авторизовавшихся пользователей и сведения о их членстве в группах, чтобы при повторном обращении не выполнять заново однажды выполненную достаточно затратную процедуру. Поскольку настройки всё-таки имеют свойство время от времени изменяться, то информация запоминается не навечно, а на некоторый промежуток времени, который в текущей версии составляет 15 минут. Кэширование может создавать проблемы, если требуется авторизация по списку домена Active Directory с переключением в контекст безопасности авторизовавшегося пользователя, - при использовании запомненных данных об авторизации такое переключение невозможно, поскольку оно требует реальной авторизации в домене AD. Кэширование включается, если при запуске сервера этот параметр имеет любое ненулевое значение. Начальное значение - **0**. | * & |
| **MaxConnections** | Максимально допустимое число одновременных подключений к серверу. Позволяет противостоять пиковым нагрузкам и целенаправленным попыткам завалить сервер путём неумеренного потребления всех ресурсов компьютера. Начальное значение - **100**. | & |
| **MaxConnectionsFromIP** | Максимально допустимое число одновременных подключений к серверу с одного IP-адреса. В текущей версии эта настройка не поддерживается и зарезервирована на будущее. Начальное значение - **10**. | & |
| **Lists** | Расположение каталога со списками настройки прокси-сервера. Начальное значение - **{Dirs[Lists]}\proxy**. | |
| **Templates** | Расположение каталога с шаблонами сообщений прокси-сервера. Начальное значение - **{Dirs[Templates]}\proxy**. | |
| **Logs** | Расположение каталога оперативных журналов прокси-сервера. Начальное значение - **{Dirs[Logs]}**. | |
| **Flags** | Расположение рабочего каталога монитора флагов для прокси-сервера. Монитор флагов представляет собой вспомогательный сервис, обслуживающий ряд расширений PigMail+PigProxy, в частности, ограничитель трафика **TrafC**. Монитор отслеживает появление в рабочем каталоге так называемых флаг-файлов и в зависимости от их наименования и содержимого инициирует выполнение различных действий. Некоторые администраторские функции web-интерфейса, в частности, управление квотами, используют возможности монитора флагов. Начальное значение - **{Dirs[Flags]}\proxy**. | & |
| **MyIpList** | Список сетевых интерфейсов компьютера с указанием, на какие из этих интерфейсов прокси-серверу разрешено принимать подключения. Это важный элемент системы безопасности сервера, позволяющий разом отсечь множество заведомо чужих пользователей, поэтому настройке этого списка надо уделить максимум внимания. Начальное значение - **{PROXY[Lists]}\MyIpList.txt**. | |
| **IpBlackList** | Список IP-адресов и подсетей, которым запрещено обращаться к прокси-серверу. Начальное значение - **{PROXY[Lists]}\IpBlackList.txt**. | |
| **LocalNetworks** | Список локальных сетей, обслуживаемых прокси-сервером. Переопределяет соответствующий параметр из секции **Lists**. Начальное значение - **{Lists[LocalNetworks]}**. | |
| **IpWhiteList** | Список доверенных IP-адресов или сетей, которые обслуживаются этим прокси-сервером. Этот список ДОПОЛНЯЕТ список локальных сетей. В нём могут быть не локальные сети, а, например, особые внешние IP-адреса. Начальное значение - **{PROXY[Lists]}\IpWhiteList.txt**. | |
| **IpMacAuth** | Файл со списком, устанавливающим соответствие между IP и MAC адресами клиентского компьютера и именем учётной записи пользователя. Переопределяет соответствующий параметр из секции **Lists**. Начальное значение - **{Lists[IpMacAuth]}**. | |

| | | |
|---|---|---|
| **IgnoreLocalNetworks** | Указывает, использовать ли при определении допустимости подключения список локальных сетей. Если в настройках сервера указан общий список локальных сетей, составленный излишне либерально с точки зрения безопасности прокси-сервера, его использование для управления доступом к прокси-серверу можно отключить, задав этому параметру любое ненулевое значение. Начальное значение - **0**, то есть, список локальных сетей при подключении клиента проверяется. | * |
| **UseIpAuth** | Указывает, использовать ли автоматическую авторизацию подключившегося пользователя на основании IP-адреса либо сочетания IP и MAC-адресов. Начальное значение - **0**, то есть, если прочие настройки сервера потребуют авторизации клиента, она должна быть выполнена явно. | * |
| **UsePerformanceTuning** | Определяет, применять ли собственное нестандартное значение следующего параметра тонкой настройки производительности или же оставить заданное в коде сервера значение по умолчанию. Если сервер успешно справляется с нагрузкой, эти настройки лучше оставить как есть. Если при запуске сервера этот параметр имеет ненулевое значение, вместо значений по умолчанию применяются собственные нестандартные значения. Начальное значение - **0**. | & |
| **PacketSize** | Задаёт размер пакета для передачи файлов. Чем больше размер пакета, тем выше производительность сервера на этапе передачи клиенту результатов обработки запроса. Однако это справедливо только при надёжных каналах связи. Если связь плохая, большой размер пакета приведёт к частым сбоям и снижению производительности. Размер пакета задаётся в байтах. Начальное значение соответствует значению по умолчанию - **65000**. | & |
| **MappingBufferSize** | Задаёт размер буфера для передачи данных через отображения портов TCP. Кроме собственно отображения портов TCP, этот режим используется HTTP-прокси при обработке запроса CONNECT, Socks-прокси и POP3-прокси. Теоретически, чем этот буфер больше, тем быстрее происходит обмен. Однако это справедливо только при надёжных каналах связи. Если связь плохая, большой размер буфера приведёт к частым сбоям и снижению производительности. Размер буфера задаётся в байтах. Начальное значение соответствует значению по умолчанию - **65000**. | & |
| **ListenQLen** | Задаёт максимальную длину очереди запросов на подключение к серверу. Чем больше очередь, тем вероятнее, что клиент, пусть даже после длительного ожидания, будет обслужен, а не получит от ворот поворот. Однако для обслуживания большой очереди требуется пропорциональное количество ресурсов сервера. Начальное значение соответствует значению по умолчанию - **1000**. | & |
| **WriteSocketRetryDelay** | Определяет величину задержки отслеживания событий при записи в основной сокет. Чем меньше значение этого параметра, тем оперативнее сервер реагирует на изменение состояния сокета, но, одновременно, тем больше потребление процессорного времени. Величина задержки задаётся в миллисекундах. Начальное значение соответствует значению по умолчанию - **4**. | & |
| **AuthCacheRefreshAge** | Задаёт длительность интервала хранения данных в кэше ускорителя авторизации. Чем меньше этот интервал, тем быстрее сервер реагирует на изменение настроек - и тем чаще вызывается процедура реальной авторизации, потребляя ресурсы сервера и вызывая задержки выполнения. Величина задержки задаётся в миллисекундах. Начальное значение соответствует значению по умолчанию - **900000** (15 минут). | & |
| **UseTcpMapping** | Указывает, использовать ли отображения портов TCP. С помощью отображений можно пропустить через прокси-сервер практически любой протокол из числа неизвестных серверу. В результате действия отображения удалённый сервер появляется в локальной сети на одном из TCP-портов прокси-сервера. Если при запуске сервера этот параметр имеет любое ненулевое значение, то загружается специальный плагин **tcpmap**. Начальное значение - **0**. | * & |

| | | |
|---|---|---|
| **UseUdpMapping** | Указывает, использовать ли отображения портов UDP. UDP - особый протокол, не использующий подтверждения доставки пакетов. Он применяется во многих случаях, в частности, для голосовой связи, для интернет-радио и для обращения к серверам DNS. Если при запуске сервера этот параметр имеет любое ненулевое значение, то загружается специальный плагин **udpmap**. Начальное значение - **0**. | * & |
| **UsePop3Proxy** | Указывает, использовать ли проксирование для почтового протокола POP3. Некоторые особенности протокола позволяют обращаться к внешним почтовым серверам с использованием "умного" прокси-сервера, а не "тупого" статического отображения TCP-портов. Если при запуске сервера этот параметр имеет любое ненулевое значение, то загружается специальный плагин **pop3proxy**. Начальное значение - **0**. | * & |
| **ConstrainTraffic** | Указывает, использовать ли управление трафиком (ограничитель TrafC). Если при запуске сервера параметр имеет ненулевое значение, загружается и активизируется плагин **TrafC**, позволяющий выделять в зависимости от вида запроса различные полосы пропускания и назначать пользователям квоты на объём принятой и переданной информации. Использовать или нет возможности плагина, определяется настройками соответствующих служб прокси-сервера. Начальное значение - **0**. | * & |
| **TrafCLists** | Расположение каталога со списками настройки ограничителя трафика. Начальное значение - **{PROXY[Lists]}\trafc**. | |
| **TrafCBandsList** | Список так называемых Band-каналов, задающих различные полосы пропускания. Этот список считывается один раз при запуске сервера. В дальнейшем список каналов поменять нельзя - можно только комбинировать, составляя из них для каждого запроса специфический набор каналов. Начальное значение - **{PROXY[TrafCLists]}\BandsList.txt**. | & |
| **TrafCQuotasList** | Список так называемых Quota-каналов, задающих различные квоты - ограничения на объём принимаемых или передаваемых данных в единицу времени. Этот список считывается один раз при запуске сервера. В дальнейшем список каналов поменять нельзя - можно только комбинировать, составляя из них для каждого запроса специфический набор каналов. Начальное значение - **{PROXY[TrafCLists]}\QuotasList.txt**. | & |
| **TrafCCanalsKitList** | Список именованных наборов каналов. Для удобства пользования часто используемые комбинации каналов можно сохранить в виде именованных наборов и в дальнейшем обращаться к ним по символическому имени. Начальное значение - **{PROXY[TrafCLists]}\CanalsKitList.txt**. | ? |
| **TrafCUserCanalsList** | Список назначения каналов для пользователей. Используется в качестве управляющего при обращении пользователей к web-интерфейсу Eserv с целью посмотреть статистику своей работы - на его основании определяется, статистику по каким именно каналам пользователь может просматривать. Начальное значение - **{PROXY[TrafCLists]}\UserCanalsList.txt**. | & |
| **UseCanalsCollect** | Указывает, собирать ли именные коллекции каналов автоматически. Если при запуске сервера этот параметр имеет ненулевое значение, загружается дополнительный модуль, который в процессе работы составляет списки каналов, выделяемых пользователям. Этот список впоследствии задействуется при пожелании пользователя посмотреть статистику своего пребывания в Сети через web-интерфейс PigMail+PigProxy. Начальное значение - **0**. | * & |
| **UseLogQPeriod** | Указывает, выполнять ли периодическое сохранение текущего состояния Quota-каналов на диск. Если значение нулевое, то сохранение не применяется. Начальное значение - **0**. | * & |

| | | |
|---|---|---|
| **LockIntruders** | Определяет, использовать ли блокировку атак. Признаком атаки считается частое повторение различных нежелательных событий - таких, как ошибки авторизации. Если частота следования таких событий для какого-либо IP-адреса клиентского подключения превышает установленную в настройках величину, то этот адрес заносится в список запрещённых сетей. IP-адреса, находящиеся в списках локальных или доверенных сетей, блокировке не подвергаются. Если при запуске сервера этот параметр имеет любое ненулевое значение, подключается плагин **ids_memo**, обеспечивающий хранение и накопление информации о нежелательных событиях. После этого параметр может использоваться для временного отключения блокировки атак, если его работа будет создавать какие-либо проблемы. Начальное значение - **{Server[LockIntruders]}**. | * |
| **AuthFailCount** | Пороговое значение числа ошибок авторизации. Если количество неудачных попыток авторизации за определённый временной интервал на одной из служб прокси-сервера для одного и того же IP-адреса клиентского подключения превышает заданную этим параметром величину, это считается атакой - со всеми вытекающими отрицательными последствиями для соответствующего клиента. Начальное значение - **{Server[AuthFailCount]}**. | * |
| **AuthFailPeriod** | Период подсчёта ошибок авторизации. Если количество неудачных попыток авторизации за определённый этим параметром временной интервал на одной из служб прокси-сервера для одного и того же IP-адреса клиентского подключения превышает заданную величину, это считается атакой - со всеми вытекающими отрицательными последствиями для соответствующего клиента. Длительность периода задаётся в минутах. Начальное значение - **{Server[AuthFailPeriod]}**. | * |
| **UseTarpit** | Указывает, использовать ли при выдаче отказов клиенту Tarpit - "липучку". В этом случае отрицательные ответы искусственно задерживаются, что уменьшает нагрузку на сеть. Начальное значение - **{Server[UseTarpit]}**. | * |
| **TarpitInterval** | Если задано использование "липучки", то этот параметр задаёт длительность задержки в секундах. Начальное значение - **{Server[TarpitInterval]}**. | * |
| **LogLevel** | Задаёт уровень детализации оперативных журналов прокси-сервера. Параметр может принимать значения от 1 до 9. Чем выше уровень, тем больше подробностей пишется в журнал. Для совместимости с ранними версиями, в которых уровень детализации не задавался, нулевое значение соответствует максимальному уровню детализации. Начальное значение - **{Server[LogLevel]}**. | |
| **LogAcl** | Указывает, вести ли дополнительный оперативный журнал обработки списков прав доступа. Если параметр имеет любое ненулевое значение, создаётся дополнительный журнал, в который записываются результаты сопоставления реквизитов пользователя и параметров запроса со списком прав доступа и предоставленные в результате права. Начальное значение - **1**. | * |
| **LogTrafC** | Указывает, вести ли дополнительный оперативный журнал ограничителя трафика TrafC. Если параметр имеет любое ненулевое значение, создаётся дополнительный журнал, в который записываются реквизиты запроса и параметры назначаемых для выполнения запроса каналов. Начальное значение - **1**. | * |
| **LogToEStat** | Определяет, ведёт ли сервер статистику в формате программы **Estat32**, разработанной **Андреем Волковым** из **EPE Labs** для обработки статистических журналов Eserv/2. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{Server[LogToEStat]}**. | |

| | | |
|---|---|---|
| **LogToAdvSoft** | Определяет, ведёт ли сервер статистику в формате программ **ProxyInspector** и **MailDetective** производства компании **AdvSoft**. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{Server[LogToAdvSoft]}**. | |
| **LogToElog** | Определяет, ведёт ли сервер статистику в формате программы **Elog**, разработанной **Игорем Панасенко** из компании **ЛЭНК** для обработки статистических журналов Eserv/3. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{Server[LogToElog]}**. | |
| **LogToMaillog** | Определяет, ведёт ли сервер статистику в собственном текстовом формате. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{Server[LogToMaillog]}**. | |
| **LogToMStat** | Определяет, используется ли подсистема ведения статистики в базе данных MStat, разработанная Андреем Матвеевым. Этот сборщик статистики имеет немалое преимущество перед текстовыми журналами, позволяя хранить и эффективно обрабатывать статистическую информацию за большие периоды времени, измеряемые годами. Но для его работы необходима установка дополнительного приложения - СУБД одного из поддерживаемых сборщиком типов. Если при запуске сервера указано любое ненулевое число, загружается специальный плагин **mstat**. В дальнейшем при возникновении проблем сбор статистики в базе данных можно временно отключить, установив нулевое значение. Начальное значение - **{Server[LogToMStat]}**. | & |

## *Секция HttpProxy - параметры настройки HTTP-прокси*

| | | |
|---|---|---|
| **DefaultAuthDomain** | Домен авторизации по умолчанию для HTTP-прокси. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[DefaultAuthDomain]}**. | $ |
| **DomainIP** | Файл со списком IP-адресов, назначенных сетевым интерфейсам компьютера. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[DomainIP]}**. | |
| **UserList** | Файл со списком пользователей формата Eserv/3 для HTTP-прокси. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[UserList]}**. | |
| **GroupList** | Файл со списком группировки пользователей формата Eserv/3 для HTTP-прокси. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[GroupList]}**. | |
| **PlainUserList** | Файл с объединённым списком пользователей формата Eserv/3 для HTTP-прокси. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[PlainUserList]}**. | ? |
| **PlainGroupList** | Файл со списком группировки пользователей формата Eserv/3 для HTTP-прокси. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[PlainGroupList]}**. | ? |
| **Eserv2Userlist** | Файл со списком пользователей HTTP-прокси, извлечённым из Eserv.ini версии Eserv/2.x. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[Eserv2Userlist]}**. | |

| | | |
|---|---|---|
| **Eserv2Grouplist** | Файл со списком группировки пользователей HTTP-прокси, извлечённым из Eserv.ini версии Eserv/2.x. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[Eserv2-Grouplist]}**. | |
| **NTdomain** | Имя домена Active Directory или локального компьютера под управлением Windows линейки NT, по списку пользователей которого выполняется авторизация пользователей HTTP-прокси, если выбран соответствующий способ авторизации (**NtLogon**). Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[NTdomain]}**. | ? |
| **DefaultAuthSource** | Имя источника авторизации на HTTP-прокси из списка источников авторизации. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[DefaultAuthSource]}**. | ? |
| **AuthMethod** | Способ авторизации на HTTP-прокси по умолчанию. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[AuthMethod]}**. | ? |
| **NtImpersonateLogon** | Определяет, требуется ли переключение в контекст безопасности пользователя при авторизации в домене Active Directory. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[NtImpersonateLogon]}**. | ? |
| **ExtendedGroupList** | Файл с расширенным списком группировки пользователей для HTTP-прокси. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[ExtendedGroupList]}**. | ? |
| **RejectNonexistentDomains** | Указывает, отвергать ли попытки авторизации, если домен авторизации не описан в настройках сервера. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[RejectNonexistentDomains]}**. | ? |
| **Active** | Определяет, активен ли HTTP-прокси. Если значение нулевое, то все попытки подключения отвергаются с кодом 4xx, что означает предложение повторить попытку позже. Если указано любое ненулевое число, сервер принимает подключения. Начальное значение - **1**. | |
| **Port** | Порт, на котором работает HTTP-прокси. Начальное значение стандартное - **3128**. | & |
| **NetworkInterface** | Адрес сетевого интерфейса, слушаемого сервером. Начальное значение - пустая строка; это означает, что сервер слушает все интерфейсы. | & |
| **Timeout** | Время бездействия, задаваемое в миллисекундах, по истечении которого сервер прекращает соединение с клиентом. Это вынужденная мера, предотвращающая утечку ресурсов при плохой связи - как правило, тайм-аут срабатывает, когда соединение уже фактически разорвано, но серверу неоткуда получить извещение об этом. Начальное значение - **30000**, что соответствует 5 минутам. | $ |
| **OutboundTimeout** | Время бездействия, задаваемое для соединений с внешними серверами. Начальное значение - **30000**, что соответствует 5 минутам. | $ |
| **ConnectTimeout** | Время бездействия до разрыва соединения с клиентом при методе доступа CONNECT, который используется при работе по защищённому соединению (SSL). Начальное значение - **30000**, что соответствует 5 минутам. | $ |
| **OutboundConnectTimeout** | Время бездействия, задаваемое для соединений с внешними серверами при методе доступа CONNECT, который используется при работе по защищённому соединению (SSL). Начальное значение - **30000**, что соответствует 5 минутам. | $ |
| **Lists** | Расположение каталога со списками настройки HTTP-прокси. Начальное значение - **{PROXY[Lists]}\httpp**. | |
| **Templates** | Расположение каталога с шаблонами сообщений HTTP-прокси. Начальное значение - **{PROXY[Templates]}\httpp**. | ? |

| | | |
|---|---|---|
| **Logs** | Расположение каталога оперативных журналов HTTP-прокси. Начальное значение - **{PROXY[Logs]}**. | $ |
| **MyIpList** | Список сетевых интерфейсов HTTP-прокси с указанием, на какие из этих интерфейсов серверу разрешено принимать подключения. Переопределяет соответствующий параметр из секции **PROXY**. Это важный элемент системы безопасности сервера, позволяющий разом отсечь множество заведомо чужих пользователей, поэтому настройке этого списка надо уделить максимум внимания. Начальное значение - **{PROXY[MyIpList]}**. | ? |
| **IpBlackList** | Список IP-адресов и подсетей, которым запрещено обращаться к HTTP-прокси. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[IpBlackList]}**. | ? |
| **LocalNetworks** | Список локальных сетей, обслуживаемых HTTP-прокси. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[LocalNetworks]}**. | ? |
| **IpWhiteList** | Список доверенных IP-адресов или сетей, которые обслуживаются этим HTTP-прокси. Переопределяет соответствующий параметр из секции **PROXY**. Этот список ДОПОЛНЯЕТ список локальных сетей. В нём могут быть не локальные сети, а, например, особые внешние IP-адреса. Начальное значение - **{PROXY[IpWhiteList]}**. | ? |
| **IpMacAuth** | Файл со списком, устанавливающим соответствие между IP и MAC адресами клиентского компьютера и именем учётной записи пользователя. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[IpMacAuth]}**. | ? |
| **IgnoreLocalNetworks** | Указывает, использовать ли при определении допустимости подключения список локальных сетей. Переопределяет соответствующий параметр из секции **PROXY**. Если в настройках сервера указан общий список локальных сетей, составленный излишне либерально с точки зрения безопасности прокси-сервера, его использование для управления доступом к прокси-серверу можно отключить, задав этому параметру любое ненулевое значение. Начальное значение - **{PROXY[IgnoreLocalNetworks]}**. | * ? |
| **UseIpAuth** | Указывает, использовать ли автоматическую авторизацию подключившегося пользователя на основании IP-адреса либо сочетания IP и MAC-адресов. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[UseIpAuth]}**. | * ? |
| **RequireAuth** | Указывает, является ли авторизация обязательной для работы с HTTP-прокси. Если задано любое ненулевое значение, то неавторизованные сессии запрещены. Начальное значение - **0**. | * ? |
| **AnonymousConnect** | Список хостов/портов, на которых разрешено анонимное (неавторизованное) подключение посредством метода CONNECT. Стандартно этот метод применяется для подключения по защищённому соединению (SSL). Однако сам по себе метод чрезвычайно универсален - даже слишком. Недаром его так полюбили спамеры и взломщики. Поскольку метод CONNECT позволяет организовать туннельное соединение по абсолютно произвольному протоколу, некорректно настроенный прокси-сервер легко превращается в открытый релей или инструмент взлома. Этот список применяется в качестве минимальной меры защиты, если не используются полнофункциональные списки прав доступа - иначе считается, что все настройки безопасности прописаны там. Начальное значение - **{HttpProxy[Lists]}\AnonymousConnect.txt**. | ? |
| **LocalReplyList** | Список шаблонов HTML-страниц, которые сервер выдаёт клиентам в качестве ответа в различных ситуациях - при отказе в выполнении запроса и при обнаружении ошибок. Шаблоны можно настраивать по своему усмотрению или заменять своими. Начальное значение - **{HttpProxy[Lists]}\LocalReplyList.txt**. | ? |

| | | |
|---|---|---|
| **LocalReplyStyles** | Расположение файла, содержащего таблицу HTML-стилей, включаемую в ответы сервера. Путём редактирования этой таблицы Вы можете изменить внешний вид всех ответов, не затрагивая содержимого. Начальное значение - **{HttpProxy[Templates]}\LocalReplyStyles.css**. | ? |
| **UseAliasing** | Указывает, использовать ли алиасинг. Механизм алиасинга позволяет вместо часто используемых длинных и замысловатых ссылок вводить в строке адреса короткие псевдонимы (например, **ya** вместо **http://www.yandex.ru/**) - прокси-сервер их распознает и перенаправит браузер по нужному адресу. Если при запуске сервера этот параметр имеет ненулевое значение, загружается специальный плагин, обеспечивающий поддержку алиасов. В дальнейшем при возникновении проблем алиасинг можно временно отключить, задав нулевое значение. Начальное значение - **0**. | * & ? |
| **UrlAlias** | Список алиасов и соответствующих им реальных адресов. Начальное значение - **{HttpProxy[Lists]}\UrlAlias.txt**. | ? |
| **UseRedirector** | Указывает, использовать ли перенаправитель. Механизм перенаправления подобен алиасингу. Основное отличие состоит в том, что сравнение с образцом выполняется с учётом всех составляющих ссылки - протокола, имени целевого узла, номера порта, логического пути, - кроме того, перенаправление может выполняться по-разному в зависимости от пользователя, времени суток и других условий. Если при запуске сервера этот параметр имеет ненулевое значение, загружается специальный плагин, обеспечивающий поддержку перенаправления. В дальнейшем при возникновении проблем перенаправление можно временно отключить, задав нулевое значение. Начальное значение - **0**. | * & ? |
| **UrlRedirect** | Список перенаправляемых ссылок. Начальное значение - **{HttpProxy[Lists]}\UrlRedirect.txt**. | ? |
| **UseAcls** | Указывает, использовать ли списки контроля доступа к внешним серверам. С помощью этих списков можно различным образом блокировать доступ к нежелательным web-ресурсам (используя либо безоговорочный запрет, либо "прозрачную" подмену рекламных страниц) и раздавать именные разрешения или запреты на обращения к web-ресурсам (с использованием авторизации). Если при запуске сервера этот параметр имеет ненулевое значение, загружается специальный плагин **acl**, обеспечивающий поддержку списков доступа. В дальнейшем при возникновении проблем обработку списков доступа можно временно отключить, задав нулевое значение. Начальное значение - **1**. | * & ? |
| **ConstrainTraffic** | Указывает, использовать ли управление трафиком (ограничитель TrafC) для HTTP-прокси. Если загружены плагины **TrafC** и **acl**, и предыдущий параметр имеет ненулевое значение, то при ненулевом значении этого параметра в случае разрешения пользователю доступа к внешним ресурсам производится выделение полосы пропускания и квоты на объём принятой и переданной информации - в зависимости от вида запроса. Если работа ограничителя трафика создаёт проблемы, его можно в любой момент отключить, задав нулевое значение. Начальное значение - **{PROXY[ConstrainTraffic]}**. | * ? |
| **ACL** | Главный список прав доступа. Списков может быть сколько угодно - они могут вызываться по цепочке, - но главный список, с которого начинается обработка, всегда один. Начальное значение - **{HttpProxy[Lists]}\ACL.txt**. | ? |
| **DefaultRealm** | Имя зоны безопасности - Realm, - используемое в запросе сервера на авторизацию, если другое имя не было задано в списке управления доступом. Начальное значение - **{HttpProxy[DefaultAuthDomain]}**. | * ? |

| | | |
|---|---|---|
| **DefaultAclAction** | Действие, которое следует применить, если его не удалось определить при анализе списка. Если действие имеет параметр, он записывается здесь же через пробел. Действие задаётся двухсимвольным кодом и может быть одним из следующих:<br>**AU** (Authorization) - задать режим запроса авторизации. Возможным, но не обязательным, параметром является имя зоны безопасности (Realm), которое следует указать в запросе авторизации;<br>**NF** (Not Found) - задать режим безусловной блокировки доступа;<br>**DI** (Disable) - задать режим безусловной блокировки доступа;<br>**BA** (Block Advertisement) - задать режим блокировки рекламы;<br>**AD** (Advertisement Disabled) - задать режим блокировки рекламы;<br>**EN** (Enable) - задать режим разрешения доступа. Возможным, но не обязательным, параметром является перечень каналов, выделяемых для выполнения запроса;<br>**LI** (List) - выполнить обработку вложенного списка. Обязательным параметром является имя файла списка;<br>**RU** (Rule) - выполнить правило. Обязательным параметром является имя встроенного или внешнего правила.<br>Начальное значение - **EN**, действие, разрешающее доступ без назначения каналов. | *<br>? |
| **DefaultTrafCPriority** | Этот параметр задаёт приоритет для назначаемого по умолчанию (в случае выбора действия **EN**) набора каналов. Приоритет задаётся числом, чем оно меньше, тем выше приоритет; наивысшему приоритету соответствует нулевое значение. Возможные значения:<br>**пусто** - используется значение приоритета, вычисленное при анализе списка правил;<br>**+nnn** - приоритет, вычисленный при анализе списка правил, понижается на nnn пунктов;<br>**-nnn** - приоритет, вычисленный при анализе списка правил, повышается на nnn пунктов;<br>**nnn** - приоритет устанавливается ровно на nnn пунктов.<br>Начальное значение - пустая строка. | ? |
| **UseHttpAutoLogon** | Указывает, использовать ли автоматическую авторизацию по протоколу HTTP на целевых серверах. Иногда это бывает полезно, если требуется обеспечить доступ некоторой группы пользователей к защищённому паролем ресурсу, не раскрывая сам пароль. Это возможно, если для доступа к ресурсу используется незащищённое соединение по протоколу HTTP. Целевой сервер должен поддерживать метод авторизации **Basic**. Если при запуске сервера этот параметр имеет любое ненулевое значение, загружается специальный плагин. В дальнейшем при возникновении проблем автоматическую авторизацию можно временно отключить, задав нулевое значение. Начальное значение - **0**. | *<br>&<br>? |
| **HttpAutoLogon** | Список управления автоматической авторизацией. Начальное значение - **{HttpProxy[Lists]}\HttpAutoLogon.txt**. | ? |
| **CascadeProxy** | Указывает, использовать ли каскадирование HTTP-прокси-серверов. Если для выхода в интернет используется не один прокси-сервер, они должны быть организованы в цепочку. Если при запуске сервера этот параметр имеет ненулевое значение, загружается специальный плагин, обеспечивающий поддержку каскадирования. В дальнейшем при возникновении проблем каскадирование можно временно отключить, задав нулевое значение. Начальное значение - **0**. | *<br>&<br>? |
| **CascadeList** | Список управления каскадированием. Начальное значение - **{HttpProxy[Lists]}\CascadeList.txt**. | ? |
| **UseDefaultCascade** | Указывает, использовать ли каскадирование в случае, когда не удалось определить вышестоящий прокси-сервер на основании списка. Если параметр имеет ненулевое значение, то по умолчанию также используется цепочка прокси-серверов. Начальное значение - **0**. | *<br>? |

| | | |
|---|---|---|
| **DefaultCascadeHost** | Если используется каскадирование по умолчанию, то этот параметр задаёт имя или адрес вышестоящего прокси-сервера. Начальное значение - пустая строка. | * ? |
| **DefaultCascadePort** | Если используется каскадирование по умолчанию, то этот параметр задаёт порт, на котором работает вышестоящий прокси-сервер. Начальное значение - **0**. | * ? |
| **DefaultCascadeUser** | Если используется каскадирование по умолчанию, то этот параметр задаёт имя пользователя на тот случай, если вышестоящий прокси-сервер требует авторизацию. Естественно, это должно быть имя пользователя именно вышестоящего прокси-сервера. Начальное значение - пустая строка. Если авторизация не требуется, имя пользователя задавать не надо. | * ? |
| **DefaultCascadePass** | Если используется каскадирование по умолчанию, то этот параметр задаёт пароль пользователя на тот случай, если вышестоящий прокси-сервер требует авторизацию. Начальное значение - пустая строка. Если авторизация не требуется, пароль задавать не надо. | * ? |
| **DefaultAllowDirect** | Если используется каскадирование по умолчанию, то этот параметр указывает, использовать ли прямое обращение в случае неудачи подключения через вышестоящий прокси-сервер - например, если вышестоящий прокси-сервер недоступен или не допускает соединение с целевым сервером. Иногда организация сети допускает такие трюки, хотя и ценой существенного снижения скорости обмена данными. Начальное значение - **1**. | * ? |
| **CacheContent** | Указывает, использовать ли локальный (на прокси-сервере) файловый кэш для хранения копий загруженных из Сети HTML-страниц, изображений, сценариев и других объектов. Применение кэширования позволяет ускорить загрузку страниц и снижает объём платного трафика, хотя в нынешней ситуации, когда почти все сайты имеют динамическую организацию, ожидать радикального изменения ситуации от использования кэша не следует. Если при запуске сервера этот параметр имеет ненулевое значение, загружается специальный плагин, обеспечивающий поддержку кэширования. В дальнейшем при возникновении проблем кэширование можно временно отключить, задав нулевое значение. Начальное значение - **1**. | * & ? |
| **CacheModeList** | Список управления режимами кэширования для различных объектов. Начальное значение - **{HttpProxy[Lists]}\CacheModeList.txt**. | ? |
| **DefaultCacheMode** | Режим кэширования, который следует применить, если его не удалось определить при анализе списка:<br>**SM** (Standard Mode) - стандартный режим: при каждом обращении производится проверка наличия изменений объекта;<br>**MT** (Minimize Traffic) - минимизация трафика: если объект уже находится в кэше, то факт его изменения не проверяется;<br>**NC** (Not Cached) - кэширование не используется;<br>**CO** (Check if Older) - наличие изменений проверяется, если объект хранится в кэше дольше, чем определённое следующим параметром число дней;<br>**CH** (Check if Hours older) - наличие изменений проверяется, если объект хранится в кэше дольше, чем определённое следующим параметром число часов.<br>Начальное значение - **SM**. | * ? |

| | | |
|---|---|---|
| **DefaultMaxCacheAge** | Если по умолчанию задан режим кэширования **CO** или **CH**, ориентирующийся на "возраст" хранимого в кэше объекта, то этот параметр задаёт предельный срок хранения до обновления объекта. Для режима **CO** возраст задаётся в сутках, 0 означает объект, хранящийся менее суток. Для режима **CH** возраст задаётся в часах, 0 означает объект, хранящийся менее часа. Начальное значение - **0**, что означает безусловное доверие только к "свежим" объектам. | * ? |
| **UseAntivirus** | Указывает, использовать ли антивирус. Если этот параметр при запуске сервера имеет ненулевое значение, то загружаются соответствующие плагины, после этого антивирусную проверку можно отключать и включать динамически. Начальное значение - **0**, то есть, антивирус не используется. | * & ? |
| **Antivirus** | Указывает, какой именно антивирус использовать. В настоящее время можно выбирать между DrWeb (**http://www.drweb.com/**) и KAV либо KAV5 (**http://www.kaspersky.ru/**). В настоящее время полноценная антивирусная проверка объектов в процессе загрузки возможна только при использовании антивирусов KAV и KAV5. Переключение активного антивируса "на лету" не предусмотрено, выбор производится при запуске прокси-сервера. Начальное значение - **KAV**. | * & |
| **AVScanList** | Список управления антивирусной проверкой. На маломощных машинах работа антивируса может оказаться параметром, ограничивающим скорость загрузки. Для ряда объектов (или заведомо надёжных web-ресурсов) проверка может быть отключена, что снизит нагрузку на процессор прокси-сервера и повысит его производительность. Начальное значение - **{HttpProxy[Lists]}\AVScanList.txt**. | ? |
| **UseSpyLog** | Указывает, использовать ли выборочное слежение за пользовательскими запросами. Эта специфическая возможность предусмотрена для нужд разработчиков web-приложений и сотрудников служб собственной безопасности, которым по долгу службы необходим подробный анализ содержимого клиентских запросов. Данные запросов, подлежащих анализу, записываются в особый журнал. Если при запуске сервера этот параметр имеет ненулевое значение, загружается специальный плагин, реализующий функции слежения. В дальнейшем при возникновении проблем слежение можно временно отключить, задав нулевое значение. Начальное значение - **0**. | * & ? |
| **SpyLogControl** | Список управления слежением, определяющий, какие сайты и разделы и на каких условиях подлежат подробному отслеживанию. Этот список также позволяет отсеять лишнюю информацию, задав перечень полей запросов, подлежащих записи в журнал. Начальное значение - **{HttpProxy[Lists]}\SpyLogControl.txt**. | ? |
| **SpyLogTemplate** | Шаблон имени файла журнала. Используя различные макросы, можно разносить данные по целой серии журналов в зависимости от даты, имени целевого узла, параметров авторизации пользователя. Начальное значение - **{Dirs[Data]}\spylog\{YYYYMMDD}HTTPP.log**. | |
| **LockIntruders** | Определяет, использовать ли блокировку атак. Признаком атаки считается частое повторение различных нежелательных событий - таких, как ошибки авторизации. Если частота следования таких событий для какого-либо IP-адреса клиентского подключения превышает установленную в настройках величину, то этот адрес заносится в список запрещённых сетей. IP-адреса, находящиеся в списках локальных или доверенных сетей, блокировке не подвергаются. Если при запуске сервера этот параметр имеет любое ненулевое значение, подключается плагин **ids_memo**, обеспечивающий хранение и накопление информации о нежелательных событиях. После этого параметр может использоваться для временного отключения блокировки атак, если его работа будет создавать какие-либо проблемы. Начальное значение - **{PROXY[LockIntruders]}**. | * ? |

| | | |
|---|---|---|
| **AuthFailCount** | Пороговое значение числа ошибок авторизации. Если количество неудачных попыток авторизации за определённый временной интервал для одного и того же IP-адреса клиентского подключения превышает заданную этим параметром величину, это считается атакой - со всеми вытекающими отрицательными последствиями для соответствующего клиента. Начальное значение - **{PROXY[AuthFailCount]}**. | * ? |
| **AuthFailPeriod** | Период подсчёта ошибок авторизации. Если количество неудачных попыток авторизации за определённый этим параметром временной интервал для одного и того же IP-адреса клиентского подключения превышает заданную величину, это считается атакой - со всеми вытекающими отрицательными последствиями для соответствующего клиента. Длительность периода задаётся в минутах. Начальное значение - **{PROXY[AuthFailPeriod]}**. | * ? |
| **UseTarpit** | Указывает, использовать ли при выдаче отказов клиенту Tarpit - "липучку". В этом случае отрицательные ответы искусственно задерживаются, что уменьшает нагрузку на сеть. Начальное значение - **{PROXY[UseTarpit]}**. | * ? |
| **TarpitInterval** | Если задано использование "липучки", то этот параметр задаёт длительность задержки в секундах. Начальное значение - **{PROXY[TarpitInterval]}**. | * ? |
| **LogLevel** | Задаёт уровень детализации оперативного журнала HTTP-прокси. Параметр может принимать значения от 1 до 9. Чем выше уровень, тем больше подробностей пишется в журнал. Для совместимости с ранними версиями, в которых уровень детализации не задавался, нулевое значение соответствует максимальному уровню детализации. Начальное значение - **{PROXY[LogLevel]}**. | $ |
| **LogAcl** | Указывает, вести ли дополнительный оперативный журнал обработки списков прав доступа. Если параметр имеет любое ненулевое значение, создаётся дополнительный журнал, в который записываются результаты сопоставления реквизитов пользователя и параметров запроса со списком прав доступа и предоставленные в результате права. Начальное значение - **{PROXY[LogAcl]}**. | ? |
| **LogTrafC** | Указывает, вести ли дополнительный оперативный журнал ограничителя трафика TrafC. Если параметр имеет любое ненулевое значение, создаётся дополнительный журнал, в который записываются реквизиты запроса и параметры назначаемых для выполнения запроса каналов. Начальное значение - **{PROXY[LogTrafC]}**. | ? |
| **LogAVEvents** | Указывает, вести ли дополнительный оперативный журнал работы антивируса. Если параметр имеет любое ненулевое значение, создаётся дополнительный журнал, в который записываются результаты антивирусной проверки загруженных объектов. Начальное значение - **1**. | * $ |
| **LogAVOkEvents** | Если ведётся дополнительный оперативный журнал работы антивируса, то этот параметр указывает, записывать ли в него информацию о кэшированных объектах, в которых вредоносный код не обнаружен. Запись ведётся при любом ненулевом значении. Отметки об успешных проверках объектов непосредственно в оперативной памяти в журнал не записываются. Начальное значение - **0**. | * $ |
| **LogToEStat** | Определяет, ведёт ли сервер статистику в формате программы **Estat32**, разработанной **Андреем Волковым** из **EPE Labs** для обработки статистических журналов Eserv/2. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{PROXY[LogToEStat]}**. | $ |

| | | |
|---|---|---|
| **LogToAdvSoft** | Определяет, ведёт ли сервер статистику в формате программ **ProxyInspector** и **MailDetective** производства компании **AdvSoft**. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{PROXY[LogToAdvSoft]}**. | $ |
| **LogToElog** | Определяет, ведёт ли сервер статистику в формате программы **Elog**, разработанной **Игорем Панасенко** из компании **ЛЭНК** для обработки статистических журналов Eserv/3. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{PROXY[LogToElog]}**. | $ |
| **LogToMaillog** | Определяет, ведёт ли сервер статистику в собственном текстовом формате. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{PROXY[LogToMaillog]}**. | $ |
| **LogToMStat** | Определяет, используется ли подсистема ведения статистики в базе данных MStat, разработанная Андреем Матвеевым. Этот сборщик статистики имеет немалое преимущество перед текстовыми журналами, позволяя хранить и эффективно обрабатывать статистическую информацию за большие периоды времени, измеряемые годами. Но для его работы необходима установка дополнительного приложения - СУБД одного из поддерживаемых сборщиком типов. Если указано любое ненулевое число, статистика в базе данных ведётся. Начальное значение - **{PROXY[LogToMStat]}**. | $ |

## *Секция FtpProxy - параметры настройки FTP-прокси*

| | | |
|---|---|---|
| **DefaultAuthDomain** | Домен авторизации по умолчанию для FTP-прокси. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[DefaultAuthDomain]}**. | $ |
| **DomainIP** | Файл со списком IP-адресов, назначенных сетевым интерфейсам компьютера. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[DomainIP]}**. | |
| **UserList** | Файл со списком пользователей формата Eserv/3 для FTP-прокси. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[UserList]}**. | |
| **GroupList** | Файл со списком группировки пользователей формата Eserv/3 для FTP-прокси. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[GroupList]}**. | |
| **PlainUserList** | Файл с объединённым списком пользователей формата Eserv/3 для FTP-прокси. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[PlainUserList]}**. | ? |
| **PlainGroupList** | Файл со списком группировки пользователей формата Eserv/3 для FTP-прокси. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[PlainGroupList]}**. | ? |
| **Eserv2Userlist** | Файл со списком пользователей FTP-прокси, извлечённым из Eserv.ini версии Eserv/2.x. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[Eserv2Userlist]}**. | |

| | | |
|---|---|---|
| **Eserv2Grouplist** | Файл со списком группировки пользователей FTP-прокси, извлечённым из Eserv.ini версии Eserv/2.x. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[Eserv2-Grouplist]}**. | |
| **NTdomain** | Имя домена Active Directory или локального компьютера под управлением Windows линейки NT, по списку пользователей которого выполняется авторизация пользователей FTP-прокси, если выбран соответствующий способ авторизации (**NtLogon**). Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[NTdomain]}**. | ? |
| **DefaultAuthSource** | Имя источника авторизации на FTP-прокси из списка источников авторизации. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[DefaultAuthSource]}**. | ? |
| **AuthMethod** | Способ авторизации на FTP-прокси по умолчанию. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[AuthMethod]}**. | ? |
| **NtImpersonateLogon** | Определяет, требуется ли переключение в контекст безопасности пользователя при авторизации в домене Active Directory. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[NtImpersonateLogon]}**. | |
| **ExtendedGroupList** | Файл с расширенным списком группировки пользователей для FTP-прокси. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[ExtendedGroupList]}**. | ? |
| **RejectNonexistentDomains** | Указывает, отвергать ли попытки авторизации, если домен авторизации не описан в настройках сервера. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[RejectNonexistentDomains]}**. | ? |
| **MaxAuthAttempts** | Максимально допустимое число попыток протокольной (не по IP/MAC-адресу) авторизации в одной сессии. Параметр относится к авторизации на прокси-сервере, а не на целевом узле. Определяет, сколько неудачных попыток авторизации допускается в течение одной сессии. Если это число превышено, подключение считается атакой и разрывается. Если значение нулевое, то ограничения на число попыток подбора пароля отсутствуют. Начальное значение - **{PROXY[MaxAuthAttempts]}**. | ? |
| **AuthDelimiter** | FTP-прокси использует несколько непривычную схему авторизации, при которой реквизиты авторизации на целевом сервере и на прокси передаются клиентом в одном "слове" - два логина в протокольной команде USER и два пароля в команде PASS. Параметр задаёт уникальную последовательность символов, используемую в качестве разделителя, слева от которого располагаются реквизиты авторизации на целевом сервере, а справа - на прокси. Начальное значение - **#**. | $ |
| **Active** | Определяет, активен ли FTP-прокси. Если значение нулевое, то все попытки подключения отвергаются с кодом 4xx, что означает предложение повторить попытку позже. Если указано любое ненулевое число, сервер принимает подключения. Начальное значение - **1**. | |
| **Port** | Порт, на котором работает FTP-прокси. Начальное значение стандартное - **3121**. | & |
| **NetworkInterface** | Адрес сетевого интерфейса, слушаемого сервером. Начальное значение - пустая строка; это означает, что сервер слушает все интерфейсы. | & |
| **Timeout** | Время бездействия, задаваемое в миллисекундах, по истечении которого сервер прекращает соединение с клиентом. Это вынужденная мера, предотвращающая утечку ресурсов при плохой связи - как правило, тайм-аут срабатывает, когда соединение уже фактически разорвано, но серверу неоткуда получить извещение об этом. Начальное значение - **60000**, что соответствует 10 минутам. | $ |
| **OutboundTimeout** | Время бездействия, задаваемое для соединений с внешними серверами. Начальное значение - **30000**, что соответствует 5 минутам. | $ |

| | | |
|---|---|---|
| **Lists** | Расположение каталога со списками настройки FTP-прокси. Начальное значение - **{PROXY[Lists]}\ftpp**. | |
| **Templates** | Расположение каталога с шаблонами сообщений FTP-прокси. Начальное значение - **{PROXY[Templates]}\ftpp**. | |
| **Logs** | Расположение каталога оперативных журналов FTP-прокси. Начальное значение - **{PROXY[Logs]}**. | $ |
| **MyIpList** | Список сетевых интерфейсов FTP-прокси с указанием, на какие из этих интерфейсов серверу разрешено принимать подключения. Переопределяет соответствующий параметр из секции **PROXY**. Это важный элемент системы безопасности сервера, позволяющий разом отсечь множество заведомо чужих пользователей, поэтому настройке этого списка надо уделить максимум внимания. Начальное значение - **{PROXY[MyIpList]}**. | |
| **IpBlackList** | Список IP-адресов и подсетей, которым запрещено обращаться к FTP-прокси. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[IpBlackList]}**. | |
| **LocalNetworks** | Список локальных сетей, обслуживаемых FTP-прокси. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[LocalNetworks]}**. | |
| **IpWhiteList** | Список доверенных IP-адресов или сетей, которые обслуживаются этим FTP-прокси. Переопределяет соответствующий параметр из секции **PROXY**. Этот список ДОПОЛНЯЕТ список локальных сетей. В нём могут быть не локальные сети, а, например, особые внешние IP-адреса. Начальное значение - **{PROXY[IpWhiteList]}**. | |
| **IpMacAuth** | Файл со списком, устанавливающим соответствие между IP и MAC адресами клиентского компьютера и именем учётной записи пользователя. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[IpMacAuth]}**. | |
| **IgnoreLocalNetworks** | Указывает, использовать ли при определении допустимости подключения список локальных сетей. Переопределяет соответствующий параметр из секции **PROXY**. Если в настройках сервера указан общий список локальных сетей, составленный излишне либерально с точки зрения безопасности прокси-сервера, его использование для управления доступом к прокси-серверу можно отключить, задав этому параметру любое ненулевое значение. Начальное значение - **{PROXY[IgnoreLocalNetworks]}**. | * |
| **UseIpAuth** | Указывает, использовать ли автоматическую авторизацию подключившегося пользователя на основании IP-адреса либо сочетания IP и MAC-адресов. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[UseIpAuth]}**. | * |
| **RequireAuth** | Указывает, является ли авторизация обязательной для работы с FTP-прокси. Если задано любое ненулевое значение, то неавторизованные сессии запрещены. Начальное значение - **0**. | * ? |
| **HostBlackList** | Список серверов, подключение к которым запрещено. Начальное значение - **{FtpProxy[Lists]}\HostBlackList.txt**. | |
| **HostWhiteList** | Список серверов, подключение к которым разрешено. Этот список перекрывает список запретов, поэтому можно запрещать целые группы серверов, разрешая доступ к некоторым серверам из запрещённой группы. Дополнительно этот список позволяет индивидуально для каждого целевого сервера определить, использовать ли при работе с ним пассивный режим. Начальное значение - **{FtpProxy[Lists]}\HostWhiteList.txt**. | |

| | | |
|---|---|---|
| **BindIpList** | Список управления привязкой IP-адресов при установлении соединения для передачи данных. Особенность протокола FTP заключается в том, что для обмена данными (загрузка файла или чтение FTP-каталога) требуется установить дополнительное соединение. При этом одна из сторон сообщает свой IP-адрес. FTP-прокси может быть такой стороной в двух случаях - если клиент выбрал пассивный режим соединения с прокси-сервером либо если в настройках самого FTP-прокси не выбран пассивный режим работы с целевыми серверами. Обычно прокси-сервер самостоятельно определяет адрес для объявления, однако при некоторых конфигурациях сети (например, наличие NAT-сервера на одном из направлений), он может выбрать неверное значение - просто потому, что реальный адрес, видимый со стороны соединения, отличается от адреса сетевого интерфейса и прокси-серверу неизвестен. Если IP-адрес клиента или целевого сервера не принадлежат локальной сети, FTP-прокси использует адрес, определённый параметром **Server[ExternIP]**. В базовых конфигурациях, когда имеется всего две сетевые карты, одна из которых подключена к локальной сети, а вторая обеспечивает непосредственный выход в глобальную сеть, этого достаточно. Если сетевых интерфейсов больше двух либо используются сложные правила маршрутизации, необходимы сложные же правила выбора объявляемого IP-адреса, записываемые в список управления привязкой. Начальное значение - **{FtpProxy[Lists]}\BindIpList.txt**. | ? |
| **UsePASV** | Указывает, использовать ли при работе с внешними FTP-серверами пассивный режим (режим работы FTP-прокси с клиентом определяет сам клиент). Если параметр имеет любое ненулевое значение, связь с внешними серверами осуществляется в пассивном режиме. Этот режим является рекомендуемым, поскольку он совместим как с различными средствами защиты (NAT, брандмауэры), так и с настройками некоторых FTP-серверов. Начальное значение - **1**. | *<br>$ |
| **UseAcls** | Указывает, использовать ли списки контроля доступа к внешним серверам. С помощью этих списков можно раздавать именные разрешения или запреты на обращения к запрашиваемым ресурсам (с использованием авторизации). Если при запуске сервера этот параметр имеет ненулевое значение, загружается специальный плагин **acl**, обеспечивающий поддержку списков доступа. В дальнейшем при возникновении проблем обработку списков доступа можно временно отключить, задав нулевое значение. Начальное значение - **1**. | *<br>&<br>? |
| **ConstrainTraffic** | Указывает, использовать ли управление трафиком (ограничитель TrafC) для FTP-прокси. Если загружены плагины **TrafC** и **acl**, и предыдущий параметр имеет ненулевое значение, то при ненулевом значении этого параметра в случае разрешения пользователю доступа к внешним ресурсам производится выделение полосы пропускания и квоты на объём принятой и переданной информации - в зависимости от вида запроса. Если работа ограничителя трафика создаёт проблемы, его можно в любой момент отключить, задав нулевое значение. Начальное значение - **{PROXY[ConstrainTraffic]}**. | *<br>? |
| **ACL** | Главный список прав доступа. Списков может быть сколько угодно - они могут вызываться по цепочке, - но главный список, с которого начинается обработка, всегда один. Начальное значение - **{FtpProxy[Lists]}\ACL.txt**. | ? |

| | | |
|---|---|---|
| **DefaultAclAction** | Действие, которое следует применить, если его не удалось определить при анализе списка. Если действие имеет параметр, он записывается здесь же через пробел. Действие задаётся двухсимвольным кодом и может быть одним из следующих:<br>**DI** (Disable) - задать режим безусловной блокировки доступа;<br>**EN** (Enable) - задать режим разрешения доступа. Возможным, но не обязательным, параметром является перечень каналов, выделяемых для выполнения запроса;<br>**LI** (List) - выполнить обработку вложенного списка. Обязательным параметром является имя файла списка;<br>**RU** (Rule) - выполнить правило. Обязательным параметром является имя встроенного или внешнего правила.<br>Начальное значение - **EN**, действие, разрешающее доступ без назначения каналов. | *<br>? |
| **DefaultTrafCPriority** | Этот параметр задаёт приоритет для назначаемого по умолчанию (в случае выбора действия **EN**) набора каналов. Приоритет задаётся числом, чем оно меньше, тем выше приоритет; наивысшему приоритету соответствует нулевое значение. Возможные значения:<br>**пусто** - используется значение приоритета, вычисленное при анализе списка правил;<br>**+nnn** - приоритет, вычисленный при анализе списка правил, понижается на nnn пунктов;<br>**-nnn** - приоритет, вычисленный при анализе списка правил, повышается на nnn пунктов;<br>**nnn** - приоритет устанавливается ровно на nnn пунктов.<br>Начальное значение - пустая строка. | ? |
| **LockIntruders** | Определяет, использовать ли блокировку атак. Признаком атаки считается частое повторение различных нежелательных событий - таких, как ошибки авторизации. Если частота следования таких событий для какого-либо IP-адреса клиентского подключения превышает установленную в настройках величину, то этот адрес заносится в список запрещённых сетей. IP-адреса, находящиеся в списках локальных или доверенных сетей, блокировке не подвергаются. Если при запуске сервера этот параметр имеет любое ненулевое значение, подключается плагин **ids_memo**, обеспечивающий хранение и накопление информации о нежелательных событиях. После этого параметр может использоваться для временного отключения блокировки атак, если его работа будет создавать какие-либо проблемы. Начальное значение - **{PROXY[LockIntruders]}**. | *<br>? |
| **AuthFailCount** | Пороговое значение числа ошибок авторизации. Если количество неудачных попыток авторизации за определённый временной интервал для одного и того же IP-адреса клиентского подключения превышает заданную этим параметром величину, это считается атакой - со всеми вытекающими отрицательными последствиями для соответствующего клиента. Начальное значение - **{PROXY[AuthFailCount]}**. | *<br>? |
| **AuthFailPeriod** | Период подсчёта ошибок авторизации. Если количество неудачных попыток авторизации за определённый этим параметром временной интервал для одного и того же IP-адреса клиентского подключения превышает заданную величину, это считается атакой - со всеми вытекающими отрицательными последствиями для соответствующего клиента. Длительность периода задаётся в минутах. Начальное значение - **{PROXY[AuthFailPeriod]}**. | *<br>? |
| **UseTarpit** | Указывает, использовать ли при выдаче отказов клиенту Tarpit - "липучку". В этом случае отрицательные ответы искусственно задерживаются, что уменьшает нагрузку на сеть. Начальное значение - **{PROXY[UseTarpit]}**. | *<br>? |
| **TarpitInterval** | Если задано использование "липучки", то этот параметр задаёт длительность задержки в секундах. Начальное значение - **{PROXY[TarpitInterval]}**. | *<br>? |

| | | |
|---|---|---|
| **LogLevel** | Задаёт уровень детализации оперативного журнала FTP-прокси. Параметр может принимать значения от 1 до 9. Чем выше уровень, тем больше подробностей пишется в журнал. Для совместимости с ранними версиями, в которых уровень детализации не задавался, нулевое значение соответствует максимальному уровню детализации. Начальное значение - **{PROXY[LogLevel]}**. | $ |
| **LogAcl** | Указывает, вести ли дополнительный оперативный журнал обработки списков прав доступа. Если параметр имеет любое ненулевое значение, создаётся дополнительный журнал, в который записываются результаты сопоставления реквизитов пользователя и параметров запроса со списком прав доступа и предоставленные в результате права. Начальное значение - **{PROXY[LogAcl]}**. | ? |
| **LogTrafC** | Указывает, вести ли дополнительный оперативный журнал ограничителя трафика TrafC. Если параметр имеет любое ненулевое значение, создаётся дополнительный журнал, в который записываются реквизиты запроса и параметры назначаемых для выполнения запроса каналов. Начальное значение - **{PROXY[LogTrafC]}**. | ? |
| **LogToEStat** | Определяет, ведёт ли сервер статистику в формате программы **Estat32**, разработанной **Андреем Волковым** из **EPE Labs** для обработки статистических журналов Eserv/2. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{PROXY[LogToEStat]}**. | $ |
| **LogToAdvSoft** | Определяет, ведёт ли сервер статистику в формате программ **ProxyInspector** и **MailDetective** производства компании **AdvSoft**. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{PROXY[LogToAdvSoft]}**. | $ |
| **LogToElog** | Определяет, ведёт ли сервер статистику в формате программы **Elog**, разработанной **Игорем Панасенко** из компании **ЛЭНК** для обработки статистических журналов Eserv/3. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{PROXY[LogToElog]}**. | $ |
| **LogToMaillog** | Определяет, ведёт ли сервер статистику в собственном текстовом формате. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{PROXY[LogToMaillog]}**. | $ |
| **LogToMStat** | Определяет, используется ли подсистема ведения статистики в базе данных MStat, разработанная Андреем Матвеевым. Этот сборщик статистики имеет немалое преимущество перед текстовыми журналами, позволяя хранить и эффективно обрабатывать статистическую информацию за большие периоды времени, измеряемые годами. Но для его работы необходима установка дополнительного приложения - СУБД одного из поддерживаемых сборщиком типов. Если указано любое ненулевое число, статистика в базе данных ведётся. Начальное значение - **{PROXY[LogToMStat]}**. | $ |

## *Секция SocksProxy - параметры настройки Socks-прокси*

| | | |
|---|---|---|
| **DefaultAuthDomain** | Домен авторизации по умолчанию для Socks-прокси. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[DefaultAuthDomain]}**. | $ |
| **DomainIP** | Файл со списком IP-адресов, назначенных сетевым интерфейсам компьютера. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[DomainIP]}**. | |
| **UserList** | Файл со списком пользователей формата Eserv/3 для Socks-прокси. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[UserList]}**. | |
| **GroupList** | Файл со списком группировки пользователей формата Eserv/3 для Socks-прокси. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[GroupList]}**. | |
| **PlainUserList** | Файл с объединённым списком пользователей формата Eserv/3 для Socks-прокси. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[PlainUserList]}**. | |
| **PlainGroupList** | Файл со списком группировки пользователей формата Eserv/3 для Socks-прокси. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[PlainGroupList]}**. | |
| **Eserv2Userlist** | Файл со списком пользователей Socks-прокси, извлечённым из Eserv.ini версии Eserv/2.x. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[Eserv2Userlist]}**. | |
| **Eserv2Grouplist** | Файл со списком группировки пользователей Socks-прокси, извлечённым из Eserv.ini версии Eserv/2.x. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[Eserv2Grouplist]}**. | |
| **NTdomain** | Имя домена Active Directory или локального компьютера под управлением Windows линейки NT, по списку пользователей которого выполняется авторизация пользователей Socks-прокси, если выбран соответствующий способ авторизации (**NtLogon**). Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[NTdomain]}**. | |
| **DefaultAuthSource** | Имя источника авторизации на Socks-прокси из списка источников авторизации. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[DefaultAuthSource]}**. | |
| **AuthMethod** | Способ авторизации на Socks-прокси по умолчанию. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[AuthMethod]}**. | |
| **NtImpersonateLogon** | Определяет, требуется ли переключение в контекст безопасности пользователя при авторизации в домене Active Directory. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[NtImpersonateLogon]}**. | |
| **ExtendedGroupList** | Файл с расширенным списком группировки пользователейдля Socks-прокси. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[ExtendedGroupList]}**. | |
| **RejectNonexistentDomains** | Указывает, отвергать ли попытки авторизации, если домен авторизации не описан в настройках сервера. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[RejectNonexistentDomains]}**. | |
| **MaxAuthAttempts** | Максимально допустимое число попыток протокольной (не по IP/MAC-адресу) авторизации в одной сессии. Определяет, сколько неудачных попыток авторизации допускается в течение одной сессии. Если это число превышено, подключение считается атакой и разрывается. Если значение нулевое, то ограничения на число попыток подбора пароля отсутствуют. Начальное значение - **{PROXY[MaxAuthAttempts]}**. | |

| | | |
|---|---|---|
| **Active** | Определяет, активен ли Socks-прокси. Если значение нулевое, то все попытки подключения отвергаются. Если указано любое ненулевое число, сервер принимает подключения. Начальное значение - **1**. | |
| **Port** | Порт, на котором работает Socks-прокси. Начальное значение стандартное - **1080**. | & |
| **NetworkInterface** | Адрес сетевого интерфейса, слушаемого сервером. Начальное значение - пустая строка; это означает, что сервер слушает все интерфейсы. | & |
| **Timeout** | Время бездействия, задаваемое в миллисекундах, по истечении которого сервер прекращает соединение с клиентом. Это вынужденная мера, предотвращающая утечку ресурсов при плохой связи - как правило, тайм-аут срабатывает, когда соединение уже фактически разорвано, но серверу неоткуда получить извещение об этом. Начальное значение - **60000**, что соответствует 10 минутам. | $ |
| **OutboundTimeout** | Время бездействия, задаваемое для соединений с внешними серверами. Начальное значение - **30000**, что соответствует 5 минутам. | $ |
| **Lists** | Расположение каталога со списками настройки Socks-прокси. Начальное значение - **{PROXY[Lists]}\socks**. | |
| **Logs** | Расположение каталога оперативных журналов Socks -прокси. Начальное значение - **{PROXY[Logs]}**. | $ |
| **MyIpList** | Список сетевых интерфейсов Socks-прокси с указанием, на какие из этих интерфейсов серверу разрешено принимать подключения. Переопределяет соответствующий параметр из секции **PROXY**. Это важный элемент системы безопасности сервера, позволяющий разом отсечь множество заведомо чужих пользователей, поэтому настройке этого списка надо уделить максимум внимания. Начальное значение - **{PROXY[MyIpList]}**. | |
| **IpBlackList** | Список IP-адресов и подсетей, которым запрещено обращаться к Socks-прокси. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[IpBlackList]}**. | |
| **LocalNetworks** | Список локальных сетей, обслуживаемых Socks-прокси. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[LocalNetworks]}**. | |
| **IpWhiteList** | Список доверенных IP-адресов или сетей, которые обслуживаются этим Socks-прокси. Переопределяет соответствующий параметр из секции **PROXY**. Этот список ДОПОЛНЯЕТ список локальных сетей. В нём могут быть не локальные сети, а, например, особые внешние IP-адреса. Начальное значение - **{PROXY[IpWhiteList]}**. | |
| **IpMacAuth** | Файл со списком, устанавливающим соответствие между IP и MAC адресами клиентского компьютера и именем учётной записи пользователя. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[IpMacAuth]}**. | |
| **IgnoreLocalNetworks** | Указывает, использовать ли при определении допустимости подключения список локальных сетей. Переопределяет соответствующий параметр из секции **PROXY**. Если в настройках сервера указан общий список локальных сетей, составленный излишне либерально с точки зрения безопасности прокси-сервера, его использование для управления доступом к прокси-серверу можно отключить, задав этому параметру любое ненулевое значение. Начальное значение - **{PROXY[IgnoreLocalNetworks]}**. | * |
| **HostBlackList** | Список серверов, подключение к которым запрещено. Используется для упрощённого управления доступом, если не подключены полнофункциональные списки контроля доступа (задано нулевое значение параметра **UseAcls**). Начальное значение - **{SocksProxy[Lists]}\HostBlackList.txt**. | |

| | | |
|---|---|---|
| **HostWhiteList** | Список серверов, подключение к которым разрешено. Используется для упрощённого управления доступом, если не подключены полнофункциональные списки контроля доступа (задано нулевое значение параметра **UseAcls**). Этот список перекрывает список запретов, поэтому можно запрещать целые группы серверов, разрешая доступ к некоторым серверам из запрещённой группы. Начальное значение - **{SocksProxy[Lists]}\HostWhiteList.txt**. | |
| **UseIpAuth** | Указывает, использовать ли автоматическую авторизацию подключившегося пользователя на основании IP-адреса либо сочетания IP и MAC-адресов. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[UseIpAuth]}**. | * |
| **RequireAuth** | Указывает, является ли авторизация обязательной для работы с Socks-прокси. Если задано любое ненулевое значение, то неавторизованные сессии запрещены. Заодно запрещается работа с протоколом Socks версии 4, не поддерживающим авторизацию. Начальное значение - **1**. | * $ |
| **UseAcls** | Указывает, использовать ли списки контроля доступа к внешним серверам. С помощью этих списков можно раздавать именные разрешения или запреты на обращения к запрашиваемым ресурсам (с использованием авторизации). Если при запуске сервера этот параметр имеет ненулевое значение, загружается специальный плагин **acl**, обеспечивающий поддержку списков доступа. В дальнейшем при возникновении проблем обработку списков доступа можно временно отключить, задав нулевое значение. Начальное значение - **1**. | * & |
| **ConstrainTraffic** | Указывает, использовать ли управление трафиком (ограничитель TrafC) для Socks-прокси. Если загружены плагины **TrafC** и **acl**, и предыдущий параметр имеет ненулевое значение, то при ненулевом значении этого параметра в случае разрешения пользователю доступа к внешним ресурсам производится выделение полосы пропускания и квоты на объём принятой и переданной информации - в зависимости от вида запроса. Если работа ограничителя трафика создаёт проблемы, его можно в любой момент отключить, задав нулевое значение. Начальное значение - **{PROXY[ConstrainTraffic]}**. | * |
| **ACL** | Главный список прав доступа. Списков может быть сколько угодно - они могут вызываться по цепочке, - но главный список, с которого начинается обработка, всегда один. Начальное значение - **{SocksProxy[Lists]}\ACL.txt**. | |
| **DefaultAclAction** | Действие, которое следует применить, если его не удалось определить при анализе списка. Если действие имеет параметр, он записывается здесь же через пробел. Действие задаётся двухсимвольным кодом и может быть одним из следующих:<br>**DI** (Disable) - задать режим безусловной блокировки доступа;<br>**EN** (Enable) - задать режим разрешения доступа. Возможным, но не обязательным, параметром является перечень каналов, выделяемых для выполнения запроса;<br>**LI** (List) - выполнить обработку вложенного списка. Обязательным параметром является имя файла списка;<br>**RU** (Rule) - выполнить правило. Обязательным параметром является имя встроенного или внешнего правила.<br>Начальное значение - **EN**, действие, разрешающее доступ без назначения каналов. | * |

| | | |
|---|---|---|
| **DefaultTrafCPriority** | Этот параметр задаёт приоритет для назначаемого по умолчанию (в случае выбора действия **EN**) набора каналов. Приоритет задаётся числом, чем оно меньше, тем выше приоритет; наивысшему приоритету соответствует нулевое значение. Возможные значения:<br>**пусто** - используется значение приоритета, вычисленное при анализе списка правил;<br>**+nnn** - приоритет, вычисленный при анализе списка правил, понижается на nnn пунктов;<br>**-nnn** - приоритет, вычисленный при анализе списка правил, повышается на nnn пунктов;<br>**nnn** - приоритет устанавливается ровно на nnn пунктов.<br>Начальное значение - пустая строка. | |
| **CascadeProxy** | Указывает, использовать ли каскадирование Socks-прокси-серверов. Если для выхода в интернет используется не один прокси-сервер, они должны быть организованы в цепочку. Если при запуске сервера этот параметр имеет ненулевое значение, загружается специальный плагин, обеспечивающий поддержку каскадирования. В дальнейшем при возникновении проблем каскадирование можно временно отключить, задав нулевое значение. Начальное значение - **0**. | * & |
| **CascadeList** | Список управления каскадированием. Начальное значение - **{SocksProxy[Lists]}\CascadeList.txt**. | |
| **UseDefaultCascade** | Указывает, использовать ли каскадирование в случае, когда не удалось определить вышестоящий прокси-сервер на основании списка. Если параметр имеет ненулевое значение, то по умолчанию также используется цепочка прокси-серверов. Начальное значение - **0**. | * |
| **DefaultCascadeHost** | Если используется каскадирование по умолчанию, то этот параметр задаёт имя или адрес вышестоящего прокси-сервера. Начальное значение - пустая строка. | * |
| **DefaultCascadePort** | Если используется каскадирование по умолчанию, то этот параметр задаёт порт, на котором работает вышестоящий прокси-сервер. Начальное значение - **0**. | * |
| **DefaultCascadeUser** | Если используется каскадирование по умолчанию, то этот параметр задаёт имя пользователя на тот случай, если вышестоящий прокси-сервер требует авторизацию. Естественно, это должно быть имя пользователя именно вышестоящего прокси-сервера. Начальное значение - пустая строка. Если авторизация не требуется, имя пользователя задавать не надо. | * |
| **DefaultCascadePass** | Если используется каскадирование по умолчанию, то этот параметр задаёт пароль пользователя на тот случай, если вышестоящий прокси-сервер требует авторизацию. Начальное значение - пустая строка. Если авторизация не требуется, имя пользователя задавать не надо. | * |
| **DefaultAllowDirect** | Если используется каскадирование по умолчанию, то этот параметр указывает, использовать ли прямое обращение в случае неудачи подключения через вышестоящий прокси-сервер. Иногда организация сети допускает такие трюки, хотя и ценой существенного снижения скорости обмена данными. Начальное значение - **1**. | * |

| | | |
|---|---|---|
| **LockIntruders** | Определяет, использовать ли блокировку атак. Признаком атаки считается частое повторение различных нежелательных событий - таких, как ошибки авторизации. Если частота следования таких событий для какого-либо IP-адреса клиентского подключения превышает установленную в настройках величину, то этот адрес заносится в список запрещённых сетей. IP-адреса, находящиеся в списках локальных или доверенных сетей, блокировке не подвергаются. Если при запуске сервера этот параметр имеет любое ненулевое значение, подключается плагин **ids_memo**, обеспечивающий хранение и накопление информации о нежелательных событиях. После этого параметр может использоваться для временного отключения блокировки атак, если его работа будет создавать какие-либо проблемы. Начальное значение - **{PROXY[LockIntruders]}**. | * |
| **AuthFailCount** | Пороговое значение числа ошибок авторизации. Если количество неудачных попыток авторизации за определённый временной интервал для одного и того же IP-адреса клиентского подключения превышает заданную этим параметром величину, это считается атакой - со всеми вытекающими отрицательными последствиями для соответствующего клиента. Начальное значение - **{PROXY[AuthFailCount]}**. | * |
| **AuthFailPeriod** | Период подсчёта ошибок авторизации. Если количество неудачных попыток авторизации за определённый этим параметром временной интервал для одного и того же IP-адреса клиентского подключения превышает заданную величину, это считается атакой - со всеми вытекающими отрицательными последствиями для соответствующего клиента. Длительность периода задаётся в минутах. Начальное значение - **{PROXY[AuthFailPeriod]}**. | * |
| **UseTarpit** | Указывает, использовать ли при выдаче отказов клиенту Tarpit - "липучку". В этом случае отрицательные ответы искусственно задерживаются, что уменьшает нагрузку на сеть. Начальное значение - **{PROXY[UseTarpit]}**. | * |
| **TarpitInterval** | Если задано использование "липучки", то этот параметр задаёт длительность задержки в секундах. Начальное значение - **{PROXY[TarpitInterval]}**. | * |
| **LogLevel** | Задаёт уровень детализации оперативного журнала Socks-прокси. Параметр может принимать значения от 1 до 9. Чем выше уровень, тем больше подробностей пишется в журнал. Для совместимости с ранними версиями, в которых уровень детализации не задавался, нулевое значение соответствует максимальному уровню детализации. Начальное значение - **{PROXY[LogLevel]}**. | $ |
| **LogAcl** | Указывает, вести ли дополнительный оперативный журнал обработки списков прав доступа. Если параметр имеет любое ненулевое значение, создаётся дополнительный журнал, в который записываются результаты сопоставления реквизитов пользователя и параметров запроса со списком прав доступа и предоставленные в результате права. Начальное значение - **{PROXY[LogAcl]}**. | |
| **LogTrafC** | Указывает, вести ли дополнительный оперативный журнал ограничителя трафика TrafC. Если параметр имеет любое ненулевое значение, создаётся дополнительный журнал, в который записываются реквизиты запроса и параметры назначаемых для выполнения запроса каналов. Начальное значение - **{PROXY[LogTrafC]}**. | |
| **LogToEStat** | Определяет, ведёт ли сервер статистику в формате программы **Estat32**, разработанной **Андреем Волковым** из **EPE Labs** для обработки статистических журналов Eserv/2. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{PROXY[LogToEStat]}**. | $ |

| | | |
|---|---|---|
| **LogToAdvSoft** | Определяет, ведёт ли сервер статистику в формате программ **ProxyInspector** и **MailDetective** производства компании **AdvSoft**. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{PROXY[LogToAdvSoft]}**. | $ |
| **LogToElog** | Определяет, ведёт ли сервер статистику в формате программы **Elog**, разработанной **Игорем Панасенко** из компании **ЛЭНК** для обработки статистических журналов Eserv/3. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{PROXY[LogToElog]}**. | $ |
| **LogToMaillog** | Определяет, ведёт ли сервер статистику в собственном текстовом формате. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{PROXY[LogToMaillog]}**. | $ |
| **LogToMStat** | Определяет, используется ли подсистема ведения статистики в базе данных MStat, разработанная Андреем Матвеевым. Этот сборщик статистики имеет немалое преимущество перед текстовыми журналами, позволяя хранить и эффективно обрабатывать статистическую информацию за большие периоды времени, измеряемые годами. Но для его работы необходима установка дополнительного приложения - СУБД одного из поддерживаемых сборщиком типов. Если указано любое ненулевое число, статистика в базе данных ведётся. Начальное значение - **{PROXY[LogToMStat]}**. | $ |

## *Секция Pop3Proxy - параметры настройки POP3-прокси*

| | | |
|---|---|---|
| **Active** | Определяет, активен ли POP3-прокси. Если значение нулевое, то все попытки подключения отвергаются с кодом 4xx, что означает предложение повторить попытку позже. Если указано любое ненулевое число, сервер принимает подключения. Начальное значение - **1**. | |
| **Port** | Порт, на котором работает POP3-прокси. Начальное значение - **111**. | & |
| **NetworkInterface** | Адрес сетевого интерфейса, слушаемого сервером. Начальное значение - пустая строка; это означает, что сервер слушает все интерфейсы. | & |
| **Timeout** | Время бездействия, задаваемое в миллисекундах, по истечении которого сервер прекращает соединение с клиентом. Это вынужденная мера, предотвращающая утечку ресурсов при плохой связи - как правило, тайм-аут срабатывает, когда соединение уже фактически разорвано, но серверу неоткуда получить извещение об этом. Начальное значение - **60000**, что соответствует 10 минутам. | $ |
| **OutboundTimeout** | Время бездействия, задаваемое для соединений с внешними серверами. Начальное значение - **30000**, что соответствует 5 минутам. | $ |
| **Lists** | Расположение каталога со списками настройки POP3-прокси. Начальное значение - **{PROXY[Lists]}\pop3p**. | |
| **Templates** | Расположение каталога с шаблонами сообщений POP3-прокси. Начальное значение - **{PROXY[Templates]}\pop3p**. | |
| **Logs** | Расположение каталога оперативных журналов POP3 -прокси. Начальное значение - **{PROXY[Logs]}**. | $ |

| | | |
|---|---|---|
| **MyIpList** | Список сетевых интерфейсов POP3-прокси с указанием, на какие из этих интерфейсов серверу разрешено принимать подключения. Переопределяет соответствующий параметр из секции **PROXY**. Это важный элемент системы безопасности сервера, позволяющий разом отсечь множество заведомо чужих пользователей, поэтому настройке этого списка надо уделить максимум внимания. Начальное значение - **{PROXY[MyIpList]}**. | |
| **IpBlackList** | Список IP-адресов и подсетей, которым запрещено обращаться к POP3-прокси. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{Pop3Proxy[Lists]}\IpBlackList.txt**. | |
| **LocalNetworks** | Список локальных сетей, обслуживаемых POP3-прокси. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[LocalNetworks]}**. | |
| **IpWhiteList** | Список доверенных IP-адресов или сетей, которые обслуживаются этим POP3-прокси. Переопределяет соответствующий параметр из секции **PROXY**. Этот список ДОПОЛНЯЕТ список локальных сетей. В нём могут быть не локальные сети, а, например, особые внешние IP-адреса. Начальное значение - **{Pop3Proxy[Lists]}\IpWhiteList.txt**. | |
| **IgnoreLocalNetworks** | Указывает, использовать ли при определении допустимости подключения список локальных сетей. Переопределяет соответствующий параметр из секции **PROXY**. Если в настройках сервера указан общий список локальных сетей, составленный излишне либерально с точки зрения безопасности прокси-сервера, его использование для управления доступом к прокси-серверу можно отключить, задав этому параметру любое ненулевое значение. Начальное значение - **{PROXY[IgnoreLocalNetworks]}**. | * |
| **HostBlackList** | Список серверов, подключение к которым запрещено. Начальное значение - **{Pop3Proxy[Lists]}\HostBlackList.txt**. | |
| **HostWhiteList** | Список серверов, подключение к которым разрешено. Этот список перекрывает список запретов, поэтому можно запрещать целые группы серверов, разрешая доступ к некоторым серверам из запрещённой группы. Начальное значение - **{Pop3Proxy[Lists]}\HostWhiteList.txt**. | |
| **UseTarpit** | Указывает, использовать ли при выдаче отказов клиенту Tarpit - "липучку". В этом случае отрицательные ответы искусственно задерживаются, что уменьшает нагрузку на сеть. Начальное значение - **{PROXY[UseTarpit]}**. | * |
| **TarpitInterval** | Если задано использование "липучки", то этот параметр задаёт длительность задержки в секундах. Начальное значение - **{PROXY[TarpitInterval]}**. | * |
| **LogLevel** | Задаёт уровень детализации оперативного журнала POP3-прокси. Параметр может принимать значения от 1 до 9. Чем выше уровень, тем больше подробностей пишется в журнал. Для совместимости с ранними версиями, в которых уровень детализации не задавался, нулевое значение соответствует максимальному уровню детализации. Начальное значение - **{PROXY[LogLevel]}**. | $ |
| **LogToEStat** | Определяет, ведёт ли сервер статистику в формате программы **Estat32**, разработанной **Андреем Волковым** из **EPE Labs** для обработки статистических журналов Eserv/2. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{PROXY[LogToEStat]}**. | $ |
| **LogToAdvSoft** | Определяет, ведёт ли сервер статистику в формате программ **ProxyInspector** и **MailDetective** производства компании **AdvSoft**. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{PROXY[LogToAdvSoft]}**. | $ |

| | | |
|---|---|---|
| **LogToElog** | Определяет, ведёт ли сервер статистику в формате программы **Elog**, разработанной **Игорем Панасенко** из компании **ЛЭНК** для обработки статистических журналов Eserv/3. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{PROXY[LogToElog]}**. | $ |
| **LogToMaillog** | Определяет, ведёт ли сервер статистику в собственном текстовом формате. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{PROXY[LogToMaillog]}**. | $ |
| **LogToMStat** | Определяет, используется ли подсистема ведения статистики в базе данных MStat, разработанная Андреем Матвеевым. Этот сборщик статистики имеет немалое преимущество перед текстовыми журналами, позволяя хранить и эффективно обрабатывать статистическую информацию за большие периоды времени, измеряемые годами. Но для его работы необходима установка дополнительного приложения - СУБД одного из поддерживаемых сборщиком типов. Если указано любое ненулевое число, статистика в базе данных ведётся. Начальное значение - **{PROXY[LogToMStat]}**. | $ |

## *Секция TCPMAP - параметры настройки отображений портов TCP*

| | | |
|---|---|---|
| **Timeout** | Время бездействия, задаваемое в миллисекундах, по истечении которого сервер прекращает соединение с клиентом. Это вынужденная мера, предотвращающая утечку ресурсов при плохой связи - как правило, тайм-аут срабатывает, когда соединение уже фактически разорвано, но серверу неоткуда получить извещение об этом. Начальное значение - **60000**, что соответствует 10 минутам. | $ |
| **OutboundTimeout** | Время бездействия, задаваемое для соединений с внешними серверами. Начальное значение - **30000**, что соответствует 5 минутам. | $ |
| **Lists** | Расположение каталога со списками настройки отображений. Начальное значение - **{PROXY[Lists]}\tcpmap**. | |
| **Logs** | Расположение каталога оперативных журналов отображений портов TCP. Начальное значение - **{PROXY[Logs]}**. | $ |
| **TcpMap** | Список отображений портов TCP - основной управляющий список, в котором задаётся соответствие локального порта порту внешнего сервера, а также дополнительные настройки для каждого отображения. Начальное значение - **{TCPMAP[Lists]}\TcpMap.txt**. | |
| **MyIpList** | Список сетевых интерфейсов прокси-сервера с указанием, на какие из этих интерфейсов серверу разрешено принимать подключения. Переопределяет соответствующий параметр из секции **PROXY**. Это важный элемент системы безопасности сервера, позволяющий разом отсечь множество заведомо чужих пользователей, поэтому настройке этого списка надо уделить максимум внимания. Начальное значение - **{PROXY[MyIpList]}**. | |
| **IpBlackList** | Список IP-адресов и подсетей, которым запрещено обращаться к прокси-серверу. Переопределяет соответствующий параметр из секции **PROXY**. Это список по умолчанию, который используется, если отображения нет в списке (то есть, оно было задано путём прямого редактирования файлов правил) либо в параметрах отображения не задан особый список. Начальное значение - **{TCPMAP[Lists]}\IpBlackList.txt**. | |
| **LocalNetworks** | Список локальных сетей, обслуживаемых прокси-сервером. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[LocalNetworks]}**. | |

| | | |
|---|---|---|
| **IpWhiteList** | Список доверенных IP-адресов или сетей, которые обслуживаются этим прокси-сервером. Переопределяет соответствующий параметр из секции **PROXY**. Этот список ДОПОЛНЯЕТ список локальных сетей. В нём могут быть не локальные сети, а, например, особые внешние IP-адреса. Это список по умолчанию, который используется, если отображения нет в списке (то есть, оно было задано путём прямого редактирования файлов правил) либо в параметрах отображения не задан особый список. Начальное значение - **{TCPMAP[Lists]}\IpWhiteList.txt**. | |
| **IgnoreLocalNetworks** | Указывает, использовать ли при определении допустимости подключения список локальных сетей. Переопределяет соответствующий параметр из секции **PROXY**. Если в настройках сервера указан общий список локальных сетей, составленный излишне либерально с точки зрения безопасности прокси-сервера, его использование для управления доступом к прокси-серверу можно отключить, задав этому параметру любое ненулевое значение. Это значение по умолчанию, которое используется, если отображения нет в списке (то есть, оно было задано путём прямого редактирования файлов правил) либо в параметрах отображения не задано никакое значение. Начальное значение - **{PROXY[IgnoreLocalNetworks]}**. | * |
| **UseTarpit** | Указывает, использовать ли при выдаче отказов клиенту Tarpit - "липучку". В этом случае отрицательные ответы искусственно задерживаются, что уменьшает нагрузку на сеть. Начальное значение - **{PROXY[UseTarpit]}**. | * |
| **TarpitInterval** | Если задано использование "липучки", то этот параметр задаёт длительность задержки в секундах. Начальное значение - **{PROXY[TarpitInterval]}**. | * |
| **LogLevel** | Задаёт уровень детализации оперативного журнала прокси-сервера. Параметр может принимать значения от 1 до 9. Чем выше уровень, тем больше подробностей пишется в журнал. Для совместимости с ранними версиями, в которых уровень детализации не задавался, нулевое значение соответствует максимальному уровню детализации. Начальное значение - **{PROXY[LogLevel]}**. | $ |
| **LogToEStat** | Определяет, ведёт ли сервер статистику в формате программы **Estat32**, разработанной **Андреем Волковым** из **EPE Labs** для обработки статистических журналов Eserv/2. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{PROXY[LogToEStat]}**. | $ |
| **LogToAdvSoft** | Определяет, ведёт ли сервер статистику в формате программ **ProxyInspector** и **MailDetective** производства компании **AdvSoft**. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{PROXY[LogToAdvSoft]}**. | $ |
| **LogToElog** | Определяет, ведёт ли сервер статистику в формате программы **Elog**, разработанной **Игорем Панасенко** из компании **ЛЭНК** для обработки статистических журналов Eserv/3. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{PROXY[LogToElog]}**. | $ |
| **LogToMaillog** | Определяет, ведёт ли сервер статистику в собственном текстовом формате. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{PROXY[LogToMaillog]}**. | $ |

| | | |
|---|---|---|
| **LogToMStat** | Определяет, используется ли подсистема ведения статистики в базе данных MStat, разработанная Андреем Матвеевым. Этот сборщик статистики имеет немалое преимущество перед текстовыми журналами, позволяя хранить и эффективно обрабатывать статистическую информацию за большие периоды времени, измеряемые годами. Но для его работы необходима установка дополнительного приложения - СУБД одного из поддерживаемых сборщиком типов. Если указано любое ненулевое число, статистика в базе данных ведётся. Начальное значение - **{PROXY[LogToMStat]}**. | $ |

## *Секция UDPMAP - параметры настройки отображений портов UDP*

| | | |
|---|---|---|
| **Lists** | Расположение каталога со списками настройки отображений. Начальное значение - **{PROXY[Lists]}\udpmap**. | |
| **Logs** | Расположение каталога оперативных журналов отображений портов UDP. Начальное значение - **{PROXY[Logs]}**. | $ |
| **UdpMap** | Список отображений портов UDP - основной управляющий список, в котором задаётся соответствие локального порта порту внешнего сервера, а также дополнительные настройки для каждого отображения. Начальное значение - **{UDPMAP[Lists]}\UdpMap.txt**. | ? |
| **IpBlackList** | Список IP-адресов и подсетей, которым запрещено обращаться к прокси-серверу. Переопределяет соответствующий параметр из секции **PROXY**. Это список по умолчанию, который используется, если отображения нет в списке (то есть, оно было задано путём прямого редактирования файлов правил) либо в параметрах отображения не задан особый список. Начальное значение - **{UDPMAP[Lists]}\IpBlackList.txt**. | ? |
| **LocalNetworks** | Список локальных сетей, обслуживаемых прокси-сервером. Переопределяет соответствующий параметр из секции **PROXY**. Начальное значение - **{PROXY[LocalNetworks]}**. | ? |
| **IpWhiteList** | Список доверенных IP-адресов или сетей, которые обслуживаются этим прокси-сервером. Переопределяет соответствующий параметр из секции **PROXY**. Этот список ДОПОЛНЯЕТ список локальных сетей. В нём могут быть не локальные сети, а, например, особые внешние IP-адреса. Это список по умолчанию, который используется, если отображения нет в списке (то есть, оно было задано путём прямого редактирования файлов правил) либо в параметрах отображения не задан особый список. Начальное значение - **{UDPMAP[Lists]}\IpWhiteList.txt**. | ? |
| **IgnoreLocalNetworks** | Указывает, использовать ли при определении допустимости подключения список локальных сетей. Переопределяет соответствующий параметр из секции **PROXY**. Если в настройках сервера указан общий список локальных сетей, составленный излишне либерально с точки зрения безопасности прокси-сервера, его использование для управления доступом к прокси-серверу можно отключить, задав этому параметру любое ненулевое значение. Это значение по умолчанию, которое используется, если отображения нет в списке (то есть, оно было задано путём прямого редактирования файлов правил) либо в параметрах отображения не задано никакое значение. Начальное значение - **{PROXY[IgnoreLocalNetworks]}**. | * ? |
| **LogLevel** | Задаёт уровень детализации оперативного журнала прокси-сервера. Параметр может принимать значения от 1 до 9. Чем выше уровень, тем больше подробностей пишется в журнал. Для совместимости с ранними версиями, в которых уровень детализации не задавался, нулевое значение соответствует максимальному уровню детализации. Начальное значение - **{PROXY[LogLevel]}**. | $ |
| **LogToEStat** | Определяет, ведёт ли сервер статистику в формате программы **Estat32**, разработанной **Андреем Волковым** из **EPE Labs** для обработки статистических журналов Eserv/2. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{PROXY[LogToEStat]}**. | $ |

| | | |
|---|---|---|
| **LogToAdvSoft** | Определяет, ведёт ли сервер статистику в формате программ **ProxyInspector** и **MailDetective** производства компании **AdvSoft**. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{PROXY[LogToAdvSoft]}**. | $ |
| **LogToElog** | Определяет, ведёт ли сервер статистику в формате программы **Elog**, разработанной **Игорем Панасенко** из компании **ЛЭНК** для обработки статистических журналов Eserv/3. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{PROXY[LogToElog]}**. | $ |
| **LogToMaillog** | Определяет, ведёт ли сервер статистику в собственном текстовом формате. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{PROXY[LogToMaillog]}**. | $ |
| **LogToMStat** | Определяет, используется ли подсистема ведения статистики в базе данных MStat, разработанная Андреем Матвеевым. Этот сборщик статистики имеет немалое преимущество перед текстовыми журналами, позволяя хранить и эффективно обрабатывать статистическую информацию за большие периоды времени, измеряемые годами. Но для его работы необходима установка дополнительного приложения - СУБД одного из поддерживаемых сборщиком типов. Если указано любое ненулевое число, статистика в базе данных ведётся. Начальное значение - **{PROXY[LogToMStat]}**. | $ |

## *Секция HTTP - параметры настройки HTTP-сервера*

| | | |
|---|---|---|
| **AdminEmail** | Почтовый адрес администратора HTTP-сервера. Может использоваться в шаблонах сообщений об ошибках, в почтовых извещениях и т.п. Начальное значение **{Server[AdminEmail]}** может быть переопределено требуемым образом. | ? |
| **AdminName** | Имя (звание, титул) администратора HTTP-сервера. Обычно подставляется в заголовки автоматически формируемых писем в поле адреса или в качестве подписи. Начальное значение **{Server[AdminName]}** может быть переопределено требуемым образом. | |
| **DefaultAuthDomain** | Домен авторизации по умолчанию для HTTP-сервера. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[DefaultAuthDomain]}**. | $ |
| **DomainIP** | Файл со списком IP-адресов, назначенных сетевым интерфейсам компьютера. Переопределяет соответствующий параметр из секции **Lists**. Начальное значение - **{Lists[DomainIP]}**. | ? |
| **UserList** | Файл со списком пользователей формата Eserv/3 для HTTP-сервера. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[UserList]}**. | |
| **GroupList** | Файл со списком группировки пользователей формата Eserv/3 для HTTP-сервера. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[GroupList]}**. | |
| **PlainUserList** | Файл с объединённым списком пользователей формата Eserv/3 для HTTP-сервера. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[PlainUserList]}**. | ? |
| **PlainGroupList** | Файл со списком группировки пользователей формата Eserv/3 для HTTP-сервера. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[PlainGroupList]}**. | ? |

| | | |
|---|---|---|
| **Eserv2Userlist** | Файл со списком пользователей HTTP-сервера, извлечённым из Eserv.ini версии Eserv/2.x. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[Eserv2Userlist]}**. | |
| **Eserv2Grouplist** | Файл со списком группировки пользователей HTTP-сервера, извлечённым из Eserv.ini версии Eserv/2.x. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[Eserv2Grouplist]}**. | |
| **NTdomain** | Имя домена Active Directory или локального компьютера под управлением Windows линейки NT, по списку пользователей которого выполняется авторизация пользователей HTTP-сервера, если выбран соответствующий способ авторизации (**NtLogon**). Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[NTdomain]}**. | ? |
| **DefaultAuthSource** | Имя источника авторизации на HTTP-сервере из списка источников авторизации. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[DefaultAuthSource]}**. | ? |
| **AuthMethod** | Способ авторизации на HTTP-сервере по умолчанию. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[AuthMethod]}**. | ? |
| **NtImpersonateLogon** | Определяет, требуется ли переключение в контекст безопасности пользователя при авторизации в домене Active Directory. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[NtImpersonateLogon]}**. | ? |
| **UseExtendedGroups** | Указывает, использовать ли расширенную (кросс-доменную) группировку пользователей. Переопределяет соответствующий параметр из секции **AUTH**. Если при запуске сервера этот параметр имеет любое ненулевое значение, то загружается специальный плагин **groups_ext**. Начальное значение - **{AUTH[UseExtendedGroups]}**. | * & |
| **ExtendedGroupList** | Файл с расширенным списком группировки пользователей для HTTP-сервера. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[ExtendedGroupList]}**. | ? |
| **RejectNonexistentDomains** | Указывает, отвергать ли попытки авторизации, если домен авторизации не описан в настройках сервера. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[RejectNonexistentDomains]}**. | ? |
| **CacheIni** | Для ускорения обработки запросов HTTP-сервер может кэшировать в оперативной памяти ряд параметров конфигурационного файла. Кэширование производится только на время сессии - от подключения клиента до его отсоединения - и не влияет на параллельные сессии. Если кэширование создаёт проблемы, его можно отключить, установив этот параметр в ноль и перезапустив HTTP-сервер. Начальное значение - **1**. | * & |
| **CacheAuth** | Для ускорения обработки запросов HTTP-сервер может кэшировать в оперативной памяти реквизиты успешно авторизовавшихся пользователей и сведения о их членстве в группах, чтобы при повторном обращении не выполнять заново однажды выполненную достаточно затратную процедуру. Поскольку настройки всё-таки имеют свойство время от времени изменяться, то информация запоминается не навечно, а на некоторый промежуток времени, который в текущей версии составляет 15 минут. Кэширование может создавать проблемы, если требуется авторизация по списку домена Active Directory с переключением в контекст безопасности авторизовавшегося пользователя, - при использовании запомненных данных об авторизации такое переключение невозможно, поскольку оно требует реальной авторизации в домене AD. Кэширование включается, если при запуске сервера этот параметр имеет любое ненулевое значение. Начальное значение - **0**. | * & |

| | | |
|---|---|---|
| **Active** | Определяет, активен ли HTTP-сервер. Если значение нулевое, то все попытки подключения отвергаются с кодом 4xx, что означает предложение повторить попытку позже. Если указано любое ненулевое число, сервер принимает подключения. Начальное значение - **1**. | |
| **Port** | Порт, на котором работает HTTP-сервер. Чтобы избежать конфликта с другим HTTP-сервером, возможно, уже работающим, начальное значение - **0**. | & |
| **SslPort** | Порт, на котором HTTP-сервер принимает подключения по защищённому соединению. Чтобы избежать конфликта с другим HTTP-сервером, возможно, уже работающим, начальное значение - **0**. | & |
| **AdminPort** | Порт, на котором работает web-интерфейс Eserv/3. Начальное значение - **3140**. | & |
| **AdminSslPort** | Порт, на котором HTTP-сервер принимает запросы к web-интерфейсу Eserv/3 по защищённому соединению. Начальное значение - **3143**. | & |
| **NetworkInterface** | Адрес сетевого интерфейса, слушаемого сервером. Начальное значение - пустая строка; это означает, что сервер слушает все интерфейсы. | & |
| **SslNetworkInterface** | Адрес сетевого интерфейса, слушаемого сервером для приёма подключений по защищённому соединению. Начальное значение - пустая строка; это означает, что сервер слушает все интерфейсы. | & |
| **AdminNetworkInterface** | Адрес сетевого интерфейса, слушаемого сервером для приёма запросов к web-интерфейсу Eserv/3. Начальное значение - пустая строка; это означает, что сервер слушает все интерфейсы. | & |
| **AdminSslNetworkInterface** | Адрес сетевого интерфейса, слушаемого сервером для приёма запросов к web-интерфейсу Eserv/3 по защищённому соединению. Начальное значение - пустая строка; это означает, что сервер слушает все интерфейсы. | & |
| **Certificate** | Имя файла формата PEM, содержащего закрытый ключ и сертификаты, используемые при организации защищённого (SSL) соединения сервера с клиентом. Переопределяет соответствующий параметр из секции **Server**. Начальное значение - **{Server[Certificate]}**. | $ |
| **SslVerifyClient** | Определяет режим проверки подлинности сертификатов клиентской стороны при установлении защищённого соединения. Переопределяет соответствующий параметр из секции **Server**. Начальное значение - **{Server[SslVerifyClient]}**. | $ |
| **MaxConnections** | Максимально допустимое число одновременных подключений к серверу. Позволяет противостоять пиковым нагрузкам и целенаправленным попыткам завалить сервер путём неумеренного потребления всех ресурсов компьютера. Начальное значение - **100**. | & |
| **MaxConnectionsFromIP** | Максимально допустимое число одновременных подключений к серверу с одного IP-адреса. В текущей версии эта настройка не поддерживается и зарезервирована на будущее. Начальное значение - **10**. | & |
| **Timeout** | Время бездействия, задаваемое в миллисекундах, по истечении которого сервер прекращает соединение с клиентом. Это вынужденная мера, предотвращающая утечку ресурсов при плохой связи - как правило, тайм-аут срабатывает, когда соединение уже фактически разорвано, но серверу неоткуда получить извещение об этом. Начальное значение - **60000**, что соответствует 10 минутам. | $ |
| **Lists** | Расположение каталога со списками настройки HTTP-сервера. Начальное значение - **{Dirs[Lists]}\http**. | |
| **Templates** | Расположение каталога с шаблонами ответов и служебных писем HTTP-сервера. Начальное значение - **{Dirs[Templates]}\http**. | ? |
| **Logs** | Расположение каталога оперативных журналов HTTP-сервера. Начальное значение - **{Dirs[Logs]}**. | $ |

| | | |
|---|---|---|
| **IpBlackList** | Список IP-адресов и подсетей, которым запрещено обращаться к HTTP-серверу. Начальное значение - **{HTTP[Lists]}\IpBlackList.txt**. | ? |
| **LocalNetworks** | Список локальных сетей, обслуживаемых HTTP-сервером. Переопределяет соответствующий параметр из секции **Lists**. Начальное значение - **{Lists[LocalNetworks]}**. | ? |
| **IpWhiteList** | Список доверенных IP-адресов или сетей, которые обслуживаются этим HTTP-сервером. Этот список ДОПОЛНЯЕТ список локальных сетей. В нём могут быть не локальные сети, а, например, особые внешние IP-адреса. Начальное значение - **{HTTP[Lists]}\IpWhiteList.txt**. | ? |
| **IpMacAuth** | Файл со списком, устанавливающим соответствие между IP и MAC адресами клиентского компьютера и именем учётной записи пользователя. Переопределяет соответствующий параметр из секции **Lists**. Начальное значение - **{Lists[IpMacAuth]}**. | ? |
| **UseIpAuth** | Указывает, использовать ли автоматическую авторизацию подключившегося пользователя на основании IP-адреса либо сочетания IP и MAC-адресов. Начальное значение - **0**, то есть, если прочие настройки сервера потребуют авторизации клиента, она должна быть выполнена явно. | * ? |
| **LocalReplyList** | Список шаблонов HTML-страниц, которые сервер выдаёт клиентам в качестве ответа в различных ситуациях - при отказе в выполнении запроса и при обнаружении ошибок. Шаблоны можно настраивать по своему усмотрению или заменять своими. Начальное значение - **{HTTP[Lists]}\LocalReplyList.txt**. | ? |
| **LocalReplyStyles** | Расположение файла, содержащего таблицу HTML-стилей, включаемую в ответы сервера. Путём редактирования этой таблицы Вы можете изменить внешний вид всех ответов, не затрагивая содержимого. Начальное значение - **{HTTP[Templates]}\LocalReplyStyles.css**. | ? |
| **AdminDocumentRoot** | Путь к корневому каталогу администраторского web-интерфейса, обеспечивающего управление всеми службами PigMail+PigProxy. Здесь же располагаются и файлы пользовательского интерфейса. Web-интерфейс администратора доступен при обращении на специальные порты, определяемые параметрами **AdminPort** и **AdminSslPort**. Пользовательский web-интерфейс может быть доступен и на стандартных портах, в зависимости от дополнительных настроек сервера. Начальное значение - **..\script\control\wwwroot.pigmail**. | ? |
| **AdminDirectoryNotfound** | Имя файла, который возвращается в ответ на запрос или интерпретируется на сервере как сценарий, если путь к запрошенному объекту отсутствует. Этот файл ищется в каталоге самого нижнего уровня, обнаруженного при анализе пути. Можно указать несколько файлов через пробел, при этом поиск файла выполняется слева направо; будет использован первый найденный файл. Этот параметр используется при работе web-интерфейса администратора PigMail+PigProxy. Начальное значение - **index.f**. | ? |
| **AdminDirectoryIndex** | Имя индексного файла, который возвращается в ответ на запрос или интерпретируется как сценарий, если в запросе указано только имя каталога (разумеется, каталога существующего, в противном случае применяется значение предыдущего параметра). Можно указать несколько файлов через пробел, при этом поиск файла выполняется слева направо; будет использован первый найденный файл. Этот параметр используется при работе web-интерфейса администратора PigMail+PigProxy. Начальное значение - **"index.f index.html index.cgi index.fxml"**. | ? |

| | | |
|---|---|---|
| **AdminUser** | Логин администратора PigMail+PigProxy, задаваемый в формате **логин@домен**. Домен авторизации, как и логин, может быть задан абсолютно произвольно, его существование не проверяется. Если домен не указан вообще, используется домен по умолчанию. Администратор не является полноценным пользователем PigMail+PigProxy - его логин и пароль используются только для доступа к web-интерфейсу. PigMail+PigProxy позволяет разрешить работу с web-интерфейсом также и обычным пользователям, при этом возможно ограничение доступа к различным разделам web-интерфейса (на основе списка управления доступом), но администратор независимо от этого имеет полный доступ к рычагам управления. Единственный способ избавиться от него - не задавать логин и пароль вообще. Начальное значение - пустая строка. | ? |
| **AdminPass** | Пароль администратора PigMail+PigProxy. На самом деле из соображений секретности пароль при первом обращении к web-интерфейсу шифруется по алгоритму MD5. Это одностороннее преобразование, и восстановить исходный пароль из зашифрованного результата возможно только подбором. Признаком шифрования HTTP-сервер считает длину строки в 32 символа - именно столько занимает хэш MD5. Поэтому собственно пароль не может иметь такую длину, иначе он никогда не будет зашифрован (или его придётся зашифровать вручную с использованием специальной утилиты MD5 из комплекта PigMail+PigProxy). Начальное значение - пустая строка. | ? |
| **VersionInformer** | Определяет, отображать ли в web-интерфейсе администратора актуальную информацию о текущей версии Eserv. Речь идёт не о версии, установленной у пользователя, а о версии, доступной в данный момент для загрузки с сайта www.eserv.ru, откуда информация и запрашивается. Если сайт по каким-либо причинам недоступен, web-интерфейс будет работать с задержками. Кроме того, такие запросы могут противоречить корпоративной политике или пожеланиям самого администратора. Если этот параметр имеет нулевое значение, никаких запросов не делается, и в web-интерфейсе отображается обычная ссылка на новостной раздел сайта. Начальное значение - **1**, то есть, информация запрашивается и отображается. | |
| **VirtualFolders** | Список виртуальных каталогов - отображений логического пути к объекту, переданного в запросе клиента, на физические каталоги сервера. Отображение может зависеть от множества параметров. Обычно в качестве ключевых параметров используются символическое имя узла сети (если на одном физическом сервере размещаются несколько сайтов), язык, поддерживаемый клиентом (если сайт имеет несколько разделов на различных языках), фрагмент пути к запрашиваемому объекту. Сопоставляя эти и другие параметры запроса с содержимым списка, сервер определяет физический каталог, в котором следует искать запрашиваемый объект. Начальное значение - **{HTTP[Lists]}\VirtualFolders.txt**. | ? |
| **DocumentRoot** | Корневой каталог сайта, который выбирается по умолчанию, если выполнить отображение по списку виртуальных каталогов не удалось. Начальное значение - **{Dirs[Pub]}\wwwroot**. | ? |
| **DirectoryNotfound** | Имя файла, который возвращается в ответ на запрос или интерпретируется на сервере как сценарий, если путь к запрошенному объекту отсутствует. Этот файл ищется в каталоге самого нижнего уровня, обнаруженного при анализе пути. Можно указать несколько файлов через пробел, при этом поиск файла выполняется слева направо; будет использован первый найденный файл. Начальное значение - **"index.php index.f"**. | ? |
| **DirectoryIndex** | Имя индексного файла, который возвращается в ответ на запрос или интерпретируется как сценарий, если в запросе указано только имя каталога (разумеется, каталога существующего, в противном случае применяется значение предыдущего параметра). Можно указать несколько файлов через пробел, при этом поиск файла выполняется слева направо; будет использован первый найденный файл. Начальное значение - **"index.f index.html index.htm index.php3 index.php index.cgi default.htm index.fxml index.e"**. | ? |

| | | |
|---|---|---|
| **ContentTypeList** | Список типов данных. HTTP-сервер в своих ответах всегда сообщает, какого типа данные он передаёт. На основании этого списка можно по расширению имени (а в особых случаях и по расположению файла на диске, поскольку по списку проверяется полный - возможно, несуществующий, - путь к файлу) определить искомое значение. По этому списку также определяется, необходимо ли в файле обнаруживать и обрабатывать так называемые Server Side Includes (SSI) - простейшие сценарии, выполняемые на сервере и генерирующие текст, включаемый в выводимую страницу. Ещё одна функция этого списка - управление кэшированием передаваемых файлов на стороне клиента. Начальное значение - **{HTTP[Lists]}\ContentTypeList.txt**. | ? |
| **DefaultContentType** | Тип данных, используемый по умолчанию, когда его не удаётся определить по списку. Начальное значение - **application/octet-stream**. | ? |
| **CharsetList** | Список определения кодировки текстовых файлов по их расположению. Информация о кодировке при её наличии также может передаваться HTTP-сервером в ответе на запрос, дабы браузер без дополнительных манипуляций пользователя выбрал правильное отображение полученного текста. Разнесение разных языковых (в том числе и различных кодировок русского языка) разделов сайта по разным каталогам фактически превратилось в стандарт. Начальное значение - **{HTTP[Lists]}\CharsetList.txt**. | ? |
| **IsapiExtensions** | Список обработчиков сценариев, подключаемых через интерфейс ISAPI. Такие обработчики запускаются в адресном пространстве сервера, поэтому работают быстрее. Обратной стороной этого преимущества является меньшая устойчивость к сбоям - ошибка в сценарии, а тем паче в самом обработчике может вызвать аварийное завершение работы сервера. Этот список обрабатывается при запуске сервера, при этом список активных обработчиков целиком загружается в память. Начальное значение - **{HTTP[Lists]}\IsapiExtensions.txt**. | & |
| **ScriptHandlers** | Список обработчиков сценариев, сопоставляющий расширения и, в некоторых случаях, расположение файлов программам-обработчикам, запускающимся на сервере и выполняющих сложную обработку запросов. Начальное значение - **{HTTP[Lists]}\ScriptHandlers.txt**. | ? |
| **Robots** | Список клиентских идентификаторов (User-Agent), которыми обозначают себя поисковые роботы. Он используется для ведения статистики в собственном текстовом формате, чтобы отделять набеги роботов от визитов "человекоуправляемых" браузеров (это имеет большое значение, если сайт получает доходы от показа рекламы). Начальное значение - **{HTTP[Lists]}\robots.txt**. | ? |
| **AutoFillRobots** | Определяет, использовать ли автоматическое пополнение списка роботов-поисковиков. Факт посещения именно робота определяется по запросу специального файла **robots.txt**, который, по всеобщему соглашению, находится в корневом каталоге сайта и определяет как подлежащие индексации в поисковых системах, так и запрещённые для индексации области сайта. Если параметр имеет ненулевое значение, список роботов пополняется по мере их появления на сайте. Начальное значение - **0**. | * ? |
| **UsePool** | Определяет, использовать ли, в отличие от классической схемы, пул обрабатывающих потоков. Если в классической схеме поток, созданный для обслуживания запроса, завершался после выполнения задания, то при наличии пула поток переходит в состояние ожидания следующего запроса. В некоторых случаях использование пула является обязательным, поскольку классическая схема приводит к утечкам памяти, как, например, при запуске сценариев PHP в режиме ISAPI, более быстром, нежели CGI. Если при запуске сервера этот параметр имеет ненулевое значение, выбирается модель работы с использованием пула потоков. Начальное значение - **0**. | * & |

| | | |
|---|---|---|
| **UsePerformanceTuning** | Определяет, применять ли собственные нестандартные значения шести перечисленных ниже параметров тонкой настройки производительности или же оставить заданные в коде сервера значения по умолчанию. Если сервер успешно справляется с нагрузкой, эти настройки лучше оставить как есть. Если при запуске сервера этот параметр имеет ненулевое значение, вместо значений по умолчанию применяются собственные нестандартные значения. Начальное значение - **0**. | & |
| **PacketSize** | Задаёт размер пакета для передачи файлов. Чем больше размер пакета, тем выше производительность сервера на этапе передачи клиенту результатов обработки запроса. Однако это справедливо только при надёжных каналах связи. Если связь плохая, большой размер пакета приведёт к частым сбоям и снижению производительности. Размер пакета задаётся в байтах. Начальное значение соответствует значению по умолчанию - **65000**. | & |
| **ListenQLen** | Задаёт максимальную длину очереди запросов на подключение к серверу. Чем больше очередь, тем вероятнее, что клиент, пусть даже после длительного ожидания, будет обслужен, а не получит от ворот поворот. Однако для обслуживания большой очереди требуется пропорциональное количество ресурсов сервера. Начальное значение соответствует значению по умолчанию - **1000**. | & |
| **WriteSocketRetryDelay** | Определяет величину задержки отслеживания событий при записи в основной сокет. Чем меньше значение этого параметра, тем оперативнее сервер реагирует на изменение состояния сокета, но, одновременно, тем больше потребление процессорного времени. Величина задержки задаётся в миллисекундах. Начальное значение соответствует значению по умолчанию - **200**. | & |
| **AuthCacheRefreshAge** | Задаёт длительность интервала хранения данных в кэше ускорителя авторизации. Чем меньше этот интервал, тем быстрее сервер реагирует на изменение настроек - и тем чаще вызывается процедура реальной авторизации, потребляя ресурсы сервера и вызывая задержки выполнения. Величина задержки задаётся в миллисекундах. Начальное значение соответствует значению по умолчанию - **900000** (15 минут). | & |
| **MaxConcurrentThreads** | Задаёт максимальное число одновременно работающих потоков сервера. Руководства по оптимизации производительности приложений рекомендуют два потока на каждый процессор. В текущей реализации этот параметр имеет смысл только при использовании модели пула потоков. Начальное значение соответствует значению по умолчанию - **10**. | & |
| **MaxSPoolLen** | Задаёт максимальную длину очереди подключений, передаваемых в пул потоков. Чем больше очередь, тем вероятнее, что клиент, пусть даже после длительного ожидания, будет обслужен, а не получит от ворот поворот. Однако для обслуживания большой очереди требуется пропорциональное количество ресурсов сервера. Начальное значение соответствует значению по умолчанию - **20**. | & |
| **MaxCgiCnt** | Задаёт максимальное количество одновременно выполняющихся сценариев CGI. Если этот предел превышен, клиент в ответ получает сообщение о высокой загрузке сервера и предложение зайти позже. Увеличение порога снижает вероятность появления этого сообщения, однако большое количество одновременно работающих сценариев создаёт большую нагрузку на сервер и может отрицательно сказаться на его производительности - вплоть до полного отказа в обслуживании. Начальное значение соответствует значению по умолчанию - **10**. | & |
| **MaxIsapiCnt** | Задаёт максимальное количество одновременно выполняющихся сценариев ISAPI. Если этот предел превышен, клиент в ответ получает сообщение о высокой загрузке сервера и предложение зайти позже. Увеличение порога снижает вероятность появления этого сообщения, однако большое количество одновременно работающих сценариев создаёт большую нагрузку на сервер и может отрицательно сказаться на его производительности - вплоть до полного отказа в обслуживании. Начальное значение соответствует значению по умолчанию - **10**. | & |

| | | |
|---|---|---|
| **MaxFcgiCnt** | Задаёт максимальное количество одновременно выполняющихся сценариев FastCGI. Если этот предел превышен, клиент в ответ получает сообщение о высокой загрузке сервера и предложение зайти позже. Увеличение порога снижает вероятность появления этого сообщения, однако большое количество одновременно работающих сценариев создаёт большую нагрузку на сервер и может отрицательно сказаться на его производительности - вплоть до полного отказа в обслуживании. Начальное значение соответствует значению по умолчанию - **10**. | & |
| **PublicUserInterface** | Определяет, доступен ли на стандартных (не администраторских) портах пользовательский web-интерфейс PigMail+PigProxy, представляющий собой виртуальный каталог **/my/**. Если параметр имеет ненулевое значение, то обращение к этому каталогу возможно при обращении на любой порт HTTP-сервера, в противном случае он автоматически доступен только на администраторских портах, и для его публикации, если таковая потребуется, придётся затратить некоторые усилия. Отключение публикации пользовательского интерфейса имеет смысл, если HTTP-сервер используется сам по себе, вне связки с прокси- и почтовым сервером, либо все пользователи находятся в пределах локальной сети. Начальное значение - **0**. | *<br>? |
| **PublicMailClassificator** | Определяет, доступен ли на стандартных (не администраторских) портах web-интерфейс переклассификатора писем, представляющий собой виртуальный каталог **/MailClassify/**. Публикация этого интерфейса имеет смысл в случае использования на почтовом сервере обучаемых спам-фильтров POPfile, SpamProtexx или LibSD, которые при детектировании спама передают отправителю соответствующую ссылку. Если параметр имеет ненулевое значение, интерфейс переклассификатора доступен при обращении к публичным портам HTTP-сервера. Начальное значение - **1**. | *<br>? |
| **UseMultiPort** | Определяет, использовать ли дополнительное расширение, позволяющее HTTP-серверу прослушивать произвольное количество портов, а не только четыре, принятые в качестве стандартных. Если при запуске сервера этот параметр имеет ненулевое значение, загружается специальный плагин **multiport**. Начальное значение - **1**. | *<br>& |
| **ListenPorts** | Список дополнительных прослушиваемых портов, используемый расширением **multiport**. Начальное значение - **{HTTP[Lists]}\ListenPorts.txt**. | |
| **UseIncludeUrl** | Определяет, использовать ли дополнительное расширение, позволяющее включать в выводимый результат содержимое, получаемое по другим ссылкам. В отличие от традиционной модели HTML-документа подгрузку стороннего содержимого организует не браузер, получивший инструкцию в тексте страницы, а сам сервер, браузер же получает "склеенный" документ. При работе с этим механизмом следует проявлять осторожность: с его "помощью" можно нагнать весьма ощутимый объём входящего трафика, поскольку все включаемые объекты предварительно загружаются на сервер (не сохраняясь при этом на самом сервере). Если при запуске сервера этот параметр имеет ненулевое значение, загружается специальный плагин **include_url**. Начальное значение - **1**. | *<br>& |
| **DirectoryListing** | Определяет, использовать ли дополнительное расширение, обеспечивающее вывод оглавления каталога, если в самом каталоге не обнаружен ни один из возможных индексных файлов (выводимых по умолчанию, если запрос содержит только имя каталога). Если при запуске сервера этот параметр имеет ненулевое значение, загружается специальный плагин **list_dir**. Начальное значение - **1**. | *<br>& |
| **UseSSI** | Определяет, использовать ли дополнительное расширение, обеспечивающее поддержку включений на стороне сервера (Server Side Includes - SSI). Этот механизм похож на включение объектов по ссылкам. Отличие заключается в том, что директивы SSI запускают специальные сценарии, результат работы которых включается в передаваемую клиенту информацию. Если при запуске сервера этот параметр имеет ненулевое значение, загружается специальный плагин **ssi**. Начальное значение - **1**. | *<br>& |

| | | |
|---|---|---|
| **DefaultSSIMode** | Определяет, использовать ли обработку директив SSI (при включённой поддержке), если режим не удалось определить по списку типов данных. Любое ненулевое значение параметра означает, что по умолчанию требуется поиск и обработка директив SSI. Начальное значение - **0**. | * ? |
| **UseDialer** | Определяет, использовать ли сервис модемного дозвона. Самому HTTP-серверу, разумеется, звонить некуда - сервис используется другими службами PigMail+PigProxy (обычно прокси-сервером). Если при запуске сервера этот параметр имеет ненулевое значение, загружается специальный плагин **day_dialer**. Начальное значение - **0**. | * & |
| **PublicDialerInterface** | Если сервис модемного дозвона задействован, то этот параметр определяет, доступен ли на стандартных (не администраторских) портах web-интерфейс модемного сервиса, представляющий собой виртуальные каталоги **/dial/** и **/hangup/**. При ненулевом значении параметра эти каталоги доступны при обращении к публичным портам. Начальное значение - **0**. | * ? |
| **DiscoverCountry** | Определяет, использовать ли дополнительное расширение, позволяющее переводить IP-адрес подключившегося клиента в географические координаты. Точность такого перевода, конечно, невелика - с точностью до государственных или административных границ, - но позволяет получить дополнительное статистическое измерение. Если при запуске сервера этот параметр имеет ненулевое значение, загружается специальный плагин **geo_ip**. Начальное значение - **1**. | * & |
| **UseRasManager** | Определяет, использовать ли дополнительное расширение - диспетчер модемных соединений. Активизированный диспетчер представляет собой встроенный сценарий, который при вызове включает в HTML-страницу список существующих модемных соединений, одновременно отображая их состояние и предоставляя возможность позвонить или, напротив, разорвать соединение. Если при запуске сервера этот параметр имеет ненулевое значение, загружается специальный плагин **ras_list**. Начальное значение - **0**. | * & |
| **UseAcls** | Указывает, использовать ли список контроля доступа к ресурсам HTTP-сервера. С помощью этого списка можно разделять исполняемые на сервере сценарии и обычные файлы данных и раздавать именные разрешения или запреты на обращения к ресурсам сервера (с использованием авторизации). Если при запуске сервера этот параметр имеет ненулевое значение, загружается специальный плагин **acl**, обеспечивающий поддержку списка доступа. В дальнейшем при возникновении проблем обработку списка доступа можно временно отключить, задав нулевое значение. Начальное значение - **1**. | * & ? |
| **AdminUseAcls** | Указывает, использовать ли списки контроля доступа к разделам web-интерфейса. С помощью этого списка можно разделять исполняемые на сервере сценарии и обычные файлы данных и раздавать именные разрешения или запреты на обращения к ресурсам сервера (с использованием авторизации). Если при запуске сервера этот параметр имеет ненулевое значение, загружается специальный плагин **acl**, обеспечивающий поддержку списка доступа. Одновременно появляется возможность предоставить право управления PigMail+PigProxy нескольким обычным пользователям PigMail+PigProxy. В дальнейшем при возникновении проблем обработку списка доступа можно временно отключить, задав нулевое значение. Начальное значение - **0**. | * & ? |
| **ACL** | Список прав доступа. Начальное значение - **{HTTP[Lists]}\ACL.txt**. | ? |
| **DefaultAccess** | Права доступа, назначаемые по умолчанию, если запрашиваемый объект не найден в списке прав доступа. Начальное значение - **ACCESS:GET**, код, который обозначает совокупность прав на чтение файла, его возможное исполнение, если это окажется сценарий, и вывод оглавления каталога, если запрашиваемым объектом окажется каталог. Подробно коды прав доступа описаны в приложении 1. | ? |

| | | |
|---|---|---|
| **DefaultRealm** | Имя зоны безопасности - Realm, - используемое в запросе сервера на авторизацию, если другое имя не было задано в списке управления доступом. Начальное значение - **{HTTP[DefaultAuthDomain]}**. | * ? |
| **DefaultForbiddenFlag** | Если в результате анализа списка контроля доступа посетитель не получает разрешения на выполнение своего запроса, существует два варианта отказа. Сервер может запросить повторную авторизацию, чтобы посетитель задал другие реквизиты, а может отказать жёстко и бескомпромиссно, без возможности выбрать более подходящий вариант авторизации. Если этот параметр имеет ненулевое значение, то в качестве умолчания (если запрашиваемый объект отсутствует в списке прав доступа, и уровень прав доступа по умолчанию не допускает выполнение запроса) выбирается жёсткий вариант. Начальное значение - **0**. | * ? |
| **PerlBin** | Путь к исполняемому файлу интерпретатора сценариев на языке **Perl**. Сам интерпретатор (на самом деле это весьма мощная система программирования, применение которой не ограничивается одними web-сценариями) в поставку не входит; при необходимости применения его следует загрузить отдельно. Современные дистрибутивы Perl включают различные варианты интерпретатора; здесь необходимо указать путь к исполняемому файлу с поддержкой режима CGI. Если в применении Perl нет необходимости, и интерпретатор не установлен, параметр можно не задавать. Начальное значение - **c:\perl\bin\perl.exe**. | * ? |
| **PhpBin** | Путь к исполняемому файлу интерпретатора сценариев на языке **PHP**. Сам интерпретатор в поставку не входит; при необходимости применения его следует загрузить отдельно. Современные дистрибутивы PHP включают различные варианты интерпретатора; здесь необходимо указать путь к исполняемому файлу с поддержкой режима CGI. Если в применении PHP нет необходимости, и интерпретатор не установлен, параметр можно не задавать. Начальное значение - **c:\php\php.exe**. | * ? |
| **PythonBin** | Путь к исполняемому файлу интерпретатора сценариев на языке **Python**. Сам интерпретатор (на самом деле это весьма мощная система программирования, применение которой не ограничивается одними web-сценариями) в поставку не входит; при необходимости применения его следует загрузить отдельно. Если в применении Python нет необходимости, и интерпретатор не установлен, параметр можно не задавать. Начальное значение - **c:\pyton20\python.exe**. | * ? |
| **ParserBin** | Путь к исполняемому файлу интерпретатора сценариев на языке **Parser**. Сам интерпретатор в поставку не входит; при необходимости применения его следует загрузить отдельно. Если в применении Parser нет необходимости, и интерпретатор не установлен, параметр можно не задавать. Начальное значение - **c:\parser\parser3.exe**. | * ? |
| **FSBin** | Путь к исполняемому файлу интерпретатора сценариев на языке **Forth**, входящего в поставку PigMail+PigProxy. Этот интерпретатор обслуживает пользовательский и администраторский web-интерфейс PigMail+PigProxy. Начальное значение - **..\script\fs\fs.exe**. | ? |
| **DefaultCgiTimeout** | Задаёт лимит времени выполнения сценариев CGI. Чтобы сценарии в результате ошибок в коде или из-за проблем взаимодействия с другими приложениями не зацикливались навечно, забивая оперативную память сервера и отбирая процессорное время, длительность их выполнения рекомендуется ограничивать. Лимит задаётся в миллисекундах. Указание нулевого значения снимает ограничение. Это общий параметр; для конкретных сценариев могут быть заданы специальные ограничения. Действие этого параметра не распространяется на сценарии web-интерфейса. Начальное значение - **0**. | * ? |

| | | |
|---|---|---|
| **NtImpersonateScripts** | Определяет, использовать ли имперсонализацию, то есть, выполнение в контексте безопасности определённого пользователя, при запуске CGI-сценариев. Использование имперсонализации позволяет ограничить доступ сценариев к критически важным системным данным и тем самым снижает опасность от использования периодически обнаруживающихся уязвимостей. Если при запуске сервера этот параметр имеет ненулевое значение, загружается специальный плагин **impersonation**, обеспечивающий поддержку имперсонализации. В дальнейшем при возникновении проблем имперсонализацию можно временно отключить, задав нулевое значение. Действие этого параметра не распространяется на сценарии web-интерфейса. Начальное значение - **0**. | * & ? |
| **NtScriptUser** | Имя учётной записи пользователя Windows NT, от имени которого следует запускать сценарии. Пользователь должен иметь необходимые для успешной работы права доступа. В минимальном варианте это право подключения к серверу по сети (именно в таком режиме происходит авторизация), права чтения и поиска файлов во всех каталогах PigMail+PigProxy, связанных с функционированием HTTP-сервера, права создания и записи файлов в каталогах оперативных и статистических журналов HTTP-сервера, а также в каталоге временных файлов. Дополнительные права определяются особенностями сценария, запускаемого от имени пользователя. Если учётная запись не задана, имперсонализация не выполняется. Это значение по умолчанию, которое может быть переопределено при анализе либо списка прав доступа, либо отдельного списка управления имперсонализацией. Начальное значение - пустая строка. | * ? |
| **NtScriptDomain** | Имя домена Active Directory или компьютера (чаще всего - локального, на котором установлен PigMail+PigProxy), по списку которого выполняется авторизация пользователя. Это значение по умолчанию, которое может быть переопределено при анализе либо списка прав доступа, либо отдельного списка управления имперсонализацией. Начальное значение - пустая строка. | * ? |
| **NtScriptPass** | Пароль пользователя Windows NT. Это значение по умолчанию, которое может быть переопределено при анализе либо списка прав доступа, либо отдельного списка управления имперсонализацией. Начальное значение - пустая строка. | * ? |
| **NtImpersonateAdminScripts** | Определяет, использовать ли имперсонализацию, то есть, выполнение в контексте безопасности определённого пользователя, при запуске CGI-сценариев web-интерфейса PigMail+PigProxy. Если требуется работать со списками пользователей и групп доменов Active Directory, то имперсонализация - наиболее удобный способ предоставить web-интерфейсу доступ к этой информации. Если при запуске сервера этот параметр имеет ненулевое значение, загружается специальный плагин **impersonation**, обеспечивающий поддержку имперсонализации. В дальнейшем при возникновении проблем имперсонализацию можно временно отключить, задав нулевое значение. Начальное значение - **0**. | * & ? |
| **NtAdminScriptUser** | Имя учётной записи пользователя Windows NT, от имени которого следует запускать сценарии web-интерфейса. Для обеспечения полной функциональности пользователь должен обладать правами администратора домена. Если учётная запись не задана, имперсонализация не выполняется. Это значение по умолчанию, которое может быть переопределено при анализе либо списка прав доступа, либо отдельного списка управления имперсонализацией. Начальное значение - пустая строка. | * ? |
| **NtAdminScriptDomain** | Имя домена Active Directory или компьютера (чаще всего - локального, на котором установлен PigMail+PigProxy), по списку которого выполняется авторизация пользователя. Это значение по умолчанию, которое может быть переопределено при анализе либо списка прав доступа, либо отдельного списка управления имперсонализацией. Начальное значение - пустая строка. | * ? |

| | | |
|---|---|---|
| **NtAdminScriptPass** | Пароль пользователя Windows NT. Это значение по умолчанию, которое может быть переопределено при анализе либо списка прав доступа, либо отдельного списка управления имперсонализацией. Начальное значение - пустая строка. | * ? |
| **SeparateImpersonationList** | Определяет, всегда ли использовать отдельный список управления имперсонализацией. Если подключён список прав доступа, то в нём тоже можно указать параметры имперсонализации для различных сценариев. Однако в некоторых случаях может быть удобнее использовать отдельный список. Если параметр имеет любое ненулевое значение, то отдельный список управления имперсонализацией используется независимо от наличия поддержки списка прав доступа. Начальное значение - **0**. | * ? |
| **ImpersonationList** | Список управления имперсонализацией. Начальное значение - **{HTTP[Lists]}\ImpersonationList.txt**. | ? |
| **LockIntruders** | Определяет, использовать ли блокировку атак. Признаком атаки считается частое повторение различных нежелательных событий - таких, как ошибки авторизации. Если частота следования таких событий для какого-либо IP-адреса клиентского подключения превышает установленную в настройках величину, то этот адрес заносится в список запрещённых сетей. IP-адреса, находящиеся в списках локальных или доверенных сетей, блокировке не подвергаются. Если при запуске сервера этот параметр имеет любое ненулевое значение, подключается плагин **ids_memo**, обеспечивающий хранение и накопление информации о нежелательных событиях. После этого параметр может использоваться для временного отключения блокировки атак, если его работа будет создавать какие-либо проблемы. Начальное значение - **{Server[LockIntruders]}**. | * ? |
| **AuthFailCount** | Пороговое значение числа ошибок авторизации. Если количество неудачных попыток авторизации за определённый временной интервал для одного и того же IP-адреса клиентского подключения превышает заданную этим параметром величину, это считается атакой - со всеми вытекающими отрицательными последствиями для соответствующего клиента. Начальное значение - **{Server[AuthFailCount]}**. | * ? |
| **AuthFailPeriod** | Период подсчёта ошибок авторизации. Если количество неудачных попыток авторизации за определённый этим параметром временной интервал для одного и того же IP-адреса клиентского подключения превышает заданную величину, это считается атакой - со всеми вытекающими отрицательными последствиями для соответствующего клиента. Длительность периода задаётся в минутах. Начальное значение - **{Server[AuthFailPeriod]}**. | * ? |
| **UseTarpit** | Указывает, использовать ли при выдаче отказов клиенту Tarpit - "липучку". В этом случае отрицательные ответы искусственно задерживаются, что уменьшает нагрузку на сеть. Начальное значение - **{Server[UseTarpit]}**. | * ? |
| **TarpitInterval** | Если задано использование "липучки", то этот параметр задаёт длительность задержки в секундах. Начальное значение - **{Server[TarpitInterval]}**. | * ? |
| **LogLevel** | Задаёт уровень детализации оперативного журнала HTTP-сервера. Параметр может принимать значения от 1 до 9. Чем выше уровень, тем больше подробностей пишется в журнал. Для совместимости с ранними версиями, в которых уровень детализации не задавался, нулевое значение соответствует максимальному уровню детализации. Начальное значение - **{Server[LogLevel]}**. | $ |

| | | |
|---|---|---|
| **LogAcl** | Указывает, вести ли дополнительный оперативный журнал обработки списков прав доступа. Если параметр имеет любое ненулевое значение, создаётся дополнительный журнал, в который записываются результаты сопоставления реквизитов пользователя и параметров запроса со списком прав доступа и предоставленные в результате права. Начальное значение - **1**. | * ? |
| **LogToEStat** | Определяет, ведёт ли сервер статистику в формате программы **Estat32**, разработанной **Андреем Волковым** из **EPE Labs** для обработки статистических журналов Eserv/2. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{Server[LogToEStat]}**. | $ |
| **LogToAdvSoft** | Определяет, ведёт ли сервер статистику в формате программ **ProxyInspector** и **MailDetective** производства компании **AdvSoft**. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{Server[LogToAdvSoft]}**. | $ |
| **LogToElog** | Определяет, ведёт ли сервер статистику в формате программы **Elog**, разработанной **Игорем Панасенко** из компании **ЛЭНК** для обработки статистических журналов Eserv/3. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{Server[LogToElog]}**. | $ |
| **LogToMaillog** | Определяет, ведёт ли сервер статистику в собственном текстовом формате. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{Server[LogToMaillog]}**. | $ |
| **LogToMStat** | Определяет, используется ли подсистема ведения статистики в базе данных MStat, разработанная Андреем Матвеевым. Этот сборщик статистики имеет немалое преимущество перед текстовыми журналами, позволяя хранить и эффективно обрабатывать статистическую информацию за большие периоды времени, измеряемые годами. Но для его работы необходима установка дополнительного приложения - СУБД одного из поддерживаемых сборщиком типов. Если при запуске сервера указано любое ненулевое число, загружается специальный плагин **mstat**. В дальнейшем при возникновении проблем сбор статистики в базе данных можно временно отключить, установив нулевое значение. Начальное значение - **{Server[LogToMStat]}**. | $ & |

## *Секция FTP - параметры настройки FTP-сервера*

| | | |
|---|---|---|
| **DefaultAuthDomain** | Домен авторизации по умолчанию для FTP-сервера. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[DefaultAuthDomain]}**. | $ |
| **DomainIP** | Файл со списком IP-адресов, назначенных сетевым интерфейсам компьютера. Переопределяет соответствующий параметр из секции **Lists**. Начальное значение - **{Lists[DomainIP]}**. | |
| **UserList** | Файл со списком пользователей формата Eserv/3 для FTP-сервера. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[UserList]}**. | |

| | | |
|---|---|---|
| **GroupList** | Файл со списком группировки пользователей формата Eserv/3 для FTP-сервера. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[GroupList]}**. | |
| **PlainUserList** | Файл с объединённым списком пользователей формата Eserv/3 для FTP-сервера. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[PlainUserList]}**. | ? |
| **PlainGroupList** | Файл со списком группировки пользователей формата Eserv/3 для FTP-сервера. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[PlainGroupList]}**. | ? |
| **Eserv2Userlist** | Файл со списком пользователей FTP-сервера, извлечённым из Eserv.ini версии Eserv/2.x. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[Eserv2Userlist]}**. | |
| **Eserv2Grouplist** | Файл со списком группировки пользователей FTP-сервера, извлечённым из Eserv.ini версии Eserv/2.x. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[Eserv2Grouplist]}**. | |
| **NTdomain** | Имя домена Active Directory или локального компьютера под управлением Windows линейки NT, по списку пользователей которого выполняется авторизация пользователей FTP-сервера, если выбран соответствующий способ авторизации (**NtLogon**). Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[NTdomain]}**. | ? |
| **DefaultAuthSource** | Имя источника авторизации на FTP-сервере из списка источников авторизации. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[DefaultAuthSource]}**. | ? |
| **AuthMethod** | Способ авторизации на FTP-сервере по умолчанию. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[AuthMethod]}**. | ? |
| **NtImpersonateLogon** | Определяет, требуется ли переключение в контекст безопасности пользователя при авторизации в домене Active Directory. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[NtImpersonateLogon]}**. | |
| **UseExtendedGroups** | Указывает, использовать ли расширенную (кросс-доменную) группировку пользователей. Переопределяет соответствующий параметр из секции **AUTH**. Если при запуске сервера этот параметр имеет любое ненулевое значение, то загружается специальный плагин **groups_ext**. Начальное значение - **{AUTH[UseExtendedGroups]}**. | * & |
| **ExtendedGroupList** | Файл с расширенным списком группировки пользователей для FTP-сервера. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[ExtendedGroupList]}**. | ? |
| **RejectNonexistentDomains** | Указывает, отвергать ли попытки авторизации, если домен авторизации не описан в настройках сервера. Переопределяет соответствующий параметр из секции **AUTH**. Начальное значение - **{AUTH[RejectNonexistentDomains]}**. | ? |
| **MaxAuthAttempts** | Максимально допустимое число попыток протокольной (не по IP/MAC-адресу) авторизации в одной сессии. Определяет, сколько неудачных попыток авторизации допускается в течение одной сессии. Если это число превышено, подключение считается атакой и разрывается. Если значение нулевое, то ограничения на число попыток подбора пароля отсутствуют. Начальное значение - **{AUTH[MaxAuthAttempts]}**. | ? |
| **CacheIni** | Для ускорения обработки запросов FTP-сервер может кэшировать в оперативной памяти ряд параметров конфигурационного файла. Кэширование производится только на время сессии - от подключения клиента до его отсоединения - и не влияет на параллельные сессии. Если кэширование создаёт проблемы, его можно отключить, установив этот параметр в ноль и перезапустив FTP-сервер. Начальное значение - **1**. | * & |

| | | |
|---|---|---|
| **Active** | Определяет, активен ли FTP-сервер. Если значение нулевое, то все попытки подключения отвергаются с кодом 4xx, что означает предложение повторить попытку позже. Если указано любое ненулевое число, сервер принимает подключения. Начальное значение - **1**. | |
| **Port** | Порт, на котором работает FTP-сервер. Начальное значение стандартное - **21**. | & |
| **SslPort** | Порт, на котором FTP-сервер принимает подключения по защищённому соединению. Начальное значение - **990**. | & |
| **NetworkInterface** | Адрес сетевого интерфейса, слушаемого сервером. Начальное значение - пустая строка; это означает, что сервер слушает все интерфейсы. | & |
| **SslNetworkInterface** | Адрес сетевого интерфейса, слушаемого сервером для приёма подключений по защищённому соединению. Начальное значение - пустая строка; это означает, что сервер слушает все интерфейсы. | & |
| **Certificate** | Имя файла формата PEM, содержащего закрытый ключ и сертификаты, используемые при организации защищённого (SSL) соединения сервера с клиентом. Переопределяет соответствующий параметр из секции **Server**. Начальное значение - **{Server[Certificate]}**. | $ |
| **SslVerifyClient** | Определяет режим проверки подлинности сертификатов клиентской стороны при установлении защищённого соединения. Переопределяет соответствующий параметр из секции **Server**. Начальное значение - **{Server[SslVerifyClient]}**. | $ |
| **MaxConnections** | Максимально допустимое число одновременных подключений к серверу. Позволяет противостоять пиковым нагрузкам и целенаправленным попыткам завалить сервер путём неумеренного потребления всех ресурсов компьютера. Начальное значение - **50**. | & |
| **MaxConnectionsFromIP** | Максимально допустимое число одновременных подключений к серверу с одного IP-адреса. В текущей версии эта настройка не поддерживается и зарезервирована на будущее. Начальное значение - **10**. | & |
| **AllowInterhost** | Позволяет разрешить так называемый режим межузловой передачи данных. По умолчанию FTP-сервер сверяет IP-адрес, указанный клиентом в команде PORT, с IP-адресом клиентского подключения, и при несовпадении отвергает команду. Если режим межузловой передачи разрешён, проверка не производится. Это позволяет размещать FTP-сервер внутри NAT или использовать в качестве источника или приёмника файлов другой узел сети, отличный от клиентского. Режим разрешён при любом ненулевом значении параметра. Это значение по умолчанию, которое может быть изменено в соответствии с настройками, заданными в списках локальных или доверенных сетей. Начальное значение - **0**. | $ |
| **Timeout** | Время бездействия, задаваемое в миллисекундах, по истечении которого сервер прекращает соединение с клиентом. Это вынужденная мера, предотвращающая утечку ресурсов при плохой связи - как правило, тайм-аут срабатывает, когда соединение уже фактически разорвано, но серверу неоткуда получить извещение об этом. Начальное значение - **60000**, что соответствует 10 минутам. | $ |
| **Lists** | Расположение каталога со списками настройки FTP-сервера. Начальное значение - **{Dirs[Lists]}\ftp**. | |
| **Templates** | Расположение каталога с шаблонами ответов FTP-сервера. Начальное значение - **{Dirs[Templates]}\ftp**. | |
| **Logs** | Расположение каталога оперативных журналов FTP-сервера. Начальное значение - **{Dirs[Logs]}**. | $ |
| **IpBlackList** | Список IP-адресов и подсетей, которым запрещено обращаться к FTP-серверу. Начальное значение - **{FTP[Lists]}\IpBlackList.txt**. | |

| | | |
|---|---|---|
| **LocalNetworks** | Список локальных сетей, обслуживаемых FTP-сервером. Переопределяет соответствующий параметр из секции **Lists**. Начальное значение - **{Lists[LocalNetworks]}**. | |
| **IpWhiteList** | Список доверенных IP-адресов или сетей, которые обслуживаются этим FTP-сервером. Этот список ДОПОЛНЯЕТ список локальных сетей. В нём могут быть не локальные сети, а, например, особые внешние IP-адреса. Начальное значение - **{FTP[Lists]}\IpWhiteList.txt**. | |
| **IpMacAuth** | Файл со списком, устанавливающим соответствие между IP и MAC адресами клиентского компьютера и именем учётной записи пользователя. Переопределяет соответствующий параметр из секции **Lists**. Начальное значение - **{Lists[IpMacAuth]}**. | |
| **UseIpAuth** | Указывает, использовать ли автоматическую авторизацию подключившегося пользователя на основании IP-адреса либо сочетания IP и MAC-адресов. Начальное значение - **0**, то есть, если прочие настройки сервера потребуют авторизации клиента, она должна быть выполнена явно. | * |
| **BindIpList** | Список управления привязкой IP-адресов при установлении соединения для передачи данных. Особенность протокола FTP заключается в том, что для обмена данными (загрузка файла или чтение FTP-каталога) требуется установить дополнительное соединение. При этом одна из сторон сообщает свой IP-адрес. FTP-сервер может оказаться такой стороной, если клиент выбрал пассивный режим соединения. Обычно он самостоятельно определяет адрес для объявления, однако при некоторых конфигурациях сети (например, наличие NAT-сервера), он может выбрать неверное значение - просто потому, что реальный адрес, видимый со стороны клиента, отличается от адреса сетевого интерфейса и FTP-серверу неизвестен. Если IP-адрес клиента не принадлежат локальной сети, FTP-сервер использует адрес, определённый параметром **Server[ExternIP]**. В базовых конфигурациях, когда имеется всего две сетевые карты, одна из которых подключена к локальной сети, а вторая обеспечивает непосредственный выход в глобальную сеть, этого достаточно. Если сетевых интерфейсов больше двух либо используются сложные правила маршрутизации, необходимы сложные же правила выбора объявляемого IP-адреса, записываемые в список управления привязкой. Начальное значение - **{FTP[Lists]}\BindIpList.txt**. | ? |
| **VirtualFolders** | Список виртуальных каталогов - отображений логического пути к объекту, переданного в запросе клиента, на физические каталоги сервера. Отображение может зависеть от множества параметров. Обычно в качестве ключевых параметров используются IP-адрес клиента, учётная запись пользователя, фрагмент пути к запрашиваемому объекту. Сопоставляя эти и другие параметры запроса с содержимым списка, сервер определяет физический каталог, в котором следует искать запрашиваемый объект. Начальное значение - **{FTP[Lists]}\VirtualFolders.txt**. | ? |
| **DefaultDocumentRoot** | Корневой каталог, который выбирается по умолчанию, если выполнить отображение по списку виртуальных каталогов не удалось. Начальное значение - **{Dirs[Pub]}\ftproot**. | ? |
| **UsePerformanceTuning** | Определяет, применять ли собственные нестандартные значения двух перечисленных ниже параметров тонкой настройки производительности или же оставить заданные в коде сервера значения по умолчанию. Если сервер успешно справляется с нагрузкой, эти настройки лучше оставить как есть. Если при запуске сервера этот параметр имеет ненулевое значение, вместо значений по умолчанию применяются собственные нестандартные значения. Начальное значение - **0**. | & |
| **PacketSize** | Задаёт размер пакета для передачи файлов. Чем больше размер пакета, тем выше производительность сервера на этапе передачи клиенту результатов обработки запроса. Однако это справедливо только при надёжных каналах связи. Если связь плохая, большой размер пакета приведёт к частым сбоям и снижению производительности. Размер пакета задаётся в байтах. Начальное значение соответствует значению по умолчанию - **65000**. | & |

| | | |
|---|---|---|
| **ListenQLen** | Задаёт максимальную длину очереди запросов на подключение к серверу. Чем больше очередь, тем вероятнее, что клиент, пусть даже после длительного ожидания, будет обслужен, а не получит от ворот поворот. Однако для обслуживания большой очереди требуется пропорциональное количество ресурсов сервера. Начальное значение соответствует значению по умолчанию - **1000**. | & |
| **WriteSocketRetryDelay** | Определяет величину задержки отслеживания событий при записи в основной сокет. Чем меньше значение этого параметра, тем оперативнее сервер реагирует на изменение состояния сокета, но, одновременно, тем больше потребление процессорного времени. Величина задержки задаётся в миллисекундах. Начальное значение соответствует значению по умолчанию - **200**. | & |
| **DiscoverCountry** | Определяет, использовать ли дополнительное расширение, позволяющее переводить IP-адрес подключившегося клиента в географические координаты. Точность такого перевода, конечно, невелика - с точностью до государственных или административных границ, - но позволяет получить дополнительное статистическое измерение. Если при запуске сервера этот параметр имеет ненулевое значение, загружается специальный плагин **geo_ip**. Начальное значение - **1**. | *<br>& |
| **UseAcls** | Указывает, использовать ли список контроля доступа к ресурсам FTP-сервера. С помощью этого списка можно раздавать именные разрешения или запреты на обращения к ресурсам сервера (с использованием авторизации). Если при запуске сервера этот параметр имеет ненулевое значение, загружается специальный плагин **acl**, обеспечивающий поддержку списка доступа. В дальнейшем при возникновении проблем обработку списка доступа можно временно отключить, задав нулевое значение. Начальное значение - **1**. | *<br>&<br>? |
| **ACL** | Список прав доступа. Начальное значение - **{FTP[Lists]}\ACL.txt**. | ? |
| **DefaultAccess** | Права доступа, назначаемые по умолчанию, если запрашиваемый объект не найден в списках прав доступа. Начальное значение - **ACCESS:NOEXEC**, код, который обозначает совокупность прав на чтение, запись и удаление файла, а также вывод оглавления каталога. Подробно коды прав доступа описаны в приложении 1. | ? |
| **DefaultGuestAccess** | Права доступа, назначаемые по умолчанию в случае гостевого входа, если запрашиваемый объект не найден в списках прав доступа. Начальное значение - **ACCESS:RETR**, код, который обозначает совокупность прав на чтение файла и вывод оглавления каталога. Подробно коды прав доступа описаны в приложении 1. | ? |
| **DefaultRealm** | Имя зоны безопасности - Realm, - используемое в ответе-отказе сервера, если другое имя не было задано в списке управления доступом. Начальное значение - **{FTP[DefaultAuthDomain]}**. | *<br>? |
| **DefaultForbiddenFlag** | Если в результате анализа списка контроля доступа посетитель не получает разрешения на выполнение своего запроса, существует два варианта отказа. Собственно отказ следует в обоих вариантах, разница лишь в форме. Сервер может сообщить имя зоны безопасности, чтобы посетитель при повторном подключении к серверу задал другие реквизиты, а может отказать жёстко и бескомпромиссно, без объяснения причин. Если этот параметр имеет ненулевое значение, то в качестве умолчания (если запрашиваемый объект отсутствует в списке прав доступа, и уровень прав доступа по умолчанию не допускает выполнение запроса) выбирается жёсткий вариант. Начальное значение - **0**. | *<br>? |

| | | |
|---|---|---|
| **AllowAnonymousAccess** | Определяет, разрешён ли к серверу анонимный доступ. Если параметр имеет ненулевое значение, то любой посетитель, указавший имя **anonymous** или **ftp** и абсолютно произвольную строку в качестве пароля, получает разрешение на гостевой доступ, при котором разрешено только чтение. Применяя список управления доступом, гостя можно ещё сильнее ограничить в правах, но сама возможность свободного входа при этом сохраняется. Отменить её можно, указав нулевое значение. Начальное значение - **1**. | * |
| **AllowPowerAnonymous** | Определяет, разрешена ли анонимным посетителям запись в каталоги FTP-сервера. По умолчанию анонимные посетители могут только читать файлы и просматривать оглавления каталогов. Значение этого параметра имеет смысл, если анонимные пользователи имеют доступ к серверу, а также используются списки контроля доступа к FTP-серверу. Если параметр имеет любое ненулевое значение, то анонимные пользователи получают принципиальную возможность записи, а права их ограничиваются только списками прав доступа. Начальное значение - **0**. | * |
| **LockIntruders** | Определяет, использовать ли блокировку атак. Признаком атаки считается частое повторение различных нежелательных событий - таких, как ошибки авторизации. Если частота следования таких событий для какого-либо IP-адреса клиентского подключения превышает установленную в настройках величину, то этот адрес заносится в список запрещённых сетей. IP-адреса, находящиеся в списках локальных или доверенных сетей, блокировке не подвергаются. Если при запуске сервера этот параметр имеет любое ненулевое значение, подключается плагин **ids_memo**, обеспечивающий хранение и накопление информации о нежелательных событиях. После этого параметр может использоваться для временного отключения блокировки атак, если его работа будет создавать какие-либо проблемы. Начальное значение - **{Server[LockIntruders]}**. | * ? |
| **AuthFailCount** | Пороговое значение числа ошибок авторизации. Если количество неудачных попыток авторизации за определённый временной интервал для одного и того же IP-адреса клиентского подключения превышает заданную этим параметром величину, это считается атакой - со всеми вытекающими отрицательными последствиями для соответствующего клиента. Начальное значение - **{Server[AuthFailCount]}**. | * ? |
| **AuthFailPeriod** | Период подсчёта ошибок авторизации. Если количество неудачных попыток авторизации за определённый этим параметром временной интервал для одного и того же IP-адреса клиентского подключения превышает заданную величину, это считается атакой - со всеми вытекающими отрицательными последствиями для соответствующего клиента. Длительность периода задаётся в минутах. Начальное значение - **{Server[AuthFailPeriod]}**. | * ? |
| **UseTarpit** | Указывает, использовать ли при выдаче отказов клиенту Tarpit - "липучку". В этом случае отрицательные ответы искусственно задерживаются, что уменьшает нагрузку на сеть. Начальное значение - **{Server[UseTarpit]}**. | * ? |
| **TarpitInterval** | Если задано использование "липучки", то этот параметр задаёт длительность задержки в секундах. Начальное значение - {**Server[TarpitInterval]}**. | * ? |
| **LogLevel** | Задаёт уровень детализации оперативного журнала FTP-сервера. Параметр может принимать значения от 1 до 9. Чем выше уровень, тем больше подробностей пишется в журнал. Для совместимости с ранними версиями, в которых уровень детализации не задавался, нулевое значение соответствует максимальному уровню детализации. Начальное значение - **{Server[LogLevel]}**. | $ |

| | | |
|---|---|---|
| **LogAcl** | Указывает, вести ли дополнительный оперативный журнал обработки списков прав доступа. Если параметр имеет любое ненулевое значение, создаётся дополнительный журнал, в который записываются результаты сопоставления реквизитов пользователя и параметров запроса со списком прав доступа и предоставленные в результате права. Начальное значение - **1**. | * ? |
| **LogToEStat** | Определяет, ведёт ли сервер статистику в формате программы **Estat32**, разработанной **Андреем Волковым** из **EPE Labs** для обработки статистических журналов Eserv/2. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{Server[LogToEStat]}**. | $ |
| **LogToAdvSoft** | Определяет, ведёт ли сервер статистику в формате программ **ProxyInspector** и **MailDetective** производства компании **AdvSoft**. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{Server[LogToAdvSoft]}**. | $ |
| **LogToElog** | Определяет, ведёт ли сервер статистику в формате программы **Elog**, разработанной **Игорем Панасенко** из компании **ЛЭНК** для обработки статистических журналов Eserv/3. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{Server[LogToElog]}**. | $ |
| **LogToMaillog** | Определяет, ведёт ли сервер статистику в собственном текстовом формате. Существует несколько различных систем обработки статистики, использующих различный формат журналов. Чтобы не перегружать диск сервера лишними файлами, можно выбрать вывод статистики вполне определённого формата. Если указано любое ненулевое число, статистика в этом формате ведётся. Начальное значение - **{Server[LogToMaillog]}**. | $ |
| **LogToMStat** | Определяет, используется ли подсистема ведения статистики в базе данных MStat, разработанная Андреем Матвеевым. Этот сборщик статистики имеет немалое преимущество перед текстовыми журналами, позволяя хранить и эффективно обрабатывать статистическую информацию за большие периоды времени, измеряемые годами. Но для его работы необходима установка дополнительного приложения - СУБД одного из поддерживаемых сборщиком типов. Если при запуске сервера указано любое ненулевое число, загружается специальный плагин **mstat**. В дальнейшем при возникновении проблем сбор статистики в базе данных можно временно отключить, установив нулевое значение. Начальное значение - **{Server[LogToMStat]}**. | $ & |

## *Секция Antivirus - общие параметры модулей антивирусной проверки*

| | | |
|---|---|---|
| **BinRoot** | Расположение базового каталога всех антивирусных ядер. Путь задаётся относительно EXE-файлов серверов, для которых "корневой" каталог является родительским. Поэтому начальное значение - **..\antivirus**. | |
| **UpdateInterval** | Период загрузки обновлений вирусных баз, задаваемый в минутах. Указание нулевого значения приостанавливает загрузку. Начальное значение - **30**. | * |
| **ReloadInterval** | Период перезагрузки обновлённых вирусных баз, задаваемый в минутах. На самом деле с заданной периодичностью выполняется проверка параметров флаг-файла, а собственно перезагрузка выполняется при их изменении. Начальное значение - **5**. | * |

| | | |
|---|---|---|
| **ProxyPerformsUpdate** | Параметр относится к настройкам прокси-сервера и указывает, выполняет ли он автоматическую загрузку обновлений вирусных баз. Начальное значение - **0**, то есть, прокси-сервер в этом не участвует. | * |
| **SMTPPerformsUpdate** | Параметр относится к настройкам SMTP-сервера и указывает, выполняет ли он автоматическую загрузку обновлений вирусных баз. Начальное значение - **0**, то есть, SMTP-сервер в этом не участвует. | * |

## *Секция AntivirusKAV - параметры настройки антивируса KAV версии 4*

| | | |
|---|---|---|
| **Bin** | Каталог расположения файлов ядра антивируса KAV версии 4. Это исполняемые файлы пакета **KAVSS**. Начальное значение - **{Antivirus[BinRoot]}\kav**. | & |
| **Data** | Каталог расположения вирусных баз KAV - это файлы с расширением **AVC** и несколько управляющих файлов. Начальное значение - **{AntivirusKAV[Bin]}\data**. | * & |
| **Updater** | Командная строка, посредством которой запускается процедура загрузки обновления вирусных баз KAV. Обратите внимание - в данном случае запуск выполняется с помощью командного файла, поэтому в командной строке указан запуск командного процессора, которому в качестве параметра передаётся команда интерпретации этого файла. Командный процессор **cmd.exe** имеется только в операционных системах класса NT (NT 4/2000/XP/2003), при использовании сервера под управлениям Windows 98 или ME следует указать другой командный процессор - **command.com**. Начальное значение - **"cmd.exe /C {AntivirusKAV[Bin]}\klav_bases_updater.bat"**. | |
| **UpdateInterval** | Период загрузки обновлений вирусных баз KAV, задаваемый в минутах. Указание нулевого значения приостанавливает загрузку. Начальное значение - **{Antivirus[UpdateInterval]}**. | |
| **ReloadInterval** | Период перезагрузки обновлённых вирусных баз KAV, задаваемый в минутах. На самом деле с заданной периодичностью выполняется проверка параметров флаг-файла, а собственно перезагрузка выполняется при их изменении. Идея такой адаптивной перезагрузки позаимствована у разработчиков Dr.Web. Начальное значение - **{Antivirus[ReloadInterval]}**. | |
| **FlagFile** | Флаг-файл, параметры которого проверяются для определения необходимости перезагрузки вирусных баз KAV. Начальное значение - **{AntivirusKAV[Data]}\u0607g.xml**, это файл-идентификатор набора баз, изменяющийся чаще всего. | |
| **ProxyPerformsUpdate** | Параметр относится к настройкам прокси-сервера и указывает, выполняет ли он автоматическую загрузку обновлений вирусных баз KAV. Такие индивидуальные настройки имеют смысл, если разные серверы используют разные антивирусы. Начальное значение - **{Antivirus[ProxyPerformsUpdate]}**. | & |
| **SMTPPerformsUpdate** | Параметр относится к настройкам SMTP-сервера и указывает, выполняет ли он автоматическую загрузку обновлений вирусных баз KAV. Такие индивидуальные настройки имеют смысл, если разные серверы используют разные антивирусы. Начальное значение - **{Antivirus[SMTPPerformsUpdate]}**. | & |

## *Секция AntivirusKAV5 - параметры настройки антивируса KAV версии 5*

| | | |
|---|---|---|
| **Bin** | Каталог расположения файлов ядра антивируса KAV версии 5. Это исполняемые файлы пакета **KAVE**. Начальное значение - **{Antivirus[BinRoot]}\kav5**. | & |
| **Data** | Каталог расположения вирусных баз KAV - это файлы с расширением **AVC** и несколько управляющих файлов. Поскольку антивирусные базы для всех версий KAV общие, то начальное значение - **{AntivirusKAV[Data]}**. | * & |

| | | |
|---|---|---|
| **MaxScanningProcesses** | Для антивирусного сканирования KAVE использует отдельный процесс, причём не обязательно один. По умолчанию число сканирующих процессов равно числу процессоров - неважно, физических или виртуальных, порождённых технологией HyperThreading. Это хорошо с точки зрения распределения нагрузки. Минус такого решения - немаленький объём оперативной памяти, занимаемой каждым процессом и определяемый в основном объёмом загружаемых вирусных баз. Этот параметр позволяет явно ограничить число создаваемых сканирующих процессов. Если при старте сервера он имеет ненулевое значение, то это значение и определит максимальное число процессов. Следует учесть, что для SMTP- и прокси-сервера создаются отдельные независимые сканирующие процессы. Начальное значение - **0**. | * & |
| **Updater** | Командная строка, посредством которой запускается процедура загрузки обновления вирусных баз KAV. Начальное значение - **"cmd.exe /C {AntivirusKAV[Bin]}\kav5_bases_updater.bat"**. | |
| **UpdateInterval** | Период загрузки обновлений вирусных баз KAV, задаваемый в минутах. Указание нулевого значения приостанавливает загрузку. Начальное значение - **{Antivirus[UpdateInterval]}**. | |
| **ReloadInterval** | Период перезагрузки обновлённых вирусных баз KAV, задаваемый в минутах. На самом деле с заданной периодичностью выполняется проверка параметров флаг-файла, а собственно перезагрузка выполняется при их изменении. Идея такой адаптивной перезагрузки позаимствована у разработчиков Dr.Web. Начальное значение - **{Antivirus[ReloadInterval]}**. | |
| **FlagFile** | Флаг-файл, параметры которого проверяются для определения необходимости перезагрузки вирусных баз KAV. Начальное значение - **{AntivirusKAV5[Data]}\u0607g.xml**, это файл-идентификатор набора баз, изменяющийся чаще всего. | |
| **ProxyPerformsUpdate** | Параметр относится к настройкам прокси-сервера и указывает, выполняет ли он автоматическую загрузку обновлений вирусных баз KAV. Такие индивидуальные настройки имеют смысл, если разные серверы используют разные антивирусы. Начальное значение - **{Antivirus[ProxyPerformsUpdate]}**. | & |
| **SMTPPerformsUpdate** | Параметр относится к настройкам SMTP-сервера и указывает, выполняет ли он автоматическую загрузку обновлений вирусных баз KAV. Такие индивидуальные настройки имеют смысл, если разные серверы используют разные антивирусы. Начальное значение - **{Antivirus[SMTPPerformsUpdate]}**. | & |

## *Секция AntivirusDrWEB - параметры настройки антивируса Dr.Web*

| | | |
|---|---|---|
| **Bin** | Каталог расположения файлов ядра антивируса Dr.Web. Это библиотека **DrWeb32.dll** и модуль обновления **DrWebUpw.exe**. Начальное значение - **{Antivirus[BinRoot]}\drweb**. | & |
| **Data** | Каталог расположения вирусных баз Dr.Web - это файлы с расширением **VDB**. Если предполагается использовать автоматическую загрузку обновлений вирусных баз, то они должны располагаться в одном каталоге с файлами ядра. Начальное значение - **{AntivirusDrWEB[Bin]}**. | * & |
| **UpdaterLog** | Путь к файлу протокола обновления вирусных баз Dr.Web. Начальное значение - **{AntivirusDrWEB[Bin]}\drwebupw.log**. | |
| **Updater** | Командная строка, посредством которой запускается процедура загрузки обновления вирусных баз Dr.Web. Начальное значение - **" {AntivirusDrWEB[Bin]}\Drwebupw.exe /go /st /dir:{"}{AntivirusDrWEB[Data] MakeFullName}{"} /rp+{"}{AntivirusDrWEB[UpdaterLog] MakeFullName}{"}"**. | |
| **UpdateInterval** | Период загрузки обновлений вирусных баз Dr.Web, задаваемый в минутах. Указание нулевого значения приостанавливает загрузку. Начальное значение - **{Antivirus[UpdateInterval]}**. | |

| | | |
|---|---|---|
| **ReloadInterval** | Период перезагрузки обновлённых вирусных баз Dr.Web, задаваемый в минутах. На самом деле с заданной периодичностью выполняется проверка параметров флаг-файла, а собственно перезагрузка выполняется при их изменении. Идея такой адаптивной перезагрузки позаимствована у разработчиков Dr.Web. Начальное значение - **{Antivirus[ReloadInterval]}**. | |
| **FlagFile** | Флаг-файл, параметры которого проверяются для определения необходимости перезагрузки вирусных баз Dr.Web. Начальное значение - **{AntivirusDrWEB[Data]}\DRWTODAY.VDB**, это файл "горячего" дополнения, изменяющийся чаще всего. | |
| **ProxyPerformsUpdate** | Параметр относится к настройкам прокси-сервера и указывает, выполняет ли он автоматическую загрузку обновлений вирусных баз Dr.Web. Такие индивидуальные настройки имеют смысл, если разные серверы используют разные антивирусы. Начальное значение - **{Antivirus[ProxyPerformsUpdate]}**. | & |
| **SMTPPerformsUpdate** | Параметр относится к настройкам SMTP-сервера и указывает, выполняет ли он автоматическую загрузку обновлений вирусных баз Dr.Web. Такие индивидуальные настройки имеют смысл, если разные серверы используют разные антивирусы. Начальное значение - **{Antivirus[SMTPPerformsUpdate]}**. | & |

## *Секция AntivirusClamAV - параметры настройки антивируса ClamAV*

| | | |
|---|---|---|
| **Bin** | Каталог расположения файлов ядра антивируса ClamAV. Это исполняемые файлы пакета, которые можно загрузить отдельно с **www.eserv.ru**. Начальное значение - **{Antivirus[BinRoot]}\clamav**. | & |
| **Data** | Каталог расположения вирусных баз ClamAV. Вообще-то ClamAV имеет свою собственную систему настроек, где указан и этот каталог. PigMail+PigProxy использует его с единственной целью - для определения даты последней актуализации вирусных баз ClamAV. Начальное значение - **{AntivirusClamAV[Bin]}\share\clamav**. | |
| **ClamD** | Командная строка, посредством которой выполняется запуск демона ClamAV. Демон функционирует как отдельный процесс, компоненты PigMail+PigProxy передают ему для проверки файлы и получают ответ. Основные настройки антивируса задаются в отдельном конфигурационном файле **clamav.conf**. Начальное значение - **"{AntivirusClamAV[Bin]}\clamd.exe"**. | |
| **Updater** | Командная строка, посредством которой запускается процедура загрузки обновления вирусных баз ClamAV. Собственно, это даже не процедура, а отдельное приложение-демон, функционирующее самостоятельно и независимо от PigMail+PigProxy в соответствии с заданными в конфигурационном файле clamav.conf настройками, - достаточно его запустить. Поэтому нет никакого смысла задавать в этой секции периодичность обновления и определять, какой из компонентов PigMail+PigProxy будет этим заниматься. Начальное значение - **"{AntivirusClamAV[Bin]}\freshclam.exe -d"**. | |

## *Секция SNMP - параметры настройки агента SNMP*

| | | |
|---|---|---|
| **UseSnmpAgent** | Указывает, задействовать ли протокол SNMP (Simple Network Management Protocol - простой протокол управления сетью). Если задано любое ненулевое значение, то каждый сервер, входящий в состав PigMail+PigProxy при своём запуске активизирует агента SNMP. Агент принимает команды на порт UDP, номер которого совпадает с номером основного порта TCP соответствующего сервера. Для SMTP-сервера это **SMTP[Port]**, для POP/IMAP-сервера - **IMAP[Port]**, для прокси-сервера - **HttpProxy[Port]**, для HTTP-сервера - **HTTP[Port]**, для FTP-сервера - **FTP[Port]**. Начальное значение - **1**. | * & |
| **NetworkInterface** | Адрес сетевого интерфейса, слушаемого агентом SNMP. Начальное значение - пустая строка; это означает, что агент слушает все интерфейсы. | * & |
| **ReadonlyCommunity** | SNMP-community - наименование группы (канала, сообщества, зоны безопасности) - для использования в запросах на получение информации. При несовпадении community, указанного в SNMP-запросе, с заданным здесь, PigMail+PigProxy не будет отвечать на запрос. Начальное значение - **pigmail_monitor**. | & |

| | | |
|---|---|---|
| **ReadwriteCommunity** | SNMP-community для использования в запросах на запись управляющей информации. При несовпадении community, указанного в SNMP-запросе, с заданным здесь, PigMail+PigProxy не будет отвечать на запрос. Начальное значение - **pigmail_control**. | & |

## *Секция FireWall - параметры настройки межсетевого экрана (брандмауэра)*

| | | |
|---|---|---|
| **UseFireWall** | Указывает, задействовать ли межсетевой экран, именуемый также брандмаэуром и файрволом. В PigMail+PigProxy экран использует стандартные для Windows (версий 2000, XP, 2003) средства фильтрации пакетов, поэтому не конфликтует ни с системой, ни с компонентами PigMail+PigProxy, ни с другими сетевыми приложениями. Если при запуске сервера параметр имеет любое ненулевое значение, активируется и настраивается фильтр пакетов IP, обслуживаемый плагином **firewall**. Начальное значение - **0**. | * & |
| **Lists** | Расположение каталога со списками настройки межсетевого экрана. Начальное значение - **{Dirs[Lists]}\firewall**. | |
| **Log** | Расположение каталога журналов межсетевого экрана. Начальное значение - **{Dirs[Logs]}**. | |
| **NetworkInterfaceList** | Список защищаемых сетевых интерфейсов сервера. Начальное значение - **{FireWall[Lists]}\InterfaceList.txt**. | & |
| **BlockList** | Список правил блокировки пакетов. Правила определяют, с какого порта какой подсети на какой порт какой подсети пакеты не должны передаваться. Начальное значение - **{FireWall[Lists]}\BlockList.txt**. | & |
| **DropStandardRules** | Определяет, устанавливать ли стандартные правила блокировки для каждого защищаемого интерфейса или же использовать только правила, явно определённые в списке. Стандартные правила блокируют входящие пакеты на 135 и 139 порты (самые уязвимые и поэтому наиболее часто атакуемые). Начальное значение - **0**, стандартные правила применяются. | * & |

## *Секция IDS - параметры настройки системы блокировки атак*

| | | |
|---|---|---|
| **UseIDS** | Указывает, задействовать ли совместно с межсетевым экраном систему блокировки атак. Работа системы основана на статистическом анализе частоты подключений с одного IP-адреса. Если число подключений за определённый оценочный период превысит заданное значение, адрес заносится в чёрный список нарушителей, и все последующие попытки подключения с этого адреса в течение некоторого времени будут отвергаться. Если частота попыток подключения за это время падает ниже пороговой, то приём подключений возобновляется. Если при запуске сервера этот параметр имеет любое ненулевое значение, и разрешено использование межсетевого экрана, то активируется система блокировки атак. Начальное значение - **1**. | * & |
| **IpStatPeriod** | Длительность периода оценки в миллисекундах. Начальное значение - **1000**. | * & |
| **IpAllowedCnt** | Допустимое за период оценки число попыток подключения с одного IP-адреса. Начальное значение - **10**. | * & |
| **IpBlockPeriods** | Количество периодов оценки, на которое блокируется доступ. Начальное значение - **5**. | * & |

## *Секция MStat - параметры настройки подсистемы ведения статистики в базе данных MStat*

| | | |
|---|---|---|
| **ConnectionDefFile** | Путь к файлу параметров подключения к базе данных. Начальное значение - **{Dirs[Lists]}\mstat\ConnectionDefs.ini**. | & |

| | | |
|---|---|---|
| **AcWebReportsOnly** | Определяет, используется ли HTTP-сервер только для построения и вывода статистических отчётов. Если параметр имеет любое ненулевое значение, считается, что другой работы у сервера нет, и вести статистику его работы нет необходимости. На самом деле ведение статистики HTTP-сервера в базе данных управляется другими настройками, а этот флаг активирует необходимый для вывода отчётов плагин **mstat**, даже если ведение статистики отключено. Начальное значение - **0**. | * & |
| **GridRecordsOnPage** | Задаёт количество записей, отображаемых на одной странице отчёта. Начальное значение - **25**. | |
| **Language** | Задаёт язык web-интерфейса плагина и формы построения отчётов. В текущей версии поддерживаются следующие языки:<br>**RU** - русский;<br>**EN** - английский.<br>Начальное значение - **RU**. | * |
| **UseGeoIP** | Определяет, использовать ли дополнительное расширение, позволяющее переводить IP-адрес подключившегося клиента в географические координаты. Точность такого перевода, конечно, невелика - с точностью до государственных или административных границ, - но позволяет получить дополнительное статистическое измерение. Если при запуске сервера этот параметр имеет ненулевое значение, загружается специальный плагин **geo_ip**. Начальное значение - **1**. | * & |

## Назначение и формат управляющих списков

Все управляющие текстовые списки имеют сходный формат, пригодный для обработки стандартным ODBC-драйвером Microsoft для текстовых файлов. Каждая строка списка представляет собой одну запись, состоящую из полей, разделённых точками с запятой. Первая строка списка определяет символические имена полей, используемые при их обработке посредством ODBC-драйвера. Поиск в списке всегда производится по первому полю без учёта регистра символов. Это поле может содержать шаблон, то есть, строку с символами подстановки: **?** (означает один любой символ) и ***** (означает любое количество, в том числе и нулевое, любых символов). Существует также специальный символ "квотирования" ("закавычивания") \, используемый для вставки в шаблон специальных символов в своём "изначальном" значении - то есть, последовательность **\?** означает уже не символ подстановки, а обычный символ знака вопроса, ***** - символ звёздочки, **** - одиночный символ обратной косой черты. Кроме того, символ квотирования применяется для задания дополнительных специальных образцов:

| | |
|---|---|
| **\q** | Символ кавычки **"**. Кавычки используются для ограничения текстовых строк, содержащих в себе пробелы и символы точки с запятой, поэтому вставить их в строку не так просто. |
| **\0** | Любая десятичная цифра. |
| **\#** | Любая шестнадцатиричная цифра. |
| **\$** | Любая латинская буква. |
| **\|** | Символ-разделитель. В текущей версии разделителями считаются пробел и символы из набора **~`'\|+-=_)(<>,.[]{}:^&*%$;#@!/?\"**. |
| **\%** | Любой символ, не являющийся десятичной цифрой. |
| **\&** | Любой символ, не являющийся шестнадцатиричной цифрой. |
| **\!** | Любой символ, не являющийся латинской буквой. |
| **\@** | Любой символ, не являющийся разделителем. |
| **\d** | Любое количество, в том числе и нулевое, десятичных цифр. |
| **\h** | Любое количество, в том числе и нулевое, шестнадцатеричных цифр. |
| **\a** | Любое количество, в том числе и нулевое, латинских букв. |
| **\s** | Любое количество, в том числе и нулевое, символов-разделителей. |
| **\D** | Любое количество, в том числе и нулевое, символов, не являющихся десятичными цифрами. |
| **\H** | Любое количество, в том числе и нулевое, символов, не являющихся шестнадцатиричными цифрами. |
| **\A** | Любое количество, в том числе и нулевое, символов, не являющихся латинскими буквами. |
| **\S** | Любое количество, в том числе и нулевое, символов, не являющихся разделителями. |

Для удобства ведения в каждом каталоге со списками помещены таблицы Microsoft Excel и OpenOffice.org Calc, содержащие те же списки в более удобном для представления виде. Каждый список представляет собой один лист книги. С помощью внедрённых в таблицы макросов, запускаемых специальными кнопками дополнительной панели инструментов, можно выполнять экспорт листов в текстовые файлы и обратный импорт.

**Замечание.** В силу внутренних ограничений OpenOffice.org версий ниже 3 имена листов книги не могут содержать специальные символы (в частности, минусы и точки), допустимые в именах файлов. Поэтому имена листов могут не совпадать с именами соответствующих файлов управляющих списков. Реальные имена файлов хранятся в примечаниях к ячейке A1 каждого листа, удалять эти примечания не рекомендуется.

### *Общие списки*

Общие списки предназначены для управления всеми серверами пакета PigMail+PigProxy. Их исходное расположение, определяемое параметром **Dirs[Lists]**, - каталог **CONF\lists**.

#### *Список локальных доменов*

В этом списке перечислены домены авторизации и почтовые домены, а также заданы необходимые параметры этих доменов.

Расположение списка задаётся параметром **Lists[LocalDomains]**, исходное - **CONF\lists\LocalDomains.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **DOMAIN** | Имя домена. |
| 2 | **AUTH** | Имя источника авторизации в домене. Это поле имеет смысл для доменов авторизации. |
| 3 | **DIRECTORY** | Расположение почтовых ящиков домена. Это поле, как и последующие, имеет смысл для почтовых доменов. |
| 4 | **FLAGS** | Строка флагов-признаков для домена:<br>**A** (Accept) - указывает, принимать ли почту на адреса несуществующих почтовых ящиков домена. Этот флаг имеет силу, если одновременно установлен глобальный флаг **SMTP[AcceptNonExistentUsers]**;<br>**K** (Keep) - указывает, надо ли сохранять почту для несуществующих получателей как недоставленную - в отдельном каталоге. Этот флаг имеет силу, если одновременно установлен глобальный флаг **SMTP[KeepNonExistentUsersUndelivered]**;<br>**C** (Create) - указывает, надо ли автоматически создавать каталоги почтовых ящиков для несуществующих получателей домена. Этот флаг имеет силу, если одновременно установлен глобальный флаг **SMTP[CreateNonExistentUsersBoxes]**. Флаг **C** имеет приоритет над флагом **K**;<br>**B** (Bounce) - указывает, принимать ли почту, поступившую на адрес "отскока". В обычном режиме сервер отклоняет письмо под предлогом отсутствия получателя. Установка этого флага при условии, что установлен глобальный флаг **SMTP[AcceptBounce]**, позволяет превратить "вышибалу" в "пылесос" - сервер принимает письма на адрес "отскока" и помещает их в отдельный каталог, не формируя автоответов;<br>**M** (Multisite) - указывает, что почтовый домен обрабатывается в многосерверном режиме. В этом режиме предполагается, что сервер локально обслуживает лишь часть почтовых ящиков домена, отсутствующие почтовые ящики могут располагаться на других серверах, которые должны быть указаны в списке перенаправления почты. Если установлен этот флаг, а также глобальный флаг **SMTP[MultiSite]**, домен считается многосерверным;<br>**R** (Relay) - указывает, что локально отсутствующим отправителям, принадлежащим многосерверному домену, разрешено посылать не только входящую (на существующие локальные адреса), но и исходящую почту. Этот флаг имеет силу, если одновременно установлен глобальный флаг **SMTP[RelayMultiSite]**. Отправка исходящей почты разрешается только отправителям, успешно прошедшим авторизацию;<br>**P** (Pop multisite) - разрешает приём почты для нелокальных адресатов многосерверного домена, если приём выполняется загрузчиком внешней POP-почты Pop3Recv. Этот режим применяется, если PigMail+PigProxy выполняет обязанности шлюза. Этот флаг имеет силу, если одновременно установлен глобальный флаг **SMTP[PopMultiSite]**. |
| 5 | **FORWARD_NEU** | Задаёт адрес, на который будет перенаправляться почта для несуществующих пользователей, если не было задано автоматическое создание каталогов почтовых ящиков или хранение писем в отдельном каталоге. |
| 6 | **SPAM_ADMIN_BOX** | Расположение почтового ящика назначенного домену администратора спама. В этот почтовый ящик перемещаются все письма, классифицированные фильтром POPfile, SpamProtexx или LibSD как мусорные и адресованные получателям, не имеющим специальной квалификации. Администратор спама выполняет всю работу по расчистке этих авгиевых конюшен, переклассификации ошибочно распознанных писем и доставке переклассифицированной почты адресатам. Если этот параметр не задан, используется значение, заданное глобальным параметром **SMTP[SpamAdmin]**. |

| | | |
|---|---|---|
| 7 | **BOUNCE_EMAIL** | Адрес "отскока" или "вышибала". Чтобы исключить переписку между почтовыми роботами, этот адрес подставляется в качестве обратного в извещения, формируемые каждым индивидуальным автоответчиком, установленным для получателей этого домена. Направленные на этот адрес письма обычно отвергаются. Путём изменения настроек можно разрешить серверу принимать такие письма, но отвечать на них он ни в коем случае не будет. |

### *Список источников авторизации*

В этом списке перечислены источники авторизации для доменов. Стандартная процедура авторизации в домене заключается в том, что по имени домена определяется источник авторизации, а по имени источника - способ и конкретные параметры.

Расположение списка задаётся параметром **AUTH[AuthSources]**, исходное - **CONF\lists\AuthSources.txt**. Назначение полей.

| | | |
|---|---|---|
| 1 | **SOURCE_NAME** | Имя источника авторизации. |
| 2 | **AUTH_TYPE** | Способ авторизации. Здесь допустимы следующие варианты:<br>**auth_nt** - авторизация в домене Active Directory, в качестве домена может выступать также и локальный компьютер;<br>**auth_e2** - авторизация по списку пользователей формата Eserv/2;<br>**auth_md5** - авторизация по списку пользователей формата Eserv/3, с паролями, зашифрованными по алгортиму MD5;<br>**auth_md5plain** - авторизация по объединённому списку пользователей формата Eserv/3, с паролями, зашифрованными по алгортиму MD5;<br>**auth_odbc** - авторизация по базе данных. |
| 3 | **AUTH_PAR** | Первый параметр авторизации, тип которого зависит от способа авторизации:<br>**auth_nt** - имя домена Active Directory или локального компьютера;<br>**auth_e2** - шаблон имени файла списка пользователей формата Eserv/2;<br>**auth_md5** - шаблон имени файла списка пользователей формата Eserv/3;<br>**auth_md5plain** - шаблон имени файла объединённого списка пользователей формата Eserv/3;<br>**auth_odbc** - строка подключения к базе данных. |
| 4 | **AUTH_OPT** | Второй параметр авторизации тип которого зависит от способа авторизации:<br>**auth_nt** - не используется;<br>**auth_e2** - шаблон имени файла списка групп формата Eserv/2;<br>**auth_md5** - шаблон имени файла списка групп формата Eserv/3;<br>**auth_md5plain** - шаблон имени файла объединённого списка групп формата Eserv/3;<br>**auth_odbc** - уточнение запроса к базе данных. |

### *Список локальных сетей*

Этот список определяет диапазоны IP-адресов, относящиеся к локальной сети предприятия. Здесь можно задавать не только физически локальные адреса; некоторые фиксированные адреса, не относящиеся к физической локальной сети, но принадлежащие предприятию, тоже могут находиться в этом списке. Пользователи, подключающиеся с IP-адресов локальных сетей, могут отправлять почту за пределы локальных доменов, пользоваться услугами прокси-сервера, получать доступ в закрытые для других пользователей разделы web- и FTP-серверов.

Если в настройках SMTP-сервера не задано требование обязательной явной авторизации - ни общее, ни для отправки исходящей почты, ни для отправки почты скрытым локальным пользователям, ни для использования локального обратного адреса, - на основании этого списка выполняется так называемая IP-авторизация: отправитель считается авторизовавшимся, и ему назначается имя, сопоставленное в списке IP-адресу подключения. Прокси-сервер, HTTP- и FTP-сервер также могут выполнять автоматическую авторизацию по этому списку, если это разрешено соответствующими параметрами настроек.

В соответствии с начальными настройками, заданными параметрами **SMTP[LocalNetworks]**, **POP[LocalNetworks]**, **IMAP[LocalNetworks]**, **PROXY[LocalNetworks]**, **HttpProxy[LocalNetworks]**, **FtpProxy[LocalNetworks]**, **SocksProxy[LocalNetworks]**, **Pop3Proxy[LocalNetworks]**, **TCPMAP[LocalNetworks]**, **UDPMAP[LocalNetworks]**, **HTTP[LocalNetworks]** и **FTP[LocalNetworks]** (исходно они наследуют глобальный параметр **Lists[LocalNetworks]**) в файле настроек **PigMail2.ini**, используется один общий список **CONF\lists\LocalNetworks.txt**. В подкаталогах управляющих списков соответствующих серверов также имеются заготовки для определения индивидуальных списков, но исходными настройками их использование не предусмотрено. Все списки имеют одинаковый формат. Назначение полей:

| | | |
|---|---|---|
| 1 | **IP_MASK** | Шаблон IP-адреса, определяющий локальную сеть. Здесь можно указать и конкретный IP-адрес. |
| 2 | **REPLY_TEXT** | Текст индивидуального приветствия, подставляемый в ответы серверов при подключении пользователей из этой локальной сети. |
| 3 | **USER** | Имя учётной записи (логин) и домен авторизации пользователя (в виде **логин@домен**), используемые при IP-авторизации. Если задано только имя учётной записи, считается, что авторизация выполняется в домене по умолчанию. Если это поле не заполнено, IP-авторизация по этой строке списка не выполняется. |
| 4 | **MAX_MSG_SIZE** | Индивидуальное ограничение на максимально допустимый размер письма. Это поле имеет смысл для SMTP-сервера. Размер письма задаётся в байтах. |
| 5 | **FLAGS** | Строка флагов-признаков для сети:<br>**S** (Spam free) - указывает, что этот диапазон IP-адресов является настолько доверенным, что отправляемые с него письма не следует подвергать спам-контролю. Этот флаг имеет смысл для SMTP-сервера;<br>**H** (Helo trust) - указывает, что имя узла, передаваемое в команде протокола SMTP HELO или EHLO, можно не проверять на соответствие IP-адресу клиента. В локальных сетях, состоящих из ограниченного числа заведомо доверенных компьютеров, эту проверку рекомендуется отключать, поскольку результатом её будет бессмысленная задержка в отправке письма - хорошо, если не очень большая. Этот флаг имеет смысл для SMTP-сервера;<br>**O** (Outbound) - указывает, что клиентам, подключившимся из данной сети, разрешено отправлять исходящую почту, даже если это запрещено настройкой по умолчанию. Этот флаг имеет смысл для SMTP-сервера;<br>**L** (Local only) - указывает, что клиентам, подключившимся из данной сети, запрещено отправлять исходящую почту, даже если это разрешено настройкой по умолчанию. Этот флаг имеет смысл для SMTP-сервера;<br>**I** (Interhost) - разрешает режим межузловой передачи данных. Этот флаг имеет смысл для FTP-сервера;<br>**D** (Disable interhost) - запрещает режим межузловой передачи данных. Этот флаг имеет смысл для FTP-сервера;<br>**1** - то же, что и **S**, этот флаг используется для корректной обработки списков старого формата. Этот флаг имеет смысл для SMTP-сервера. |

### *Списки пользователей локальных доменов*

Эти списки используются при авторизации по способам **auth_md5** и **auth_md5plain**. В первом случае для каждого домена авторизации используется свой список. Во втором случае предполагается использование единого (объединённого) списка.

Для способа авторизации **auth_md5** расположение списков задаётся параметрами **SMTP[UserList]**, **POP[UserList]**, **IMAP[UserList]**, **PROXY[UserList]**, **HttpProxy[UserList]**, **FtpProxy[UserList]**, **SocksProxy[UserList]**, **HTTP[UserList]**, **FTP[UserList]** (исходно они наследуют глобальный параметр **AUTH[UserList]**) в файле настроек **PigMail2.ini**. В соответствии с начальными настройками имена списков имеют вид **UserList-{домен}.txt**. Для способа **auth_md5plain** расположение списка задаётся параметрами **SMTP[PlainUserList]**, **POP[PlainUserList]**, **IMAP[PlainUserList]**, **PROXY[PlainUserList]**, **HttpProxy[PlainUserList]**, **FtpProxy[PlainUserList]**, **SocksProxy[PlainUserList]**, **HTTP[PlainUserList]**, **FTP[PlainUserList**], исходно наследующими глобальный параметр **AUTH[PlainUserList]**; в соответствии с начальными настройками это файл **PlainUserList.txt**. Исходно предполагается, что списки располагаются в каталоге **CONF\lists**. Назначение полей:

| | | |
|---|---|---|
| 1 | **USER** | Для способа авторизации **auth_md5** - имя учётной записи (логин) пользователя. Для способа авторизации **auth_md5plain** - полное имя учётной записи пользователя в формате **логин@домен**. |
| 2 | **PASS** | Пароль, зашифрованный по алгоритму MD5. |
| 3 | **ACTIVE** | Флаг, указывающий, активен ли пользователь. Это очень удобно - пользователей в случае чего не придётся удалять, а потом восстанавливать, достаточно просто заблокировать учётную запись. |
| 4 | **FNAME** | Человеческое имя пользователя. |

| | | |
|---|---|---|
| 5 | **LNAME** | Фамилия пользователя. |
| 6 | **EMAIL** | Адрес электронной почты пользователя. Если запущен почтовый сервер, это поле надо заполнять обязательно, поскольку оно используется POP/IMAP-сервером для определения расположения почтового ящика пользователя. |
| 7 | **HOMEPAGE** | Ссылка на личную web-страницу пользователя. |

### *Списки группировки пользователей*

Эти списки используются для объединения пользователей в группы - впоследствии группам можно будет назначать права, общие для всех членов группы. Описываемые списки используются для группировки пользователей, прошедших авторизацию по способам **auth_md5** и **auth_md5plain**. В первом случае для каждого домена авторизации используется свой список. Во втором случае предполагается использование единого (объединённого) списка. Кроме того, существует список расширенной кросс-доменной группировки, позволяющий объединять в группы пользователей, принадлежащих к разным доменам, - этот список используется, если загружен специальный плагин **groups_ext**.

Для способа авторизации **auth_md5** расположение списков задаётся параметрами **SMTP[GroupList]**, **PROXY[GroupList]**, **HttpProxy[GroupList]**, **FtpProxy[GroupList]**, **SocksProxy[GroupList]**, **HTTP[GroupList]**, **FTP[GroupList]** (исходно они наследуют глобальный параметр **AUTH[GroupList]**) в файле настроек **PigMail2.ini**. В соответствии с начальными настройками имена списков имеют вид **GroupsList-{домен}.txt**. Для способа **auth_md5plain** расположение списка задаётся параметрами **SMTP[PlainGroupsList]**, **PROXY[PlainGroupList]**, **HttpProxy[PlainGroupList]**, **FtpProxy[PlainGroupList]**, **SocksProxy[PlainGroupList]**, **HTTP[PlainGroupList]**, **FTP[PlainGroupList]**, исходно наследующими глобальный параметр **AUTH[PlainGroupList]**; в соответствии с начальными настройками это файл **PlainGroupsList.txt**. Расположение списка расширенной группировки задаётся параметрами **SMTP[ExtendedGroupList]**, **PROXY[ExtendedGroupList]**, **HttpProxy[ExtendedGroupList]**, **FtpProxy[ExtendedGroupList]**, **SocksProxy[ExtendedGroupList]**, **HTTP[ExtendedGroupList]**, **FTP[ExtendedGroupList]**, которые наследуют значение глобального параметра **AUTH[ExtendedGroupList]**; в соответствии с начальными настройками это файл **ExtendedGroupsList.txt**. Исходно предполагается, что списки располагаются в каталоге **CONF\lists**. Назначение полей:

| | | |
|---|---|---|
| 1 | **USER** | Для способа авторизации **auth_md5** - имя учётной записи (логин) пользователя. Для способа авторизации **auth_md5plain** и списка расширенной группировки - полное имя учётной записи пользователя в формате **логин@домен**. |
| 2 | **IN_GROUP** | Для способа авторизации **auth_md5** - имя группы, при этом считается, что группа относится к тому же домену авторизации, что и входящий в неё пользователь. Для списка расширенной группировки это поле содержит полное имя группы в формате **имя@домен**. Для способа авторизации **auth_md5plain** содержимое этого поля анализируется по-разному в зависимости от наличия поддержки расширенной группировки - если плагин **groups_ext** подключён, ожидается полное имя группы в формате **имя@домен**, если же нет, то имя группы сравнивается "как есть"; для этого способа авторизации допускается частичная кросс-доменность группировки с условием, что все домены имеют один тип авторизации. |

### *Списки соответствия доменов авторизации IP-адресам сетевых интерфейсов*

С помощью этих списков можно назначать домен авторизации по умолчанию (используемый в ситуации, когда подключившаяся клиентская программа передаёт только имя учётной записи пользователя) в зависимости от того, на какой из сетевых интерфейсов сервера (то есть, из какой именно подсети) произошло подключение. Такой механизм позволяет более гибко управляться со сложными сетями. Если адрес подключения в списке не обнаруживается, используется глобальный домен авторизации, определённый в настройках соответствующего сервера.

Этот же список используется для выбора параметров защищённого (SSL) соединения сервера с клиентом - используемого сертификата сервера и режима проверки подлинности сертификатов клиентской стороны. Если адрес подключения в списке не обнаруживается, используются параметры по умолчанию, определённые в настройках соответствующего сервера. Прокси-сервер сам по себе не использует защищённые соединения с клиентами (хотя и поддерживает установку защищённых соединений клиентов с целевыми серверами), поэтому для него эти настройки не имеют смысла.

В соответствии с начальными настройками, заданными параметрами **SMTP[DomainIP]**, **POP[DomainIP]** и **IMAP[DomainIP]**, **PROXY[DomainIP]**, **HttpProxy[DomainIP]**, **FtpProxy[DomainIP]**, **SocksProxy[DomainIP]**, **HTTP[DomainIP]**, **FTP[DomainIP]** (исходно они наследуют глобальный параметр **Lists[DomainIP]**) в файле настроек **PigMail2.ini**, используется один общий список **CONF\lists\DomainIP.txt**. В подкаталогах управляющих списков соответствующих серверов также имеются заготовки для определения индивидуальных

списков, но исходными настройками их использование не предусмотрено. Все списки имеют одинаковый формат. Назначение полей:

| | | |
|---|---|---|
| 1 | **IP** | IP-адрес сетевого интерфейса. |
| 2 | **DOMAIN** | Назначаемый при подключении к этому интерфейсу домен авторизации по умолчанию. Здесь допускается использование макросов (**{}**). Если поле пустое, используется глобальный домен авторизации, определённый в настройках соответствующего сервера. |
| 3 | **SSL_CERT** | Имя файла формата PEM, содержащего закрытый ключ и сертификаты, используемые при организации защищённого (SSL) соединения сервера с клиентом. Здесь допускается использование макросов (**{}**). Если поле пустое, используется сертификат по умолчанию, определённый в настройках соответствующего сервера. Это поле не используется в настройках прокси-сервера. |
| 4 | **SSL_VERIFY** | Определяет режим проверки подлинности сертификатов клиентской стороны при установлении защищённого соединения. Задаётся либо числовым кодом, либо символьным обозначением:<br>**SSL_VERIFY:NONE** - сертификат клиента не запрашивается (числовое значение 0);<br>**SSL_VERIFY:STANDARD** - сертификат клиента запрашивается, но соединение устанавливается и при отсутствии сертификата; при переустановке соединения сертификат запрашивается повторно (числовое значение 1);<br>**SSL_VERIFY:FORCE** - сертификат клиента запрашивается, при его отсутствии соединение не устанавливается; при переустановке соединения сертификат запрашивается повторно (числовое значение 3);<br>**SSL_VERIFY:ONCE** - сертификат клиента запрашивается, но соединение устанавливается и при отсутствии сертификата; при переустановке соединения сертификат повторно не запрашивается (числовое значение 5);<br>**SSL_VERIFY:ONCE_FORCE** - сертификат клиента запрашивается, при его отсутствии соединение не устанавливается; при переустановке соединения сертификат повторно не запрашивается (числовое значение 7).<br>Здесь допускается использование макросов (**{}**). Если поле пустое, используется режим по умолчанию, определённый в настройках соответствующего сервера. Это поле не используется в настройках прокси-сервера. |
| 5 | **COMMENT** | Примечание. Это поле не используется серверами и предназначено для заметок администратора. |

### *Списки авторизации по аппаратным идентификаторам сетевых адаптеров*

Назначение этих списков - альтернативный вариант автоматической авторизации подключившегося клиента. Альтернативный дважды - во-первых, по отношению к явной авторизации путём передачи в протоколе имени учётной записи и пароля, а во-вторых, по отношению к авторизации по спискам локальных и доверенных сетей, ориентирующихся на IP-адрес подключения. В этих списках IP-адрес также присутствует, но в качестве дополнительного идентификатора, повышающего надёжность авторизации, участвует также и MAC-адрес - уникальный аппаратный идентификатор сетевого адаптера, присваиваемый ему производителем. Этот идентификатор доступен только в пределах локальной сети, так что злоупотреблять его применением не следует.

Списки авторизации с использованием MAC-адресов имеют самый низший приоритет - они применяются, если не произошло авторизации на основании IP-списков. Кроме того, любая автоматическая авторизация перекрывается явной авторизацией.

В соответствии с начальными настройками, заданными параметрами **SMTP[IpMacAuth]**, **PROXY[IpMacAuth]**, **HttpProxy[IpMacAuth]**, **FtpProxy[IpMacAuth]**, **SocksProxy[IpMacAuth]**, **HTTP[IpMacAuth]**, **FTP[IpMacAuth]** (исходно они наследуют глобальный параметр **Lists[IpMacAuth]**) в файле настроек **PigMail2.ini**, используется общий список **CONF\lists\IpMacAuth.txt**. В подкаталоге управляющих списков SMTP-сервера также имеется заготовка для определения отдельного списка, но исходными настройками его использование не предусмотрено. Все списки имеют одинаковый формат. Назначение полей:

| | | |
|---|---|---|
| 1 | **CLIENT_IP** | Шаблон IP-адреса подключения. |

| | | |
|---|---|---|
| 2 | **CLIENT_MAC** | Шаблон MAC-адреса клиента. MAC-адрес записывается в виде последовательности из шести байтов, разделённых дефисом, в шестнадцатиричной нотации, например: **00-0C-6E-AD-29-58**. |
| 3 | **SET_USER** | Имя учётной записи (логин) и домен авторизации пользователя (в виде **логин@домен**), используемые при автоматической авторизации. Если задано только имя учётной записи, считается, что авторизация выполняется в домене по умолчанию. |
| 4 | **COMMENT** | Примечание. Это поле не используется серверами и предназначено для заметок администратора. |

### *Список соответствия пользовательских учётных записей и почтовых ящиков*

Поскольку пользовательские учётные записи не тождественны адресам электронной почты (наилучшая политика безопасности состоит как раз в том, чтобы имя учётной записи - логин - не совпадало с именем почтового ящика), POP/IMAP-сервер при авторизации должен каким-то образом получить дополнительную информацию о пользователе. Если используется авторизация по списку пользователей формата Eserv/3 или по базе данных, это несложно - адреса электронной почты легко доступны. При авторизации по списку пользователей формата Eserv/2 или домена Active Directory эта информация либо отсутствует вообще, либо (в текущей версии) недоступна. Тогда в качестве источника информации выступает этот список.

В соответствии с начальными настройками, заданными параметрами **POP[UserMailBoxes]** и **IMAP[UserMailBoxes]** (исходно они наследуют глобальный параметр **Lists[UserMailBoxes]**) в файле настроек **PigMail2.ini**, используется один общий список **CONF\lists\UserMailBoxes.txt**. В подкаталогах управляющих списков соответствующих серверов также имеются заготовки для определения индивидуальных списков, но исходными настройками их использование не предусмотрено. Все списки имеют одинаковый формат. Назначение полей:

| | | |
|---|---|---|
| 1 | **USER_ID** | Полное (в формате **логин@домен**) имя учётной записи пользователя. |
| 2 | **MBOX_ID** | Адрес электронной почты - полное имя почтового ящика пользователя. |

## *Управляющие списки SMTP-сервера*

Эти списки предназначены для управления SMTP-сервером, их исходное расположение, определяемое параметрами **SMTP[Lists]**, **SMTP[MailingLists]** и **SMTP[Filters]**, - каталог **CONF\lists\smtp** и его подкаталоги.

### *Список доверенных сетей*

Это так называемый "белый" список доверенных IP-адресов или сетей, которые обслуживаются этим SMTP-сервером, то есть, которым позволено отправлять через него почту на внешние домены, а не только на локальные. Этот список ДОПОЛНЯЕТ список локальных сетей. В нём могут быть не локальные сети, а, например, особые внешние IP-адреса, не входящие логически в локальную сеть предприятия.

Если в настройках SMTP-сервера не задано требование обязательной явной авторизации - ни общее, ни для отправки исходящей почты, ни для отправки почты скрытым локальным пользователям, ни для использования локального обратного адреса, - на основании этой пары списков выполняется так называемая IP-авторизация: отправитель считается авторизовавшимся, и ему назначается имя, сопоставленное в списке IP-адресу подключения.

Расположение списка задаётся параметром **SMTP[IpWhiteList]**, исходное - **CONF\lists\smtp\IpWhiteList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **IP_MASK** | Шаблон IP-адреса, определяющий доверенную сеть. Здесь можно указать и конкретный IP-адрес. |
| 2 | **REPLY_TEXT** | Текст индивидуального приветствия, подставляемый в ответы серверов при подключении пользователей из этой доверенной сети. |
| 3 | **USER** | Имя учётной записи (логин) и домен авторизации пользователя (в виде **логин@домен**), используемые при IP-авторизации. Если задано только имя учётной записи, считается, что авторизация выполняется в домене по умолчанию. Если это поле не заполнено, IP-авторизация по этой строке списка не выполняется. |
| 4 | **MAX_MSG_SIZE** | Индивидуальное ограничение на максимально допустимый размер письма. Размер письма задаётся в байтах. |

| | | |
|---|---|---|
| 5 | **FLAGS** | Строка флагов-признаков для сети:<br>**S** (Spam free) - указывает, что этот диапазон IP-адресов является настолько доверенным, что отправляемые с него письма не следует подвергать спам-контролю;<br>**H** (Helo trust) - указывает, что имя узла, передаваемое в команде протокола SMTP HELO или EHLO, можно не проверять на соответствие IP-адресу клиента. В локальных сетях, состоящих из ограниченного числа заведомо доверенных компьютеров, эту проверку рекомендуется отключать, поскольку результатом её будет бессмысленная задержка в отправке письма - хорошо, если не очень большая;<br>**O** (Outbound) - указывает, что клиентам, подключившимся из данной сети, разрешено отправлять исходящую почту, даже если это запрещено настройкой по умолчанию;<br>**L** (Local only) - указывает, что клиентам, подключившимся из данной сети, запрещено отправлять исходящую почту, даже если это разрешено настройкой по умолчанию;<br>**1** - то же, что и **S**, этот флаг используется для корректной обработки списков старого формата. |

## *Список запрещённых сетей*

Это список IP-адресов и подсетей, которым запрещено обращаться к SMTP-серверу. В отличие от стандартной конфигурации, он позволяет управлять отказами более гибко - от самого жёсткого немедленного отказа до приёма почты в карантин для последующего рассмотрения администратором. При этом выставленный режим не является окончательным - он может быть переопределён впоследствии при анализе приветствия клиента и адреса отправителя.

Расположение списка задаётся параметром **SMTP[IpBlackList]**, исходное - **CONF\lists\smtp\IpBlackList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **IP_MASK** | Шаблон IP-адреса, определяющий запрещённую сеть. |
| 2 | **REPLY_TEXT** | Индивидуальный текст ответа сервера, поясняющий причину отказа. |
| 3 | **FLAGS** | Строка флагов-признаков для сети:<br>**Q** (Quarantine) - указывает, что почту из этой сети надлежит принимать в карантин, то есть, помещать в специальный каталог, определяемый параметров **SMTP[Quarantined]**. Практически в любой сети обитают как злостные спамеры, так и вполне благонамеренные граждане. И пропустить полезную информацию только из-за того, что конкретная сеть конкретного провайдера наводнена спамерами, не всегда желательно;<br>**U** (Unconditional) - указывает, что подключение из этой сети следует отвергать жёстко и бескомпромиссно. По умолчанию (в отсутствие флага) у отправителя остаётся возможность подать жалобу на специальный адрес (abuse). Как правило, возможность подачи жалобы следует оставлять и применять жёсткие меры только к самым обнаглевшим отправителям, использующим специальный адрес для рассылки спама. Этот флаг имеет приоритет над флагом приёма в карантин;<br>**L** (Local only) - указывает, что клиентам, подключившимся из данной сети, запрещено отправлять исходящую почту, даже если это разрешено настройкой по умолчанию. |

## *Список сервисов блокировки IP-адресов отправителей*

Помимо собственного списка запрещённых сетей можно использовать различные онлайновые сервисы подобного назначения, обычно называемые RBL (сокращение от Realtime Blackhole List). Первоначально можно было использовать только два таких сервиса, ORDB (прекратил работу с 1 января 2007 года) и MAPS (**http://mail-abuse.org/**), работа с которыми включалась и отключалась посредством задания специальных параметров конфигурационного файла. В текущей версии можно использовать список таких сервисов достаточно произвольного размера (не слишком большого, поскольку обращение к онлайновым службам может в итоге потребовать значительного времени) и состава.

Все RBL построены по одной простой, но эффективной схеме - список публикуется с помощью сервера DNS. Каждому блокированному системой IP-адресу соответствует сформированное по определённым правилам доменное имя; все они принадлежат особому корневому домену соответствующей системы.

Расположение списка задаётся параметром **SMTP[RBLSystemList]**, исходное - **CONF\lists\smtp\RBLSystemList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **RBL_ROOT** | Доменное имя корневой зоны сервиса. |
| 2 | **RBL_NAME** | Наименование сервиса. |
| 3 | **LOOKUP_URL** | Ссылка на web-интерфейс сервиса, позволяющий проверить факт блокировки определённого адреса и выяснить причину блокировки. |
| 4 | **ACTIVE** | Флаг, определяющий, использовать ли данный сервис для фильтрации по IP-адресу отправителя, или же нет. Если значение нулевое, то сервис не используется, а информация о нём просто хранится до подходящего случая. |
| 5 | **IS_QUARANTINED** | Флаг, определяющий, принимать ли почту с IP-адресов, блокированных этим чёрным списком, в карантин. Практически в любой сети обитают как злостные спамеры, так и вполне благонамеренные граждане. И пропустить полезную информацию только из-за того, что конкретный IP-адрес попал в чей-то чёрный список (ещё неизвестно, насколько обоснованно), не всегда желательно. Если установлено ненулевое значение, письма с заблокированных этим списком IP-адресов будут приниматься и помещаться в специальный каталог, определяемый параметром **SMTP[Quarantined]**. |
| 6 | **IS_UNCONDITIONAL** | Флаг, определяющий, отвергать ли подключение с IP-адресов, блокированных этим чёрным списком, жёстко и бескомпромиссно или предоставить возможность отправителю подать жалобу на специальный адрес (abuse). Если установлено ненулевое значение, подключение с заблокированных этим списком IP-адресов отвергается незамедлительно. Как правило, возможность подачи жалобы следует оставлять и применять жёсткие меры только к самым обнаглевшим отправителям, использующим специальный адрес для рассылки спама. Этот флаг имеет приоритет над флагом приёма в карантин. |

### *Список надёжных сетей*

В отличие от списков локальных и доверенных сетей, действие этого списка ограничено работой с онлайновыми сервисами RBL. По умолчанию фильтрация по IP-адресу не выполняется, если IP-адрес клиента находится в списке локальных, доверенных или, напротив, запрещённых сетей (в этом случае явно заданные локальные настройки перекрывают действие глобальных фильтров), а также принадлежит одному из зарезервированных диапазонов, выделенных для локальных сетей (эти адреса не могут принадлежать Интернету, поэтому в глобальные фильтры не вносятся). Кроме того, есть возможность исключить фильтрацию отдельных подсетей или конкретных IP-адресов, указав их в этом списке.

Расположение списка задаётся параметром **SMTP[RBLWhiteList]**, исходное - **CONF\lists\smtp\RBL-WhiteList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **IP_MASK** | Шаблон IP-адреса, определяющий надёжную сеть, не подлежащую проверке по RBL. Здесь можно указать и конкретный IP-адрес. |
| 2 | **COMMENT** | Примечание. Это поле не используется сервером и предназначено для заметок администратора. |

### *Список запрещённых имён клиентских узлов*

Это список запрещённых имён клиентских компьютеров, сообщаемых в командах HELO и EHLO - ещё один рубеж защиты от нежелательного трафика, сгенерированного вирусами и спамерами, научившимися подделывать обратные адреса, но пока не освоившими искусство подделки имён узлов. Даже поверхностный анализ спамерских подключений показывает, что число используемых для рассылки спама сетей и их доменных имён не так уж и велико - гораздо меньше, чем постоянно пополняющийся список поддельных обратных адресов. Видимо, существует достаточно веская причина, по которой рассыльщики мусора вынуждены использовать реальные доменные имена - хотя ситуация, похоже, меняется: в последнее время наблюдается рост числа поддельных доменных имён, извлекаемых из того же списка, что и поддельные обратные адреса. Почтовые же черви в массе своей просто не блещут фантазией и большей частью используют для приветствия доменное имя будущей жертвы либо заранее заложенную автором строку.

В отличие от стандартной конфигурации, этот список позволяет управлять отказами более гибко - от самого жёсткого немедленного отказа до приёма почты в карантин для последующего рассмотрения администратором. При этом выставленный режим не является окончательным - он может быть переопределён впоследствии при анализе адреса отправителя.

В ходе представления SMTP-сервер выполняет простейший анализ переданного ему доменного имени. В результате проверки могут быть выявлены три возможные ситуации:

- Доменному имени сопоставлен IP-адрес, совпадающий с адресом подключившегося клиента, - то есть, имя не поддельное. На него можно ориентироваться - если среди ваших партнёров и знакомых нет жи-

телей Бразилии (где в лесах, как известно, много-много диких обезьян), то приветствие из домена **что-то-там.net.br** почти наверняка означает доставляемый таким кружным путём спам;

- Доменному имени сопоставлен IP-адрес, не совпадающий с адресом подключившегося клиента, - имя заведомо поддельное. Почти наверняка это происки спамеров;
- Доменному имени не сопоставлен никакой IP-адрес. Большей частью этим грешат одиноко стоящие домашние и мелкоофисные компьютеры, хотя случаются и просто некорректно настроенные (по бедности или от великой лени) домены. Спамеры здесь тоже обязательно отметятся - в их списках попадаются несуществующие (или, скорее всего, внутреннего для чьих-то локальных сетей пользования) почтовые домены. Не равна нулю также и вероятность временных проблем с доступностью соответствующего DNS-сервера. В отличие от первых двух случаев, это ситуация полной неопределённости.

В зависимости от степени достоверности предъявленного при знакомстве доменного имени SMTP-сервер может по-разному реагировать на одно и то же имя. Например, письмо от реального **mail.microsoft.com** (если таковой существует в природе) можно благосклонно принять, как будто этого имени вообще нет в списке запрещённых, а от поддельного - отвергнуть, может быть, даже жёстко и безапеляционно.

Расположение списка задаётся параметром **SMTP[HeloBlackList]**, исходное - **CONF\lists\smtp\HeloBlackList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **HELO_MASK** | Шаблон имени узла, определяющий запрещённое доменное имя. |
| 2 | **REPLY_TEXT** | Индивидуальный текст ответа сервера, поясняющий причину отказа. |
| 3 | **IS_QUARANTINED** | Строка флагов, определяющая, принимать ли (и если да, то в каких ситуациях) почту из этого домена или от данного конкретного узла в карантин. Практически в любой сети обитают как злостные спамеры, так и вполне благонамеренные граждане. И пропустить полезную информацию только из-за того, что конкретная сеть конкретного провайдера наводнена спамерами, не всегда желательно. Флаги могут быть следующими:<br>**M** (Matched) - условие срабатывает, если доменное имя достоверно;<br>**U** (Unmatched) - условие срабатывает, если доменное имя заведомо поддельное;<br>**E** (Error) - условие срабатывает, если имя не имеет IP-адреса;<br>**D** (Don't check) - условие срабатывает, если проверка доменного имени отменена заданием флага **H** в свойствах локальной или доверенной сети;<br>**A** (Always) - условие срабатывает всегда (соответствует также комбинации всех четырёх предыдущих флагов);<br>**1** - то же, что и **A**, этот флаг используется для корректной обработки списков старого формата.<br>Если сработало какое-либо из перечисленных условий, письма из этого домена будут приниматься и помещаться в специальный каталог, определяемый параметром **SMTP[Quarantined]**. |
| 4 | **IS_UNCONDITIONAL** | Строка флагов, определяющая, отвергать ли почту из этого домена или от данного конкретного узла жёстко и бескомпромиссно или предоставить возможность отправителю подать жалобу на специальный адрес (abuse). Флаги могут быть следующими:<br>**M** (Matched) - условие срабатывает, если доменное имя достоверно;<br>**U** (Unmatched) - условие срабатывает, если доменное имя заведомо поддельное;<br>**E** (Error) - условие срабатывает, если имя не имеет IP-адреса;<br>**D** (Don't check) - условие срабатывает, если проверка доменного имени отменена заданием флага **H** в свойствах локальной или доверенной сети;<br>**A** (Always) - условие срабатывает всегда (соответствует также комбинации всех четырёх предыдущих флагов);<br>**1** - то же, что и **A**, этот флаг используется для корректной обработки списков старого формата.<br>Если сработало какое-либо из перечисленных условий, подключение из этого домена отвергается незамедлительно. Как правило, возможность подачи жалобы следует оставлять и применять жёсткие меры только к самым обнаглевшим отправителям, использующим специальный адрес для рассылки спама. Эта строка флагов имеет второй по значимости приоритет и может перекрывать условия строки флагов приёма в карантин. |

| | | |
|---|---|---|
| 5 | **IS_SKIPPED** | Строка флагов, определяющая, в каких ситуациях домен не следует блокировать, а надлежит тихо проигнорировать его наличие в списке запрещённых. Флаги могут быть следующими:<br>**M** (Matched) - условие срабатывает, если доменное имя достоверно;<br>**U** (Unmatched) - условие срабатывает, если доменное имя заведомо поддельное;<br>**E** (Error) - условие срабатывает, если имя не имеет IP-адреса;<br>**D** (Don't check) - условие срабатывает, если проверка доменного имени отменена заданием флага **H** в свойствах локальной или доверенной сети;<br>**A** (Always) - условие срабатывает всегда (соответствует также комбинации всех четырёх предыдущих флагов);<br>**1** - то же, что и **A**, этот флаг используется для корректной обработки списков старого формата;<br>**пусто** - соответствует **D**.<br>Если сработало какое-либо из перечисленных условий, SMTP-сервер делает вид, что списке ничего не обнаружено. Эта строка флагов имеет наивысший приоритет - если срабатывает её условие, прочие флаги не анализируются. |

## *Список прав пользователей*

Этот список используется для назначения прав пользователей по данным их авторизации на SMTP-сервере, то есть, на основании имени учётной записи и домена авторизации. Поскольку с SMTP-сервером имеют дело исключительно отправители, то и права задаются в отношении отправки почты: является ли пользователь администратором сервера (возможно, с правом обхода списка запрещённых получателей), имеет ли он право отправки писем за пределы локальных доменов, какие у него ограничения на размер писем. Назначение прав по этому списку производится один раз за время почтовой сессии при явной авторизации пользователя, на автоматическую или IP-авторизацию действие списка не распространяется. Назначенные права используются в качестве базовых и могут быть изменены (в сторону повышения) на основании данных из списка локальных почтовых ящиков.

Расположение списка задаётся параметром **SMTP[ACL]**, исходное - **CONF\lists\smtp\ACL.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **USER** | Пользователь, к которому относится эта строка. Если поле пустое, то его проверка не производится. Если поле содержит символ звёздочки *****, то строка считается относящейся к любому авторизованному пользователю. Любое другое содержимое рассматривается как шаблон сравнения, могущий содержать символы групповой операции ***** и **?**. SMTP-сервер ожидает задания полного имени пользователя в формате **логин@домен**; если же домен не задан, считается, что искомый пользователь авторизуется в домене по умолчанию. |
| 2 | **GROUP** | Имя группы пользователей, к которой относится эта строка. В зависимости от наличия поддержки расширенной группировки оно может быть задано по-разному. Если расширенная группировка не применяется, то считается, что группа относится к тому же домену авторизации, что и входящий в неё пользователь. В противном случае SMTP-сервер ожидает задания полного имени группы в формате **группа@домен**; если же домен не указан, считается, что проверяемая группа принадлежит домену по умолчанию. Если поле пустое, членство пользователя в группе не проверяется. |

| | | |
|---|---|---|
| 3 | **FLAGS** | Строка флагов разрешений и признаков для пользователя:<br>**W** (Worldwide) - при наличии этого флага пользователю разрешена отправка почты за пределы локального домена. Его действие распространяется только на полностью авторизованных пользователей, если требование авторизации не отменено в файле настроек **PigMail2.ini**;<br>**O** (Override limit) - при наличии этого флага пользователю разрешено отправлять своим получателям письма большего размера, чем определено в настройках почтовых ящиков получателей;<br>**D** (aDministrator) - при наличии этого флага пользователь получает права администратора - он может использовать любой обратный адрес, отправлять сколько угодно писем, задавая для них любое количество адресатов, и, возможно, обходить список запрещённых получателей. Для повышения безопасности права администратора предоставляются только в случае подключения клиента из локальной сети либо по защищённому (SSL) соединению;<br>**L** (bLack List) - если пользователь получил права администратора, то при наличии этого флага он получает дополнительное право адресовать письма получателям, попавшим в список запрещённых. |
| 4 | **IN_MSG_SIZE** | Максимально допустимый размер письма, которое этот пользователь может отправлять своим получателям. Это ослабляющее ограничение, то есть, пользователь может отправить в локальный домен письмо размером более установленного при анализе его IP-адреса, если в его параметрах записано соответствующее значение. Размер письма задаётся в байтах. Если указано нулевое значение, используется уже существующее ограничение. |
| 5 | **EXT_MSG_SIZE** | Максимально допустимый размер письма, которое этот пользователь может отправлять своим получателям, находящимся вне пределов локальной сети. Это усиливающее ограничение, поскольку изначально никакого ограничения не задано. Размер письма задаётся в байтах. Если указано нулевое значение, дополнительное ограничение не накладывается. |
| 6 | **OUT_MSG_SIZE** | Максимально допустимый размер письма, которое этот пользователь может отправлять нелокальным получателям. Это ослабляющее ограничение, то есть, пользователь может отправить письмо большего размера, чем определено общими настройками сервера. Размер письма задаётся в байтах. Если указано нулевое значение, используется уже существующее ограничение. |
| 7 | **ADMIN_REPLY** | Приветствие, подставляемое в ответы сервера при подключении администратора. |

Список всегда просматривается с начала до конца. Если по какой-либо строке зафиксировано совпадение имени пользователя или членства в группе, выполняется назначение заданных в строке прав, причём права-флаги суммируются с ранее установленными, а ограничения на размер писем корректируются в сторону ослабления. В дальнейшем права могут быть скорректированы по этому же принципу на основании данных из списка локальных почтовых ящиков.

### *Список локальных почтовых ящиков*

Это общий список обслуживаемых сервером локальных почтовых ящиков. Ключевым для них является уникальный адрес электронной почты, поэтому список единый. Здесь задаются особые права каждого пользователя по части отправки и получения почты.

Неудобство существования двух пересекающихся списков пользователей является следствием механизма поиска по текстовым спискам - поиск выполняется только по первому полю. Если пользователей немного, необходимость ведения двух списков компенсируется простотой их редактирования. При большом количестве пользователей требуется другое решение на основе баз данных.

Расположение списка задаётся параметром **SMTP[LocalDomainUsers]**, исходное - **CONF\lists\smtp\LocalDomainUsers.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **EMAIL** | Адрес электронной почты. |

| | | |
|---|---|---|
| 2 | **MUST_LOGIN_AS** | Имя учётной записи (логин) и домен авторизации пользователя (в формате **логин@домен**), сопоставленные данному адресу. Если домен не указан, считается, что пользователь должен авторизоваться в домене по умолчанию. Если пользователь прошёл обычную процедуру авторизации и его логин/домен соответствуют адресу, он считается полностью авторизованным. Если это поле пустое, то полностью авторизованным будет считаться любой успешно авторизовавшийся пользователь. В PigMail+PigProxy принято, что если для отправки почты за пределы локального домена требуется обязательная авторизация, только полностью авторизованные пользователи наделяются таким правом. |
| 3 | **FLAGS** | Строка флагов разрешений и признаков для пользователя:<br>**W** (Worldwide) - при наличии этого флага пользователю разрешена отправка почты за пределы локального домена. Его действие распространяется только на полностью авторизованных пользователей, если требование авторизации не отменено в файле настроек **PigMail2.ini**;<br>**G** (Global) - при наличии этого флага пользователь является общедоступным, в противном случае это скрытый адрес только для своих. Отправлять почту на скрытый адрес могут либо полностью авторизованные пользователи, либо, если обязательная авторизация для этого не требуется, отправители, указавшие правильный обратный адрес, принадлежащий локальному домену;<br>**E** (External) - наличие этого флага означает, что владелец ящика не является клиентом локальной сети. Если получатель расположен вне локальной сети, включаются дополнительные ограничения на размер письма;<br>**O** (Override limit) - при наличии этого флага владельцу ящика разрешено отправлять своим получателям письма большего размера, чем определено в настройках почтовых ящиков получателей;<br>**A** (Abuse) - наличие этого флага означает, что адрес является специальным получателем - abuse. На такой адрес могут отправлять сообщения даже отправители, находящиеся в списке запрещённых адресов электронной почты;<br>**B** (Bounce) - наличие этого флага означает, что адрес является адресом "отскока" (bounce - вышибала). В зависимости от настроек сервера почта на этот адрес либо не принимается, либо принимается и помещается в специальный каталог, определяемый параметром **SMTP[Bounce]**, без формирования автоответа, даже если он был запрошен;<br>**S** (Spamreader) - наличие этого флага означает, что пользователь достаточно опытен и может самостоятельно выполнять переклассификацию спама. Такой пользователь при соответствующих настройках SMTP-сервера получает письма, признанные за мусор, в специальную папку своего почтового ящика. Если такого флага нет, письмо передаётся для анализа специальному "администратору спама";<br>**M** (spam adMinistrator) - наличие этого флага означает, что пользователь имеет привилегии "администратора спама". В отличие от обычного "читателя спама", такой пользователь получает спам-почту не в одну папку, а в несколько, в соответствии с детальной классификацией письма. Только такой пользователь может получить письма, отнесённые спам-фильтрами к вирусным, и оценить правильность такой классификации;<br>**I** (Inbox) - наличие этого флага совместно с флагом **S** или **M** означает, что письма, признанные спамом, доставляются не в отдельную папку, доступную по IMAP, а непосредственно в папку Входящие;<br>**L** (List) - наличие этого флага означает, что ящик включён в динамический список общедоменной рассылки. Рассылка такого типа обслуживается специальным почтовым роботом, в список автоматически включаются все локальные почтовые ящики, принадлежащие тому же домену, что и получивший письмо робот, и помеченные этим флагом. |

| | | |
|---|---|---|
| 4 | **Q_SIZE** | Ограничение (квота) на общий объём почтового ящика. Если объём ящика превышает заданное ограничение, то доставка писем в этот ящик прекращается. При явном указании адреса сервер будет выдавать отказ с соответствующей случаю диагностикой. Объём задаётся в мегабайтах. Нулевое значение отключает проверку объёма. Проверка квот должна быть разрешена настройками сервера. |
| 5 | **Q_FILES** | Ограничение (квота) на количество писем в почтовом ящике. Если число писем в ящике превышает заданное ограничение, то доставка писем в этот ящик прекращается. При явном указании адреса сервер будет выдавать отказ с соответствующей случаю диагностикой. Нулевое значение отключает проверку количества писем. Проверка квот должна быть разрешена настройками сервера. |
| 6 | **RCV_MSG_SIZE** | Максимально допустимый размер письма, которое свои отправители могут послать этому получателю. Если значения из списков локальных и доверенных сетей могут ослаблять исходное ограничение, то это усиливающее ограничение. Чтобы ограничение вступило в силу, отправитель должен принадлежать к одному из локальных доменов. Размер письма задаётся в байтах. Если указано нулевое значение, дополнительное ограничение не накладывается. |
| 7 | **IN_MSG_SIZE** | Максимально допустимый размер письма, которое этот отправитель может послать своим получателям. Это ослабляющее ограничение, то есть, отправитель может направить в локальный домен письмо размером более установленного при анализе его IP-адреса, если в его параметрах записано соответствующее значение. Чтобы это ограничение вступило в силу, отправитель должен быть правильно авторизованным. На администраторов действие этого параметра не распространяется. Размер письма задаётся в байтах. Если указано нулевое значение, используется уже существующее ограничение. |
| 8 | **EXT_MSG_SIZE** | Максимально допустимый размер письма, которое этот отправитель может послать своим получателям, находящимся вне пределов локальной сети. Это ограничение является ослабляющим для аналогичного параметра, определённого при анализе списка прав пользователей. Однако, следует держать в голове, что изначально по этому параметру ограничения нет вообще. Чтобы это ограничение вступило в силу, отправитель должен быть правильно авторизованным. На администраторов действие этого параметра не распространяется. Размер письма задаётся в байтах. Если указано нулевое значение, дополнительное ограничение не накладывается. |
| 9 | **OUT_MSG_SIZE** | Максимально допустимый размер письма, которое этот отправитель может послать нелокальным получателям. Это ослабляющее ограничение, то есть, отправитель может послать письмо большего размера, чем определено общими настройками сервера. Чтобы это ограничение вступило в силу, отправитель должен быть правильно авторизованным. На администраторов действие этого параметра не распространяется. Размер письма задаётся в байтах. Если указано нулевое значение, используется уже существующее ограничение. |
| 10 | **R4** | Зарезервировано для будущих расширений. |
| 11 | **NAME** | Человеческое имя владельца ящика, подставляемое в ответы сервера. |

### *Список локальных политик для отправителя*

Это список правил, на основании которых SMTP-сервер сопоставляет IP-адрес клиентского подключения, переданное в команде HELO или EHLO имя клиентского узла и собственно адрес отправителя и определяет, насколько достоверной является переданная информация - подделан обратный адрес или ему можно доверять. Доверие в данном случае не относится к самому отправителю - даже если адрес не поддельный, отправитель может оказаться ненадёжным, поэтому подтверждение достоверности адреса вовсе не означает автоматическую отмену всех последующих проверок.

Локальные политики могут применяться как самостоятельно, так и в сочетании с глобальными политиками Sender Policy Framework (SPF). Во втором случае локальные политики используются для дополнения или переопределения соответствующих глобальных политик.

Расположение списка задаётся параметром **SMTP[LocalSenderPolicy]**, исходное - **CONF\lists\smtp\LocalSenderPolicy.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **IP_MASK** | Шаблон IP-адреса клиентского подключения. Если поле пустое, проверка не производится. |

| | | |
|---|---|---|
| 2 | **NOT_1** | Признак проверки на несовпадение. |
| 3 | **INCOMINGHOST** | Шаблон имени клиентского узла. Если поле пустое, проверка не производится, за исключением проверки на использование IP-адреса в качестве имени. |
| 4 | **MODE** | Дополнительный признак статуса имени клиентского узла:<br>**I** - в качестве имени использован IP-адрес подключения. Этот признак может быть использован только в "чистом виде", без указания других признаков;<br>**M** - имя найдено в DNS и соответствует IP-адресу подключения;<br>**U** - имя найдено в DNS, но не соответствует IP-адресу подключения;<br>**E** - имя не найдено в DNS;<br>**D** - имя не проверялось в соответствии с настройками сети;<br>**пусто** - соответствует **MEUD**. |
| 5 | **NOT_2** | Признак проверки на несовпадение. |
| 6 | **EMAIL** | Шаблон обратного адреса отправителя. Если поле содержит символ минуса **-**, это означает, что строка относится к пустому адресу отправителя. Если поле пустое, проверка не производится. |
| 7 | **NOT_3** | Признак проверки на несовпадение. |
| 8 | **G_NOT** | Признак инверсии общего результата проверки. |
| 9 | **RESULT** | Код применяемой политики:<br>**AM** (Accept Matched) - сочетание признано истинным, адрес отправителя достоверен, дополнительная проверка не требуется;<br>**WL** (White List) - сочетание признано истинным, адрес отправителя достоверен, отправитель надёжен, дополнительная проверка не требуется, проверка по спискам запрещённых и доверенных отправителей и проверка на спам отключаются;<br>**RF** (Reject Forged) - сочетание признано невозможным, адрес отправителя подделан, дополнительная проверка не требуется;<br>**FA** (Fail) - требуется дополнительная проверка по SPF, отказать при уровне недостоверности FAIL;<br>**SF** (SoftFail) - требуется дополнительная проверка по SPF, отказать при уровне недостоверности SOFTFAIL;<br>**NE** (Neutral) - требуется дополнительная проверка по SPF, отказать при уровне недостоверности NEUTRAL. |

Список обрабатывается построчно сверху вниз. В каждой строке производится проверка каждого из трёх параметров с учётом признака инверсии (проверки на несовпадение). Затем все три результата объединяются по И, полученный результат может быть инвертирован в зависимости от значения флага **G_NOT**. Если в результате получено значение логической истины, анализ списка заканчивается и применяется заданная в этой строке политика. Если совпадение не было выявлено ни в одной строке, применяется политика по умолчанию **FA**.

### *Список доверенных отправителей*

Это список адресов, почта от которых принимается в любом случае, независимо от других условий (кроме одного - отправитель должен указать допустимый адрес получателя) и настроек. Он имеет приоритет над списком запрещённых адресов, что позволяет блокировать целые почтовые домены, но для отдельных отправителей делать исключения. Кроме того, список содержит дополнительные параметры, позволяющие выключать спам-фильтрацию для конкретного отправителя.

Расположение списка задаётся параметром **SMTP[FromEmailWhiteList]**, исходное - **CONF\lists\smtp\FromEmailWhiteList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **EMAIL** | Шаблон доверенного адреса. |

| | | |
|---|---|---|
| 2 | **IS_NO_SPAM** | Флаговая строка, определяющая, при каких условиях следует отключать спам-фильтрацию почты от этого отправителя. Флаги определяют взаимодействие списка с результатами проверки локальных и глобальных политик и могут быть следующими:<br>**L** (Local) - отправитель локальный (IP-адрес принадлежит локальной сети или самому серверу), поэтому политики не проверялись;<br>**K** (Known) - отправитель известен, поскольку успешно авторизовался на сервере;<br>**W** (Whitelist) - по результатам проверки локальных политик отправитель признан особо доверенным (код политики **WL**; в этом случае до анализа данного списка дело не доходит, так что этот флаг никакого смысла не имеет);<br>**M** (Match) - по результатам проверки локальных политик адрес отправителя признан действительным (код политики **AM**);<br>**P** (Pass) - по результатам проверки глобальных политик адрес отправителя признан действительным;<br>**N** (None) - проверка глобальных политик не выявила никакой информации в отношении отправителя;<br>**E** (Error) - проверка глобальных политик не удалась из-за ошибки при получении информации;<br>**U** (Unknown) - проверка глобальных политик не дала однозначный результат;<br>**T** (neuTral) - по результатам проверки локальных политик отправитель признан крайне подозрительным и подлежащим дополнительной проверке по глобальным политикам с отказом при уровне недостоверности NEUTRAL (код политики **NE**);<br>**R** (neutRal) - по результатам проверки глобальных политик отправитель признан незначительно нарушающим правила (уровень недостоверности NEUTRAL);<br>**O** (sOftfail) - по результатам проверки локальных политик отправитель признан подозрительным и подлежащим дополнительной проверке по глобальным политикам с отказом при уровне недостоверности SOFTFAIL (код политики **SF**);<br>**S** (Softfail) - по результатам проверки глобальных политик отправитель признан нарушающим правила (уровень недостоверности SOFTFAIL);<br>**F** (Fail) - по результатам проверки локальных политик отправитель признан обычным и подлежащим дополнительной проверке по глобальным политикам с отказом при уровне недостоверности FAIL (код политики **FA**);<br>**#** - условие срабатывает, если проверка политик (и локальных, и глобальных) отключена;<br>**A** (Always) - условие срабатывает всегда, в том числе при полностью отключённой проверке политик;<br>**1** - то же, что и **A**, этот флаг используется для корректной обработки списков старого формата.<br>Если условие соответствует установленной для отправителя политике, система фильтрации спама отключается. |
| 3 | **REPLY_TEXT** | Индивидуальный текст приветствия, подставляемый в ответ сервера. |

| | | |
|---|---|---|
| 4 | **IS_SKIPPED** | Флаговая строка, определяющая, при каких условиях следует игнорировать нахождение адреса в списке доверенных отправителей. Флаги определяют взаимодействие списка с результатами проверки локальных и глобальных политик и могут быть следующими:<br>**L** (Local) - отправитель локальный (IP-адрес принадлежит локальной сети или самому серверу), поэтому политики не проверялись;<br>**K** (Known) - отправитель известен, поскольку успешно авторизовался на сервере;<br>**W** (Whitelist) - по результатам проверки локальных политик отправитель признан особо доверенным (код политики **WL**; в этом случае до анализа данного списка дело не доходит, так что этот флаг никакого смысла не имеет);<br>**M** (Match) - по результатам проверки локальных политик адрес отправителя признан действительным (код политики **AM**);<br>**P** (Pass) - по результатам проверки глобальных политик адрес отправителя признан действительным;<br>**N** (None) - проверка глобальных политик не выявила никакой информации в отношении отправителя;<br>**E** (Error) - проверка глобальных политик не удалась из-за ошибки при получении информации;<br>**U** (Unknown) - проверка глобальных политик не дала однозначный результат;<br>**T** (neuTral) - по результатам проверки локальных политик отправитель признан крайне подозрительным и подлежащим дополнительной проверке по глобальным политикам с отказом при уровне недостоверности NEUTRAL (код политики **NE**);<br>**R** (neutRal) - по результатам проверки глобальных политик отправитель признан незначительно нарушающим правила (уровень недостоверности NEUTRAL);<br>**O** (sOftfail) - по результатам проверки локальных политик отправитель признан подозрительным и подлежащим дополнительной проверке по глобальным политикам с отказом при уровне недостоверности SOFTFAIL (код политики **SF**);<br>**S** (Softfail) - по результатам проверки глобальных политик отправитель признан нарушающим правила (уровень недостоверности SOFTFAIL);<br>**F** (Fail) - по результатам проверки локальных политик отправитель признан обычным и подлежащим дополнительной проверке по глобальным политикам с отказом при уровне недостоверности FAIL (код политики **FA**);<br>**#** - условие срабатывает, если проверка политик (и локальных, и глобальных) отключена;<br>**A** (Always) - условие срабатывает всегда, в том числе при полностью отключённой проверке политик;<br>**1** - то же, что и **A**, этот флаг используется для корректной обработки списков старого формата.<br>Если условие соответствует установленной для отправителя политике, сервер игнорирует его обнаружение в списке доверенных отправителей. Этот флаг имеет наивысший приоритет. |

## *Список запрещённых отправителей*

Это список адресов, почта от которых НЕ принимается в любом случае, независимо от других условий и настроек. Действие списка может быть перекрыто списком доверенных отправителей, поэтому можно с чистой совестью блокировать целые почтовые домены. Жёсткостью отказа можно управлять - от приёма в карантин до запрета даже на подачу жалобы.

Расположение списка задаётся параметром **SMTP[FromEmailBlackList]**, исходное - **CONF\lists\smtp\FromEmailBlackList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **EMAIL** | Шаблон запрещённого адреса. |

| | | |
|---|---|---|
| 2 | **IS_QUARANTINED** | Флаговая строка, определяющая, при каких условиях почту с этого адреса следует принимать в карантин. Существует целый ряд бесплатных почтовых систем (например, Mail.ru), адреса которых используют как злостные спамеры, так и вполне благонамеренные граждане. И пропустить полезную информацию только из-за того, что почтовый домен отправителя наводнён спамерами, не всегда желательно. Флаги определяют взаимодействие списка с результатами проверки локальных и глобальных политик и могут быть следующими:<br>**L** (Local) - отправитель локальный (IP-адрес принадлежит локальной сети или самому серверу), поэтому политики не проверялись;<br>**K** (Known) - отправитель известен, поскольку успешно авторизовался на сервере;<br>**W** (Whitelist) - по результатам проверки локальных политик отправитель признан особо доверенным (код политики **WL**; в этом случае до анализа данного списка дело не доходит, так что этот флаг никакого смысла не имеет);<br>**M** (Match) - по результатам проверки локальных политик адрес отправителя признан действительным (код политики **AM**);<br>**P** (Pass) - по результатам проверки глобальных политик адрес отправителя признан действительным;<br>**N** (None) - проверка глобальных политик не выявила никакой информации в отношении отправителя;<br>**E** (Error) - проверка глобальных политик не удалась из-за ошибки при получении информации;<br>**U** (Unknown) - проверка глобальных политик не дала однозначный результат;<br>**T** (neuTral) - по результатам проверки локальных политик отправитель признан крайне подозрительным и подлежащим дополнительной проверке по глобальным политикам с отказом при уровне недостоверности NEUTRAL (код политики **NE**);<br>**R** (neutRal) - по результатам проверки глобальных политик отправитель признан незначительно нарушающим правила (уровень недостоверности NEUTRAL);<br>**O** (sOftfail) - по результатам проверки локальных политик отправитель признан подозрительным и подлежащим дополнительной проверке по глобальным политикам с отказом при уровне недостоверности SOFTFAIL (код политики **SF**);<br>**S** (Softfail) - по результатам проверки глобальных политик отправитель признан нарушающим правила (уровень недостоверности SOFTFAIL);<br>**F** (Fail) - по результатам проверки локальных политик отправитель признан обычным и подлежащим дополнительной проверке по глобальным политикам с отказом при уровне недостоверности FAIL (код политики **FA**);<br>**#** - условие срабатывает, если проверка политик (и локальных, и глобальных) отключена;<br>**A** (Always) - условие срабатывает всегда, в том числе при полностью отключённой проверке политик;<br>**1** - то же, что и **A**, этот флаг используется для корректной обработки списков старого формата.<br>Если условие соответствует установленной для отправителя политике, письма с этого адреса будут приниматься и помещаться в специальный каталог, определяемый параметром **SMTP[Quarantined]**. |

| | | |
|---|---|---|
| 3 | **IS_UNCONDITIONAL** | Флаговая строка, определяющая, при каких условиях этого отправителя следует отвергать жёстко и бескомпромиссно вместо того, чтобы предоставить ему возможность подать жалобу на специальный адрес (abuse). Флаги определяют взаимодействие списка с результатами проверки локальных и глобальных политик и могут быть следующими:<br>**L** (Local) - отправитель локальный (IP-адрес принадлежит локальной сети или самому серверу), поэтому политики не проверялись;<br>**K** (Known) - отправитель известен, поскольку успешно авторизовался на сервере;<br>**W** (Whitelist) - по результатам проверки локальных политик отправитель признан особо доверенным (код политики **WL**; в этом случае до анализа данного списка дело не доходит, так что этот флаг никакого смысла не имеет);<br>**M** (Match) - по результатам проверки локальных политик адрес отправителя признан действительным (код политики **AM**);<br>**P** (Pass) - по результатам проверки глобальных политик адрес отправителя признан действительным;<br>**N** (None) - проверка глобальных политик не выявила никакой информации в отношении отправителя;<br>**E** (Error) - проверка глобальных политик не удалась из-за ошибки при получении информации;<br>**U** (Unknown) - проверка глобальных политик не дала однозначный результат;<br>**T** (neuTral) - по результатам проверки локальных политик отправитель признан крайне подозрительным и подлежащим дополнительной проверке по глобальным политикам с отказом при уровне недостоверности NEUTRAL (код политики **NE**);<br>**R** (neutRal) - по результатам проверки глобальных политик отправитель признан незначительно нарушающим правила (уровень недостоверности NEUTRAL);<br>**O** (sOftfail) - по результатам проверки локальных политик отправитель признан подозрительным и подлежащим дополнительной проверке по глобальным политикам с отказом при уровне недостоверности SOFTFAIL (код политики **SF**);<br>**S** (Softfail) - по результатам проверки глобальных политик отправитель признан нарушающим правила (уровень недостоверности SOFTFAIL);<br>**F** (Fail) - по результатам проверки локальных политик отправитель признан обычным и подлежащим дополнительной проверке по глобальным политикам с отказом при уровне недостоверности FAIL (код политики **FA**);<br>**#** - условие срабатывает, если проверка политик (и локальных, и глобальных) отключена;<br>**A** (Always) - условие срабатывает всегда, в том числе при полностью отключённой проверке политик;<br>**1** - то же, что и **A**, этот флаг используется для корректной обработки списков старого формата.<br>Если условие соответствует установленной для отправителя политике, почта с этого адреса отвергается незамедлительно. Как правило, возможность подачи жалобы следует оставлять и применять жёсткие меры только к самым обнаглевшим отправителям, использующим специальный адрес для рассылки спама. Этот флаг имеет приоритет над флагом приёма в карантин. |
| 4 | **REPLY** | Индивидуальный текст ответа сервера, поясняющий причину отказа. |

| | | |
|---|---|---|
| 5 | **IS_SKIPPED** | Флаговая строка, определяющая, при каких условиях следует игнорировать нахождение адреса в списке запрещённых отправителей. Флаги определяют взаимодействие списка с результатами проверки локальных и глобальных политик и могут быть следующими:<br>**L** (Local) - отправитель локальный (IP-адрес принадлежит локальной сети или самому серверу), поэтому политики не проверялись;<br>**K** (Known) - отправитель известен, поскольку успешно авторизовался на сервере;<br>**W** (Whitelist) - по результатам проверки локальных политик отправитель признан особо доверенным (код политики **WL**; в этом случае до анализа данного списка дело не доходит, так что этот флаг никакого смысла не имеет);<br>**M** (Match) - по результатам проверки локальных политик адрес отправителя признан действительным (код политики **AM**);<br>**P** (Pass) - по результатам проверки глобальных политик адрес отправителя признан действительным;<br>**N** (None) - проверка глобальных политик не выявила никакой информации в отношении отправителя;<br>**E** (Error) - проверка глобальных политик не удалась из-за ошибки при получении информации;<br>**U** (Unknown) - проверка глобальных политик не дала однозначный результат;<br>**T** (neuTral) - по результатам проверки локальных политик отправитель признан крайне подозрительным и подлежащим дополнительной проверке по глобальным политикам с отказом при уровне недостоверности NEUTRAL (код политики **NE**);<br>**R** (neutRal) - по результатам проверки глобальных политик отправитель признан незначительно нарушающим правила (уровень недостоверности NEUTRAL);<br>**O** (sOftfail) - по результатам проверки локальных политик отправитель признан подозрительным и подлежащим дополнительной проверке по глобальным политикам с отказом при уровне недостоверности SOFTFAIL (код политики **SF**);<br>**S** (Softfail) - по результатам проверки глобальных политик отправитель признан нарушающим правила (уровень недостоверности SOFTFAIL);<br>**F** (Fail) - по результатам проверки локальных политик отправитель признан обычным и подлежащим дополнительной проверке по глобальным политикам с отказом при уровне недостоверности FAIL (код политики **FA**);<br>**#** - условие срабатывает, если проверка политик (и локальных, и глобальных) отключена;<br>**A** (Always) - условие срабатывает всегда, в том числе при полностью отключённой проверке политик;<br>**1** - то же, что и **A**, этот флаг используется для корректной обработки списков старого формата.<br>Если условие соответствует установленной для отправителя политике, сервер игнорирует его обнаружение в списке запрещённых отправителей. Этот флаг имеет наивысший приоритет. |

## *Список ограниченных отправителей*

В отличие от двух предыдущих списков, традиционно называемых белым и чёрным, этот список можно назвать серым. В него заносятся отправители, которым разрешено отправлять почту не кому угодно, а некоему ограниченному и жёстко заданному кругу получателей. В качестве таких получателей могут выступать локальные пользователи, внешние адресаты, роботы и списки рассылки. Не действует этот список только на алиасы - их перечень к этому моменту уже обработан, так что сервер в случае срабатывания алиаса будет проверять уже результаты переадресации. Если отправитель обнаруживается в данном списке, сервер ищет строку, сопоставляющую его адрес с адресом получателя, и если такой записи не обнаружится, письмо будет отвергнуто.

Расположение списка задаётся параметром **SMTP[RestrictedFromEmails]**, исходное - **CONF\lists\smtp\RestrictedFromEmails.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **EMAIL** | Шаблон адреса отправителя. |

| | | |
|---|---|---|
| 2 | **RECIPIENTS_LIST** | Путь к файлу со списком разрешённых для этого отправителя получателей. |
| 3 | **REPLY_TEXT** | Пояснение причины отказа в приёме, подставляемое в ответ сервера. |
| 4 | **COMMENT** | Примечание. Это поле не используется сервером и предназначено для заметок администратора. |

Предполагается, что списки разрешённых получателей располагаются в каталоге **CONF\lists\smtp\restricted**, что определяется параметром **SMTP[Restricted]**. Конкретное имя и расположение каждого списка определяются в поле **RECIPIENTS_LIST**. Все списки имеют одинаковый формат. Назначение полей:

| | | |
|---|---|---|
| 1 | **EMAIL** | Адрес разрешённого получателя. |
| 2 | **COMMENT** | Примечание. Это поле не используется сервером и предназначено для заметок администратора. |

### *Список отправителей, подлежащих обязательной авторизации*

Это список "подозрительных" или критических адресов, для отправки писем с которых обязательно требуется SMTP-авторизация (или IP-авторизация по спискам локальных и доверенных сетей, если не установлено требование обязательной SMTP-авторизации) с заданным именем.

Расположение списка задаётся параметром **SMTP[FromEmailNeedAuthList]**, исходное - **CONF\lists\smtp\FromEmailNeedAuthList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **EMAIL** | Шаблон подозрительного адреса. |
| 2 | **MUST_LOGIN_AS** | Имя учётной записи (логин) и домен авторизации пользователя (в формате **логин@домен**), сопоставленные данному адресу. Если домен не указан, считается, что пользователь должен авторизоваться в домене по умолчанию. Если это поле пустое, то разрешение получит любой успешно авторизовавшийся пользователь. |
| 3 | **COMMENT** | Индивидуальный текст ответа сервера, поясняющий причину отказа в случае неверной авторизации. |

### *Список отправителей, которых надо авторизовать автоматически*

Это список адресов, для которых надо выполнять автоматическую авторизацию. Используется в ситуации, когда для отправки почты требуется SMTP-авторизация, а отправитель не умеет её выполнять и изменить его поведение не представляется возможным. Автоматическая авторизация запускается только тогда, когда пользователь ещё не прошёл авторизацию (либо SMTP-, либо по спискам локальных и доверенных сетей, в зависимости от настроек), и использование автомата разрешено.

Расположение списка задаётся параметром **SMTP[FromEmailAutoLogon]**, исходное - **CONF\lists\smtp\FromEmailAutoLogon.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **EMAIL** | Шаблон адреса, подлежащего автоматической авторизации. |
| 2 | **ALLOWED_IP** | Шаблон IP-адреса, при подключении с которого разрешена автоматическая авторизация. |
| 3 | **USER** | Имя учётной записи (логин) и домен авторизации пользователя (в виде **логин@домен**), используемые при автоматической авторизации. Если задано только имя учётной записи, считается, что авторизация выполняется в домене по умолчанию. |
| 4 | **COMMENT** | Примечание. Это поле не используется сервером и предназначено для заметок администратора. |

### *Список специальных отправителей*

Это ещё один список, позволяющий серверу обрабатывать почту, генерируемую специфическими программами - в данном случае это программы, использующие некорректный адрес отправителя. Ответ на такие адреса невозможен, но эти программы работают непосредственно на сервере и создаваемые ими письма предназначены локальным пользователям, поэтому необходимо обеспечить их приём.

Расположение списка задаётся параметром **SMTP[SpecialSenders]**, исходное - **CONF\lists\smtp\SpecialSenders.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **EMAIL_MASK** | Шаблон разрешённого некорректного адреса. |

| | | |
|---|---|---|
| 2 | **IP_MASK** | Шаблон IP-адреса, с которого разрешено представляться таким некорректным адресом. |
| 3 | **COMMENT** | Примечание. Это поле не используется сервером и предназначено для заметок администратора. |

### *Список отправителей, которым не следует отвечать*

Это список адресов, на письма с которых ни в коем случае не следует формировать автоответы - обычно это списки рассылки, которые в случае автоответа могут из списка рассылки автоматически исключить, или завяжется переписка роботов.

Расположение списка задаётся параметром **SMTP[NoAutoReplyTo]**, исходное - **CONF\lists\smtp\NoAutoReplyTo.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **EMAIL_MASK** | Шаблон адреса. |
| 2 | **COMMENT** | Примечание. Это поле не используется сервером и предназначено для заметок администратора. |

### *Список отправителей с особым режимом архивации*

Это список отправителей с особым режимом архивации отправляемых ими писем. Здесь задаются особые архивные каталоги для таких отправителей. Кроме того, в режиме архивации всех писем этот список можно использовать для исключения некоторых отправителей - посылаемые ими письма не будут помещаться в архив.

Расположение списка задаётся параметром **SMTP[ArchiveSenders]**, исходное - **CONF\lists\smtp\ArchiveSenders.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **EMAIL_MASK** | Шаблон адреса отправителя. Используя символы групповой операции, можно управлять архивацией почты для целых доменов. |
| 2 | **ARCHIVE_DIR** | Шаблон особого каталога для архивирования писем, посылаемых этим отправителем. Здесь допускается использование макросов (**{}**). Пустое значение обрабатывается в зависимости от режима архивации. Если в архив помещаются все письма, то пустое значение этого поля отключает архивацию для данного отправителя. Если в архив помещаются только письма, посылаемые отправителями из этого списка, то пустое значение заменяется на каталог архива по умолчанию, соответствующий категории архивируемых писем. |
| 3 | **COMMENT** | Примечание. Это поле не используется сервером и предназначено для заметок администратора. |

### *Список псевдонимов (алиасов)*

Это список адресов, вместо которых подставляются реальные адреса ПОЛУЧАТЕЛЕЙ. На адреса отправителей алиасы не действуют. Здесь задаются только алиасы. Списки рассылки обрабатываются отдельно.

Список алиасов обрабатывается в первую очередь (более высокий приоритет имеет только описанный ниже список переадресации по адресу отправителя), дальнейший анализ выполняется уже по отношению к адресу перенаправления - но от отправителя факт перенаправления скрывается. Рекурсивная обработка алиасов не поддерживается.

Расположение списка задаётся параметром **SMTP[ToEmailAliases]**, исходное - **CONF\lists\smtp\ToEmailAliases.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **EMAIL** | Исходный адрес-псевдоним. |
| 2 | **ALIAS** | Реальный адрес получателя. Здесь допускается использование макросов (**{}**). |
| 3 | **IS_GLOBAL** | Флаг, определяющий, является ли алиас общедоступным либо это скрытый адрес только для своих. Установка нулевого значения делает алиас скрытым; использовать его могут либо полностью авторизованные пользователи, либо, если обязательная авторизация для этого не требуется, отправители, указавшие правильный обратный адрес, принадлежащий локальному домену. |
| 4 | **IGNORE** | Флаг, позволяющий временно исключать алиасы из обработки, не удаляя саму информацию об алиасе. |
| 5 | **COMMENT** | Примечание. Это поле не используется сервером и предназначено для заметок администратора. |

### *Список переадресации по адресу отправителя*

Иногда возникает необходимость выбирать получателя письма в зависимости от адреса отправителя, а вовсе не в соответствии с передаваемыми клиентом адресами получателей, - например, когда партнёрская рассылка вместо собственного списка рассылки упорно поступает на чей-то личный адрес. Для исправления таких огрехов предназначен особый список - похожий по своему действию на список псевдонимов, но отталкивающийся от адреса отправителя сообщения. Как и в списке алиасов, в этом списке одному адресу отправителя можно сопоставить только один адрес получателя. При необходимости доставки сообщения нескольким адресатам можно использовать переадресацию на список рассылки.

Этот список обрабатывается в самую первую очередь, дальнейший анализ выполняется уже по отношению к адресу перенаправления - но от отправителя факт перенаправления скрывается.

Расположение списка задаётся параметром **SMTP[FromEmailAliasesTo]**, исходное - **CONF\lists\smtp\FromEmailAliasesTo.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **EMAIL** | Адрес отправителя. |
| 2 | **ALIAS** | Реальный адрес получателя, сопоставленный адресу отправителя. Здесь допускается использование макросов (**{}**). |
| 3 | **DESCRIPTION** | Комментарий - для Вашего сведения. |
| 4 | **IGNORE** | Флаг, позволяющий временно исключать алиасы из обработки, не удаляя саму информацию об алиасе. |

### *Список доверенных получателей*

Это список адресов получателей, почта для которых принимается в любом случае, независимо от других условий (кроме одного - отправителю должно быть разрешено воспользоваться услугами сервера) и настроек. Он имеет приоритет над списком запрещённых адресов, что позволяет блокировать целые почтовые домены, но для отдельных получателей делать исключения.

Расположение списка задаётся параметром **SMTP[ToEmailWhiteList]**, исходное - **CONF\lists\smtp\ToEmailWhiteList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **EMAIL** | Шаблон доверенного адреса. |
| 2 | **REPLY_TEXT** | Индивидуальный текст подтверждения, подставляемый в ответ сервера. |

### *Список запрещённых получателей*

Список адресов, почта для которых НЕ принимается в любом случае, независимо от других условий и настроек. Единственное исключение - отправитель является администратором, которому разрешено обходить это ограничение. Действие списка может быть перекрыто списком доверенных получателей, поэтому можно с чистой совестью блокировать целые почтовые домены.

Расположение списка задаётся параметром **SMTP[ToEmailBlackList]**, исходное - **CONF\lists\smtp\ToEmailBlackList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **EMAIL** | Шаблон запрещённого адреса. |
| 2 | **REPLY_TEXT** | Индивидуальный текст ответа сервера, поясняющий причину отказа. |

### *Список ограниченных получателей*

В отличие от двух предыдущих списков, традиционно называемых белым и чёрным, этот список можно назвать серым. В него заносятся получатели, которым разрешено принимать почту не от кого угодно, а от некоего ограниченного и жёстко заданного круга отправителей. В качестве получателей могут выступать локальные пользователи, внешние адресаты, роботы и списки рассылки. Не действует этот список только на алиасы - их перечень к этому моменту уже обработан, так что сервер в случае срабатывания алиаса будет проверять уже результаты переадресации. Если получатель обнаруживается в данном списке, сервер ищет строку, сопоставляющую его адрес с адресом отправителя, и если такой записи не обнаружится, письмо будет отвергнуто.

Расположение списка задаётся параметром **SMTP[RestrictedEmails]**, исходное - **CONF\lists\smtp\RestrictedEmails.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **EMAIL** | Шаблон адреса получателя. |
| 2 | **SENDERS_LIST** | Путь к файлу со списком разрешённых для этого получателя отправителей. |
| 3 | **REPLY_TEXT** | Пояснение причины отказа в приёме, подставляемое в ответ сервера. |

| | | |
|---|---|---|
| 4 | **COMMENT** | Примечание. Это поле не используется сервером и предназначено для заметок администратора. |

Предполагается, что списки разрешённых отправителей располагаются в каталоге **CONF\lists\smtp\restricted**, что определяется параметром SMTP[Restricted]. Конкретное имя и расположение каждого списка определяются в поле **SENDERS_LIST**. Все списки имеют одинаковый формат. Назначение полей:

| | | |
|---|---|---|
| 1 | **EMAIL** | Адрес разрешённого отправителя. |
| 2 | **COMMENT** | Примечание. Это поле не используется сервером и предназначено для заметок администратора. |

### *Список получателей "чужих" доменов*

Это список адресов и SMTP-серверов, куда надлежит переправлять почту для этих получателей. Используется в случаях, если почтовый сервер обслуживает "чужие" домены и должен пересылать почту этих доменов на другой SMTP-сервер, не пользуясь MX-маршрутизацией. Используется также в качестве управляющего файла планировщика для доставки писем-возвратов от агентов отправки smtpsend3 и smtpsend4.

Расположение списка задаётся параметром **SMTP[EmailSmtpForward]**, исходное - **CONF\lists\smtp\EmailSmtpForward.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **EMAIL_MASK** | Шаблон адреса перенаправляемого получателя. Используя символы групповой операции, можно организовать перенаправление почты для целых доменов. |
| 2 | **FORWARD_TO_SERVER** | Имя или IP-адрес сервера, на который перенаправляется почта. |
| 3 | **PORT** | Номер порта, на котором работает почтовый сервер-получатель. Если подключён расширенный сервис доставки исходящей почты SmtpSend, может быть указано нулевое значение, тогда порт выбирается автоматически в зависимости от выбранного режима безопасности передачи. |
| 4 | **LOGIN** | Если для отправки почты требуется авторизация на сервере, то здесь задаётся имя учётной записи (логин) пользователя. В противном случае поле следует оставить пустым. При использовании расширенного сервиса доставки исходящей почты SmtpSend это и следующее поле задают реквизиты авторизации по умолчанию, которые могут быть переопределены в зависимости от адреса отправителя письма. |
| 5 | **PASSW** | Если для отправки почты требуется авторизация на сервере, то здесь задаётся пароль пользователя. |
| 6 | **POP_SERVER** | Если сервер назначения требует авторизацию на сервере POP3 (такой механизм называется POP-before-SMTP), то здесь задаётся имя или IP-адрес сервера POP3. В текущей версии этот механизм не реализован, поле зарезервировано для последующего применения. |
| 7 | **TREAT_AS_LOCAL** | Поскольку "чужие" домены не относятся к локальным, отправлять почту по их адресам могут только правильно авторизованные локальные пользователи. Чтобы обеспечить приём писем на такие адреса от внешних отправителей, этот флаг в нужных строках должен иметь ненулевое значение - тогда соответствующие адреса (или домены целиком) будут интерпретироваться сервером как локальные. |
| 8 | **DON'T_DELIVER** | Позволяет блокировать самостоятельную доставку писем на сервер-получатель. Эта возможность применяется в особых случаях, когда SMTP-сервер работает в связке с другой почтовой системой, передавая ей всю поступающую почту для дальнейшей обработки и доставки. Достаточно задать в нужных строках ненулевое значение этого флага, чтобы исключить соответствующий целевому серверу каталог из списка просматриваемых агентом отправки. |

| | | |
|---|---|---|
| 9 | **SECURITY** | Требуемый режим безопасности при передаче писем на данный сервер. Задаётся комбинацией следующих ключевых слов:<br>**SSL** - использовать полностью защищённое соединение;<br>**TLS** - использовать подключение в незащищённом режиме с последующим переключением в защищённый режим;<br>**NONE** - допускается использование незащищённого режима.<br>Если не задано ни одно ключевое слово, используется незащищённый режим. Если номер порта фиксирован, то режим SSL не может быть задан совместно с другими режимами. При наличии нескольких вариантов сервер пробует все указанные режимы, начиная с самого защищённого. Это поле используется только расширенным сервисом доставки исходящей почты SmtpSend и задаёт режим по умолчанию, который может быть переопределён в зависимости от адресов отправителя и получателя. |
| 10 | **SSL_CERT** | Имя файла формата PEM, содержащего закрытый ключ и сертификаты, используемые при организации защищённого (SSL) соединения с целевым сервером. Это поле используется только расширенным сервисом доставки исходящей почты SmtpSend и задаёт сертификат по умолчанию, который может быть переопределён в зависимости от адресов отправителя и получателя. Здесь допускается использование макросов (**{}**). Если поле пустое, используется сертификат по умолчанию, определённый в настройках сервиса. |
| 11 | **SSL_VERIFY** | Определяет режим проверки подлинности сертификатов целевого сервера при установлении защищённого соединения. Задаётся либо числовым кодом, либо символьным обозначением:<br>**SSL_VERIFY:IGNORE** - сертификат целевого сервера проверяется, но соединение устанавливается независимо от результата проверки, при этом клиентский сертификат серверу не предъявляется (числовое значение -1);<br>**SSL_VERIFY:NONE** - сертификат целевого сервера проверяется, но соединение устанавливается независимо от результата проверки (числовое значение 0);<br>**SSL_VERIFY:STANDARD** - сертификат целевого сервера проверяется, при отрицательном результате проверки соединение незамедлительно разрывается (числовое значение 1).<br>Это поле используется только расширенным сервисом доставки исходящей почты SmtpSend и задаёт режим по умолчанию, который может быть переопределён в зависимости от адресов отправителя и получателя. Здесь допускается использование макросов (**{}**). Если поле пустое, используется режим по умолчанию, определённый в настройках сервиса. |
| 12 | **COMMENT** | Примечание. Это поле не используется сервером и предназначено для заметок администратора. |

## *Список автоответчиков*

Это список адресов, на которых работает автоответчик. В этой конфигурации автоответчик можно сопоставить только адресам из списка локальных почтовых ящиков. Автоответ генерируется только в ответ на явное обращение по адресу (в том числе посредством алиаса). При доставке письма через список рассылки автоответы не формируются.

Расположение списка задаётся параметром **SMTP[AutoReply]**, исходное - **CONF\lists\smtp\AutoReply.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **EMAIL_MASK** | Шаблон адреса автоответчика. |
| 2 | **MESSAGE_FILE** | Путь к файлу шаблона автоответа. Предполагается, что все используемые SMTP-сервером шаблоны располагаются в каталоге **CONF\templates\smtp**, но можно указать любое другое расположение. |
| 3 | **URL** | Дополнительный параметр. В изначальном варианте - ссылка на web-страницу с дополнительной информацией. В шаблоне письма этот параметр доступен через слово **REPLYURL**. |

| | | |
|---|---|---|
| 4 | **VACATION_NAME** | Дополнительный параметр. В изначальном варианте - имя пользователя-автоответчика. В шаблоне письма этот параметр доступен через слово **REPLYNAME**. |
| 5 | **IGNORE** | Флаг, позволяющий временно исключать автоответчики из обработки, не удаляя саму информацию об автоответчике. |
| 6 | **COMMENT** | Примечание. Это поле не используется сервером и предназначено для заметок администратора. |
| 7 | **REPLY_LIST** | Путь к файлу со списком отправителей, которым разрешено отвечать. Если список задан, то автоответы будут формироваться только для отправителей из этого списка. Предполагается, что списки разрешённых отправителей располагаются в каталоге **CONF\lists\smtp\autoresponders**, но можно указать любое расположение. |

### *Списки разрешённых отправителей автоответчиков*

В этих списках перечисляются отправители, в адрес которых разрешено отправлять автоответы.

Предполагается, что списки разрешённых отправителей располагаются в каталоге **CONF\lists\smtp\autoresponders**, что определяется параметром **SMTP[Autoresponders]**. Конкретное имя и действительное расположение каждого списка задаются в списке автоответчиков. Все списки имеют одинаковый формат. Назначение полей:

| | | |
|---|---|---|
| 1 | **EMAIL** | Адрес отправителя. |
| 2 | **COMMENT** | Примечание. Это поле не используется сервером и предназначено для заметок администратора. |

### *Перечень списков рассылки*

Список адресов, являющихся списками рассылки. Этот список особым образом дополняет список локальных почтовых ящиков и задаёт дополнительные параметры каждого списка.

Расположение списка задаётся параметром **SMTP[ToEmailMailLists]**, исходное - **CONF\lists\smtp\ToEmailMailLists.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **EMAIL** | Адрес списка рассылки. |
| 2 | **LISTFILE** | Путь к файлу со списком рассылки. Предполагается, что все списки рассылки располагаются (в соответствии со значением параметра **SMTP[MailingLists]**) в каталоге **CONF\lists\smtp\maillists**, но можно указать любое расположение. |
| 3 | **ENABLED** | Флаг, определяющий, активен список или нет. Ненулевое значение указывает, что в список можно отправлять сообщения, в противном случае сервер ответит, что список временно заблокирован. |
| 4 | **IS_GLOBAL** | Флаг, определяющий, является ли список рассылки общедоступным либо это скрытый адрес только для своих. Установка нулевого значения делает список рассылки скрытым; использовать его могут либо полностью авторизованные пользователи, либо, если обязательная авторизация для этого не требуется, отправители, указавшие правильный обратный адрес, принадлежащий локальному домену. |
| 5 | **CHECK_SENDERS** | Флаг, определяющий, является ли список открытым или частным. Если задано ненулевое значение, отправлять сообщения в этот список могут только отправители, перечисленные в особом списке. |
| 6 | **IS_ABUSE** | Флаг, определяющий, является ли список рассылки специальным получателем - abuse. На такой адрес могут отправлять сообщения даже отправители, находящиеся в списке запрещённых адресов электронной почты. |
| 7 | **MAX_MSG_SIZE** | Максимально допустимый размер письма, которое можно отправить участникам этого списка рассылки. Если значения из списков локальных и доверенных сетей могут ослаблять исходное ограничение, то это усиливающее ограничение. Чтобы ограничение вступило в силу, отправитель должен принадлежать к одному из локальных доменов. Размер письма задаётся в байтах. Если указано нулевое значение, дополнительное ограничение не накладывается. |

| | | |
|---|---|---|
| 8 | **SENDERS_LIST** | Путь к файлу со списком разрешённых отправителей. Используется, если список рассылки помечен как частный. Предполагается, что списки разрешённых отправителей, как и сами списки рассылки, располагаются в каталоге **CONF\lists\smtp\maillists**, но можно указать любое расположение. |
| 9 | **REPLY** | Индивидуальный текст подтверждения, подставляемый в ответ сервера. |
| 10 | **IGNORE** | Флаг, позволяющий временно исключать списки из обработки, не удаляя саму информацию о списке. Этот флаг имеет приоритет над флагом **ENABLED**. |
| 11 | **COMMENT** | Примечание. Это поле не используется сервером и предназначено для заметок администратора. |

### *Списки рассылки*

В этих списках перечислены получатели писем, отсылаемых в соответствующий список рассылки. Это могут быть как локальные получатели, так и внешние. При обработке списка не проверяется, имеет ли отправитель право посылать почту за пределы локального домена, сам же список рассылки представлен локальным адресом. Поэтому для общего доступа рекомендуется открывать только списки, предназначенные для рассылки среди локальных пользователей. Списки рассылки, выполняющие отправку почты за пределы локального домена, следует объявить либо скрытыми, либо частными.

Предполагается, что все списки рассылки располагаются в каталоге **CONF\lists\maillists**, что определяется параметром **SMTP[MailLists]**. Конкретное имя и действительное расположение каждого списка задаются в перечне списков рассылки. Все списки имеют одинаковый формат. Назначение полей:

| | | |
|---|---|---|
| 1 | **EMAIL** | Адрес получателя. |
| 2 | **COMMENT** | Примечание. Это поле не используется сервером и предназначено для заметок администратора. |

### *Списки разрешённых отправителей рассылки*

В этих списках перечисляются отправители, которым разрешено посылать сообщения в частные списки рассылки.

Как и сами списки рассылки, они предположительно располагаются в каталоге **CONF\lists\maillists**, что определяется параметром **SMTP[MailLists]**. Конкретное имя и действительное расположение каждого списка задаются в перечне списков рассылки. Все списки имеют одинаковый формат. Назначение полей:

| | | |
|---|---|---|
| 1 | **EMAIL** | Адрес отправителя. |
| 2 | **NEED_AUTH** | Флаг, указывающий, требуется ли авторизация для подтверждения подлинности этого отправителя. Если значение ненулевое, то требуется. |
| 3 | **MUST_LOGIN_AS** | Если требуется авторизация отправителя, то здесь указывается его имя учётной записи (логин) и домен авторизации (в формате **логин@домен**), сопоставленные адресу. Если указано только имя учётной записи, считается, что отправитель должен быть авторизован в домене по умолчанию. Если это поле пустое, то разрешение (при условии совпадения обратного адреса) получит любой успешно авторизовавшийся пользователь. |

### *Список нерассылки*

В этом списке перечислены адреса, по которым приходящие по рассылке письма доставляться не должны. Если некий сотрудник, занесённый в десяток списков внутренней рассылки, уходит в отпуск, проще занести его адрес в один список запрета, нежели исключать из всех списков, а затем восстанавливать. Этот список действует только на списки рассылки; письма, поступающие непосредственно на адрес (в том числе и по переадресации), будут доставляться.

По принадлежности этот список размещается в том же каталоге, что и списки рассылки, и отличается от остальных списков специфическим именем. Расположение списка задаётся параметром **SMTP[ToEmailDNDList]**, исходное - **CONF\lists\smtp\maillists\--DND--.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **EMAIL** | Адрес получателя, исключаемого из рассылки. |
| 2 | **COMMENT** | Примечание. Это поле не используется сервером и предназначено для заметок администратора. |

### *Список извещения владельцев локальных почтовых ящиков*

В этом списке перечислены локальные почтовые ящики, владельцев которых следует немедленно извещать о поступлении входящей почты. Извещение не генерируется, если сервер посчитал входящее письмо спамом, а также если почтовый ящик получателя отсутствует в списке локальных почтовых ящиков (например, в случае автоматического создания неописанного ящика в локальном домене).

Расположение списка задаётся параметром **SMTP[ToEmailNotify]**, исходное - **CONF\lists\smtp\ToEmailNotify.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **MAILBOX** | Адрес локального почтового ящика, владельца которого следует извещать о приходе почты. |
| 2 | **NOTIFY_TO** | Адрес, на который следует отправлять письмо-извещение. Допускается использование макроподстановок (**{}**). В шаблоне письма этот параметр доступен через слово **NOTIFY-TO**. |
| 3 | **MESSAGE_FILE** | Путь к файлу шаблона извещения. Предполагается, что все используемые SMTP-сервером шаблоны располагаются в каталоге **CONF\templates\smtp**, но можно указать любое другое расположение. |
| 4 | **PARAM1** | Дополнительный параметр, который можно использовать в тексте шаблона. Допускается использование макроподстановок (**{}**). В шаблоне письма этот параметр доступен через слово **NOTE-PARAM1**. |
| 5 | **PARAM2** | Дополнительный параметр, который можно использовать в тексте шаблона. Допускается использование макроподстановок (**{}**). В шаблоне письма этот параметр доступен через слово **NOTE-PARAM2**. |
| 6 | **IGNORE** | Флаг, позволяющий временно исключать извещения из обработки, не удаляя саму информацию об извещении. |
| 7 | **COMMENT** | Примечание. Это поле не используется сервером и предназначено для заметок администратора. |

### *Список почтовых роботов*

В этом списке перечислены адреса, на которых функционируют почтовые роботы - специальные программы, обрабатывающие поступающие к ним письма особого формата. С помощью роботов можно выполнять любую обработку почты - от простой доставки в нужный почтовый ящик до выполнения сложных запросов к различным информационным системам с последующей отправкой сформированного ответа. В состав PigMail+PigProxy уже входят несколько готовых к применению роботов, их описание приведено в приложении 3.

Этот список особым образом дополняет список локальных почтовых ящиков и задаёт дополнительные параметры каждого робота. Робот считается локальным получателем, поэтому послать ему запрос может любой отправитель. Робот должен сам определять, имеет ли отправитель право на выполнение запрошенных действий.

Роботу выделяется отдельная рабочая копия письма, создаваемая в каталоге для временных файлов (определяемом параметром **Dirs[Temp]**), - поэтому, если налажена регулярная очистка этого каталога, робот может не заботиться о своевременном её удалении. Имя файла рабочей копии доступно через специальные слова **ROBOTFILENAME** и **ROBOTFILE** - второе слово возвращает имя, закавыченное в соответствии со стандартами записи длинных имён.

Расположение списка задаётся параметром **SMTP[ToEmailRobots]**, исходное - **CONF\lists\smtp\ToEmailRobots.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **EMAIL** | Адрес почтового робота. |
| 2 | **ENABLED** | Флаг, определяющий, активен робот или нет. Ненулевое значение указывает, что роботу можно отправлять сообщения, в противном случае сервер ответит, что сервис временно заблокирован. |
| 3 | **IS_GLOBAL** | Флаг, определяющий, является ли робот общедоступным либо это скрытый адрес только для своих. Установка нулевого значения делает робота скрытым; использовать его могут либо полностью авторизованные пользователи, либо, если обязательная авторизация для этого не требуется, отправители, указавшие правильный обратный адрес, принадлежащий локальному домену. |

| | | |
|---|---|---|
| 4 | **IS_ABUSE** | Флаг, определяющий, является ли робот специальным получателем - abuse. На такой адрес могут отправлять сообщения даже отправители, находящиеся в списке запрещённых адресов электронной почты. |
| 5 | **MAX_MSG_SIZE** | Максимально допустимый размер письма, которое можно отправить на этот адрес. Если значения из списков локальных и доверенных сетей могут ослаблять исходное ограничение, то это усиливающее ограничение. Чтобы ограничение вступило в силу, отправитель должен принадлежать к одному из локальных доменов. Размер письма задаётся в байтах. Если указано нулевое значение, дополнительное ограничение не накладывается. |
| 6 | **IS_INLINE** | Почтовые роботы могут быть двух типов - внешние приложения и встроенные (например, в виде дополнительных модулей расширения) правила сервера. Ненулевое значение этого параметра определяет, что используется встроенное правило. Необходимо учесть, что выполнение встроенного правила (если не принять специальных мер) может сильно задержать доставку письма другим получателям, если таковые имеются. Поэтому предпочтительным вариантом является использование внешних приложений - тем более что такие приложения можно создавать с использованием любого языка программирования. |
| 7 | **COMMAND** | Команда запуска робота. Для внешнего приложения это обычная командная строка запуска приложения; имя файла рабочей копии письма подставляется в неё в виде **{ROBOTFILENAME}** или **{"}{ROBOTFILENAME}{"}** (в обрамляющих фигурных скобках присутствуют не кавычки, а сдвоенные апострофы). Второй вариант возвращает имя файла, закавыченное в соответствии со стандартами записи длинных имён, у него есть более удобный синоним **{ROBOTFILE}**. Для встроенного робота это имя вычисляемого правила; поскольку правило выполняется в контексте самого сервера, ему доступны все необходимые переменные, в том числе и имя файла рабочей копии. |
| 8 | **REPLY** | Индивидуальный текст подтверждения, подставляемый в ответ сервера. |
| 9 | **IGNORE** | Флаг, позволяющий временно исключать роботов из обработки, не удаляя саму информацию о роботе. Этот флаг имеет приоритет над флагом **ENABLED**. |
| 10 | **COMMENT** | Примечание. Это поле не используется сервером и предназначено для заметок администратора. |
| 11 | **PLUGIN** | Путь к каталогу плагина, который необходимо загрузить для обеспечения поддержки данного робота. Здесь допускается использование макросов (**{}**). Плагин загружается при старте SMTP-сервера, независимо от состояния флагов **ENABLED** и **IGNORE**. Если робот не нуждается в загрузке особого плагина, это поле следует оставить пустым. |

### *Список получателей с особым режимом архивации*

Это список адресатов с особым режимом архивации предназначенных им писем. Здесь задаются особые архивные каталоги для таких адресатов. Кроме того, в режиме архивации всех писем этот список можно использовать для исключения некоторых адресатов - предназначенные им письма не будут помещаться в архив.

Расположение списка задаётся параметром **SMTP[ArchiveRecipients]**, исходное - **CONF\lists\smtp\ArchiveRecipients.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **EMAIL_MASK** | Шаблон адреса получателя. Используя символы групповой операции, можно управлять архивацией почты для целых доменов. |
| 2 | **ARCHIVE_DIR** | Шаблон особого каталога для архивирования писем, предназначенных этому получателю. Здесь допускается использование макросов (**{}**). Пустое значение обрабатывается в зависимости от режима архивации. Если в архив помещаются все письма, то пустое значение этого поля отключает архивацию для данного адресата. Если в архив помещаются только письма, предназначенные получателям из этого списка, то пустое значение заменяется на каталог архива по умолчанию, соответствующий категории архивируемых писем. |
| 3 | **COMMENT** | Примечание. Это поле не используется сервером и предназначено для заметок администратора. |

### *Список запоминаемых заголовочных полей письма*

В этом списке перечислены заголовочные поля письма, содержимое которых используется различными обработчиками - упрощённым фильтром содержимого, автоответчиком или обработчиком "магических слов". Содержимое каждого поля запоминается под условным именем во время предварительной обработки письма (в процессе приёма или сразу по его окончанию - в зависимости от способа получения) и впоследствии может быть получено по этому условному имени.

Расположение списка задаётся параметром **SMTP[Headers]**, исходное - **CONF\lists\smtp\Headers.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **HEADER_NAME** | Имя заголовочного поля без финального двоеточия - например, **Reply-To**. Регистр букв значения не имеет. Символы групповой операции в этом поле недопустимы. |
| 2 | **HEADER_CODE** | Условное имя, под которым сохраняется содержимое заголовочного поля. Регистр букв значения не имеет. |
| 3 | **DECODED** | Ряд заголовочных полей, включая наиболее важные для анализа содержания, при формировании письма обычно подвергаются MIME-кодированию с целью беспрепятственного прохождения через почтовые серверы. Если параметр имеет ненулевое значение, запоминается декодированное значение заголовочного поля, в противном случае - исходное, как оно представлено в письме. |
| 4 | **HSKIP** | Если этот параметр имеет ненулевое значение, то при запоминании от содержимого заголовочного поля отрезается его имя, включая двоеточие и последующий разделительный пробел. В противном случае заголовочное поле запоминается целиком. |

### *Список недопустимых типов данных*

Этот список по смыслу относится к подсистеме фильтрации содержания, но стоит несколько особняком, поскольку анализ типов данных управляется отдельным глобальным флагом **SMTP[UseContentTypeFilter]**. По изначальному замыслу этот список предназначен для отсеивания нечитаемых писем, написанных в китайской кодировке. Нежелательное содержимое ищется в заголовочных полях Content-Type и Subject. Письма, не прошедшие через фильтр, помещаются в каталог, определяемый параметром **SMTP[Nonreadable]**.

Расположение списка задаётся параметром **SMTP[BlackListContentType]**, исходное - **CONF\lists\smtp\filters\BlackListContentType.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **MASK** | Шаблон кода недопустимого типа данных. |
| 2 | **REPLY_TEXT** | Индивидуальный текст ответа сервера, поясняющий причину отказа в приёме письма. |

### *Список "магических" слов в заголовке письма*

Этот список позволяет задавать простые правила маршрутизации писем в зависимости от содержания заголовочных полей. Если указанные заголовочные поля (из сохранённых для обработки в соответствии со списком запоминания) соответствуют или не соответствуют в заданном сочетании заданному в списке набору шаблонов, в перечень получателей письма добавляется ещё один адрес, сопоставленный сработавшему сочетанию.

Список представляет собой программу на сильно упрощённом языке, позволяющую описывать довольно замысловатые сочетания, могущие встретиться в заголовках писем. Он обрабатывается сверху вниз, и добавление получателя происходит при каждом выявлении совпадения. Анализ можно досрочно прервать, чтобы исключить "дурную множественность" при большом количестве совпадающих слов.

Расположение списка задаётся параметром **SMTP[MagicWords]**, исходное - **CONF\lists\smtp\MagicWords.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **HEADER_CODE** | Условное имя, под которым сохранено содержимое заголовочного поля. Оно должно соответствовать имени из списка запоминаемых заголовочных полей. Регистр букв значения не имеет, символы групповой операции недопустимы. |
| 2 | **MASK** | Шаблон содержимого указанного поля. |
| 3 | **NOT1** | Если этот параметр имеет ненулевое значение, проверка выполняется на несовпадение с шаблоном. |
| 4 | **OR** | Если этот параметр имеет ненулевое значение, полученный результат объединяется с ранее определённым по правилу логического ИЛИ, в противном случае - по правилу логического И. Для первой строки составного условия ранее определённым результатом считается логическая истина. |

| | | |
|---|---|---|
| 5 | **NOT2** | Если этот параметр имеет ненулевое значение, полученный общий результат инвертируется. |
| 6 | **LAST** | Признак завершения условия. Список организован так, что сложное условие записывается в несколько строк - по одной на каждое простое условие. Если этот параметр имеет ненулевое значение, это означает, что данная строка является последней в составном условии. |
| 7 | **EMAIL** | Адрес, который следует добавить в список получателей письма, если в результате обработки условия получена логическая истина. |
| 8 | **TERMINATE** | Определяет, прерывать обработку списка, если условие сработало, или продолжать дальше. Ненулевое значение вызывает прерывание. Если условие не сработало, обработка списка продолжается дальше независимо от значения этого параметра. Если строка не является последней строкой составного условия, параметр также не проверяется. |

### *Список субшаблонов для писем-извещений о задержании вируса*

Этот вспомогательный список предназначен для составления более детализированных (или более внятных), чем это возможно при использовании единственного шаблона, писем-извещений, отсылаемых при выявлении вируса в письме. Дело в том, что сервер, в зависимости от настроек, может как помещать заражённые письма в карантин для последующего анализа, так и удалять их незамедлительно. Использование механизма субшаблонов позволяет, затратив минимум усилий, поместить в письмо фрагмент, сообщающий имя файла либо, напротив, извещающий о факте удаления файла.

Расположение списка задаётся параметром **SMTP[InfectedFileNameAddOns]**, исходное - **CONF\lists\smtp\InfectedFileNameAddOns.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **ADDON_ID** | Строка-идентификатор субшаблона. |
| 2 | **ADDON_ACTIVE** | Субшаблон, подставляемый, если заражённое письмо помещено в карантин. Указывается полный путь к файлу шаблона, допускается использование макроподстановок. |
| 3 | **ADDON_PASSIVE** | Субшаблон, подставляемый, если заражённое письмо удалено. Указывается полный путь к файлу шаблона, допускается использование макроподстановок. |

## *Управляющие списки загрузчика внешней POP-почты Pop2Smtp*

Эти списки предназначены для управления загрузчиком внешней POP-почты Pop2Smtp, их исходное расположение - каталог **CONF\lists\pop2smtp**.

### *Список опрашиваемых почтовых ящиков*

Этот список устанавливает соответствие между расположенными на внешних серверах почтовыми ящиками, подлежащими опросу по протоколу POP3, и SMTP-серверами, на которые следует пересылать загружаемые из почтовых ящиков сообщения.

Расположение списка задаётся параметром **Pop2Smtp[Boxes]**, исходное - **CONF\lists\pop2smtp\Boxes.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **POP3SERVER** | Имя или IP-адрес POP-сервера. |
| 2 | **POP3PORT** | Номер порта на POP-сервере. |
| 3 | **POP3LOGIN** | Имя учётной записи почтового ящика. |
| 4 | **POP3PASSW** | Пароль учётной записи почтового ящика. |
| 5 | **SMTPSERVER** | Имя или IP-адрес SMTP-сервера. |
| 6 | **SMTPPORT** | Номер порта на SMTP-сервере. |
| 7 | **SMTPLOGIN** | Имя учётной записи пользователя на SMTP-сервере (если требуется). |
| 8 | **SMTPPASSW** | Пароль учётной записи пользователя на SMTP-сервере (если требуется). |
| 9 | **DEFAULT_EMAIL** | Адрес получателя по умолчанию. Используется, если из заголовков письма не удаётся выделить ни один допустимый для сервера назначения адрес получателя. |
| 10 | **DELETE_AFTER_RETR** | Определяет, удалять ли почту из ящика после загрузки. |

## *Управляющие списки загрузчика внешней POP-почты Pop3Recv*

Эти списки предназначены для управления загрузчиком внешней POP-почты Pop3Recv, их исходное расположение, определяемое параметром **Pop3Recv[Lists]**, - каталог **CONF\lists\pop3recv**.

### *Список опрашиваемых почтовых ящиков*

Этот список задаёт параметры расположенных на внешних серверах почтовых ящиков, подлежащих опросу по протоколу POP3.

Расположение списка задаётся параметром **Pop3Recv[Boxes]**, исходное - **CONF\lists\pop3recv\Boxes.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **POP3SERVER** | Имя или IP-адрес POP-сервера. |
| 2 | **POP3PORT** | Номер порта на POP-сервере. |
| 3 | **POP3LOGIN** | Имя учётной записи почтового ящика. |
| 4 | **POP3PASSW** | Пароль учётной записи почтового ящика. |
| 5 | **DEFAULT_EMAIL** | Адрес получателя по умолчанию. Используется, если из заголовков письма не удаётся выделить ни один допустимый адрес получателя. |
| 6 | **DELETE_AFTER_RETR** | Определяет, удалять ли почту из ящика после загрузки. |
| 7 | **ALLOW_EMPTY_SENDER** | Если ни один из выделенных адресов отправителя не прошёл проверку, ненулевое значение этого параметра позволяет принять письмо, используя пустой обратный адрес. |
| 8 | **SAVE_REJECTED** | Если при проверке были отвергнуты все возможные адреса отправителя либо все выделенные адреса получателей, ненулевое значение этого параметра позволяет всё-таки сохранить письмо для последующего анализа - без выполнения доставки. |
| 9 | **DELETE_REJECTED** | Если письмо не принято ни в штатном режиме, ни для последующего анализа, оно рискует навечно остаться в почтовом ящике. Ненулевое значение этого параметра позволяет удалять отвергнутые письма. |
| 10 | **FILE_NAME** | Если отвергнутые письма сохраняются, то этот параметр задаёт путь и шаблон для формирования имени файла, в котором будет сохраняться письмо. Шаблон не обязательно задавать для каждого почтового ящика - если он опущен, будет использовано значение по умолчанию **Pop3Recv[FileName]**, заданное в конфигурационном файле PigMail2.ini. |
| 11 | **MAX_MESSAGE_SIZE** | Задаёт максимально допустимый размер письма, которое может быть доставлено получателю. Это значение действует для всех "чужих" отправителей (для "своих" ограничения устанавливаются динамически и более изощрённым способом). Размер письма задаётся в байтах. Для отключения контроля за размером писем достаточно задать нулевое значение. Если этот параметр опущен, используется значение по умолчанию **Pop3Recv[MaxMessageSize]**, заданное в конфигурационном файле PigMail2.ini. |
| 12 | **DELETE_OVERQUOTED** | Определяет, удалять ли из ящика письма, превышающие ограничения на размер, без их загрузки, - радикальный способ ограничения платного трафика, чреватый потерей информации. Если значение параметра нулевое, то письма загружаются независимо от их размера и далее сортируются по правилам, заданным для SMTP-сервера. |
| 13 | **POLL_SCHEDULE** | Дополнительное (по отношению ко всем прочим) условие проверки почтового ящика. Имеет такой же смысл, что и параметр **Pop3Recv[PollSchedule]** конфигурационного файла PigMail2.ini. Ящик проверяется тогда и только тогда, когда оба условия выполняются (если условие не задано, оно считается всегда истинным). |

| | | |
|---|---|---|
| 14 | **MAX_MSGNUM** | Ограничение на число писем, загружаемых из ящика за одну сессию. Если связь неважная и при большом количестве писем соединение часто срывается, а почтовый сервер строго придерживается стандарта и в случае обрыва связи не удаляет из ящика уже загруженные письма, выручит загрузка писем несколькими мелкими порциями. За одно подключение к ящику загружается не более заданного этим параметром количества писем. Если значение нулевое, то ограничения нет. |
| 15 | **PRIVATE** | Определяет личный ящик. Для таких ящиков не выполняется выборка адресатов из заголовков письма; в качестве адреса получателя используется значение поля **DEFAULT_EMAIL**. |
| 16 | **SECURITY** | Требуемый режим безопасности при приёме писем из данного ящика. Задаётся комбинацией следующих ключевых слов:<br>**SSL** - использовать полностью защищённое соединение;<br>**TLS** - использовать подключение в незащищённом режиме с последующим переключением в защищённый режим;<br>**NONE** - допускается использование незащищённого режима.<br>Если не задано ни одно ключевое слово, используется незащищённый режим. При наличии нескольких вариантов загрузчик пробует все указанные режимы, начиная с самого защищённого. |
| 17 | **SSL_CERT** | Имя файла формата PEM, содержащего закрытый ключ и сертификаты, используемые при организации защищённого (SSL) соединения с целевым сервером. Здесь допускается использование макросов (**{}**). Если поле пустое, используется сертификат по умолчанию, определённый в настройках загрузчика. |
| 18 | **SSL_VERIFY** | Определяет режим проверки подлинности сертификатов целевого сервера при установлении защищённого соединения. Задаётся либо числовым кодом, либо символьным обозначением:<br>**SSL_VERIFY:IGNORE** - сертификат целевого сервера проверяется, но соединение устанавливается независимо от результата проверки, при этом клиентский сертификат серверу не предъявляется (числовое значение -1);<br>**SSL_VERIFY:NONE** - сертификат целевого сервера проверяется, но соединение устанавливается независимо от результата проверки (числовое значение 0);<br>**SSL_VERIFY:STANDARD** - сертификат целевого сервера проверяется, при отрицательном результате проверки соединение незамедлительно разрывается (числовое значение 1).<br>Здесь допускается использование макросов (**{}**). Если поле пустое, используется режим по умолчанию, определённый в настройках загрузчика. |

### *Список обрабатываемых полей заголовка письма*

Этот список позволяет управлять обработкой заголовка принимаемого письма. Поскольку набор заголовочных полей, в которых могут оказаться адреса отправителя и получателей, вообще говоря, открыт для расширения, жёстко запрограммировать их обработку невозможно. Этот список позволяет связать имя поля с действием, которое следует предпринять для выделения адреса.

Расположение списка задаётся параметром **Pop3Recv[Headers]**, исходное - **CONF\lists\pop3recv\Headers.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **HEADER_NAME** | Имя заголовочного поля письма. |
| 2 | **ACTION** | Имя сопоставленного полю исполняемого правила. |

Исполняемые правила определены в плагине **pop3recv**. В текущей версии доступны следующие правила:

| | |
|---|---|
| **ParseEnvFrom** | Выделение и фиксация основного адреса отправителя. Это правило следует сопоставить полю, в которое почтовый сервер помещает параметр SMTP-команды **MAIL FROM**. В примере это поле **Envelope-From:**. |
| **ParseFrom** | Выделение и фиксация "запасного" адреса отправителя - как правило, из поля **From:**. |

| | |
|---|---|
| **ParseReplyTo** | Выделение и фиксация ещё одного "запасного" адреса отправителя - как правило, из поля **Reply-To:**. |
| **ParseRcpt** | Выделение и фиксация адреса получателя из простого адресного поля (**To:**, **Cc:**, **X-Deliver-To:** и т.д.). |
| **ParseRcptFor** | Выделение и фиксация адреса получателя из поля **Received:**. Это поле содержит большое количество различной информации, а адрес получателя, если присутствует, предваряется ключевым словом **for**. |

## *Управляющие списки расширенного сервиса доставки исходящей почты SmtpSend*

Эти списки предназначены для управления расширенным сервисом доставки исходящей почты SmtpSend, их исходное расположение, определяемое параметром **SmtpSend[Lists]**, - каталог **CONF\lists\smtpsend**.

### *Список подмены адресов отправителя*

Как правило, адрес отправителя однозначно определяется ещё до попадания письма в очередь доставки и даже до его приёма SMTP-сервером - этим ведают настройки сформировавшей письмо программы-клиента. В большинстве случаев этот адрес сохраняется в неизменности. Однако, если есть существенная необходимость (например, из-за некорректно написанной клиентской программы, выдающей на-гора недопустимый к использованию адрес), одного отправителя можно выдать за другого, выполнив подмену адреса на основании этого списка.

Расположение списка задаётся параметром **SmtpSend[FromEmailAliases]**, исходное - **CONF\lists\smtpsend\FromEmailAliases.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **EMAIL** | Шаблон исходного адреса отправителя, подлежащего замене. |
| 2 | **ALIAS** | Адрес отправителя, от имени которого будет отсылаться письмо. Здесь допускается использование макросов (**{}**). |
| 3 | **COMMENT** | Примечание. Это поле не используется сервером и предназначено для заметок администратора. |

### *Список управления режимами возврата недоставленных писем*

Различные почтовые системы могут иметь различные представления о правилах хорошего тона. Одни либерально относятся к множественным попыткам доставить письмо по несуществующему адресу, зато не озадачиваются согласованием списков пользователей основного и резервного серверов. Другие (как, например, Yahoo! или Google Mail) активно используют технологию грейлистинга (отправителю несколько раз предлагается "зайти в следующий раз", прежде чем сервер соизволит принять письмо к рассмотрению) и крайне болезненно реагируют на слишком настойчивых отправителей, не воспринимающих сообщение об отсутствии адресата. С помощью этого списка можно выбрать режим, наиболее соответствующий нравам почтового сервера получателя.

Расположение списка задаётся параметром **SmtpSend[RcptReturnMode]**, исходное - **CONF\lists\smtpsend\RcptReturnMode.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **EMAIL** | Шаблон адреса получателя письма. |

| | | |
|---|---|---|
| 2 | **MODE** | Назначаемый режим возврата. Режим задаётся двухсимвольным кодом и может быть одним из следующих:<br>**RO** (Reject Only) - возврат выполняется, если все испробованные почтовые серверы категорически отвергли адрес получателя, выдав ответ с кодом 5xx. Это наиболее агрессивный и, как ни странно, наиболее применимый режим;<br>**WR** (Was Rejected) - возврат выполняется, если из испробованных почтовых серверов хотя бы один категорически отверг адрес получателя, выдав ответ с кодом 5xx. Этот режим наилучшим образом подходит для почтовых систем типа Yahoo! или Google Mail, где списки пользователей на серверах согласованы, зато механизм грейлистинга постоянно ставит препоны в виде временных отказов с кодом 4xx;<br>**AE** (Any Error) - возврат выполняется, если доставка не удалась ни на один из испробованных почтовых серверов. При этом неважно, был отказ категорическим (с кодом 5xx), временным (4xx) или имели место технические проблемы, например, отсутствие связи с сервером. Этот режим предназначен для очень особых случаев. |

### *Список дополнительных транзитных серверов*

В этом списке перечислены по убыванию предпочтительности дополнительные транзитные SMTP-серверы, которые используются для доставки писем, если прямая доставка запрещена настройками или оказалась невозможной.

Расположение списка задаётся параметром **SmtpSend[AltRelayList]**, исходное - **CONF\lists\smtpsend\AltRelayList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **TARGET_HOST** | Имя или IP-адрес дополнительного сервера. |
| 2 | **SENDER_MASK** | Шаблон адреса отправителя с учётом, возможно, уже выполненной подмены, которому разрешено использовать данный сервер в качестве транзитного. Используется для серверов, ограничивающих перечень допустимых отправителей - таковыми обычно являются клиентские SMTP-серверы публичных почтовых систем Mail.ru, GMail.com и других. Если это поле пустое, то сервер разрешено использовать в сочетании с любым адресом отправителя. |
| 3 | **COMMENT** | Примечание. Это поле не используется сервером и предназначено для заметок администратора. |

### *Список параметров авторизации на почтовых серверах адресатов*

Прямая доставка, как правило, не требует авторизации - чужие списки пользователей, по идее, представляют тайну не хуже государственной. А вот транзитный сервер провайдера вполне может потребовать подтверждения прав на проталкивание через него исходящих писем. По этому списку на основании сочетания адреса отправителя и имени почтового сервера можно определить требуемые реквизиты авторизации.

Расположение списка задаётся параметром **SmtpSend[TargetAuthList]**, исходное - **CONF\lists\smtpsend\TargetAuthList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **TARGET_HOST** | Шаблон имени или IP-адреса сервера-адресата. Сервис при поиске не выполняет преобразование имени в IP-адрес и обратно, значение в этом поле должно быть записано так, как его возвращает DNS-сервер (если используется прямая доставка писем), или так, как оно задано в списке дополнительных серверов. |
| 2 | **FROM_EMAIL** | Шаблон адреса отправителя с учётом, возможно, уже выполненной подмены. |
| 3 | **LOGIN** | Имя учётной записи для данного отправителя на данном сервере-получателе. Если это поле пустое, то реквизиты авторизации не изменяются. |
| 4 | **PASSW** | Пароль учётной записи для данного отправителя на данном сервере-получателе. |
| 5 | **COMMENT** | Примечание. Это поле не используется сервером и предназначено для заметок администратора. |

### *Список выбора режима безопасности*

Обычно передача электронной почты выполняется открытым текстом, и это нормально, учитывая полное отсутствие тайны электронной переписки. Однако бывают ситуации, когда передачу необходимо защитить от прослушивания. По этому списку на основании адреса отправителя, адреса получателя и имени почтового сервера можно определить необходимый уровень безопасности при передаче письма, а также указать

особые параметры настройки защищённого соединения - клиентский сертификат и режим проверки подлинности сертификата сервера.

Расположение списка задаётся параметром **SmtpSend[TransferSecurityList]**, исходное - **CONF\lists\smtpsend\TransferSecurityList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **TARGET_HOST** | Шаблон имени или IP-адреса сервера-адресата. Сервис при поиске не выполняет преобразование имени в IP-адрес и обратно, значение в этом поле должно быть записано так, как его возвращает DNS-сервер (если используется прямая доставка писем), или так, как оно задано в списке дополнительных серверов. |
| 2 | **TO_EMAIL** | Шаблон адреса получателя письма. |
| 3 | **FROM_EMAIL** | Шаблон исходного (без учёта возможных подмен) адреса отправителя. |
| 4 | **SECURITY** | Требуемый режим безопасности при передаче писем на данный сервер. Задаётся комбинацией следующих ключевых слов:<br>**SSL** - использовать полностью защищённое соединение;<br>**TLS** - использовать подключение в незащищённом режиме с последующим переключением в защищённый режим;<br>**NONE** - допускается использование незащищённого режима.<br>Если не задано ни одно ключевое слово, используется незащищённый режим. В режиме групповой доставки доступные режимы определяются параметрами всех адресатов письма, обнаруженных в списке и имеющих явно заданные параметры безопасности. При наличии нескольких вариантов сервис пробует все указанные режимы, начиная с самого защищённого. |
| 5 | **SSL_CERT** | Имя файла формата PEM, содержащего закрытый ключ и сертификаты, используемые при организации защищённого (SSL) соединения с целевым сервером. В режиме групповой доставки, если в списке обнаруживается несколько адресатов письма, применяется достаточно случайным образом выбранный сертификат, явно сопоставленный одному из адресатов. Здесь допускается использование макросов (**{}**). Если поле пустое, используется сертификат по умолчанию, определённый в настройках сервиса. |
| 6 | **SSL_VERIFY** | Определяет режим проверки подлинности сертификатов целевого сервера при установлении защищённого соединения. Задаётся либо числовым кодом, либо символьным обозначением:<br>**SSL_VERIFY:IGNORE** - сертификат целевого сервера проверяется, но соединение устанавливается независимо от результата проверки, при этом клиентский сертификат серверу не предъявляется (числовое значение -1);<br>**SSL_VERIFY:NONE** - сертификат целевого сервера проверяется, но соединение устанавливается независимо от результата проверки (числовое значение 0);<br>**SSL_VERIFY:STANDARD** - сертификат целевого сервера проверяется, при отрицательном результате проверки соединение незамедлительно разрывается (числовое значение 1).<br>В режиме групповой доставки, если в списке обнаруживается несколько адресатов письма, применяется достаточно случайным образом выбранный режим, явно сопоставленный одному из адресатов. Здесь допускается использование макросов (**{}**). Если поле пустое, используется режим по умолчанию, определённый в настройках сервиса. |
| 7 | **COMMENT** | Примечание. Это поле не используется сервером и предназначено для заметок администратора. |

## *Список выбора имени узла*

Одним из обязательных шагов открытия сессии для отправки письма является взаимное представление отправителя и получателя. При этом отправитель сообщает своё сетевое имя. Каждый почтовый сервер имеет свои предпочтения относительно этого имени. Кто-то требует обязательного соответствия имени и IP-адреса, кто-то по IP-адресу отыскивает имя в обратной зоне DNS и сравнивает с переданным в команде, кого-то категорически не устраивает честное, но сконструированное на основе IP-адреса шаблонное имя вида host-www-xxx-yyy-zzz.pppoe.provider.com. К тому же сам сервер-отправитель может иметь несколько IP-адресов, которым сопоставлены разные имена. Этот список позволяет решить проблему выбора.

Расположение списка задаётся параметром **SmtpSend[HeloIP]**, исходное - **CONF\lists\smtpsend\HeloIP.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **IP** | Шаблон IP-адреса сетевого интерфейса, использующегося для подключения к серверу-получателю. |
| 2 | **TARGET_HOST** | Шаблон имени или IP-адреса сервера-адресата. Сервис при поиске не выполняет преобразование имени в IP-адрес и обратно, значение в этом поле должно быть записано так, как его возвращает DNS-сервер (если используется прямая доставка писем), или так, как оно задано в списке дополнительных серверов. |
| 3 | **HELO_NAME** | Имя узла, которое следует сообщить серверу-получателю. Здесь допускается использование макросов (**{}**). Если поле пустое, используется имя по умолчанию, определённое в настройках сервиса. |
| 4 | **SSL_CERT** | Имя файла формата PEM, содержащего закрытый ключ и сертификаты, используемые при организации защищённого (SSL) соединения с целевым сервером. Здесь допускается использование макросов (**{}**). Если поле пустое, используется сертификат, определённый другими настройками сервиса. |
| 5 | **SSL_VERIFY** | Определяет режим проверки подлинности сертификатов целевого сервера при установлении защищённого соединения. Задаётся либо числовым кодом, либо символьным обозначением:<br>**SSL_VERIFY:IGNORE** - сертификат целевого сервера проверяется, но соединение устанавливается независимо от результата проверки, при этом клиентский сертификат серверу не предъявляется (числовое значение -1);<br>**SSL_VERIFY:NONE** - сертификат целевого сервера проверяется, но соединение устанавливается независимо от результата проверки (числовое значение 0);<br>**SSL_VERIFY:STANDARD** - сертификат целевого сервера проверяется, при отрицательном результате проверки соединение незамедлительно разрывается (числовое значение 1).<br>Здесь допускается использование макросов (**{}**). Если поле пустое, используется режим, определённый другими настройками сервиса. |
| 6 | **COMMENT** | Примечание. Это поле не используется сервером и предназначено для заметок администратора. |

### *Список отправителей, которым не следует возвращать недоставленные письма*

Это список отправителей, которым не следует формировать и доставлять письма-возвраты и письма-предупреждения. Как правило, это специальные адреса - "вышибалы" и почтовые роботы. Они всё равно не в состоянии понять смысл послания и правильно на него отреагировать.

Расположение списка задаётся параметром **SmtpSend[NoAutoReplyTo]**, исходное - **CONF\lists\smtpsend\NoAutoReplyTo.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **EMAIL_MASK** | Шаблон адреса. |
| 2 | **COMMENT** | Примечание. Это поле не используется сервером и предназначено для заметок администратора. |

## *Общие управляющие списки спам-фильтров*

Эти списки предназначены для управления всеми спам-фильтрами, их исходное расположение, определяемое параметром **Antispam[Lists]**, - каталог **CONF\lists\antispam**.

### *Список доверенных сетей спам-фильтра*

Это ещё один список доверенных сетей - дополнительный по отношению к спискам локальных и доверенных сетей SMTP-сервера в целом. Доверие к этим IP-адресам не настолько велико, чтобы считать находящихся там отправителей "своими", но известно, что спам из этих сетей не приходит.

Расположение списка задаётся параметром **Antispam[IpWhiteList]**, исходное - **CONF\lists\antispam\IpWhiteList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **IP_MASK** | Шаблон IP-адреса, определяющий доверенную сеть. Здесь можно указать и конкретный IP-адрес. |

| | | |
|---|---|---|
| 2 | **COMMENT** | Примечание. Это поле не используется сервером и предназначено для заметок администратора. |

### *Список доверенных отправителей спам-фильтра*

Это ещё один список доверенных отправителей - дополнительный по отношению к списку доверенных отправителей SMTP-сервера в целом. Доверие к этим адресам не настолько велико, чтобы включить их в основной "белый" список, но известно, что спам с этих адресов не приходит.

Расположение списка задаётся параметром **Antispam[FromEmailWhiteList]**, исходное - **CONF\lists\antispam\FromEmailWhiteList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **EMAIL** | Шаблон доверенного адреса. |
| 2 | **COMMENT** | Примечание. Это поле не используется сервером и предназначено для заметок администратора. |

### *Список особых получателей спам-фильтра*

Это список "узкого круга" получателей, обладающих особыми функциями - это либо администраторы, либо ящики-ловушки, специально выставленные в качестве наживки. Если все получатели письма состоят в этом списке, то письмо не будет подвергаться спам-фильтрации, в противном случае решение об отмене проверки будет приниматься исходя из других условий.

Расположение списка задаётся параметром **Antispam[ToEmailWhiteList]**, исходное - **CONF\lists\antispam\ToEmailWhiteList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **EMAIL** | Шаблон адреса особого получателя. |
| 2 | **COMMENT** | Примечание. Это поле не используется сервером и предназначено для заметок администратора. |

## *Управляющие списки упрощённого фильтра содержания*

Действие этих списков распространяется только на упрощённый фильтр содержания. Их исходное расположение, определяемое параметром **SMTP[Filters]**, - каталог **CONF\lists\smtp\filters**.

### *Список спам-фильтров по заголовочным полям письма*

Это управляющий список упрощённого фильтра содержания, определяющий, по каким заголовочным полям следует выполнять фильтрацию, и какие списки шаблонов спамерского содержимого используются для фильтрации.

Расположение списка задаётся параметром **ContentFilter[FiltersList]**, исходное - **CONF\lists\smtp\filters\FiltersList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **HEADER_CODE** | Условное имя, под которым сохранено содержимое заголовочного поля. Оно должно соответствовать имени из списка запоминаемых заголовочных полей. Регистр букв значения не имеет, символы групповой операции недопустимы. |
| 2 | **FILTER_LIST** | Имя файла со списком шаблонов спамерского содержимого, сопоставленного проверяемому заголовочному полю. Допускается использование макроподстановок. |

### *Списки спам-фильтров содержания*

Это целое семейство списков, позволяющее выполнять поиск признаков спама в ряде полей заголовка, а также в теле письма.

В текущей версии PigMail+PigProxy перечень фильтруемых заголовочных полей определяется отдельным списком. В дистрибутив в качестве примера включены списки фильтрации по содержимому следующих полей:

| Поле | Условное имя поля | Файл списка |
|---|---|---|
| **Cc** | D-CC | CONF\lists\smtp\filters\BlackListCc.txt |
| **From** | D-FROM | CONF\lists\smtp\filters\BlackListFrom.txt |
| **Organization** | D-ORGANIZATION | CONF\lists\smtp\filters\BlackListOrganization.txt |
| **Reply-To** | D-REPLY-TO | CONF\lists\smtp\filters\BlackListReply-To.txt |
| **Subject** | D-SUBJECT | CONF\lists\smtp\filters\BlackListSubject.txt |

| | | |
|---|---|---|
| **To** | D-TO | CONF\lists\smtp\filters\BlackListTo.txt |
| **X-Comment** | D-X-COMMENT | CONF\lists\smtp\filters\BlackListX-Comment.txt |
| **X-Mailer** | D-X-MAILER | CONF\lists\smtp\filters\BlackListX-Mailer.txt |
| **X-Sender** | D-X-SENDER | CONF\lists\smtp\filters\BlackListX-Sender.txt |

Расположение списка фильтрации по телу письма задаётся параметром **ContentFilter[BlackListBody]**, исходное - **CONF\lists\smtp\filters\BlackListBody.txt**. Все списки имеют один формат. Назначение полей:

| | | |
|---|---|---|
| 1 | **MASK** | Шаблон спамерского содержимого. |
| 2 | **FILTER_ID** | Идентификатор фильтра, подставляемый в сообщение сервера об отказе в приёме письма. Впоследствии по этому идентификатору можно определить строку списка, из-за которой было ошибочно отклонено благонамеренное письмо. |

## *Управляющие списки POP-сервера*

Эти списки предназначены для управления POP-сервером, их исходное расположение, определяемое параметром **POP[Lists]**, - каталог **CONF\lists\pop**.

### *Список прав пользователей*

Этот список используется для назначения прав пользователей по данным их авторизации на POP-сервере, то есть, на основании имени учётной записи и домена авторизации. Поскольку с POP-сервером имеют дело исключительно получатели, то и права задаются в отношении получения почты. Назначение прав по этому списку производится один раз за время почтовой сессии.

Расположение списка задаётся параметром **POP[ACL]**, исходное - **CONF\lists\pop\ACL.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **USER** | Пользователь, к которому относится эта строка. Если поле пустое, то его проверка не производится. Если поле содержит символ звёздочки *****, то строка считается относящейся к любому авторизованному пользователю. Любое другое содержимое рассматривается как шаблон сравнения, могущий содержать символы групповой операции ***** и **?**. POP-сервер ожидает задания полного имени пользователя в формате **логин@домен**; если же домен не задан, считается, что искомый пользователь авторизуется в домене по умолчанию. |
| 2 | **GROUP** | Имя группы пользователей, к которой относится эта строка. В зависимости от наличия поддержки расширенной группировки оно может быть задано по-разному. Если расширенная группировка не применяется, то считается, что группа относится к тому же домену авторизации, что и входящий в неё пользователь. В противном случае POP-сервер ожидает задания полного имени группы в формате **группа@домен**; если же домен не указан, считается, что проверяемая группа принадлежит домену по умолчанию. Если поле пустое, членство пользователя в группе не проверяется. |
| 3 | **FLAGS** | Строка флагов разрешений и признаков для пользователя:<br>**E** (Enable) - при наличии этого флага пользователю разрешено подключение к почтовому ящику и получение писем. |

Список всегда просматривается с начала до конца. Если по какой-либо строке зафиксировано совпадение имени пользователя или членства в группе, выполняется назначение заданных в строке прав, причём права-флаги суммируются с ранее установленными.

### *Список особых пользователей*

В этом списке перечислены особые пользователи, которым в качестве почтовых ящиков открываются особые каталоги. Это могут быть каталоги, в которые помещается спам, карантинные каталоги; администратору можно предоставить доступ ко всей иерархии почтовых каталогов. Поскольку могут использоваться разные домены авторизации, пользователи в этом списке перечисляются с указанием домена - в стандартном для PigMail+PigProxy виде **логин@домен**.

Расположение списка задаётся параметром **POP[SpecialFolders]**; изначально он наследует значение аналогичного параметра IMAP-сервера (таким образом, оба сервера используют один общий список), но в каталоге управляющих списков POP-сервера также присутствует файл-заготовка **CONF\lists\pop\SpecialFolders.txt** на случай, когда списки потребуется разделить. Назначение полей:

| | | |
|---|---|---|
| 1 | **EMAIL** | Это не почтовый адрес, а имя учётной записи (логин) и домен авторизации пользователя (в формате **логин@домен**), для которых назначается специальный каталог почтового ящика. |
| 2 | **FOLDER** | Путь к специальному каталогу. |

### *Список доверенных сетей*

Это так называемый "белый" список доверенных IP-адресов или сетей, которые обслуживаются этим POP-сервером. Этот список ДОПОЛНЯЕТ список локальных сетей. В нём могут быть не локальные сети, а, например, особые внешние IP-адреса, не входящие логически в локальную сеть предприятия.

Расположение списка задаётся параметром **POP[IpWhiteList]**, исходное - **CONF\lists\pop\IpWhiteList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **IP_MASK** | Шаблон IP-адреса, определяющий доверенную сеть. Здесь можно указать и конкретный IP-адрес. |
| 2 | **REPLY_TEXT** | Текст индивидуального приветствия, подставляемый в ответы серверов при подключении пользователей из этой доверенной сети. |
| 3 | **USER** | Для POP-сервера этот параметр не имеет смысла и оставлен для сохранения единого формата списков. |
| 4 | **MAX_MSG_SIZE** | Для POP-сервера этот параметр не имеет смысла и оставлен для сохранения единого формата списков. |
| 5 | **FLAGS** | Строка флагов-признаков для сети. Для POP-сервера этот параметр не имеет смысла и оставлен для сохранения единого формата списков. |

### *Список запрещённых сетей*

Это список IP-адресов и подсетей, которым запрещено обращаться к POP-серверу.

Расположение списка задаётся параметром **POP[IpBlackList]**, исходное - **CONF\lists\pop\IpBlackList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **IP_MASK** | Шаблон IP-адреса, определяющий запрещённую сеть. |
| 2 | **REPLY_TEXT** | Индивидуальный текст ответа сервера, поясняющий причину отказа. |
| 3 | **FLAGS** | Строка флагов-признаков для сети. Для POP-сервера этот параметр не имеет смысла и оставлен для сохранения единого формата списков. |

## *Управляющие списки IMAP-сервера*

Эти списки предназначены для управления IMAP-сервером, их исходное расположение, определяемое параметром **IMAP[Lists]**, - каталог **CONF\lists\imap**.

### *Список прав пользователей*

Этот список используется для назначения прав пользователей по данным их авторизации на IMAP-сервере, то есть, на основании имени учётной записи и домена авторизации. Поскольку с IMAP-сервером имеют дело исключительно получатели, то и права задаются в отношении получения почты и управления содержимым почтового ящика. Назначение прав по этому списку производится один раз за время почтовой сессии.

Расположение списка задаётся параметром **IMAP[ACL]**, исходное - **CONF\lists\imap\ACL.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **USER** | Пользователь, к которому относится эта строка. Если поле пустое, то его проверка не производится. Если поле содержит символ звёздочки *****, то строка считается относящейся к любому авторизованному пользователю. Любое другое содержимое рассматривается как шаблон сравнения, могущий содержать символы групповой операции ***** и **?**. IMAP-сервер ожидает задания полного имени пользователя в формате **логин@домен**; если же домен не задан, считается, что искомый пользователь авторизуется в домене по умолчанию. |

| | | |
|---|---|---|
| 2 | **GROUP** | Имя группы пользователей, к которой относится эта строка. В зависимости от наличия поддержки расширенной группировки оно может быть задано по-разному. Если расширенная группировка не применяется, то считается, что группа относится к тому же домену авторизации, что и входящий в неё пользователь. В противном случае IMAP-сервер ожидает задания полного имени группы в формате **группа@домен**; если же домен не указан, считается, что проверяемая группа принадлежит домену по умолчанию. Если поле пустое, членство пользователя в группе не проверяется. |
| 3 | **FLAGS** | Строка флагов разрешений и признаков для пользователя:<br>**E** (Enable) - при наличии этого флага пользователю разрешено подключение к почтовому ящику и получение писем;<br>**S** (Spamclassifier) - при наличии этого флага пользователю разрешено выполнять переклассификацию писем в спам-фильтрах POPfile, SpamProtexx и LibSD;<br>**R** (Resend) - при наличии этого флага пользователю разрешено выполнять переposылку писем. |

Список всегда просматривается с начала до конца. Если по какой-либо строке зафиксировано совпадение имени пользователя или членства в группе, выполняется назначение заданных в строке прав, причём права-флаги суммируются с ранее установленными.

### *Список особых пользователей*

В этом списке перечислены особые пользователи, которым в качестве почтовых ящиков открываются особые каталоги. Это могут быть каталоги, в которые помещается спам, карантинные каталоги; администратору можно предоставить доступ ко всей иерархии почтовых каталогов. Поскольку могут использоваться разные домены авторизации, пользователи в этом списке перечисляются с указанием домена - в стандартном для PigMail+PigProxy виде **логин@домен**.

Расположение списка задаётся параметром **IMAP[SpecialFolders]**, исходное - **CONF\lists\imap\SpecialFolders.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **EMAIL** | Это не почтовый адрес, а имя учётной записи (логин) и домен авторизации пользователя (в формате **логин@домен**), для которых назначается специальный каталог почтового ящика. |
| 2 | **FOLDER** | Путь к специальному каталогу. |

### *Список доверенных сетей*

Это так называемый "белый" список доверенных IP-адресов или сетей, которые обслуживаются этим IMAP-сервером. Этот список ДОПОЛНЯЕТ список локальных сетей. В нём могут быть не локальные сети, а, например, особые внешние IP-адреса, не входящие логически в локальную сеть предприятия.

Расположение списка задаётся параметром **IMAP[IpWhiteList]**, исходное - **CONF\lists\imap\IpWhiteList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **IP_MASK** | Шаблон IP-адреса, определяющий доверенную сеть. Здесь можно указать и конкретный IP-адрес. |
| 2 | **REPLY_TEXT** | Текст индивидуального приветствия, подставляемый в ответы серверов при подключении пользователей из этой доверенной сети. |
| 3 | **USER** | Для IMAP-сервера этот параметр не имеет смысла и оставлен для сохранения единого формата списков. |
| 4 | **MAX_MSG_SIZE** | Для IMAP-сервера этот параметр не имеет смысла и оставлен для сохранения единого формата списков. |
| 5 | **FLAGS** | Строка флагов-признаков для сети. Для IMAP-сервера этот параметр не имеет смысла и оставлен для сохранения единого формата списков. |

### *Список запрещённых сетей*

Это список IP-адресов и подсетей, которым запрещено обращаться к IMAP-серверу.

Расположение списка задаётся параметром **IMAP[IpBlackList]**, исходное - **CONF\lists\imap\IpBlackList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **IP_MASK** | Шаблон IP-адреса, определяющий запрещённую сеть. |

| | | |
|---|---|---|
| 2 | **REPLY_TEXT** | Индивидуальный текст ответа сервера, поясняющий причину отказа. |
| 3 | **FLAGS** | Строка флагов-признаков для сети. Для IMAP-сервера этот параметр не имеет смысла и оставлен для сохранения единого формата списков. |

### *Список действий, назначенных папкам IMAP*

Этот список позволяет назначить для пары папок IMAP различные действия, который будут выполняться над каждым письмом, перемещаемым из одной папки в другую. Это может быть переклассификация писем посредством POPfile, SpamProtexx или LibSD, повторная отправка письма адресатам (если с письмом разбирается спам-администратор). Применение механизма шаблонов позволяет задавать как конкретные папки, так и группы папок. Действия определяются сопоставляемыми с папками файлами правил.

Расположение списка задаётся параметром **IMAP[ImapFolderActions]**, исходное - **CONF\lists\imap\ImapFolderActions.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **TO_FOLDER** | Шаблон имени папки IMAP, в которую выполняется перемещение. |
| 2 | **FROM_FOLDER** | Шаблон имени папки IMAP, из которой выполняется перемещение. |
| 3 | **ACTION** | Имя правила, выполняющего назначенные для папки действия. |
| 4 | **TARGET_BUCKET** | Задаёт целевую категорию ("ведро", bucket) письма для операций переклассификации. |
| 5 | **ON_RECLASSIFY** | Это флаговое поле действует на совмещённые операции переклассификации и последующей перепосылки письма. Если задано любое ненулевое значение, то перепосылка производится только по действительному факту переклассификации, в противном случае - независимо от исхода первого этапа. |

В текущей версии реализованы следующие правила-действия (все они расположены в каталоге **imap**):

| | |
|---|---|
| **ReclassifyMessage** | Выполняет переклассификацию письма в категорию, заданную параметром **TARGET_BUCKET**. Если такой категории в настройках фильтра нет или письмо уже принадлежит этой категории, переклассификация не производится. Переклассификация выполняется отдельно для POPfile, SpamProtexx и LibSD, факт выполнения переклассификации запоминается для последующего анализа. Это действие доступно при наличии у пользователя права на переклассификацию писем. |
| **ReclassifyToClear** | Это правило, унаследованное от предыдущих версий, выполняет переклассификацию письма в категорию **clear** независимо от значения параметра **TARGET_BUCKET**. Если такой категории в настройках фильтра нет или письмо уже принадлежит этой категории, переклассификация не производится. Переклассификация выполняется отдельно для POPfile, SpamProtexx и LibSD, факт выполнения переклассификации запоминается для последующего анализа. Это действие доступно при наличии у пользователя права на переклассификацию писем. |
| **ReclassifyToSpam** | Это правило, унаследованное от предыдущих версий, выполняет переклассификацию письма в категорию **spam** независимо от значения параметра **TARGET_BUCKET**. Если такой категории в настройках фильтра нет или письмо уже принадлежит этой категории, переклассификация не производится. Переклассификация выполняется отдельно для POPfile, SpamProtexx и LibSD, факт выполнения переклассификации запоминается для последующего анализа. Это действие доступно при наличии у пользователя права на переклассификацию писем. |
| **ResendMessage** | Выполняет безусловную перепосылку письма путём перемещения в специальный каталог перепосылки, заданный параметром **Antispam[ResendDir]**. В папке назначения письмо не сохраняется. Это действие доступно при наличии у пользователя права на перепосылку писем. |

| | |
|---|---|
| **ReclassifyAndResend** | Выполняет переклассификацию письма в категорию, заданную параметром **TARGET_BUCKET**. Если такой категории в настройках фильтра нет или письмо уже принадлежит этой категории, переклассификация не производится. Переклассификация выполняется отдельно для POPfile, SpamProtexx и LibSD, факт выполнения переклассификации запоминается для последующего анализа. Если переклассификация состоялась либо параметр **ON_RECLASSIFY** имеет нулевое значение, выполняется перепосылка письма. Перепосылка выполняется путём перемещения в специальный каталог перепосылки, заданный параметром **Antispam[ResendDir]**, в этом случае в папке назначения письмо не сохраняется. Это действие доступно при одновременном наличии у пользователя прав на переклассификацию и перепосылку писем. |
| **ReclassifyToClearAndResend** | Это правило, унаследованное от предыдущих версий, выполняет переклассификацию письма в категорию **clear** независимо от значения параметра **TARGET_BUCKET**. Если такой категории в настройках фильтра нет или письмо уже принадлежит этой категории, переклассификация не производится. Переклассификация выполняется отдельно для POPfile, SpamProtexx и LibSD. Независимо от исхода переклассификации выполняется перепосылка письма. Перепосылка выполняется путём перемещения в специальный каталог перепосылки, заданный параметром **Antispam[ResendDir]**, в этом случае в папке назначения письмо не сохраняется. Это действие доступно при одновременном наличии у пользователя прав на переклассификацию и перепосылку писем. |

## *Управляющие списки прокси-сервера в целом*

Как следует из названия, эти списки определяют поведение всех служб прокси-сервера. Их исходное расположение, определяемое параметром **PROXY[Lists]**, - каталог **CONF\lists\proxy**.

### *Список разрешённых сетевых интерфейсов*

Плохо закрытый от внешних глаз прокси-сервер способен доставить своему владельцу немало проблем в виде лишнего (обычно платного) трафика и попадания в различные чёрные списки. Простейший и первейший (но далеко не единственный) способ защиты - разграничение доступа по сетевым интерфейсам. В простейшем случае, когда одна сетевая карта "смотрит" в локальную сеть, а другая - в большой мир, можно обойтись указанием адреса сетевой карты из локальной сети. В тяжёлых случаях приходится прослушивать все интерфейсы, в том числе и те, подключения с которых приёму не подлежат. Список разрешённых сетевых интерфейсов предназначен как раз для отделения овец от козлищ.

К сожалению, при работе с UDP-пакетами определить сетевой интерфейс, принявший пакет, возможно только если порт явно привязан к интерфейсу. Поэтому в проверке по списку разрешённых сетевых интерфейсов нет смысла - если привязка выполнена явно, то подключение уже разрешено, а если порт открыт на всех доступных интерфейсах, то данные для проверки отсутствуют. Во избежание случайного превращения в открытый прокси отображаемые порты UDP рекомендуется явно связывать с сетевыми интерфейсами.

В соответствии с начальными настройками, заданными параметрами **HttpProxy[MylpList]**, **FtpProxy[MylpList]**, **SocksProxy[MylpList]**, **Pop3Proxy[MylpList]** и **TCPMAP[MylpList]** (исходно они наследуют значение параметра **PROXY[MylpList]**) в файле настроек **PigMail2.ini**, используется один общий список **CONF\lists\proxy\MylpList.txt**. В подкаталогах управляющих списков соответствующих служб прокси-сервера также имеются заготовки для определения индивидуальных списков, но исходными настройками их использование не предусмотрено. Все списки имеют одинаковый формат. Назначение полей:

| | | |
|---|---|---|
| 1 | **INTERFACE** | IP-адрес слушаемого сетевого интерфейса. |
| 2 | **ALLOW** | Если это поле имеет любое ненулевое значение, подключения на этот интерфейс принимаются. Если значение нулевое, подключения отвергаются - таким образом, любой ранее разрешённый интерфейс может быть временно заблокирован без удаления его из списка. |

### *Список доверенных сетей*

Это так называемый "белый" список доверенных IP-адресов или сетей, которые обслуживаются этим прокси-сервером. Этот список ДОПОЛНЯЕТ список локальных сетей. В нём могут быть не локальные сети, а, например, особые внешние IP-адреса, не входящие логически в локальную сеть предприятия.

Если разрешено настройками сервера, на основании этой пары списков выполняется так называемая IP-авторизация: подключившийся клиент считается авторизовавшимся, и ему назначается имя, сопоставленное в списке IP-адресу подключения.

В соответствии с начальными настройками, заданными параметрами **HttpProxy[IpWhiteList]**, **FtpProxy[IpWhiteList]** и **SocksProxy[IpWhiteList]** (исходно они наследуют значение параметра **PROXY[IpWhiteList]**) в файле настроек **PigMail2.ini**, основные службы прокси-сервера используют один общий список **CONF\lists\proxy\IpWhiteList.txt**. В подкаталогах управляющих списков соответствующих служб прокси-сервера также имеются заготовки для определения индивидуальных списков, но исходными настройками их использование не предусмотрено. Для POP3-прокси и отображений портов TCP и UDP списки доверенных сетей определяются особым образом, поэтому описаны отдельно. Все списки имеют одинаковый формат. Назначение полей:

| | | |
|---|---|---|
| 1 | **IP_MASK** | Шаблон IP-адреса, определяющий доверенную сеть. Здесь можно указать и конкретный IP-адрес, если список используется в том числе и для автоматической авторизации пользователей. |
| 2 | **REPLY_TEXT** | Текст индивидуального приветствия, подставляемый в ответы серверов при подключении пользователей из этой доверенной сети. HTTP-прокси и Socks-прокси не используют этот параметр. |
| 3 | **USER** | Имя учётной записи (логин) и домен авторизации пользователя (в виде **логин@домен**), используемые при IP-авторизации, если таковая разрешена. Следует учесть, что IP-авторизация (как и авторизация вообще) поддерживается только HTTP-, FTP- и Socks-прокси. Если задано только имя учётной записи, считается, что авторизация выполняется в домене по умолчанию. Если это поле не заполнено, IP-авторизация по этой строке списка не выполняется. |
| 4 | **MAX_MSG_SIZE** | Для прокси-сервера этот параметр не имеет смысла и оставлен для сохранения единого формата списков. |
| 5 | **FLAGS** | Строка флагов-признаков для сети. Для прокси-сервера этот параметр не имеет смысла и оставлен для сохранения единого формата списков. |

### *Список запрещённых сетей*

Это список IP-адресов и подсетей, которым запрещено обращаться к прокси-серверу.

В соответствии с начальными настройками, заданными параметрами **HttpProxy[IpBlackList]**, **FtpProxy[IpBlackList]** и **SocksProxy[IpBlackList]** (исходно они наследуют значение параметра **PROXY[IpBlackList]**) в файле настроек **PigMail2.ini**, основные службы прокси-сервера используют один общий список **CONF\lists\imap\IpBlackList.txt**. В подкаталогах управляющих списков соответствующих служб прокси-сервера также имеются заготовки для определения индивидуальных списков, но исходными настройками их использование не предусмотрено. Для POP3-прокси и отображений портов TCP и UDP списки запрещённых сетей определяются особым образом, поэтому описаны отдельно. Все списки имеют одинаковый формат. Назначение полей:

| | | |
|---|---|---|
| 1 | **IP_MASK** | Шаблон IP-адреса, определяющий запрещённую сеть. |
| 2 | **REPLY_TEXT** | Индивидуальный текст ответа сервера, поясняющий причину отказа. HTTP-прокси и Socks-прокси не используют этот параметр. |
| 3 | **FLAGS** | Строка флагов-признаков для сети. Для прокси-сервера этот параметр не имеет смысла и оставлен для сохранения единого формата списков. |

## *Управляющие списки ограничителя трафика TrafC*

Действие этих списков также распространяется на ряд служб прокси-сервера. Они определяют общие настройки подсистемы ограничения трафика TrafC. Их исходное расположение, определяемое параметром **PROXY[TrafCLists]**, - каталог **CONF\lists\proxy\trafc**.

### *Список Band-каналов ограничителя трафика TrafC*

Так называемые Band-каналы, задающие различные полосы пропускания, представляют собой элементы конструктора, из которых строится результирующая полоса, предоставляемая для выполнения запроса. Каждому каналу присваивается уникальное имя, используемое в дальнейшем для ссылки на канал. Каналы могут быть входящими и исходящими.

Расположение списка задаётся параметром **PROXY[TrafCBandsList]**, исходное - **CONF\lists\proxy\trafc\BandsList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **NAME** | Уникальное имя канала. При выборе имени рекомендуется использовать только буквы латинского алфавита, цифры, символы точки и подчёркивания. Прочие символы - особенно двоеточие и нелатинские буквы - могут привести к некорректной работе ограничителя трафика. |
| 2 | **CPS** | Полоса пропускания канала, определяемая в байтах в секунду. |
| 3 | **DIRECTION** | Направление канала:<br>**IN** - входящий канал;<br>**OUT** - исходящий канал. |
| 4 | **ISCLASS** | Ненулевое значение этого флага означает, что строка описывает не конкретный канал, а целый класс каналов - сами каналы будут формироваться по мере обнаружения в списке правил ссылок на них. Ссылки имеют вид **класс::имя**. Если при обнаружении такой ссылки канал с указанным именем ещё не определён, в списке ищется определение класса канала, и канал определяется на лету. |

### *Список Quota-каналов ограничителя трафика TrafC*

Так называемые Quota-каналы, задающие различные элементарные квоты трафика, представляют собой элементы конструктора, из которых строится результирующая квота, предоставляемая для выполнения запроса. Каждому каналу присваивается уникальное имя, используемое в дальнейшем для ссылки на канал. Каналы могут быть входящими и исходящими.

Расположение списка задаётся параметром **PROXY[TrafCQuotasList]**, исходное - **CONF\lists\proxy\trafc\QuotasList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **NAME** | Уникальное имя канала. При выборе имени рекомендуется использовать только буквы латинского алфавита, цифры, символы точки и подчёркивания. Прочие символы - особенно двоеточие и нелатинские буквы - могут привести к некорректной работе ограничителя трафика. |
| 2 | **VOLUME** | Объём квоты, выделяемой при использовании канала. Обязательно указание не только самого объёма, но и единиц, в которых он измеряется, например: **10 Mb**. |
| 3 | **PERIOD** | Длительность периода, на который выделяется квота. По истечении этого периода квота будет выделена заново (неиспользованный остаток при этом не переносится на следующий период). Обязательно указание не только собственно длительности, но и единиц, в которых она измеряется, например: **1 Hours**. |
| 4 | **DIRECTION** | Направление канала:<br>**IN** - входящий канал;<br>**OUT** - исходящий канал. |
| 5 | **ISCLASS** | Ненулевое значение этого флага означает, что строка описывает не конкретный канал, а целый класс каналов - сами каналы будут формироваться по мере обнаружения в списке правил ссылок на них. Ссылки имеют вид **класс::имя**. Если при обнаружении такой ссылки канал с указанным именем ещё не определён, в списке ищется определение класса канала, и канал определяется на лету. |

### *Список именованных наборов каналов ограничителя трафика TrafC*

Этот вспомогательный список позволяет упростить выделение каналов в зависимости от различных условий. Часто используемые наборы каналов можно сохранить в этом списке под условными именами и в дальнейшем обращаться к ним по этим условным именам.

Расположение списка задаётся параметром **PROXY[TrafCCanalsKitList]**, исходное - **CONF\lists\proxy\trafc\CanalsKitList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **NAME** | Уникальное имя набора каналов. В отличие от имён каналов здесь можно использовать любые символы. |
| 2 | **CANALS** | Перечень каналов, входящих в набор. Имена каналов разделяются пробелом. Здесь допускается использование макроподстановок (**{}**). |

| | | |
|---|---|---|
| 3 | **PRIORITY** | Приоритет, задаваемый при назначении данного набора каналов. Приоритет задаётся числом, чем оно меньше, тем выше приоритет; наивысшему приоритету соответствует нулевое значение. Возможные значения:<br>**пусто** - используется значение приоритета, вычисленное к моменту назначения при анализе списка правил;<br>**+nnn** - приоритет, вычисленный при анализе списка правил, понижается на nnn пунктов;<br>**-nnn** - приоритет, вычисленный при анализе списка правил, повышается на nnn пунктов;<br>**nnn** - приоритет устанавливается ровно на nnn пунктов. |

Перечень каналов может содержать ссылки трёх видов.

Во-первых, это могут быть имена каналов, статически определённых посредством вышеописанных списков.

Во-вторых, это могут быть ссылки на классы каналов. Классы каналов применимы, например, в случаях, когда пользователей достаточно много, и каждому из них надо выделить индивидуальную квоту стандартного значения. Класс канала позволяет избавиться от определения индивидуальных каналов - они будут создаваться автоматически по первому требованию. Ссылка на класс канала имеет вид **класс::имя**, при этом в одном из списков должен быть определён соответствующий класс каналов. Чтобы каналы были действительно индивидуальными, их имена необходимо генерировать с помощью макросов, возвращающих имя учётной записи, желательно, во избежание неоднозначности, в полном виде **логин@домен**. Пусть, например, в системе имеется описание класса Quota-каналов **Q10W** (пусть это означает 10 мегабайт в неделю), а при обработке запроса встречается назначение канала вида **Q10W::{LUserEmail}_Q10W**. Это означает, что на основе данного шаблона каждому авторизованному пользователю будет назначен индивидуальный канал с именем, основанном на полном имени учётной записи пользователя (что определяется макросом **{LUserEmail})**. Поскольку имена каналов регистрозависимы, а имена учётных записей и доменов - нет, выбран макрос, автоматически приводящий имя учётной записи к нижнему регистру. В принципе, можно приводить и к верхнему; собственно регистр значения не имеет, важно единообразие.

В-третьих, можно рекурсивно сослаться на другой именованный набор каналов. Такие ссылки имеют вид **::имя_набора**. Впрочем, хотя возможность и существует, но злоупотреблять ею не рекомендуется.

### *Список пользовательских наборов каналов*

Этот список предназначен для управления просмотром с помощью web-интерфейса пользовательской статистики по каналам и определяет, статистику по каким каналам может просматривать каждый пользователь. Список может заполняться как вручную, так и автоматически - это определяется параметром **PROXY[UseCanalsCollect]**.

Расположение списка задаётся параметром **PROXY[TrafCUserCanalsList]**, исходное - **CONF\lists\proxy\trafc\UserCanalsList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **USERNAME** | Имя учётной записи пользователя в формате **логин@домен**. |
| 2 | **CANALSLIST** | Перечень каналов, доступных пользователю. Имена каналов разделяются пробелом. В отличие от других списков, здесь можно указывать только реально определённые имена каналов - ссылки на классы и именованные наборы каналов неприменимы. |

## *Управляющие списки HTTP-прокси*

Эти списки предназначены для управления HTTP-прокси, их исходное расположение, определяемое параметром **HttpProxy[Lists]**, - каталог **CONF\lists\proxy\httpp**.

### *Список управления доступом к HTTP-прокси*

Пожалуй, это один из самых сложных среди всех управляющих списков прокси-сервера - как и сама система управления доступом, которая поневоле должна иметь множество настроечных параметров, чтобы предусмотреть самые различные ситуации. По сути список представляет собой программу на сильно упрощённом языке, которую прокси-сервер интерпретирует при обработке каждого пользовательского запроса. В зависимости от результатов выполнения этой программы определяется реакция сервера на запрос - будет ли это разрешение или жёсткий отказ, или запрос на идентификацию пользователя, или выдача клиенту вместо запрошенных данных некоего стандартного содержимого.

Этот же список используется для установления режима ограничения трафика, если используется ограничитель **TrafC**.

Расположение списка задаётся параметром **HttpProxy[ACL]**, исходное - **CONF\lists\proxy\httpp\ACL.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **PROTO** | Протокол, к которому относится строка списка. HTTP-прокси использует протоколы **http:**, **ftp:** и **connect:** - последний скорее не протокол, а универсальный метод соединения клиента с внешним сервером с организацией туннеля, применяемый при работе с защищённым соединением (SSL) и в ряде других случаев. Можно указать несколько протоколов, перечислив их через пробел. Если это поле пустое или содержит символ звёздочки *****, это означает любой используемый протокол. |
| 2 | **HOST** | Шаблон имени (в качестве которого может выступать и IP-адрес) внешнего сервера. В шаблоне допускается использование символов групповой операции ***** и **?**. Если поле пустое, то допустимым считается любое имя. На этом этапе прокси-сервер не пытается определять адрес по имени и наоборот, сравнение шаблона производится с фрагментом переданной клиентом ссылки. |
| 3 | **PORT** | Порт внешнего сервера, к которому происходит обращение. Если поле пустое либо содержит символ звёздочки ***** или нули, допустимым считается любой номер порта. Если переданная ссылка не содержит явного указания порта, прокси-сервер использует стандартные номера портов для каждого протокола: 80 для **http:**, 21 для **ftp:** и 443 для **connect:**. |
| 4 | **URI** | Остаток ссылки, определяющий конкретный объект или ресурс на внешнем сервере. Это шаблон, в котором допускается использование символов групповой операции ***** и **?**. Если поле пустое, то данная строка относится к серверу в целом. |
| 5 | **USER** | Пользователь, к которому относится эта строка. Если поле пустое, то его проверка не производится. Если поле содержит символ звёздочки *****, то строка считается относящейся к любому авторизованному пользователю. Если поле содержит символ минуса **-**, то строка относится только к неавторизованным сессиям. Любое другое содержимое рассматривается как шаблон сравнения, могущий содержать символы групповой операции ***** и **?**. Прокси-сервер ожидает задания полного имени пользователя в формате **логин@домен**; если же домен не задан, считается, что искомый пользователь авторизуется в домене по умолчанию. |
| 6 | **GROUP** | Имя группы пользователей, к которой относится эта строка. В зависимости от наличия поддержки расширенной группировки оно может быть задано по-разному. Если расширенная группировка не применяется, то считается, что группа относится к тому же домену авторизации, что и входящий в неё пользователь. В противном случае прокси-сервер ожидает задания полного имени группы в формате **группа@домен**; если же домен не указан, считается, что проверяемая группа принадлежит домену по умолчанию. Если поле пустое, членство пользователя в группе не проверяется. Если сессия неавторизованная, она не относится ни к одной группе пользователей. |
| 7 | **TIME** | Момент или интервал времени, определяемый с точностью до минуты, к которому относится эта строка. Момент задаётся в виде **чч:мм**, интервал - в виде **чч:мм-чч:мм**. Если поле пустое, то проверка условия не производится. |
| 8 | **RULE** | Дополнительное условие, записанное на языке Форт. Это условие должно вернуть на стеке единственное значение, которое будет интерпретироваться как логическое - ноль означает, что совпадение условий по этой строке не выявлено (ложь), любое другое значение - совпадение всех условий (истина). Перечень базовых правил, которые можно использовать при написании составного правила, приведён в приложении 2. Если поле пустое, считается, что правило вернуло истину. |

| | | |
|---|---|---|
| 9 | **ACTION** | Двухсимвольный код действия, которое следует предпринять, если все проверяемые поля строки успешно прошли проверку:<br>**AU** (Authorization) - задать режим запроса авторизации. Этот код унаследован из стандартной конфигурации;<br>**NF** (Not Found) - задать режим безусловной блокировки доступа. Этот код унаследован из стандартной конфигурации;<br>**DI** (Disable) - задать режим безусловной блокировки доступа;<br>**BA** (Block Advertisement) - задать режим блокировки рекламы;<br>**AD** (Advertisement Disabled) - задать режим блокировки рекламы. Этот код унаследован из стандартной конфигурации;<br>**пусто** - задать режим блокировки рекламы. Этот код унаследован из стандартной конфигурации;<br>**EN** (Enable) - задать режим разрешения доступа и, если возможно, определить используемые для выполнения запроса каналы управления трафиком;<br>**LI** (List) - выполнить обработку вложенного списка;<br>**RU** (Rule) - выполнить правило. |
| 10 | **TERMINATE** | Если это поле имеет любое ненулевое значение, то при совпадении всех условий (и выполнении заданного действия) анализ списка прерывается. Это флаг глобального действия, прерывающий обработку всей иерархии списков независимо от уровней вложенности. Если значение поля нулевое, обработка продолжается дальше - это позволяет выполнить предварительную установку действия, которая может быть изменена при дальнейшей обработке. |
| 11 | **PRIORITY** | Приоритет, задаваемый при назначении канала или набора каналов в случае разрешения доступа при выборе действия **EN**. Приоритет задаётся числом, чем оно меньше, тем выше приоритет; наивысшему приоритету соответствует нулевое значение. Возможные значения:<br>**пусто** - используется значение приоритета, вычисленное к моменту назначения при анализе предыдущих строк списка правил;<br>**+nnn** - ранее вычисленный приоритет понижается на nnn пунктов;<br>**-nnn** - ранее вычисленный приоритет повышается на nnn пунктов;<br>**nnn** - приоритет устанавливается ровно на nnn пунктов. |
| 12 | **PARAM** | Дополнительный параметр, требуемый для выполнения некоторых действий:<br>**AU** - имя зоны безопасности (Realm), которое следует указать в запросе авторизации;<br>**EN** - перечень выделяемых для выполнения запроса каналов управления трафиком;<br>**LI** - имя файла вложенного списка;<br>**RU** - имя встроенного или внешнего правила.<br>При задании параметра допускается использование макроподстановок (**{}**). |
| 13 | **ACL_ID** | Уникальный идентификатор строки, который выводится в специальный журнал, чтобы при возникновении проблем можно было выяснить, какая именно строка списка была тому причиной. |

Список просматривается сверху вниз. В каждой строке последовательно проверяются поля-условия 1 - 8. Если какое-либо условие не пройдёт проверку, прокси-сервер переходит к следующей строке. Если все проверки пройдены, прокси-сервер фиксирует идентификатор строки и выполняет заданное действие. Если при этом установлен флаг **TERMINATE**, обработка списка (точнее, всей системы списков независимо от уровня вложенности) прерывается. Необходимо учесть, что большинство действий являются "отложенными" - они только задают режим обработки запроса, который при дальнейшей обработке может быть изменён. Немедленно выполняются только вызов правила и переход к обработке вложенного списка.

Идентификаторы строк, в которых произошло совпадение условий, собираются в один составной идентификатор, по которому можно определить как перечень сработавших строк, так и порядок их срабатывания, что немаловажно при поиске источника проблем. Чтобы журнал получился более "читабельным", для некоторых вспомогательных строк, не изменяющих режим (например, вызывающих вложенные списки), идентификаторы можно не задавать.

Каналы управления трафиком перечисляются в перечне через пробел. Это могут быть ссылки трёх видов.

Во-первых, это могут быть имена каналов, статически определённых посредством списков Band- и Quota-каналов.

Во-вторых, это могут быть ссылки на классы каналов. Классы каналов применимы, например, в случаях, когда пользователей достаточно много, и каждому из них надо выделить индивидуальную квоту стандартного значения. Класс канала позволяет избавиться от определения индивидуальных каналов - они будут создаваться автоматически по первому требованию. Ссылка на класс канала имеет вид **класс::имя**, при этом в одном из списков должен быть определён соответствующий класс каналов. Чтобы каналы были действи-

тельно индивидуальными, их имена необходимо генерировать с помощью макросов, возвращающих имя учётной записи, желательно, во избежание неоднозначности, в полном виде **логин@домен**. Пусть, например, в системе имеется описание класса Quota-каналов **Q10W** (пусть это означает 10 мегабайт в неделю), а при обработке запроса встречается назначение канала вида **Q10W::{LUserEmail}_Q10W**. Это означает, что на основе данного шаблона каждому авторизованному пользователю будет назначен индивидуальный канал с именем, основанном на полном имени учётной записи пользователя (что определяется макросом **{LUserEmail})**. Поскольку имена каналов регистрозависимы, а имена учётных записей и доменов - нет, выбран макрос, автоматически приводящий имя учётной записи к нижнему регистру. В принципе, можно приводить и к верхнему; собственно регистр значения не имеет, важно единообразие.

В-третьих, можно сослаться на именованный набор каналов. Такие ссылки имеют вид **::имя_набора**.

Блокировка рекламы может выполняться различными способами в зависимости от обрабатываемого запроса. Если используется туннельное подключение по методу **connect:**, прокси-сервер просто генерирует отказ в доступе - это единственно возможный в данной ситуации ответ. Если клиент запрашивает сценарий Flash (это определяется по расширению **.SWF** в имени объекта; Flash-рекламы нынче полным-полно во всех баннерообменных сетях), прокси-сервер в ответ передаёт специальный сценарий-пустышку. Во всех остальных случаях прокси-сервер возвращает прозрачное GIF-изображение размером в одну точку. Впрочем, это настройки по умолчанию, и ответы сервера можно скорректировать по собственному вкусу.

Рекомендуется использовать следующую организацию списка: вначале выполняются все безусловные (независимые от авторизации) разрешения и запреты, затем следуют действия для неавторизованных сессий, в последней строке этой части списка задаётся запрос авторизации, далее перечисляются действия, назначенные для групп и индивидуальных пользователей. Для наглядности рекомендуется каждую часть вынести в отдельный список, при этом запретный список лучше разделить на два отдельных списка - явные запреты отдельно, блокировка рекламы отдельно.

## *Список разрешения анонимного доступа по методу CONNECT*

Этот список используется для ограничения доступа к прокси-серверу с использованием туннельного подключения по методу CONNECT. Доступ должен быть непременно ограничен, поскольку метод CONNECT предоставляет слишком много возможностей - даже если прокси-сервер надёжно прикрыт от внешних атак, просочившаяся по чьей-то оплошности в локальную сеть троянская программа может доставить немало неприятностей (простейший пример - спам, рассылаемый через туннельное подключение к внешнему почтовому серверу). Этот список используется, если не применяется описанная выше система списков управления доступом, - иначе считается, что все запреты и разрешения определяются в них. Список проверяется при анонимном (неавторизованном) обращении. Если запрос не соответствует ни одной строке списка, он отвергается.

Расположение списка задаётся параметром **HttpProxy[AnonymousConnect]**, исходное - **CONF\lists\proxy\httpp\AnonymousConnect.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **HOST** | Шаблон имени (в качестве которого может выступать и IP-адрес) внешнего сервера. В шаблоне допускается использование символов групповой операции ***** и **?**. Если поле пустое, то допустимым считается любое имя. На этом этапе прокси-сервер не пытается определять адрес по имени и наоборот, сравнение шаблона производится с фрагментом переданной клиентом ссылки. |
| 2 | **PORT** | Порт внешнего сервера, к которому происходит обращение. Если поле пустое либо содержит символ звёздочки ***** или нули, допустимым считается любой номер порта. |

## *Список стандартных ответов HTTP-прокси*

С помощью этого списка можно в некоторых пределах менять стандартную реакцию прокси-сервера на различные предусмотренные ситуации. Хотя в большинстве случаев всё решается путём редактирования соответствующих шаблонов, иногда этого недостаточно (особенно при необходимости поменять формат ответа - например, сменить HTML на обычный текст).

Расположение списка задаётся параметром **HttpProxy[LocalReplyList]**, исходное - **CONF\lists\proxy\httpp\LocalReplyList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **ACTION** | Выполняемая прокси-сервером команда - список возможных команд приведён ниже. |
| 2 | **CONTENT_TYPE** | Тип передаваемой в ответе информации, например:<br>**text/html** - текст в формате HTML;<br>**text/plain** - обычный текст;<br>**image/gif** - изображение формата GIF;<br>**application/x-shockwave-flash** - мультимедиа-ролик в формате Macromedia Shockwave Flash;<br>**application/octet-stream** - двоичные данные произвольного формата. |

| | | |
|---|---|---|
| 3 | **REPLY_FILE** | Полный путь к файлу ответа, учитывающему язык запроса клиента - браузер обычно передаёт в запросе информацию о языковых настройках. При задании параметра допускается использование макроподстановок (**{}**). |
| 4 | **ALTERNATE_REPLY** | Полный путь к альтернативному файлу ответа (обычно на универсальном английском языке), который используется, если предпочитаемый клиентом язык общения не был предусмотрен при настройке прокси-сервера. При задании параметра допускается использование макроподстановок (**{}**). |

Команды представляют собой "волшебные слова", обозначающие выполняемую прокси-сервером операцию. В текущей версии предусмотрены следующие команды:

| | |
|---|---|
| **DISABLED** | Жёсткий безусловный отказ в доступе к прокси-серверу. |
| **LOCAL-REDIRECT** | Выполняется перенаправление на локально размещённую HTML-страницу (HTTP-прокси способен исполнять роль простейшего web-сервера). Ссылка на страницу содержится в слове **REDIRECT-TO**. |
| **NOT-FOUND** | Выводится сообщение о том, что HTTP-прокси не обнаружил запрошенную локальную web-страницу. |
| **TCP_DENIED** | Выводится запрос на авторизацию на HTTP-прокси. Имя зоны безопасности содержится в слове **REALM**. Эта команда возможна при активированном плагине поддержки HTTP-авторизации **auth**, который является вспомогательным для плагина поддержки списков управления доступом **acl**. |
| **TCP_DISABLED** | Жёсткий безусловный отказ в доступе к прокси-серверу на основании списков управления доступом. В отличие от команды **DISABLED** используется другой код и несколько другой текст ответа. Эта команда возможна при активированном плагине поддержки HTTP-авторизации **auth**, который является вспомогательным для плагина поддержки списков управления доступом **acl**. |
| **ADV_BLOCK** | Выполняется блокировка рекламы - стандартно это передача прозрачного GIF-изображения. Эта команда возможна при активированном плагине поддержки списков управления доступом **acl**. |
| **ADVC_BLOCK** | Выполняется блокировка рекламы при туннельном подключении по методу CONNECT. Здесь подмена вывода невозможна, единственный вариант - передача HTML-страницы с текстом отказа. Эта команда возможна при активированном плагине поддержки списков управления доступом **acl**. |
| **ADVS_BLOCK** | Выполняется блокировка рекламы, выполненной в виде ролика Shockwave Flash, - передаётся пустой ролик. Эта команда возможна при активированном плагине поддержки списков управления доступом **acl**. |
| **HTTP-ALIAS** | Выполняется перенаправление на внешний сервер на основании результатов анализа списка алиасов. Эта команда возможна при активированном плагине поддержки алиасов **alias**. |
| **HTTP-REDIRECT** | Выполняется перенаправление на внешний сервер на основании результатов анализа списка перенаправления. Эта команда возможна при активированном плагине поддержки перенаправления **redirect**. |
| **UNKNOWN-METHOD** | Выводится сообщение о получении ошибочной команды HTTP. |

### *Список управления антивирусной проверкой*

Антивирусная проверка, хотя и является настоятельно рекомендуемым вариантом, отнимает значительные вычислительные ресурсы системы. С помощью этого списка можно исключить из проверки ряд объектов - как размещённые на заведомо надёжных серверах, так и имеющие формат, принципиально не содержащий вредоносного кода. К сожалению, количество таких объектов сильно ограничено - самые надёжные серверы время от времени взламывают, а в обработчиках самых пассивных форматов обнаруживают дыры, позволяющие всадить в систему троянского коня при просмотре безобиднейшей картинки. Тем не менее, возможность отключения антивируса при загрузке некоторых ресурсов существует, - для того, чтобы ей грамотно воспользоваться.

Каждый клиентский запрос проверяется по списку. Если совпадение не обнаружено, загружаемый объект будет проверяться антивирусом - это настройка по умолчанию, не подлежащая изменению. При обнаружении совпадения режим проверки определяется содержимым соответствующей строки списка.

Расположение списка задаётся параметром **HttpProxy[AVScanList]**, исходное - **CONF\lists\proxy\httpp\AVScanList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **PROTO** | Протокол, к которому относится строка списка. HTTP-прокси использует протоколы **http:**, **ftp:** и **connect:** - последний скорее не протокол, а универсальный метод соединения клиента с внешним сервером с организацией туннеля, применяемый при работе с защищённым соединением (SSL) и в ряде других случаев. К сожалению, эта особенность не позволяет организовать полноценную антивирусную проверку такого соединения. Можно указать несколько протоколов, перечислив их через пробел. Если это поле пустое или содержит символ звёздочки *****, это означает любой используемый протокол. |
| 2 | **HOST** | Шаблон имени (в качестве которого может выступать и IP-адрес) внешнего сервера. В шаблоне допускается использование символов групповой операции ***** и **?**. Если поле пустое, то допустимым считается любое имя. На этом этапе прокси-сервер не пытается определять адрес по имени и наоборот, сравнение шаблона производится с фрагментом переданной клиентом ссылки. |
| 3 | **PORT** | Порт внешнего сервера, к которому происходит обращение. Если поле пустое либо содержит символ звёздочки ***** или нули, допустимым считается любой номер порта. Если переданная ссылка не содержит явного указания порта, прокси-сервер использует стандартные номера портов для каждого протокола: 80 для **http:**, 21 для **ftp:** и 443 для **connect:**. |
| 4 | **URI** | Остаток ссылки, определяющий конкретный объект или ресурс на внешнем сервере. Это шаблон, в котором допускается использование символов групповой операции ***** и **?**. Если поле пустое, то данная строка относится к серверу в целом. |
| 5 | **AV_SCAN** | Флаг, определяющий, подвергать ли описываемый объект антивирусной проверке. Нулевое значение означает, что проверка объекта не производится. |

## *Список управления режимом кэширования*

Кэширование, то есть, локальное хранение загруженных объектов и выдача их в ответ на запросы вместо повторной загрузки с внешнего сервера, одновременно ускоряет работу и уменьшает объём оплачиваемого трафика. В то же время у кэширования имеется своя изнанка: ряд часто обновляемых данных могут "залипнуть" в кэше в старом, причём не обязательно согласованном, состоянии. Этот список позволяет задавать различные режимы кэширования для различных ресурсов, а для некоторых вообще отключить кэширование.

В текущей версии кэшируются только объекты, загружаемые по протоколу HTTP.

Расположение списка задаётся параметром **HttpProxy[CacheModeList]**, исходное - **CONF\lists\proxy\httpp\CacheModeList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **HOST** | Шаблон имени (в качестве которого может выступать и IP-адрес) внешнего сервера. В шаблоне допускается использование символов групповой операции ***** и **?**. Если поле пустое, то допустимым считается любое имя. На этом этапе прокси-сервер не пытается определять адрес по имени и наоборот, сравнение шаблона производится с фрагментом переданной клиентом ссылки. |
| 2 | **PORT** | Порт внешнего сервера, к которому происходит обращение. Если поле пустое либо содержит символ звёздочки ***** или нули, допустимым считается любой номер порта. Если переданная ссылка не содержит явного указания порта, прокси-сервер использует стандартный для протокола HTTP номер порта 80. |
| 3 | **URI** | Остаток ссылки, определяющий конкретный объект или ресурс на внешнем сервере. Это шаблон, в котором допускается использование символов групповой операции ***** и **?**. Если поле пустое, то данная строка относится к серверу в целом. |

| | | |
|---|---|---|
| 4 | **CACHE_MODE** | Режим кэширования объекта:<br>**SM** (Standard Mode) - стандартный режим: при каждом обращении производится проверка наличия изменений объекта;<br>**MT** (Minimize Traffic) - минимизация трафика: если объект уже находится в кэше, то факт его изменения не проверяется;<br>**NC** (Not Cached) - кэширование не используется;<br>**CO** (Check if Older) - наличие изменений проверяется, если объект хранится в кэше дольше, чем определённое следующим параметром число дней;<br>**CH** (Check if Hours older) - наличие изменений проверяется, если объект хранится в кэше дольше, чем определённое следующим параметром число часов. |
| 5 | **MAX_CACHE_AGE** | Предельный "возраст" хранимого в кэше объекта для режимов **CO** и **CH**. Для режима **CO** возраст задаётся в сутках, 0 означает объект, хранящийся менее суток. Для режима **CH** возраст задаётся в часах, 0 означает объект, хранящийся менее часа. |

## *Список управления каскадированием HTTP-прокси*

При наличии нескольких вариантов организации цепочек прокси-серверов этот список позволяет динамически управлять построением таких цепочек в зависимости от целевого сервера, времени суток и других условий.

Расположение списка задаётся параметром **HttpProxy[CascadeList]**, исходное - **CONF\lists\proxy\httpp\CascadeList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **PROTO** | Протокол, к которому относится строка списка. HTTP-прокси использует протоколы **http:**, **ftp:** и **connect:** - последний скорее не протокол, а универсальный метод соединения клиента с внешним сервером с организацией туннеля, применяемый при работе с защищённым соединением (SSL) и в ряде других случаев. Можно указать несколько протоколов, перечислив их через пробел. Если это поле пустое или содержит символ звёздочки *****, это означает любой используемый протокол. |
| 2 | **TARGET_HOST** | Шаблон имени (в качестве которого может выступать и IP-адрес) внешнего сервера. В шаблоне допускается использование символов групповой операции ***** и **?**. Если поле пустое, то допустимым считается любое имя. На этом этапе прокси-сервер не пытается определять адрес по имени и наоборот, сравнение шаблона производится с фрагментом переданной клиентом ссылки. |
| 3 | **TARGET_PORT** | Порт внешнего сервера, к которому происходит обращение. Если поле пустое либо содержит символ звёздочки ***** или нули, допустимым считается любой номер порта. Если переданная ссылка не содержит явного указания порта, прокси-сервер использует стандартные номера портов для каждого протокола: 80 для **http:**, 21 для **ftp:** и 443 для **connect:**. |
| 4 | **URI** | Остаток ссылки, определяющий конкретный объект или ресурс на внешнем сервере. Это шаблон, в котором допускается использование символов групповой операции ***** и **?**. Если поле пустое, то данная строка относится к серверу в целом. |
| 5 | **TIME** | Момент или интервал времени, определяемый с точностью до минуты, к которому относится эта строка. Момент задаётся в виде **чч:мм**, интервал - в виде **чч:мм-чч:мм**. Если поле пустое, то проверка условия не производится. |
| 6 | **RULE** | Дополнительное условие, записанное на языке Форт. Это условие должно вернуть на стеке единственное значение, которое будет интерпретироваться как логическое - ноль означает, что совпадение условий по этой строке не выявлено (ложь), любое другое значение - совпадение всех условий (истина). Перечень базовых правил, которые можно использовать при написании составного правила, приведён в приложении 2. Если поле пустое, считается, что правило вернуло истину. |
| 7 | **CASCADE_HOST** | Имя или IP-адрес вышестоящего прокси-сервера. |
| 8 | **CASCADE_PORT** | Номер порта, на котором работает вышестоящий прокси-сервер. |
| 9 | **CASCADE_USER** | Если вышестоящий прокси-сервер требует авторизацию, то этот параметр задаёт имя пользователя вышестоящего прокси-сервера. |

| | | |
|---|---|---|
| 10 | **CASCADE_PASS** | Если вышестоящий прокси-сервер требует авторизацию, то этот параметр задаёт пароль пользователя вышестоящего прокси-сервера. |
| 11 | **ALLOW_DIRECT** | Определяет, следует ли пытаться установить прямое соединение с целевым сервером в случае неудачи подключения через вышестоящий прокси-сервер, - например, если вышестоящий прокси-сервер недоступен или его настройки не позволяют установить соединение с целевым сервером. |
| 12 | **NOCASCADE** | Запрещает использовать каскадирование для данного сочетания параметров. Смысл этого магического действия двоякий: во-первых, можно временно исключить каскад, не удаляя строки из списка, а во-вторых, можно задать каскадное подключение по умолчанию и определить список исключений. |

## *Список алиасов HTTP-прокси*

Механизм алиасинга позволяет вместо часто используемых длинных и замысловатых ссылок вводить в строке адреса короткие псевдонимы (например, **ya** вместо **http://www.yandex.ru/**) - прокси-сервер их распознает и перенаправит браузер по нужному адресу. Этот список используется для сопоставления алиасов и соответствующих им реальных адресов.

Расположение списка задаётся параметром **HttpProxy[UrlAlias]**, исходное - **CONF\lists\proxy\httpp\UrlAlias.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **ALIAS** | Алиас. |
| 2 | **REDIRECT** | Реальная ссылка на внешний ресурс, соответствующий алиасу. |

## *Список перенаправления HTTP-прокси*

Механизм перенаправления подобен алиасингу. Основное отличие состоит в том, что сравнение с образцом выполняется с учётом всех составляющих ссылки - протокола, имени целевого узла, номера порта, логичкского пути, - кроме того, перенаправление может выполняться по-разному в зависимости от пользователя, времени суток и других условий. Этот список используется для сопоставления перенаправляемых и соответствующих им реальных адресов.

Расположение списка задаётся параметром **HttpProxy[UrlRedirect]**, исходное - **CONF\lists\proxy\httpp\UrlRedirect.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **PROTO** | Протокол, к которому относится строка списка. HTTP-прокси использует протоколы **http:**, **ftp:** и **connect:** - последний скорее не протокол, а универсальный метод соединения клиента с внешним сервером с организацией туннеля, применяемый при работе с защищённым соединением (SSL) и в ряде других случаев. Можно указать несколько протоколов, перечислив их через пробел. Если это поле пустое или содержит символ звёздочки *****, это означает любой используемый протокол. |
| 2 | **HOST** | Шаблон имени (в качестве которого может выступать и IP-адрес) внешнего сервера. В шаблоне допускается использование символов групповой операции ***** и **?**. Если поле пустое, то допустимым считается любое имя. На этом этапе прокси-сервер не пытается определять адрес по имени и наоборот, сравнение шаблона производится с фрагментом переданной клиентом ссылки. |
| 3 | **PORT** | Порт внешнего сервера, к которому происходит обращение. Если поле пустое либо содержит символ звёздочки ***** или нули, допустимым считается любой номер порта. Если переданная ссылка не содержит явного указания порта, прокси-сервер использует стандартные номера портов для каждого протокола: 80 для **http:**, 21 для **ftp:** и 443 для **connect:**. |
| 4 | **URI** | Остаток ссылки, определяющий конкретный объект или ресурс на внешнем сервере. Это шаблон, в котором допускается использование символов групповой операции ***** и **?**. Если поле пустое, то данная строка относится к серверу в целом. |
| 5 | **USER** | Пользователь, к которому относится эта строка. Если поле пустое, то его проверка не производится. Если поле содержит символ звёздочки *****, то строка считается относящейся к любому авторизованному пользователю. Если поле содержит символ минуса **-**, то строка относится только к неавторизованным сессиям. Любое другое содержимое рассматривается как шаблон сравнения, могущий содержать символы групповой операции ***** и **?**. Прокси-сервер ожидает задания полного имени пользователя в формате **логин@домен**; если же домен не задан, считается, что искомый пользователь авторизуется в домене по умолчанию. |

| | | |
|---|---|---|
| 6 | **GROUP** | Имя группы пользователей, к которой относится эта строка. В зависимости от наличия поддержки расширенной группировки оно может быть задано по-разному. Если расширенная группировка не применяется, то считается, что группа относится к тому же домену авторизации, что и входящий в неё пользователь. В противном случае прокси-сервер ожидает задания полного имени группы в формате **группа@домен**; если же домен не указан, считается, что проверяемая группа принадлежит домену по умолчанию. Если поле пустое, членство пользователя в группе не проверяется. Если сессия неавторизованная, она не относится ни к одной группе пользователей. |
| 7 | **TIME** | Момент или интервал времени, определяемый с точностью до минуты, к которому относится эта строка. Момент задаётся в виде **чч:мм**, интервал - в виде **чч:мм-чч:мм**. Если поле пустое, то проверка условия не производится. |
| 8 | **RULE** | Дополнительное условие, записанное на языке Форт. Это условие должно вернуть на стеке единственное значение, которое будет интерпретироваться как логическое - ноль означает, что совпадение условий по этой строке не выявлено (ложь), любое другое значение - совпадение всех условий (истина). Перечень базовых правил, которые можно использовать при написании составного правила, приведён в приложении 2. Если поле пустое, считается, что правило вернуло истину. |
| 9 | **REDIRECT_TO** | Соответствующая реальная ссылка на внешний ресурс. |

## *Список управления отслеживанием запросов HTTP-прокси*

Список управления слежением определяет, какие сайты и разделы и на каких условиях подлежат подробному отслеживанию. Этот список также позволяет отсеять лишнюю информацию, задав перечень полей запросов, подлежащих записи в журнал.

Расположение списка задаётся параметром **HttpProxy[SpyLogControl]**, исходное - **CONF\lists\proxy\httpp\SpyLogControl.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **PROTO** | Протокол, к которому относится строка списка. HTTP-прокси использует протоколы **http:**, **ftp:** и **connect:** - последний скорее не протокол, а универсальный метод соединения клиента с внешним сервером с организацией туннеля, применяемый при работе с защищённым соединением (SSL) и в ряде других случаев. Можно указать несколько протоколов, перечислив их через пробел. Если это поле пустое или содержит символ звёздочки *****, это означает любой используемый протокол. |
| 2 | **HOST** | Шаблон имени (в качестве которого может выступать и IP-адрес) внешнего сервера. В шаблоне допускается использование символов групповой операции ***** и **?**. Если поле пустое, то допустимым считается любое имя. На этом этапе прокси-сервер не пытается определять адрес по имени и наоборот, сравнение шаблона производится с фрагментом переданной клиентом ссылки. |
| 3 | **PORT** | Порт внешнего сервера, к которому происходит обращение. Если поле пустое либо содержит символ звёздочки ***** или нули, допустимым считается любой номер порта. Если переданная ссылка не содержит явного указания порта, прокси-сервер использует стандартные номера портов для каждого протокола: 80 для **http:**, 21 для **ftp:** и 443 для **connect:**. |
| 4 | **URI** | Остаток ссылки, определяющий конкретный объект или ресурс на внешнем сервере. Это шаблон, в котором допускается использование символов групповой операции ***** и **?**. Если поле пустое, то данная строка относится к серверу в целом. |
| 5 | **USER** | Пользователь, к которому относится эта строка. Если поле пустое, то его проверка не производится. Если поле содержит символ звёздочки *****, то строка считается относящейся к любому авторизованному пользователю. Если поле содержит символ минуса **-**, то строка относится только к неавторизованным сессиям. Любое другое содержимое рассматривается как шаблон сравнения, могущий содержать символы групповой операции ***** и **?**. Прокси-сервер ожидает задания полного имени пользователя в формате **логин@домен**; если же домен не задан, считается, что искомый пользователь авторизуется в домене по умолчанию. |

| | | |
|---|---|---|
| 6 | **GROUP** | Имя группы пользователей, к которой относится эта строка. В зависимости от наличия поддержки расширенной группировки оно может быть задано по-разному. Если расширенная группировка не применяется, то считается, что группа относится к тому же домену авторизации, что и входящий в неё пользователь. В противном случае прокси-сервер ожидает задания полного имени группы в формате **группа@домен**; если же домен не указан, считается, что проверяемая группа принадлежит домену по умолчанию. Если поле пустое, членство пользователя в группе не проверяется. Если сессия неавторизованная, она не относится ни к одной группе пользователей. |
| 7 | **TIME** | Момент или интервал времени, определяемый с точностью до минуты, к которому относится эта строка. Момент задаётся в виде **чч:мм**, интервал - в виде **чч:мм-чч:мм**. Если поле пустое, то проверка условия не производится. |
| 8 | **RULE** | Дополнительное условие, записанное на языке Форт. Это условие должно вернуть на стеке единственное значение, которое будет интерпретироваться как логическое - ноль означает, что совпадение условий по этой строке не выявлено (ложь), любое другое значение - совпадение всех условий (истина). Перечень базовых правил, которые можно использовать при написании составного правила, приведён в приложении 2. Если поле пустое, считается, что правило вернуло истину. |
| 9 | **RFIELDS** | Фильтр на обрабатываемые поля запроса. Здесь можно через пробел перечислить наименования параметров из URI запроса и/или тела POST-запроса, которые подлежат фиксации в журнале. Если это и следующее поле пустые, в журнал выводятся все данные запроса. |
| 10 | **CFIELDS** | Фильтр на обрабатываемые поля cookies. Наименования полей cookies, подлежащих фиксации в журнале, перечисляются через пробел. Если это и предыдущее поле пустые, в журнал выводятся все данные cookies. |

### *Список управления автоматической авторизацией на целевых HTTP-серверах*

Этот список используется для управления автоматической авторизацией отдельных пользователей на отдельных целевых HTTP-серверах - в ситуации, когда группу пользователей надо допустить к защищённому паролем ресурсу, не раскрывая сам пароль. Доступ к целевому серверу должен обеспечиваться по незащищённому протоколу HTTP, а сам сервер должен поддерживать метод авторизации **Basic**. Список определяет, при каких условиях используется автоматическая авторизация.

Расположение списка задаётся параметром **HttpProxy[HttpAutoLogon]**, исходное - **CONF\lists\proxy\httpp\HttpAutoLogon.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **HOST** | Шаблон имени (в качестве которого может выступать и IP-адрес) внешнего сервера. В шаблоне допускается использование символов групповой операции ***** и **?**. Если поле пустое, то допустимым считается любое имя. На этом этапе прокси-сервер не пытается определять адрес по имени и наоборот, сравнение шаблона производится с фрагментом переданной клиентом ссылки. |
| 2 | **PORT** | Порт внешнего сервера, к которому происходит обращение. Если поле пустое либо содержит символ звёздочки ***** или нули, допустимым считается любой номер порта. Если переданная ссылка не содержит явного указания порта, прокси-сервер использует стандартные номера портов для каждого протокола: 80 для **http:**, 21 для **ftp:** и 443 для **connect:**. |
| 3 | **URI** | Остаток ссылки, определяющий конкретный объект или ресурс на внешнем сервере. Это шаблон, в котором допускается использование символов групповой операции ***** и **?**. Если поле пустое, то данная строка относится к серверу в целом. |
| 4 | **USER** | Пользователь, к которому относится эта строка. Если поле пустое, то его проверка не производится. Если поле содержит символ звёздочки *****, то строка считается относящейся к любому авторизованному пользователю. Если поле содержит символ минуса **-**, то строка относится только к неавторизованным сессиям. Любое другое содержимое рассматривается как шаблон сравнения, могущий содержать символы групповой операции ***** и **?**. Прокси-сервер ожидает задания полного имени пользователя в формате **логин@домен**; если же домен не задан, считается, что искомый пользователь авторизуется в домене по умолчанию. |

| | | |
|---|---|---|
| 5 | **GROUP** | Имя группы пользователей, к которой относится эта строка. В зависимости от наличия поддержки расширенной группировки оно может быть задано по-разному. Если расширенная группировка не применяется, то считается, что группа относится к тому же домену авторизации, что и входящий в неё пользователь. В противном случае прокси-сервер ожидает задания полного имени группы в формате **группа@домен**; если же домен не указан, считается, что проверяемая группа принадлежит домену по умолчанию. Если поле пустое, членство пользователя в группе не проверяется. Если сессия неавторизованная, она не относится ни к одной группе пользователей. |
| 6 | **TIME** | Момент или интервал времени, определяемый с точностью до минуты, к которому относится эта строка. Момент задаётся в виде **чч:мм**, интервал - в виде **чч:мм-чч:мм**. Если поле пустое, то проверка условия не производится. |
| 7 | **RULE** | Дополнительное условие, записанное на языке Форт. Это условие должно вернуть на стеке единственное значение, которое будет интерпретироваться как логическое - ноль означает, что совпадение условий по этой строке не выявлено (ложь), любое другое значение - совпадение всех условий (истина). Перечень базовых правил, которые можно использовать при написании составного правила, приведён в приложении 2. Если поле пустое, считается, что правило вернуло истину. |
| 8 | **TARGET_USER** | Имя учётной записи (логин) пользователя целевого сервера, используемое для авторизации. |
| 9 | **TARGET_PASS** | Пароль пользователя целевого сервера, используемый для авторизации. |
| 10 | **ACTIVE** | Разрешает работу с этой строкой списка. Если надобность в автоматической авторизации на каком-либо ресурсе временно отпадает, можно отключить конкретную запись, не удаляя её из списка. |

## *Управляющие списки FTP-прокси*

Эти списки предназначены для управления FTP-прокси, их исходное расположение, определяемое параметром **FtpProxy[Lists]**, - каталог **CONF\lists\proxy\ftpp**.

### *Список разрешённых серверов*

Это так называемый "белый" список FTP-серверов, к которым заведомо разрешено обращение через FTP-прокси.

Расположение списка задаётся параметром **FtpProxy[HostWhiteList]**, исходное - **CONF\lists\proxy\ftpp\HostWhiteList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **HOST_MASK** | Шаблон имени (в качестве которого может выступать и IP-адрес) внешнего FTP-сервера. |
| 2 | **PASV** | Определяет, использовать ли при работе с данным сервером пассивный режим. Если поле содержит нулевое значение, то пассивный режим не используется, если ненулевое - используется. Если поле пустое, то используется режим, заданный параметром **FtpProxy[UsePASV]**. |

### *Список запрещённых серверов*

Это список серверов, доступ к которым через FTP-прокси категорически запрещён.

Расположение списка задаётся параметром **FtpProxy[HostBlackList]**, исходное - **CONF\lists\proxy\ftpp\HostBlackList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **HOST_MASK** | Шаблон имени (в качестве которого может выступать и IP-адрес) внешнего FTP-сервера. |
| 2 | **REPLY_TEXT** | Индивидуальный текст ответа FTP-прокси, поясняющий причину отказа. |

### *Список управления привязкой IP-адресов*

Особенность протокола FTP заключается в том, что для обмена данными (загрузка файла или чтение FTP-каталога) требуется установить дополнительное соединение. При этом одна из сторон сообщает свой IP-адрес. FTP-прокси может быть такой стороной в двух случаях - если клиент выбрал пассивный режим соединения с прокси-сервером либо если в настройках самого FTP-прокси не выбран пассивный режим работы с целевыми серверами. Обычно прокси-сервер самостоятельно определяет адрес для объявления, од-

нако при некоторых конфигурациях сети (например, наличие NAT-сервера на одном из направлений), он может выбрать неверное значение - просто потому, что реальный адрес, видимый со стороны соединения, отличается от адреса сетевого интерфейса и прокси-серверу неизвестен. Если IP-адрес клиента или целевого сервера не принадлежат локальной сети, FTP-прокси использует адрес, определённый параметром **Server[ExternIP]**. В базовых конфигурациях, когда имеется всего две сетевые карты, одна из которых подключена к локальной сети, а вторая обеспечивает непосредственный выход в глобальную сеть, этого достаточно. Если сетевых интерфейсов больше двух либо используются сложные правила маршрутизации, необходимы сложные же правила выбора объявляемого IP-адреса, записываемые в список управления привязкой.

Расположение списка задаётся параметром **FtpProxy[BindIpList]**, исходное - **CONF\lists\proxy\ftpp\BindIpList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **INTERFACE** | Шаблон IP-адреса сетевого интерфейса, на который принимается подключение. |
| 2 | **HOST** | Шаблон IP-адреса узла сети, от которого принимается подключение. Это может быть как FTP-клиент, подключающийся из-за пределов локальной сети, так и целевой сервер. |
| 3 | **BIND_IP** | IP-адрес, который в этом случае следует сообщить удалённой стороне. |

## *Список управления доступом к FTP-прокси*

Пожалуй, это один из самых сложных среди всех управляющих списков прокси-сервера - как и сама система управления доступом, которая поневоле должна иметь множество настроечных параметров, чтобы предусмотреть самые различные ситуации. По сути список представляет собой программу на сильно упрощённом языке, которую прокси-сервер интерпретирует при обработке каждого пользовательского запроса. В зависимости от результатов выполнения этой программы определяется реакция сервера на запрос - будет ли это разрешение или отказ.

Этот же список используется для установления режима ограничения трафика, если используется ограничитель **TrafC**.

Расположение списка задаётся параметром **FtpProxy[ACL]**, исходное - **CONF\lists\proxy\ftpp\ACL.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **HOST** | Шаблон имени (в качестве которого может выступать и IP-адрес) внешнего сервера. В шаблоне допускается использование символов групповой операции ***** и **?**. Если поле пустое, то допустимым считается любое имя. На этом этапе прокси-сервер не пытается определять адрес по имени и наоборот, сравнение шаблона производится с фрагментом переданной клиентом ссылки. |
| 2 | **PORT** | Порт внешнего сервера, к которому происходит обращение. Если поле пустое либо содержит символ звёздочки ***** или нули, допустимым считается любой номер порта. |
| 3 | **URI** | Путь, определяющий конкретный объект или ресурс на внешнем сервере. Это шаблон, в котором допускается использование символов групповой операции ***** и **?**. Если поле пустое, то данная строка относится к серверу в целом. |
| 4 | **USER** | Пользователь, к которому относится эта строка. Если поле пустое, то его проверка не производится. Если поле содержит символ звёздочки *****, то строка считается относящейся к любому авторизованному пользователю. Если поле содержит символ минуса **-**, то строка относится только к неавторизованным сессиям. Любое другое содержимое рассматривается как шаблон сравнения, могущий содержать символы групповой операции ***** и **?**. Прокси-сервер ожидает задания полного имени пользователя в формате **логин@домен**; если же домен не задан, считается, что искомый пользователь авторизуется в домене по умолчанию. |
| 5 | **GROUP** | Имя группы пользователей, к которой относится эта строка. В зависимости от наличия поддержки расширенной группировки оно может быть задано по-разному. Если расширенная группировка не применяется, то считается, что группа относится к тому же домену авторизации, что и входящий в неё пользователь. В противном случае прокси-сервер ожидает задания полного имени группы в формате **группа@домен**; если же домен не указан, считается, что проверяемая группа принадлежит домену по умолчанию. Если поле пустое, членство пользователя в группе не проверяется. Если сессия неавторизованная, она не относится ни к одной группе пользователей. |

| | | |
|---|---|---|
| 6 | **TARGET_USER** | Имя учётной записи (логин) пользователя целевого сервера. Если поле пустое, то его проверка не производится. Любое другое содержимое рассматривается как шаблон сравнения, могущий содержать символы групповой операции ***** и **?**. |
| 7 | **TIME** | Момент или интервал времени, определяемый с точностью до минуты, к которому относится эта строка. Момент задаётся в виде **чч:мм**, интервал - в виде **чч:мм-чч:мм**. Если поле пустое, то проверка условия не производится. |
| 8 | **RULE** | Дополнительное условие, записанное на языке Форт. Это условие должно вернуть на стеке единственное значение, которое будет интерпретироваться как логическое - ноль означает, что совпадение условий по этой строке не выявлено (ложь), любое другое значение - совпадение всех условий (истина). Перечень базовых правил, которые можно использовать при написании составного правила, приведён в приложении 2. Если поле пустое, считается, что правило вернуло истину. |
| 9 | **ACTION** | Двухсимвольный код действия, которое следует предпринять, если все проверяемые поля строки успешно прошли проверку:<br>**DI** (Disable) - задать режим безусловной блокировки доступа;<br>**EN** (Enable) - задать режим разрешения доступа и, если возможно, определить используемые для выполнения запроса каналы управления трафиком;<br>**LI** (List) - выполнить обработку вложенного списка;<br>**RU** (Rule) - выполнить правило. |
| 10 | **TERMINATE** | Если это поле имеет любое ненулевое значение, то при совпадении всех условий (и выполнении заданного действия) анализ списка прерывается. Это флаг глобального действия, прерывающий обработку всей иерархии списков независимо от уровней вложенности. Если значение поля нулевое, обработка продолжается дальше - это позволяет выполнить предварительную установку действия, которая может быть изменена при дальнейшей обработке. |
| 11 | **PRIORITY** | Приоритет, задаваемый при назначении канала или набора каналов в случае разрешения доступа при выборе действия **EN**. Приоритет задаётся числом, чем оно меньше, тем выше приоритет; наивысшему приоритету соответствует нулевое значение. Возможные значения:<br>**пусто** - используется значение приоритета, вычисленное к моменту назначения при анализе предыдущих строк списка правил;<br>**+nnn** - ранее вычисленный приоритет понижается на nnn пунктов;<br>**-nnn** - ранее вычисленный приоритет повышается на nnn пунктов;<br>**nnn** - приоритет устанавливается ровно на nnn пунктов. |
| 12 | **PARAM** | Дополнительный параметр, требуемый для выполнения некоторых действий:<br>**EN** - перечень выделяемых для выполнения запроса каналов управления трафиком;<br>**LI** - имя файла вложенного списка;<br>**RU** - имя встроенного или внешнего правила.<br>При задании параметра допускается использование макроподстановок (**{}**). |
| 13 | **ACL_ID** | Уникальный идентификатор строки, который выводится в специальный журнал, чтобы при возникновении проблем можно было выяснить, какая именно строка списка была тому причиной. |

Список просматривается сверху вниз. В каждой строке последовательно проверяются поля-условия 1 - 8. Если какое-либо условие не пройдёт проверку, прокси-сервер переходит к следующей строке. Если все проверки пройдены, прокси-сервер фиксирует идентификатор строки и выполняет заданное действие. Если при этом установлен флаг **TERMINATE**, обработка списка (точнее, всей системы списков независимо от уровня вложенности) прерывается. Необходимо учесть, что большинство действий являются "отложенными" - они только задают режим обработки запроса, который при дальнейшей обработке может быть изменён. Немедленно выполняются только вызов правила и переход к обработке вложенного списка.

Идентификаторы строк, в которых произошло совпадение условий, собираются в один составной идентификатор, по которому можно определить как перечень сработавших строк, так и порядок их срабатывания, что немаловажно при поиске источника проблем. Чтобы журнал получился более "читабельным", для некоторых вспомогательных строк, не изменяющих режим (например, вызывающих вложенные списки), идентификаторы можно не задавать.

Каналы управления трафиком перечисляются в перечне через пробел. Это могут быть ссылки трёх видов.

Во-первых, это могут быть имена каналов, статически определённых посредством списков Band- и Quota-каналов.

Во-вторых, это могут быть ссылки на классы каналов. Классы каналов применимы, например, в случаях, когда пользователей достаточно много, и каждому из них надо выделить индивидуальную квоту стандартного значения. Класс канала позволяет избавиться от определения индивидуальных каналов - они будут создаваться автоматически по первому требованию. Ссылка на класс канала имеет вид **класс::имя**, при этом в одном из списков должен быть определён соответствующий класс каналов. Чтобы каналы были действительно индивидуальными, их имена необходимо генерировать с помощью макросов, возвращающих имя учётной записи, желательно, во избежание неоднозначности, в полном виде **логин@домен**. Пусть, например, в системе имеется описание класса Quota-каналов **Q10W** (пусть это означает 10 мегабайт в неделю), а при обработке запроса встречается назначение канала вида **Q10W::{LUserEmail}_Q10W**. Это означает, что на основе данного шаблона каждому авторизованному пользователю будет назначен индивидуальный канал с именем, основанном на полном имени учётной записи пользователя (что определяется макросом **{LUserEmail})**. Поскольку имена каналов регистрозависимы, а имена учётных записей и доменов - нет, выбран макрос, автоматически приводящий имя учётной записи к нижнему регистру. В принципе, можно приводить и к верхнему; собственно регистр значения не имеет, важно единообразие.

В-третьих, можно сослаться на именованный набор каналов. Такие ссылки имеют вид **::имя_набора**.

Рекомендуется использовать следующую организацию списка: вначале выполняются все безусловные (независимые от авторизации) разрешения и запреты, затем следуют действия для неавторизованных сессий, далее перечисляются действия, назначенные для групп и индивидуальных пользователей. Для наглядности рекомендуется каждую часть вынести в отдельный список.

## *Управляющие списки Socks-прокси*

Эти списки предназначены для управления Socks-прокси, их исходное расположение, определяемое параметром **SocksProxy[Lists]**, - каталог **CONF\lists\proxy\socks**.

### *Список разрешённых серверов*

Это так называемый "белый" список серверов, к которым заведомо разрешено обращение через Socks-прокси. Он используется, если не подключены списки управления доступом.

Расположение списка задаётся параметром **SocksProxy[HostWhiteList]**, исходное - **CONF\lists\proxy\socks\HostWhiteList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **HOST_MASK** | Шаблон имени (в качестве которого может выступать и IP-адрес) внешнего сервера. |

### *Список запрещённых серверов*

Это список серверов, доступ к которым через Socks-прокси категорически запрещён. Он используется, если не подключены списки управления доступом.

Расположение списка задаётся параметром **SocksProxy[HostBlackList]**, исходное - **CONF\lists\proxy\socks\HostBlackList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **HOST_MASK** | Шаблон имени (в качестве которого может выступать и IP-адрес) внешнего сервера. |

### *Список управления доступом к Socks-прокси*

Пожалуй, это один из самых сложных среди всех управляющих списков прокси-сервера - как и сама система управления доступом, которая поневоле должна иметь множество настроечных параметров, чтобы предусмотреть самые различные ситуации. По сути список представляет собой программу на сильно упрощённом языке, которую прокси-сервер интерпретирует при обработке каждого пользовательского запроса. В зависимости от результатов выполнения этой программы определяется реакция сервера на запрос - будет ли это разрешение или отказ.

Этот же список используется для установления режима ограничения трафика, если используется ограничитель **TrafC**. Следует учесть, что в текущей версии ограничение трафика доступно не во всех методах работы протокола Socks, а только в двух основных - CONNECT и BIND; дополнительный метод UDP_ASSOC, доступный при использовании Socks версии 5 и выше, не ограничивается.

Расположение списка задаётся параметром **SocksProxy[ACL]**, исходное - **CONF\lists\proxy\socks\ACL.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **PROTO** | "Протокол", точнее - метод Socks-подключения, к которому относится строка списка. Socks-прокси использует методы **connect:**, **bind:** и **udp:**; последний доступен только при использовании Socks версии 5 и выше. Какой именно метод изберёт для работы клиентская программа - зависит от её реализации и настроек. Можно указать несколько методов, перечислив их через пробел. Если это поле пустое или содержит символ звёздочки *****, это означает любой используемый метод. |

| | | |
|---|---|---|
| 2 | **HOST** | Шаблон имени (в качестве которого может выступать и IP-адрес) внешнего сервера. В шаблоне допускается использование символов групповой операции ***** и **?**. Если поле пустое, то допустимым считается любое имя. На этом этапе прокси-сервер не пытается определять адрес по имени и наоборот, сравнение шаблона производится с фрагментом переданной клиентом ссылки. |
| 3 | **PORT** | Порт внешнего сервера, к которому происходит обращение. Если поле пустое либо содержит символ звёздочки ***** или нули, допустимым считается любой номер порта. |
| 4 | **USER** | Пользователь, к которому относится эта строка. Если поле пустое, то его проверка не производится. Если поле содержит символ звёздочки *****, то строка считается относящейся к любому авторизованному пользователю. Если поле содержит символ минуса **-**, то строка относится только к неавторизованным сессиям. Любое другое содержимое рассматривается как шаблон сравнения, могущий содержать символы групповой операции ***** и **?**. Прокси-сервер ожидает задания полного имени пользователя в формате **логин@домен**; если же домен не задан, считается, что искомый пользователь авторизуется в домене по умолчанию. |
| 5 | **GROUP** | Имя группы пользователей, к которой относится эта строка. В зависимости от наличия поддержки расширенной группировки оно может быть задано по-разному. Если расширенная группировка не применяется, то считается, что группа относится к тому же домену авторизации, что и входящий в неё пользователь. В противном случае прокси-сервер ожидает задания полного имени группы в формате **группа@домен**; если же домен не указан, считается, что проверяемая группа принадлежит домену по умолчанию. Если поле пустое, членство пользователя в группе не проверяется. Если сессия неавторизованная, она не относится ни к одной группе пользователей. |
| 6 | **TIME** | Момент или интервал времени, определяемый с точностью до минуты, к которому относится эта строка. Момент задаётся в виде **чч:мм**, интервал - в виде **чч:мм-чч:мм**. Если поле пустое, то проверка условия не производится. |
| 7 | **RULE** | Дополнительное условие, записанное на языке Форт. Это условие должно вернуть на стеке единственное значение, которое будет интерпретироваться как логическое - ноль означает, что совпадение условий по этой строке не выявлено (ложь), любое другое значение - совпадение всех условий (истина). Перечень базовых правил, которые можно использовать при написании составного правила, приведён в приложении 2. Если поле пустое, считается, что правило вернуло истину. |
| 8 | **ACTION** | Двухсимвольный код действия, которое следует предпринять, если все проверяемые поля строки успешно прошли проверку:<br>**DI** (Disable) - задать режим безусловной блокировки доступа;<br>**EN** (Enable) - задать режим разрешения доступа и, если возможно, определить используемые для выполнения запроса каналы управления трафиком;<br>**LI** (List) - выполнить обработку вложенного списка;<br>**RU** (Rule) - выполнить правило. |
| 9 | **TERMINATE** | Если это поле имеет любое ненулевое значение, то при совпадении всех условий (и выполнении заданного действия) анализ списка прерывается. Это флаг глобального действия, прерывающий обработку всей иерархии списков независимо от уровней вложенности. Если значение поля нулевое, обработка продолжается дальше - это позволяет выполнить предварительную установку действия, которая может быть изменена при дальнейшей обработке. |
| 10 | **PRIORITY** | Приоритет, задаваемый при назначении канала или набора каналов в случае разрешения доступа при выборе действия **EN**. Приоритет задаётся числом, чем оно меньше, тем выше приоритет; наивысшему приоритету соответствует нулевое значение. Возможные значения:<br>**пусто** - используется значение приоритета, вычисленное к моменту назначения при анализе предыдущих строк списка правил;<br>**+nnn** - ранее вычисленный приоритет понижается на nnn пунктов;<br>**-nnn** - ранее вычисленный приоритет повышается на nnn пунктов;<br>**nnn** - приоритет устанавливается ровно на nnn пунктов. |

| | | |
|---|---|---|
| 11 | **PARAM** | Дополнительный параметр, требуемый для выполнения некоторых действий:<br>**EN** - перечень выделяемых для выполнения запроса каналов управления трафиком;<br>**LI** - имя файла вложенного списка;<br>**RU** - имя встроенного или внешнего правила.<br>При задании параметра допускается использование макроподстановок (**{}**). |
| 12 | **ACL_ID** | Уникальный идентификатор строки, который выводится в специальный журнал, чтобы при возникновении проблем можно было выяснить, какая именно строка списка была тому причиной. |

Список просматривается сверху вниз. В каждой строке последовательно проверяются поля-условия 1 - 7. Если какое-либо условие не пройдёт проверку, прокси-сервер переходит к следующей строке. Если все проверки пройдены, прокси-сервер фиксирует идентификатор строки и выполняет заданное действие. Если при этом установлен флаг **TERMINATE**, обработка списка (точнее, всей системы списков независимо от уровня вложенности) прерывается. Необходимо учесть, что большинство действий являются "отложенными" - они только задают режим обработки запроса, который при дальнейшей обработке может быть изменён. Немедленно выполняются только вызов правила и переход к обработке вложенного списка.

Идентификаторы строк, в которых произошло совпадение условий, собираются в один составной идентификатор, по которому можно определить как перечень сработавших строк, так и порядок их срабатывания, что немаловажно при поиске источника проблем. Чтобы журнал получился более "читабельным", для некоторых вспомогательных строк, не изменяющих режим (например, вызывающих вложенные списки), идентификаторы можно не задавать.

Каналы управления трафиком перечисляются в перечне через пробел. Это могут быть ссылки трёх видов.

Во-первых, это могут быть имена каналов, статически определённых посредством списков Band- и Quota-каналов.

Во-вторых, это могут быть ссылки на классы каналов. Классы каналов применимы, например, в случаях, когда пользователей достаточно много, и каждому из них надо выделить индивидуальную квоту стандартного значения. Класс канала позволяет избавиться от определения индивидуальных каналов - они будут создаваться автоматически по первому требованию. Ссылка на класс канала имеет вид **класс::имя**, при этом в одном из списков должен быть определён соответствующий класс каналов. Чтобы каналы были действительно индивидуальными, их имена необходимо генерировать с помощью макросов, возвращающих имя учётной записи, желательно, во избежание неоднозначности, в полном виде **логин@домен**. Пусть, например, в системе имеется описание класса Quota-каналов **Q10W** (пусть это означает 10 мегабайт в неделю), а при обработке запроса встречается назначение канала вида **Q10W::{LUserEmail}_Q10W**. Это означает, что на основе данного шаблона каждому авторизованному пользователю будет назначен индивидуальный канал с именем, основанном на полном имени учётной записи пользователя (что определяется макросом **{LUserEmail}**). Поскольку имена каналов регистрозависимы, а имена учётных записей и доменов - нет, выбран макрос, автоматически приводящий имя учётной записи к нижнему регистру. В принципе, можно приводить и к верхнему; собственно регистр значения не имеет, важно единообразие.

В-третьих, можно сослаться на именованный набор каналов. Такие ссылки имеют вид **::имя_набора**.

В текущей версии трафик можно ограничивать только для методов **connect:** и **bind:**.

Рекомендуется использовать следующую организацию списка: вначале выполняются все безусловные (независимые от авторизации) разрешения и запреты, затем следуют действия для неавторизованных сессий, далее перечисляются действия, назначенные для групп и индивидуальных пользователей. Для наглядности рекомендуется каждую часть вынести в отдельный список.

## *Список управления каскадированием Socks-прокси*

При наличии нескольких вариантов организации цепочек прокси-серверов этот список позволяет динамически управлять построением таких цепочек в зависимости от целевого сервера, времени суток и других условий.

Расположение списка задаётся параметром **SocksProxy[CascadeList]**, исходное - **CONF\lists\proxy\socks\CascadeList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **TARGET_HOST** | Шаблон имени (в качестве которого может выступать и IP-адрес) внешнего сервера. В шаблоне допускается использование символов групповой операции ***** и **?**. Если поле пустое, то допустимым считается любое имя. На этом этапе прокси-сервер не пытается определять адрес по имени и наоборот, сравнение шаблона производится с фрагментом переданной клиентом ссылки. |
| 2 | **TARGET_PORT** | Порт внешнего сервера, к которому происходит обращение. Если поле пустое либо содержит символ звёздочки ***** или нули, допустимым считается любой номер порта. |

| | | |
|---|---|---|
| 3 | **TIME** | Момент или интервал времени, определяемый с точностью до минуты, к которому относится эта строка. Момент задаётся в виде **чч:мм**, интервал - в виде **чч:мм-чч:мм**. Если поле пустое, то проверка условия не производится. |
| 4 | **RULE** | Дополнительное условие, записанное на языке Форт. Это условие должно вернуть на стеке единственное значение, которое будет интерпретироваться как логическое - ноль означает, что совпадение условий по этой строке не выявлено (ложь), любое другое значение - совпадение всех условий (истина). Перечень базовых правил, которые можно использовать при написании составного правила, приведён в приложении 2. Если поле пустое, считается, что правило вернуло истину. |
| 5 | **CASCADE_HOST** | Имя или IP-адрес вышестоящего прокси-сервера. |
| 6 | **CASCADE_PORT** | Номер порта, на котором работает вышестоящий прокси-сервер. |
| 7 | **CASCADE_USER** | Если вышестоящий прокси-сервер требует авторизацию, то этот параметр задаёт имя пользователя вышестоящего прокси-сервера. |
| 8 | **CASCADE_PASS** | Если вышестоящий прокси-сервер требует авторизацию, то этот параметр задаёт пароль пользователя вышестоящего прокси-сервера. |
| 9 | **ALLOW_DIRECT** | Определяет, следует ли пытаться установить прямое соединение с целевым сервером в случае неудачи подключения через вышестоящий прокси-сервер, - например, если вышестоящий прокси-сервер недоступен или его настройки не позволяют установить соединение с целевым сервером. |
| 10 | **NOCASCADE** | Запрещает использовать каскадирование для данного сочетания параметров. Смысл этого магического действия двоякий: во-первых, можно временно исключить каскад, не удаляя строки из списка, а во-вторых, можно задать каскадное подключение по умолчанию и определить список исключений. |

## *Управляющие списки POP3-прокси*

Эти списки предназначены для управления POP3-прокси, их исходное расположение, определяемое параметром **Pop3Proxy[Lists]**, - каталог **CONF\lists\proxy\pop3proxy**.

### *Список доверенных сетей*

Это так называемый "белый" список доверенных IP-адресов или сетей, которые обслуживаются этим прокси-сервером. Этот список ДОПОЛНЯЕТ список локальных сетей. В нём могут быть не локальные сети, а, например, особые внешние IP-адреса, не входящие логически в локальную сеть предприятия.

Расположение списка задаётся параметром **Pop3Proxy[IpWhiteList]**, исходное - **CONF\lists\proxy\pop3p\IpWhiteList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **IP_MASK** | Шаблон IP-адреса, определяющий доверенную сеть. |
| 2 | **REPLY_TEXT** | Текст индивидуального приветствия, подставляемый в ответы сервера при подключении пользователей из этой доверенной сети. |
| 3 | **USER** | Для POP3-прокси этот параметр не имеет смысла и оставлен для сохранения единого формата списков. |
| 4 | **MAX_MSG_SIZE** | Для POP3-прокси этот параметр не имеет смысла и оставлен для сохранения единого формата списков. |
| 5 | **FLAGS** | Строка флагов-признаков для сети. Для POP3-прокси этот параметр не имеет смысла и оставлен для сохранения единого формата списков. |

### *Список запрещённых сетей*

Это список IP-адресов и подсетей, которым запрещено обращаться к прокси-серверу.

Расположение списка задаётся параметром **Pop3Proxy[IpBlackList]**, исходное - **CONF\lists\proxy\pop3p\IpBlackList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **IP_MASK** | Шаблон IP-адреса, определяющий запрещённую сеть. |
| 2 | **REPLY_TEXT** | Индивидуальный текст ответа сервера, поясняющий причину отказа. |

| | | |
|---|---|---|
| 3 | **FLAGS** | Строка флагов-признаков для сети. Для POP3-прокси этот параметр не имеет смысла и оставлен для сохранения единого формата списков. |

### *Список разрешённых серверов*

Это так называемый "белый" список почтовых серверов, к которым заведомо разрешено обращение через POP3-прокси.

Расположение списка задаётся параметром **Pop3Proxy[HostWhiteList]**, исходное - **CONF\lists\proxy\pop3p\HostWhiteList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **HOST_MASK** | Шаблон имени (в качестве которого может выступать и IP-адрес) внешнего почтового сервера. |

### *Список запрещённых серверов*

Это список почтовых серверов, доступ к которым через POP3-прокси категорически запрещён.

Расположение списка задаётся параметром **Pop3Proxy[HostBlackList]**, исходное - **CONF\lists\proxy\pop3p\HostBlackList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **HOST_MASK** | Шаблон имени (в качестве которого может выступать и IP-адрес) внешнего почтового сервера. |
| 2 | **REPLY_TEXT** | Индивидуальный текст ответа POP3-прокси, поясняющий причину отказа. |

## *Управляющие списки отображения портов TCP*

Механизм отображения портов TCP удобен для обхода ограничений как прокси-сервера, распознающего далеко не все из существующих в природе сетевых протоколов (кстати, не все протоколы можно запустить через прокси-сервер просто потому, что это не предусмотрено стандартом, как, например, в случае протокола SMTP), так и клиентских программ, не ведающих о существовании прокси-сервера. С помощью отображений можно пропустить через прокси-сервер практически любой протокол. В результате действия отображения удалённый сервер появляется в локальной сети на одном из TCP-портов прокси-сервера.

Эти списки предназначены для управления отображениями портов TCP, их исходное расположение, определяемое параметром **TCPMAP[Lists]**, - каталог **CONF\lists\proxy\tcpmap**.

### *Основной список отображений портов TCP*

Этот список задаёт соответствие портов, открываемых прокси-сервером, портам на удалённых серверах.

Расположение списка задаётся параметром **TCPMAP[TcpMap]**, исходное - **CONF\lists\proxy\tcpmap\TcpMap.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **LISTEN_PORT** | Номер локального порта, на который выполняется отображение. |
| 2 | **TARGET_HOST** | Имя или IP-адрес отображаемого внешнего сервера. |
| 3 | **TARGET_PORT** | Номер отображаемого порта на внешнем сервере. |
| 4 | **LISTEN_INTERFACE** | Имя или IP-адрес сетевого интерфейса, на котором открывается локальный порт. Если ничего не задано, то порт открывается на всех доступных сетевых интерфейсах. |
| 5 | **MY_IP_LIST** | Если порт отображения открывается на всех доступных сетевых интерфейсах, то этот параметр задаёт имя файла со списком интерфейсов, разрешённых для приёма клиентских подключений. Если ничего не задано, используется список по умолчанию, задаваемый параметром **TCPMAP[MyIpList]**. |
| 6 | **IP_BLACK_LIST** | Этот параметр задаёт имя файла со списком запрещённых сетей. Если ничего не задано, используется список по умолчанию, задаваемый параметром **TCPMAP[IpBlackList]**. |
| 7 | **IP_WHITE_LIST** | Этот параметр задаёт имя файла со списком доверенных сетей. Если ничего не задано, используется список по умолчанию, задаваемый параметром **TCPMAP[IpWhiteList]**. |

| | | |
|---|---|---|
| 8 | **IGNORE_LOCAL_NETWORKS** | Указывает, использовать ли при определении допустимости подключения список локальных сетей. Если в настройках сервера указан общий список локальных сетей, составленный излишне либерально с точки зрения безопасности прокси-сервера, его использование для управления доступом к прокси-серверу можно отключить, задав этому параметру любое ненулевое значение. Если ничего не задано, используется значение по умолчанию, задаваемое параметром **TCPMAP[IgnoreLocalNetworks]**. |
| 9 | **TIMEOUT** | Время бездействия, задаваемое в миллисекундах, по истечении которого сервер прекращает соединение с клиентом. Это вынужденная мера, предотвращающая утечку ресурсов при плохой связи - как правило, тайм-аут срабатывает, когда соединение уже фактически разорвано, но серверу неоткуда получить извещение об этом. Если ничего не задано, используется значение по умолчанию, задаваемое параметром **TCPMAP[Timeout]**. |
| 10 | **OUTBOUND_TIMEOUT** | Время бездействия, задаваемое для соединений с внешними серверами. Если ничего не задано, используется значение по умолчанию, задаваемое параметром **TCPMAP[OutboundTimeout]**. |

### *Список доверенных сетей*

Это так называемый "белый" список доверенных IP-адресов или сетей, которые обслуживаются этим прокси-сервером. Этот список ДОПОЛНЯЕТ список локальных сетей. В нём могут быть не локальные сети, а, например, особые внешние IP-адреса, не входящие логически в локальную сеть предприятия.

Расположение списка задаётся параметром **TCPMAP[IpWhiteList]**, исходное - **CONF\lists\proxy\tcpmap\IpWhiteList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **IP_MASK** | Шаблон IP-адреса, определяющий доверенную сеть. Здесь можно указать и конкретный IP-адрес. |
| 2 | **REPLY_TEXT** | Для TCPMAP-прокси этот параметр не имеет смысла и оставлен для сохранения единого формата списков. |
| 3 | **USER** | Для TCPMAP-прокси этот параметр не имеет смысла и оставлен для сохранения единого формата списков. |
| 4 | **MAX_MSG_SIZE** | Для TCPMAP-прокси этот параметр не имеет смысла и оставлен для сохранения единого формата списков. |
| 5 | **FLAGS** | Строка флагов-признаков для сети. Для TCPMAP-прокси этот параметр не имеет смысла и оставлен для сохранения единого формата списков. |

### *Список запрещённых сетей*

Это список IP-адресов и подсетей, которым запрещено обращаться к прокси-серверу.

Расположение списка задаётся параметром **TCPMAP[IpBlackList]**, исходное - **CONF\lists\proxy\tcpmap\IpBlackList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **IP_MASK** | Шаблон IP-адреса, определяющий запрещённую сеть. |
| 2 | **REPLY_TEXT** | Для TCPMAP-прокси этот параметр не имеет смысла и оставлен для сохранения единого формата списков. |
| 3 | **FLAGS** | Строка флагов-признаков для сети. Для TCPMAP-прокси этот параметр не имеет смысла и оставлен для сохранения единого формата списков. |

## *Управляющие списки отображения портов UDP*

Протокол UDP (User Datagram Protocol), в отличие от большинства интернет-протоколов верхнего уровня, не использует ни сеансовые соединения между двумя узлами сети, ни механизмы гарантированной доставки данных (подтверждения приёма, повторные посылки при потере данных и т.д.). Основа UDP - отдельные пакеты данных, дальнейшая судьба которых передающий узел нисколько не интересует. Поэтому у протокола своя экологическая ниша, которую условно можно определить словом "вещание". Сюда относятся различные протоколы потоковой (то есть, в реальном времени) передачи голоса и изображения, а также обмен данными между инфраструктурными компонентами сети - маршрутизаторами и серверами DNS. Механизм отображения портов UDP позволяет пропустить через прокси-сервер практически любой протокол, в основе

которого лежит UDP. В результате действия отображения удалённый сервер появляется в локальной сети на одном из UDP-портов прокси-сервера.

Эти списки предназначены для управления отображениями портов UDP, их исходное расположение, определяемое параметром **UDPMAP[Lists]**, - каталог **CONF\lists\proxy\udpmap**.

### *Основной список отображений портов UDP*

Этот список задаёт соответствие портов, открываемых прокси-сервером, портам на удалённых серверах.

Расположение списка задаётся параметром **UDPMAP[UdpMap]**, исходное - **CONF\lists\proxy\udpmap\UdpMap.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **LISTEN_PORT** | Номер локального порта, на который выполняется отображение. |
| 2 | **TARGET_HOST** | Имя или IP-адрес отображаемого внешнего сервера. |
| 3 | **TARGET_PORT** | Номер отображаемого порта на внешнем сервере. |
| 4 | **LISTEN_INTERFACE** | Имя или IP-адрес сетевого интерфейса, на котором открывается локальный порт. Если ничего не задано, то порт открывается на всех доступных сетевых интерфейсах. |
| 5 | **IP_BLACK_LIST** | Этот параметр задаёт имя файла со списком запрещённых сетей. Если ничего не задано, используется список по умолчанию, задаваемый параметром **UDPMAP[IpBlackList]**. |
| 6 | **IP_WHITE_LIST** | Этот параметр задаёт имя файла со списком доверенных сетей. Если ничего не задано, используется список по умолчанию, задаваемый параметром **UDPMAP[IpWhiteList]**. |
| 7 | **IGNORE_LOCAL_NETWORKS** | Указывает, использовать ли при определении допустимости подключения список локальных сетей. Если в настройках сервера указан общий список локальных сетей, составленный излишне либерально с точки зрения безопасности прокси-сервера, его использование для управления доступом к прокси-серверу можно отключить, задав этому параметру любое ненулевое значение. Если ничего не задано, используется значение по умолчанию, задаваемое параметром **UDPMAP[IgnoreLocalNetworks]**. |

### *Список доверенных сетей*

Это так называемый "белый" список доверенных IP-адресов или сетей, которые обслуживаются этим прокси-сервером. Этот список ДОПОЛНЯЕТ список локальных сетей. В нём могут быть не локальные сети, а, например, особые внешние IP-адреса, не входящие логически в локальную сеть предприятия.

Расположение списка задаётся параметром **UDPMAP[IpWhiteList]**, исходное - **CONF\lists\proxy\udpmap\IpWhiteList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **IP_MASK** | Шаблон IP-адреса, определяющий доверенную сеть. Здесь можно указать и конкретный IP-адрес. |
| 2 | **REPLY_TEXT** | Для UDPMAP-прокси этот параметр не имеет смысла и оставлен для сохранения единого формата списков. |
| 3 | **USER** | Для UDPMAP-прокси этот параметр не имеет смысла и оставлен для сохранения единого формата списков. |
| 4 | **MAX_MSG_SIZE** | Для UDPMAP-прокси этот параметр не имеет смысла и оставлен для сохранения единого формата списков. |
| 5 | **FLAGS** | Строка флагов-признаков для сети. Для UDPMAP-прокси этот параметр не имеет смысла и оставлен для сохранения единого формата списков. |

### *Список запрещённых сетей*

Это список IP-адресов и подсетей, которым запрещено обращаться к прокси-серверу.

Расположение списка задаётся параметром **UDPMAP[IpBlackList]**, исходное - **CONF\lists\proxy\udpmap\IpBlackList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **IP_MASK** | Шаблон IP-адреса, определяющий запрещённую сеть. |

| | | |
|---|---|---|
| 2 | **REPLY_TEXT** | Для UDPMAP-прокси этот параметр не имеет смысла и оставлен для сохранения единого формата списков. |
| 3 | **FLAGS** | Строка флагов-признаков для сети. Для UDPMAP-прокси этот параметр не имеет смысла и оставлен для сохранения единого формата списков. |

## *Управляющие списки HTTP-сервера*

Эти списки предназначены для управления HTTP-сервером, их исходное расположение, определяемое параметром **HTTP[Lists]**, - каталог **CONF\lists\http**.

### *Список доверенных сетей*

Это так называемый "белый" список доверенных IP-адресов или сетей, которые обслуживаются этим HTTP-сервером. Этот список ДОПОЛНЯЕТ список локальных сетей. В нём могут быть не локальные сети, а, например, особые внешние IP-адреса, не входящие логически в локальную сеть предприятия.

Если разрешено настройками сервера, на основании этой пары списков выполняется так называемая IP-авторизация: отправитель считается авторизовавшимся, и ему назначается имя, сопоставленное в списке IP-адресу подключения.

Расположение списка задаётся параметром **HTTP[IpWhiteList]**, исходное - **CONF\lists\http\IpWhiteList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **IP_MASK** | Шаблон IP-адреса, определяющий доверенную сеть. Здесь можно указать и конкретный IP-адрес, если список используется в том числе и для автоматической авторизации пользователей. |
| 2 | **REPLY_TEXT** | Для HTTP-сервера этот параметр не имеет смысла и оставлен для сохранения единого формата списков. |
| 3 | **USER** | Имя учётной записи (логин) и домен авторизации пользователя (в виде **логин@домен**), используемые при IP-авторизации. Если задано только имя учётной записи, считается, что авторизация выполняется в домене по умолчанию. Если это поле не заполнено, IP-авторизация по этой строке списка не выполняется. |
| 4 | **MAX_MSG_SIZE** | Для HTTP-сервера этот параметр не имеет смысла и оставлен для сохранения единого формата списков. |
| 5 | **FLAGS** | Строка флагов-признаков для сети. Для HTTP-сервера этот параметр не имеет смысла и оставлен для сохранения единого формата списков. |

### *Список запрещённых сетей*

Это список IP-адресов и подсетей, которым запрещено обращаться к HTTP-серверу.

Расположение списка задаётся параметром **HTTP[IpBlackList]**, исходное - **CONF\lists\http\IpBlackList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **IP_MASK** | Шаблон IP-адреса, определяющий запрещённую сеть. |
| 2 | **REPLY_TEXT** | Для HTTP-сервера этот параметр не имеет смысла и оставлен для сохранения единого формата списков. |
| 3 | **FLAGS** | Строка флагов-признаков для сети. Для HTTP-сервера этот параметр не имеет смысла и оставлен для сохранения единого формата списков. |

### *Список стандартных ответов HTTP-сервера*

С помощью этого списка можно в некоторых пределах менять стандартную реакцию HTTP-сервера на различные предусмотренные ситуации. Хотя в большинстве случаев всё решается путём редактирования соответствующих шаблонов, иногда этого недостаточно (особенно при необходимости поменять формат ответа - например, сменить HTML на обычный текст).

Расположение списка задаётся параметром **HTTP[LocalReplyList]**, исходное - **CONF\lists\http\LocalReplyList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **ACTION** | Выполняемая HTTP-сервером команда - список возможных команд приведён ниже. |

| | | |
|---|---|---|
| 2 | **CONTENT_TYPE** | Тип передаваемой в ответе информации, например:<br>**text/html** - текст в формате HTML;<br>**text/plain** - обычный текст;<br>**image/gif** - изображение формата GIF;<br>**application/x-shockwave-flash** - мультимедиа-ролик в формате Macromedia Shockwave Flash;<br>**application/octet-stream** - двоичные данные произвольного формата. |
| 3 | **REPLY_FILE** | Полный путь к файлу ответа, учитывающему язык запроса клиента - браузер обычно передаёт в запросе информацию о языковых настройках. При задании параметра допускается использование макроподстановок (**{}**). |
| 4 | **ALTERNATE_REPLY** | Полный путь к альтернативному файлу ответа (обычно на универсальном английском языке), который используется, если предпочитаемый клиентом язык общения не был предусмотрен при настройке HTTP-сервера. При задании параметра допускается использование макроподстановок (**{}**). |

Команды представляют собой "волшебные слова", обозначающие выполняемую прокси-сервером операцию. В текущей версии предусмотрены следующие команды:

| | |
|---|---|
| **DISABLED** | Жёсткий безусловный отказ в доступе к HTTP-серверу. |
| **UNAVAILABLE** | Жёсткий безусловный отказ в доступе к HTTP-серверу, вызванный слишком высокой нагрузкой. В отличие от команды **DISABLED** текст ответа содержит предложение повторить попытку позже. |
| **REDIRECT** | Выполняется перенаправление (с кодом 302) на другую ссылку, которая содержится в слове **REDIRECT-TO**. |
| **MOVED** | Выполняется перенаправление (с кодом 301) на другую ссылку, которая содержится в слове **REDIRECT-TO**. |
| **NOT_FOUND** | Выводится сообщение о том, что HTTP-сервер не обнаружил запрошенный объект. |
| **UNAUTHORIZED** | Выводится запрос на авторизацию на HTTP-сервере. Имя зоны безопасности содержится в слове **REALM**. |
| **FORBIDDEN** | Жёсткий безусловный отказ в доступе к запрошенному объекту на основании списка управления доступом. В отличие от команды **DISABLED** используется другой код и несколько другой текст ответа. |
| **ERR_EACTION** | Выводится сообщение о сбое при выполнении запроса в результате неверной настройки сервера. |
| **ERR_ROOT** | Выводится сообщение о том, что в результате неверной настройки сервера не удалось определить корневой каталог сайта. |
| **ERR_FILE** | Выводится сообщение о том, что в результате неверной настройки сервера не удалось выполнить преобразование логического пути в физический. |
| **ERR_ACTION** | Выводится сообщение о том, что в результате неверной настройки сервера не удалось определить способ выполнения запроса. |
| **ERR_ONREQ** | Выводится сообщение о сбое при предварительной обработке запроса в результате неверной настройки сервера. |
| **UNKNOWN_METHOD** | Выводится сообщение о получении ошибочной команды HTTP. |

### *Список дополнительных прослушиваемых портов HTTP-сервера*

Этот список используется специальным расширением, обеспечивающим HTTP-серверу работу с использованием произвольного количества прослушиваемых портов.

Расположение списка задаётся параметром **HTTP[ListenPorts]**, исходное - **CONF\lists\http\ListenPorts.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **LISTEN_PORT** | Номер прослушиваемого порта. |
| 2 | **LISTEN_INTERFACE** | Имя или IP-адрес сетевого интерфейса, на котором открывается порт. Если ничего не задано, то порт открывается на всех доступных сетевых интерфейсах. |

| | | |
|---|---|---|
| 3 | **SSL** | Признак использования работы по защищённому соединению (SSL) на данном порту. Если флаг имеет любое ненулевое значение, считается, что порт предназначен для приёма подключений по защищённому соединению. |
| 4 | **COMMENT** | Примечание. Это поле не используется сервером и предназначено для заметок администратора. |

### *Список виртуальных каталогов HTTP-сервера*

Этот список определяет структуру сервера - какие web-сайты он обслуживает, как они расположены на диске, и как выполняется отображение логического пути к объекту, переданного в запросе клиента, на физические каталоги сервера. Отображение может зависеть от множества параметров. Обычно в качестве ключевых параметров используются символическое имя узла сети (если на одном физическом сервере размещаются несколько сайтов), язык, поддерживаемый клиентом (если сайт имеет несколько разделов на различных языках), порт сервера, на который поступил запрос, фрагмент пути к запрашиваемому объекту. Сопоставляя эти и другие параметры запроса с содержимым списка, сервер определяет физический каталог, в котором следует искать запрашиваемый объект.

Расположение списка задаётся параметром **HTTP[VirtualFolders]**, исходное - **CONF\lists\http\VirtualFolders.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **HOST** | Шаблон доменного имени web-сайта, к которому выполняется обращение. В шаблоне допускается использование символов групповой операции ***** и **?**. Если поле пустое, то допустимым считается любое имя. |
| 2 | **PORT** | Номер порта сервера, на который поступил запрос. Если поле пустое либо содержит символ звёздочки ***** или нули, допустимым считается любой номер порта. |
| 3 | **URI** | Шаблон логического пути к запрашиваемому объекту. Здесь использование символов групповой операции не допускается. Проверяется совпадение части пути, переданного в запросе, с содержимым поля, причём совпавшая часть должна быть выровнена влево. Например, если запрашиваемый объект **/Elog/cgi-bin/Elog.cgi**, то совпадение будет зафиксировано с шаблонами **/Elog/** и **/Elog/cgi-bin/**, но не с шаблоном **/cgi-bin/**. Необходимо учитывать, что логический путь всегда является абсолютным, то есть, начинается с разделителя каталогов /, - соответственно, шаблон тоже должен начинаться с этого символа. Если совпадение фиксируется в нескольких строках, сервер выбирает строку с наиболее длинным шаблоном. Если поле пустое, то совпавшим считается любой запрошенный путь. |
| 4 | **LANG** | Язык запроса клиента. В текущей версии сервер распознаёт шесть языков - русский (**ru**), немецкий (**de**), французский (**fr**), испанский (**es**), итальянский (**it**) и английский (**en**); последний является языком по умолчанию, принимаемым в случае неподдерживаемого языка. Если поле содержит символ звёздочки *****, то допустимым признаётся любой язык. Если поле пустое, язык не анализируется. |
| 5 | **RULE** | Дополнительное условие, записанное на языке Форт. Это условие должно вернуть на стеке единственное значение, которое будет интерпретироваться как логическое - ноль означает, что совпадение условий по этой строке не выявлено (ложь), любое другое значение - совпадение всех условий (истина). Перечень базовых правил, которые можно использовать при написании составного правила, приведён в приложении 2. Если поле пустое, считается, что правило вернуло истину. |
| 6 | **ROOTPATH** | Физический каталог сервера, в котором будет выполняться поиск запрашиваемого объекта, - корневой каталог сайта. При задании параметра допускается использование макроподстановок (**{}**). |
| 7 | **VIRTUAL** | Признак виртуального корня. Обычно логический путь к объекту без преобразования состыковывается с корневым каталогом, образуя полный физический путь. Если в этом поле находится ненулевое значение, с корневым каталогом состыковывается не совпавший с содержимым поля **URI** остаток логического пути. |
| 8 | **REPLACE** | Если это поле не пустое, то логический путь подвергается дополнительному преобразованию - совпавшая с содержимым поля **URI** часть заменяется содержимым данного поля. Такая манипуляция может потребоваться при выполнении некоторых сценариев, ожидающих вполне определённого пути в запросе. При задании параметра допускается использование макроподстановок (**{}**). |

| | | |
|---|---|---|
| 9 | **REDIRECT** | Если это поле не пустое, то его содержимое интерпретируется как ссылка, на которую следует перенаправить обратившегося клиента. Ссылка может указывать как на другой локальный объект, так и на внешний web- (и не только; протокол может быть указан любой) сервер. Указание корневого каталога при этом смысла не имеет, а вот замена совпавшей части пути может пригодиться, если в ссылке предполагается использовать фрагмент клиентского запроса. При задании параметра допускается использование макроподстановок (**{}**). |
| 10 | **INDEX** | Имя индексного файла, который возвращается в ответ на запрос или интерпретируется как сценарий, если в запросе указано только имя каталога (разумеется, каталога существующего, в противном случае применяется значение следующего параметра). Можно указать несколько файлов через пробел, при этом поиск файла выполняется слева направо; будет использован первый найденный файл. Если это поле пустое, используется перечень индексных файлов по умолчанию, заданный параметром **HTTP[DirectoryIndex]**. |
| 11 | **NOT_FOUND** | Имя файла, который возвращается в ответ на запрос или интерпретируется на сервере как сценарий, если путь к запрошенному объекту отсутствует. Этот файл ищется в каталоге самого нижнего уровня, обнаруженного при анализе пути. Можно указать несколько файлов через пробел, при этом поиск файла выполняется слева направо; будет использован первый найденный файл. Если это поле пустое, используется перечень замещающих файлов по умолчанию, заданый параметров **HTTP[DirectoryNotfound]**. |

Список всегда просматривается полностью, в процессе просмотра сервер ищет наилучшее совпадение, то есть, строку, в которой совпавший логический путь (**URI**) имеет наибольшую длину.

### *Список типов данных*

HTTP-сервер в своих ответах всегда сообщает тип передаваемых данных. На основании этого списка можно по расширению имени (а в особых случаях и по расположению файла на диске, поскольку по списку проверяется полный - возможно, несуществующий, - путь к файлу) определить искомое значение. По этому списку также определяется, необходимо ли в файле обнаруживать и обрабатывать так называемые Server Side Includes (SSI) - простейшие сценарии, выполняемые на сервере и генерирующие текст, включаемый в выводимую страницу. Ещё одна функция этого списка - управление кэшированием передаваемых файлов на стороне клиента.

Расположение списка задаётся параметром **HTTP[ContentTypeList]**, исходное - **CONF\lists\http\ContentTypeList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **FILETYPE** | Шаблон имени запрашиваемого файла. Обычно проверяется только расширение, но, поскольку с шаблоном сравнивается полный физический путь к файлу, можно в некоторых случаях ориентироваться и на расположение. |
| 2 | **CTYPE** | Тип данных, соответствующий шаблону. |
| 3 | **SSI** | Определяет, требуется ли для файла обработка директив SSI. Любое ненулевое значение является признаком необходимости обработки. |
| 4 | **NOCACHE** | Управляет кэшированием файлов в браузере. Любое ненулевое значение запрещает кэширование файлов, соответствующих шаблону. По умолчанию - для файлов, не соответствующих ни одному шаблону из списка, - кэширование разрешено. |

### *Список определения кодировки текстовых файлов*

На основании этого списка сервер определяет кодировку файлов текстовых форматов (обычный текст и HTML), передаваемую в ответе на запрос, дабы браузер без дополнительных манипуляций пользователя выбрал правильное отображение полученного текста. Разнесение разных языковых (в том числе и различных кодировок русского языка) разделов сайта по разным каталогам фактически превратилось в стандарт.

Расположение списка задаётся параметром **HTTP[CharsetList]**, исходное - **CONF\lists\http\CharsetList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **PATH** | Шаблон физического пути к запрашиваемому объекту. Здесь использование символов групповой операции не допускается. Проверяется совпадение части пути, переданного в запросе, с содержимым поля, причём совпавшая часть должна быть выровнена влево. Например, если запрашиваемый объект **..\Elog\cgi-bin\Elog.cgi**, то совпадение будет зафиксировано с шаблонами **..\Elog** и **..\Elog\cgi-bin**, но не с шаблоном **..\cgi-bin** или **\cgi-bin**. Следует учесть, что сервер не выполняет приведение пути к единому унифицированному формату. **..\Elog\cgi-bin** и **C:\Eserv3\Elog\cgi-bin** считаются разными путями, даже если они на самом деле указывают на один каталог; поэтому для заполнения списка виртуальных каталогов следует принять один из вариантов записи путей в качестве стандарта и в дальнейшем всегда его придерживаться. Если совпадение фиксируется в нескольких строках, сервер выбирает строку с наиболее длинным шаблоном. Если поле пустое, то совпавшим считается любой путь. |
| 2 | **CHARSET** | Кодировка данных, соответствующая шаблону. |

Список просматривается сверху вниз. В процессе просмотра сервер ищет наилучшее совпадение, то есть, строку, в которой совпавший физический путь (**PATH**) имеет наибольшую длину.

## *Список расширений ISAPI*

Этот список определяет подключаемые при запуске сервера обработчики сценариев, использующие интерфейс ISAPI. Такие обработчики запускаются в адресном пространстве сервера, поэтому работают быстрее. Обратной стороной этого преимущества является меньшая устойчивость к сбоям - ошибка в сценарии, а тем паче в самом обработчике может вызвать аварийное завершение работы сервера. Этот список обрабатывается при запуске сервера, при этом список активных обработчиков целиком загружается в память.

Расположение списка задаётся параметром **HTTP[IsapiExtensions]**, исходное - **CONF\lists\http\IsapiExtensions.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **NAME** | Условное имя обработчика, по которому он будет вызываться из списка обработчиков сценариев. Теоретически имя может быть любым, на практике же мелкие, но чувствительные особенности реализации обработчиков ISAPI для различных языков вынуждают в большинстве случаев использовать фиксированные имена, на которые ориентируются встроенные в HTTP-сервер процедуры подготовки среды выполнения. Для языка PHP версии 5.2.5 и выше следует использовать имя **PHP5**, для языка Perl версии 5.8.8 и выше - **PERL**. В противном случае сценарии либо вообще не будут работать, либо будут работать не так, как задумывалось их разработчиками. |
| 2 | **HANDLER** | Путь к исполняемому файлу (DLL-библиотеке) обработчика. При задании параметра допускается использование макроподстановок (**{}**). |
| 3 | **ACTIVE** | Признак активности расширения. Если в этом поле находится ненулевое значение, сервер при анализе списка загружает расширение. |

## *Список обработчиков сценариев*

Этот список сопоставляет расширения и, в некоторых случаях, расположение файлов программам-обработчикам, запускающимся на сервере и выполняющих сложную обработку запросов.

Расположение списка задаётся параметром **HTTP[ScriptHandlers]**, исходное - **CONF\lists\http\ScriptHandlers.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **FILETYPE** | Шаблон имени запрашиваемого файла. Обычно проверяется только расширение, но, поскольку с шаблоном сравнивается полный физический путь к файлу, можно в некоторых случаях ориентироваться и на расположение. |
| 2 | **HANDLER** | Обозначение обработчика сценария. Для CGI-сценариев это путь к исполняемому файлу программы-обработчика. Если поле пустое, то считается, что файл сам по себе является программой-обработчиком, как, например, двоичные исполняемые файлы формата EXE. Поскольку файлы такого типа могут быть и обычными пассивными данными, здесь крайней нежелательно ограничиваться только расширением - в идеале следует указывать полные пути к файлам такого типа. Для FastCGI-сценариев поле задаёт номер порта TCP для связи с соответствующим сервером FastCGI. Для ISAPI-сценариев здесь следует указывать условное имя ISAPI-обработчика. При задании параметра допускается использование макроподстановок (**{}**). |

| | | |
|---|---|---|
| 3 | **MODE** | Определяет режим выполнения сценария. Возможны следующие значения:<br>**пусто** - для совместимости со старым форматом списка определяет наиболее распространённый режим **CGI**;<br>**CGI** - определяет режим **CGI**;<br>**FCGI** - определяет режим **FastCGI**;<br>**ISAPI** - определяет режим **ISAPI**;<br>**FS** - определяет специальный режим встроенного в HTTP-сервер обработчика сценариев на языке **ForthScript**. |
| 4 | **COMPAT** | Задаёт режим передачи параметров, совместимый с CGI-обработчиками типа Parser, полагающими сценариями себя. В этом режиме CGI-параметры SCRIPT_NAME, PATH_INFO и DOCUMENT_ROOT принимают другие значения. |
| 5 | **TIMEOUT** | Задаёт лимит времени выполнения сценариев CGI. Чтобы сценарии в результате ошибок в коде или из-за проблем взаимодействия с другими приложениями не зацикливались навечно, забивая оперативную память сервера и отбирая процессорное время, длительность их выполнения рекомендуется ограничивать. Лимит задаётся в миллисекундах. Указание нулевого значения снимает ограничение. Если поле пустое, используется глобальное значение, определяемое параметром **HTTP[DefaultCgiTimeout]**. |

## *Список идентификации поисковых роботов*

Это список клиентских идентификаторов (User-Agent), которыми обозначают себя поисковые роботы. Он используется для ведения статистики в собственном текстовом формате, чтобы отделять набеги роботов от визитов "человекоуправляемых" браузеров (это имеет большое значение, если сайт получает доходы от показа рекламы). Если разрешено параметром **HTTP[AutoFillRobots]**, то этот список автоматически пополняется. Робот определяется по запросу специального управляющего файла **robots.txt**, который, по всеобщему соглашению, должен находиться в корневом каталоге каждого сайта; в этом файле содержится управляющая информация, определяющая, какие разделы сайта подлежат индексации в поисковых системах, а какие нет.

Расположение списка задаётся параметром **HTTP[Robots]**, исходное - **CONF\lists\http\robots.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **ROBOT** | Идентификатор робота. |
| 2 | **IP** | IP-адрес, с которого обращается робот. |
| 3 | **NAME** | Краткое, но, в отличие от маловразумительных, хотя и длинных, идентификаторов, внятное имя робота. Это поле всегда заполняется вручную, при автоматической регистрации в него записывается слово **NAME**. |
| 4 | **COUNTRY** | Географический идентификатор, определяемый при автоматическом заполнении по результатам анализа IP-адреса. Чтобы значение имело смысл, должен быть подключён плагин **geo_ip**. |
| 5 | **DATE** | Дата и время первого посещения робота. |

## *Список управления доступом к HTTP-серверу*

На основании анализа этого списка сервер определяет возможность выполнения запроса. Во избежание дурной множественности объектом, для которого назначаются права, является физический путь к файлу на диске.

Расположение списка задаётся параметром **HTTP[ACL]**, исходное - **CONF\lists\http\ACL.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **PATH** | Шаблон физического пути к запрашиваемому объекту. Здесь использование символов групповой операции не допускается. Проверяется совпадение части пути, переданного в запросе, с содержимым поля, причём совпавшая часть должна быть выровнена влево. Например, если запрашиваемый объект **..\Elog\cgi-bin\Elog.cgi**, то совпадение будет зафиксировано с шаблонами **..\Elog** и **..\Elog\cgi-bin**, но не с шаблоном **..\cgi-bin** или **\cgi-bin**. Следует учесть, что сервер не выполняет приведение пути к единому унифицированному формату. **..\Elog\cgi-bin** и **C:\Eserv3\Elog\cgi-bin** считаются разными путями, даже если они на самом деле указывают на один каталог; поэтому для заполнения списка виртуальных каталогов следует принять один из вариантов записи путей в качестве стандарта и в дальнейшем всегда его придерживаться. Если совпадение фиксируется в нескольких строках, сервер выбирает строку с наиболее длинным шаблоном. Если строк с одинаковым шаблоном несколько, сервер суммирует права, назначенные этими строками. Если поле пустое, то совпавшим считается любой путь. |
| 2 | **USER** | Пользователь, к которому относится эта строка. Если поле пустое, то его проверка не производится. Если поле содержит символ звёздочки *****, то строка считается относящейся к любому авторизованному пользователю. Если поле содержит символ минуса **-**, то строка относится только к неавторизованным сессиям. Любое другое содержимое рассматривается как шаблон сравнения, могущий содержать символы групповой операции ***** и **?**. HTTP-сервер ожидает задания полного имени пользователя в формате **логин@домен**; если же домен не задан, считается, что искомый пользователь авторизуется в домене по умолчанию. |
| 3 | **GROUP** | Имя группы пользователей, к которой относится эта строка. В зависимости от наличия поддержки расширенной группировки оно может быть задано по-разному. Если расширенная группировка не применяется, то считается, что группа относится к тому же домену авторизации, что и входящий в неё пользователь. В противном случае HTTP-сервер ожидает задания полного имени группы в формате **группа@домен**; если же домен не указан, считается, что проверяемая группа принадлежит домену по умолчанию. Если поле пустое, членство пользователя в группе не проверяется. Если сессия неавторизованная, она не относится ни к одной группе пользователей. |
| 4 | **TIME** | Момент или интервал времени, определяемый с точностью до минуты, к которому относится эта строка. Момент задаётся в виде **чч:мм**, интервал - в виде **чч:мм-чч:мм**. Если поле пустое, то проверка условия не производится. |
| 5 | **RULE** | Дополнительное условие, записанное на языке Форт. Это условие должно вернуть на стеке единственное значение, которое будет интерпретироваться как логическое - ноль означает, что совпадение условий по этой строке не выявлено (ложь), любое другое значение - совпадение всех условий (истина). Перечень базовых правил, которые можно использовать при написании составного правила, приведён в приложении 2. Если поле пустое, считается, что правило вернуло истину. |
| 6 | **ACCESS** | Код прав доступа, назначаемых при выявлении совпадения. Это может быть либо число, либо специальный символьный код. Число является суммой кодов следующих элементарных прав:<br>**1** - право выполнения файлов (относится к сценариям CGI);<br>**2** - право создания и записи файлов;<br>**4** - право чтения файлов;<br>**8** - право чтения оглавления каталогов;<br>**16** - право удаления файлов и подкаталогов.<br>Перечень символьных кодов приведён в приложении 1. |
| 7 | **FORBIDDEN** | Если этот флаг имеет ненулевое значение, то при недостатке прав доступа к объекту сервер не будет запрашивать авторизацию в надежде, что посетитель подберёт правильные реквизиты авторизации, а ответит жёстким бескомпромиссным отказом. |
| 8 | **REALM** | Имя зоны безопасности (Realm), которое следует указать в запросе авторизации, если при недостатке прав доступа выполняется именно он. При задании параметра допускается использование макроподстановок (**{}**). |

| | | |
|---|---|---|
| 9 | **NTUSER** | Имя учётной записи пользователя Windows NT, от имени которого следует запускать CGI-сценарии, расположенные по этому пути. Пользователь должен иметь необходимые для успешной работы права доступа. В минимальном варианте это право подключения к серверу по сети (именно в таком режиме происходит авторизация), права чтения и поиска файлов во всех каталогах Eserv, связанных с функционированием HTTP-сервера, права создания и записи файлов в каталогах оперативных и статистических журналов HTTP-сервера, а также в каталоге временных файлов. Дополнительные права определяются особенностями сценария, запускаемого от имени пользователя, - например, сценарии web-интерфейса желательно запускать от имени администратора домена, в противном случае часть функций будет недоступна. Используется, если включена поддержка имперсонализации. |
| 10 | **NTDOMAIN** | Имя домена Active Directory или компьютера (чаще всего - локального, на котором установлен Eserv), по списку которого выполняется авторизация пользователя. Используется, если включена поддержка имперсонализации. |
| 11 | **NTPASS** | Пароль пользователя Windows NT. Используется, если включена поддержка имперсонализации. |

Список просматривается сверху вниз. В процессе просмотра сервер ищет наилучшее совпадение, то есть, строку, в которой совпавший физический путь (**PATH**) имеет наибольшую длину. В начале просмотра эта длина нулевая, права доступа, имя зоны безопасности и флаг жёсткого отказа имеют значения по умолчанию, определённые в конфигурационном файле параметрами **HTTP[DefaultAccess]**, **HTTP[DefaultRealm]** и **HTTP[DefaultForbiddenFlag]** соответственно. При обнаружении совпадения физического пути и поля **PATH** сервер сравнивает длину шаблона в текущей строке и длину ранее зафиксированного совпадения. Если шаблон в текущей строке короче, строка пропускается. Если текущий шаблон длиннее, то права доступа сбрасываются в состояние запрета, одновременно фиксируются новые значения для имени зоны безопасности, признака жёсткого отказа и параметров имперсонализации. Также фиксируется новая длина совпавшего шаблона. Далее - независимо от того, длиннее текущий шаблон или совпадает с уже зафиксированным - проверяются прочие условия, и при их выполнении заданные в строке права доступа добавляются (посредством побитовой операции ИЛИ) к текущему значению. Таким образом, имя зоны безопасности и признак жёсткого отказа всегда определяются самой верхней строкой, давшей наилучшее совпадение пути. Это следует учитывать при назначении прав различным пользователям и группам пользователей (то есть, с использованием нескольких строк, имеющих одинаковое значение в поле **PATH**) на один и тот же каталог или файл.

Список всегда просматривается до конца. Для повышения быстродействия рекомендуется отсортировать его в виде "опрокинутого" дерева каталогов - так, чтобы самые длинные шаблоны были в верхней части списка.

## *Список управления имперсонализацией*

Этот список позволяет сопоставить различным каталогам и даже файлам реквизиты пользователя Windows NT, от имени которого будут запускаться доступные по этому пути CGI-сценарии. Список применяется при наличии поддержки имперсонализации в двух случаяю: если не подключена поддержка списка прав доступа (в этом списке также можно указать реквизиты имперсонализации) либо если использование этого списка определено параметром **HTTP[SeparateImpersonationList]**.

Расположение списка задаётся параметром **HTTP[ImpersonationList]**, исходное - **CONF\lists\http\ImpersonationList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **PATH** | Шаблон физического пути к запрашиваемому объекту. Здесь использование символов групповой операции не допускается. Проверяется совпадение части пути, переданного в запросе, с содержимым поля, причём совпавшая часть должна быть выровнена влево. Например, если запрашиваемый объект **..\Elog\cgi-bin\Elog.cgi**, то совпадение будет зафиксировано с шаблонами **..\Elog** и **..\Elog\cgi-bin**, но не с шаблоном **..\cgi-bin** или **\cgi-bin**. Следует учесть, что сервер не выполняет приведение пути к единому унифицированному формату. **..\Elog\cgi-bin** и **C:\Eserv3\Elog\cgi-bin** считаются разными путями, даже если они на самом деле указывают на один каталог; поэтому для заполнения списка виртуальных каталогов следует принять один из вариантов записи путей в качестве стандарта и в дальнейшем всегда его придерживаться. Если совпадение фиксируется в нескольких строках, сервер выбирает строку с наиболее длинным шаблоном. Если поле пустое, то совпавшим считается любой путь. |

| | | |
|---|---|---|
| 2 | **NTUSER** | Имя учётной записи пользователя Windows NT, от имени которого следует запускать CGI-сценарии, расположенные по этому пути. Пользователь должен иметь необходимые для успешной работы права доступа. В минимальном варианте это право подключения к серверу по сети (именно в таком режиме происходит авторизация), права чтения и поиска файлов во всех каталогах Eserv, связанных с функционированием HTTP-сервера, права создания и записи файлов в каталогах оперативных и статистических журналов HTTP-сервера, а также в каталоге временных файлов. Дополнительные права определяются особенностями сценария, запускаемого от имени пользователя, - например, сценарии web-интерфейса желательно запускать от имени администратора домена, в противном случае часть функций будет недоступна. |
| 3 | **NTDOMAIN** | Имя домена Active Directory или компьютера (чаще всего - локального, на котором установлен Eserv), по списку которого выполняется авторизация пользователя. |
| 4 | **NTPASS** | Пароль пользователя Windows NT. |

Список просматривается сверху вниз. В процессе просмотра сервер ищет наилучшее совпадение, то есть, строку, в которой совпавший физический путь (**PATH**) имеет наибольшую длину.

## *Управляющие списки FTP-сервера*

Эти списки предназначены для управления FTP-сервером, их исходное расположение, определяемое параметром **FTP[Lists]**, - каталог **CONF\lists\ftp**.

### *Список доверенных сетей*

Это так называемый "белый" список доверенных IP-адресов или сетей, которые обслуживаются этим FTP-сервером. Этот список ДОПОЛНЯЕТ список локальных сетей. В нём могут быть не локальные сети, а, например, особые внешние IP-адреса, не входящие логически в локальную сеть предприятия.

Если разрешено настройками сервера, на основании этой пары списков выполняется так называемая IP-авторизация: отправитель считается авторизовавшимся, и ему назначается имя, сопоставленное в списке IP-адресу подключения.

Расположение списка задаётся параметром **FTP[IpWhiteList]**, исходное - **CONF\lists\ftp\IpWhiteList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **IP_MASK** | Шаблон IP-адреса, определяющий доверенную сеть. Здесь можно указать и конкретный IP-адрес, если список используется в том числе и для автоматической авторизации пользователей. |
| 2 | **REPLY_TEXT** | Текст индивидуального приветствия, подставляемый в ответы сервера при подключении пользователей из этой доверенной сети. |
| 3 | **USER** | Имя учётной записи (логин) и домен авторизации пользователя (в виде **логин@домен**), используемые при IP-авторизации. Если задано только имя учётной записи, считается, что авторизация выполняется в домене по умолчанию. Вообще-то для протокола FTP авторизация по IP-адресу большого смысла не имеет, поскольку по стандарту клиент должен авторизоваться на сервере явно, что перебивает все выполненные ранее настройки. Тем не менее, в текущей реализации действует следующее соглашение - если была выполнена авторизация по IP-адресу, а явная авторизация выполняется от имени гостя (с использованием специального имени учётной записи **anonymous** или **ftp**), сохраняются реквизиты, присвоенные при IP-авторизации. Если это поле не заполнено, IP-авторизация по этой строке списка не выполняется. |
| 4 | **MAX_MSG_SIZE** | Для FTP-сервера этот параметр не имеет смысла и оставлен для сохранения единого формата списков. |
| 5 | **FLAGS** | Строка флагов-признаков для сети:<br>**I** (Interhost) - разрешает режим межузловой передачи данных;<br>**D** (Disable interhost) - запрещает режим межузловой передачи данных. |

### *Список запрещённых сетей*

Это список IP-адресов и подсетей, которым запрещено обращаться к FTP-серверу.

Расположение списка задаётся параметром **FTP[IpBlackList]**, исходное - **CONF\lists\ftp\IpBlackList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **IP_MASK** | Шаблон IP-адреса, определяющий запрещённую сеть. |

| | | |
|---|---|---|
| 2 | **REPLY_TEXT** | Индивидуальный текст ответа сервера, поясняющий причину отказа. |
| 3 | **FLAGS** | Строка флагов-признаков для сети. Для FTP-сервера этот параметр не имеет смысла и оставлен для сохранения единого формата списков. |

### *Список управления привязкой IP-адресов*

Особенность протокола FTP заключается в том, что для обмена данными (загрузка файла или чтение FTP-каталога) требуется установить дополнительное соединение. При этом одна из сторон сообщает свой IP-адрес. FTP-сервер может оказаться такой стороной, если клиент выбрал пассивный режим соединения. Обычно он самостоятельно определяет адрес для объявления, однако при некоторых конфигурациях сети (например, наличие NAT-сервера), он может выбрать неверное значение - просто потому, что реальный адрес, видимый со стороны клиента, отличается от адреса сетевого интерфейса и FTP-серверу неизвестен. Если IP-адрес клиента не принадлежат локальной сети, FTP-сервер использует адрес, определённый параметром **Server[ExternIP]**. В базовых конфигурациях, когда имеется всего две сетевые карты, одна из которых подключена к локальной сети, а вторая обеспечивает непосредственный выход в глобальную сеть, этого достаточно. Если сетевых интерфейсов больше двух либо используются сложные правила маршрутизации, необходимы сложные же правила выбора объявляемого IP-адреса, записываемые в список управления привязкой.

Расположение списка задаётся параметром **FTP[BindIpList]**, исходное - **CONF\lists\ftp\BindIpList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **INTERFACE** | Шаблон IP-адреса сетевого интерфейса, на который принимается подключение. |
| 2 | **HOST** | Шаблон IP-адреса клиента, от которого принимается подключение. |
| 3 | **BIND_IP** | IP-адрес, который в этом случае следует сообщить клиенту. |

### *Список виртуальных каталогов FTP-сервера*

Этот список определяет, как выполняется отображение логического пути к объекту, переданного в запросе клиента, на физические каталоги сервера. Отображение может зависеть от множества параметров. Обычно в качестве ключевых параметров используются IP-адрес клиента, реквизиты авторизации пользователя, фрагмент пути к запрашиваемому объекту. Сопоставляя эти и другие параметры запроса с содержимым списка, сервер определяет физический каталог, в котором следует искать запрашиваемый объект.

Расположение списка задаётся параметром **FTP[VirtualFolders]**, исходное - **CONF\lists\ftp\VirtualFolders.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **IP** | Шаблон IP-адреса сетевого интерфейса, к которому подключился клиент. В шаблоне допускается использование символов групповой операции ***** и **?**. Если поле пустое, то допустимым считается любой интерфейс. |
| 2 | **USER** | Пользователь, к которому относится эта строка. Если поле пустое, то его проверка не производится. Если поле содержит символ звёздочки *****, то строка считается относящейся к любому авторизованному пользователю, не являющемуся гостем. Если поле содержит символ минуса **-**, то строка относится только к гостевым сессиям. Любое другое содержимое рассматривается как шаблон сравнения, могущий содержать символы групповой операции ***** и **?**. FTP-сервер ожидает задания полного имени пользователя в формате **логин@домен**; если же домен не задан, считается, что искомый пользователь авторизуется в домене по умолчанию. |
| 3 | **GROUP** | Имя группы пользователей, к которой относится эта строка. В зависимости от наличия поддержки расширенной группировки оно может быть задано по-разному. Если расширенная группировка не применяется, то считается, что группа относится к тому же домену авторизации, что и входящий в неё пользователь. В противном случае FTP-сервер ожидает задания полного имени группы в формате **группа@домен**; если же домен не указан, считается, что проверяемая группа принадлежит домену по умолчанию. Если поле пустое, членство пользователя в группе не проверяется. Если сессия неавторизованная или гостевая, она не относится ни к одной группе пользователей. |

| | | |
|---|---|---|
| 4 | **URI** | Шаблон логического пути к запрашиваемому объекту. Здесь использование символов групповой операции не допускается. Проверяется совпадение части пути, переданного в запросе, с содержимым поля, причём совпавшая часть должна быть выровнена влево. Например, если запрашиваемый объект **/Elog/cgi-bin/Elog.cgi**, то совпадение будет зафиксировано с шаблонами **/Elog/** и **/Elog/cgi-bin/**, но не с шаблоном **/cgi-bin/**. Необходимо учитывать, что логический путь всегда является абсолютным, то есть, начинается с разделителя каталогов **/**, - соответственно, шаблон тоже должен начинаться с этого символа. Если совпадение фиксируется в нескольких строках, сервер выбирает строку с наиболее длинным шаблоном. Если поле пустое, то совпавшим считается любой запрошенный путь. |
| 5 | **RULE** | Дополнительное условие, записанное на языке Форт. Это условие должно вернуть на стеке единственное значение, которое будет интерпретироваться как логическое - ноль означает, что совпадение условий по этой строке не выявлено (ложь), любое другое значение - совпадение всех условий (истина). Перечень базовых правил, которые можно использовать при написании составного правила, приведён в приложении 2. Если поле пустое, считается, что правило вернуло истину. |
| 6 | **ROOTPATH** | Физический каталог сервера, в котором будет выполняться поиск запрашиваемого объекта, - корневой каталог отображения. При задании параметра допускается использование макроподстановок (**{}**). |
| 7 | **VIRTUAL** | Признак виртуального корня. Обычно логический путь к объекту без преобразования состыковывается с корневым каталогом, образуя полный физический путь. Если в этом поле находится ненулевое значение, с корневым каталогом состыковывается не совпавший с содержимым поля **URI** остаток логического пути. |
| 8 | **REPLACE** | Если это поле не пустое, то над логическим путём выполняется дополнительное преобразование - совпавшая с содержимым поля **URI** часть заменяется содержимым данного поля. При задании параметра допускается использование макроподстановок (**{}**). |

Список всегда просматривается полностью, в процессе просмотра сервер ищет наилучшее совпадение, то есть, строку, в которой совпавший логический путь (**URI**) имеет наибольшую длину.

### *Список управления доступом к FTP-серверу*

На основании анализа этого списка сервер определяет возможность выполнения запроса. Во избежание дурной множественности объектом, для которого назначаются права, является физический путь к файлу на диске.

Расположение списка задаётся параметром **FTP[ACL]**, исходное - **CONF\lists\ftp\ACL.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **PATH** | Шаблон физического пути к запрашиваемому объекту. Здесь использование символов групповой операции не допускается. Проверяется совпадение части пути, переданного в запросе, с содержимым поля, причём совпавшая часть должна быть выровнена влево. Например, если запрашиваемый объект **..\Elog\cgi-bin\Elog.cgi**, то совпадение будет зафиксировано с шаблонами **..\Elog** и **..\Elog\cgi-bin**, но не с шаблоном **..\cgi-bin** или **\cgi-bin**. Следует учесть, что сервер не выполняет приведение пути к единому унифицированному формату. **..\Elog\cgi-bin** и **C:\Eserv3\Elog\cgi-bin** считаются разными путями, даже если они на самом деле указывают на один каталог; поэтому для заполнения списка виртуальных каталогов следует принять один из вариантов записи путей в качестве стандарта и в дальнейшем всегда его придерживаться. Если совпадение фиксируется в нескольких строках, сервер выбирает строку с наиболее длинным шаблоном. Если строк с одинаковым шаблоном несколько, сервер суммирует права, назначенные этими строками. Если поле пустое, то совпавшим считается любой путь. |
| 2 | **USER** | Пользователь, к которому относится эта строка. Если поле пустое, то его проверка не производится. Если поле содержит символ звёздочки *****, то строка считается относящейся к любому авторизованному пользователю. Если поле содержит символ минуса **-**, то строка относится только к гостевым сессиям. Любое другое содержимое рассматривается как шаблон сравнения, могущий содержать символы групповой операции ***** и **?**. FTP-сервер ожидает задания полного имени пользователя в формате **логин@домен**; если же домен не задан, считается, что искомый пользователь авторизуется в домене по умолчанию. |

| | | |
|---|---|---|
| 3 | **GROUP** | Имя группы пользователей, к которой относится эта строка. В зависимости от наличия поддержки расширенной группировки оно может быть задано по-разному. Если расширенная группировка не применяется, то считается, что группа относится к тому же домену авторизации, что и входящий в неё пользователь. В противном случае FTP-сервер ожидает задания полного имени группы в формате **группа@домен**; если же домен не указан, считается, что проверяемая группа принадлежит домену по умолчанию. Если поле пустое, членство пользователя в группе не проверяется. Если сессия неавторизованная или гостевая, она не относится ни к одной группе пользователей. |
| 4 | **TIME** | Момент или интервал времени, определяемый с точностью до минуты, к которому относится эта строка. Момент задаётся в виде **чч:мм**, интервал - в виде **чч:мм-чч:мм**. Если поле пустое, то проверка условия не производится. |
| 5 | **RULE** | Дополнительное условие, записанное на языке Форт. Это условие должно вернуть на стеке единственное значение, которое будет интерпретироваться как логическое - ноль означает, что совпадение условий по этой строке не выявлено (ложь), любое другое значение - совпадение всех условий (истина). Перечень базовых правил, которые можно использовать при написании составного правила, приведён в приложении 2. Если поле пустое, считается, что правило вернуло истину. |
| 6 | **ACCESS** | Код прав доступа, назначаемых при выявлении совпадения. Это может быть либо число, либо специальный символьный код. Число является суммой кодов следующих элементарных прав:<br>**1** - право выполнения файлов (для FTP-сервера смысла не имеет);<br>**2** - право создания и записи файлов;<br>**4** - право чтения файлов;<br>**8** - право чтения оглавления каталогов;<br>**16** - право удаления файлов и подкаталогов.<br>Перечень символьных кодов приведён в приложении 1. |
| 7 | **FORBIDDEN** | Если этот флаг имеет ненулевое значение, то при недостатке прав доступа к объекту сервер ответит жёстким бескомпромиссным отказом. Если значение нулевое, отказ будет тоже безусловным, но сервер при этом сообщит имя зоны безопасности (Realm), в которой находится запрашиваемый объект. |
| 8 | **REALM** | Имя зоны безопасности (Realm), которое следует указать в ответе сервера, если это разрешено. При задании параметра допускается использование макроподстановок (**{}**). |

Список просматривается сверху вниз. В процессе просмотра сервер ищет наилучшее совпадение, то есть, строку, в которой совпавший физический путь (**PATH**) имеет наибольшую длину. В начале просмотра эта длина нулевая, права доступа, имя зоны безопасности и флаг жёсткого отказа имеют значения по умолчанию, определённые в конфигурационном файле параметрами **FTP[DefaultAccess]** (или, в случае гостевого входа, **FTP[DefaultGuestAccess]**), **FTP[DefaultRealm]** и **FTP[DefaultForbiddenFlag]** соответственно. При обнаружении совпадения физического пути и поля **PATH** сервер сравнивает длину шаблона в текущей строке и длину ранее зафиксированного совпадения. Если шаблон в текущей строке короче, строка пропускается. Если текущий шаблон длиннее, то права доступа сбрасываются в состояние запрета, одновременно фиксируются новые значения для имени зоны безопасности и признака жёсткого отказа. Также фиксируется новая длина совпавшего шаблона. Далее - независимо от того, длиннее текущий шаблон или совпадает с уже зафиксированным - проверяются прочие условия, и при их выполнении заданные в строке права доступа добавляются (посредством побитовой операции ИЛИ) к текущему значению. Таким образом, имя зоны безопасности и признак жёсткого отказа всегда определяются самой верхней строкой, давшей наилучшее совпадение пути. Это следует учитывать при назначении прав различным пользователям и группам пользователей (то есть, с использованием нескольких строк, имеющих одинаковое значение в поле **PATH**) на один и тот же каталог или файл.

Список всегда просматривается до конца. Для повышения быстродействия рекомендуется отсортировать его в виде "опрокинутого" дерева каталогов - так, чтобы самые длинные шаблоны были в верхней части списка.

## *Управляющие списки межсетевого экрана*

Эти списки предназначены для управления межсетевым экраном, их исходное расположение, определяемое параметром **FireWall[Lists]**, - каталог **CONF\lists\firewall**.

### *Список защищаемых сетевых интерфейсов*

В этом списке перечислены защищаемые сетевые интерфейсы сервера.

Расположение списка задаётся параметром **FireWall[NetworkInterfaceList]**, исходное - **CONF\lists\firewall\InterfaceList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **INTERFACE** | IP-адрес защищаемого сетевого интерфейса. |

### *Список правил блокировки пакетов*

В этом списке перечислены нестандартные правила фильтрации (блокировки) IP-пакетов в зависимости от IP-адреса и порта источника и адресата.

Расположение списка задаётся параметром **FireWall[BlockList]**, исходное - **CONF\lists\firewall\BlockList.txt**. Назначение полей:

| | | |
|---|---|---|
| 1 | **FROMHOST** | IP-адрес источника блокируемых пакетов. Это может быть как конкретный адрес, так и групповой адрес подсети. |
| 2 | **FROMMASK** | Маска подсети источника блокируемых пакетов. Нулевая маска в сочетании с нулевым адресом (0.0.0.0 0.0.0.0) означает любой сетевой адрес. |
| 3 | **FROMPORT** | Порт источника блокируемых пакетов. Ноль означает любой порт. |
| 4 | **TOHOST** | IP-адрес адресата блокируемых пакетов. Это может быть как конкретный адрес, так и групповой адрес подсети. |
| 5 | **TOMASK** | Маска подсети адресата блокируемых пакетов. Нулевая маска в сочетании с нулевым адресом (0.0.0.0 0.0.0.0) означает любой сетевой адрес. |
| 6 | **TOPORT** | Порт адресата блокируемых пакетов. Ноль означает любой порт. |
| 7 | **PROTO** | Тип блокируемого протокола:<br>**ANY** - протокол любого типа (полная блокировка);<br>**ICMP** - протоколы класа Internet Control Message Protocol (этот класс протокола используется утилитами ping и tracert);<br>**TCP** - протоколы класса TCP (все протоколы на основе сессий - HTTP, FTP, SMTP и т.п.);<br>**UDP** - протоколы класса User Datagram Protocol. |

Задавать правила с указанием протоколов **ICMP** и **ANY** следует с большой осторожностью. Дело в том, что протокол ICMP не признаёт такого понятия, как порт. В результате правило, использующее собирательный протокол ANY, блокирует любые соединения между источником и приёмником. Если требуется избирательная блокировка порта, лучше написать несколько отдельных правил для каждого конкретного протокола.

# Шаблоны

Шаблоны представляют собой ещё один инструмент для тонкой настройки поведения сервера. На основании шаблонов автоматически формируются извещения о доставке письма и о поимке вируса, шаблоны также можно использовать для изменения ответов на различные команды протокола. Изначально предполагается, что все шаблоны располагаются в каталоге **CONF\templates**, что определяется параметром **Dirs[Templates]**.

## *Шаблоны SMTP-сервера*

Шаблоны SMTP-сервера изначально располагаются в каталоге **CONF\templates\smtp**, что определяется параметром **SMTP[Templates]**.

### *Шаблон ответа сервера при подключении клиента*

Файл шаблона **OnThreadConnect.pat.txt** задаёт идентификатор сервера, подставляемый во все варианты положительных (означающих, что подключение принимается) ответов.

### *Шаблоны ответа на команду EHLO*

Команда **EHLO** означает, что почтовый клиент использует расширенную версию протокола SMTP - Enhanced SMTP, или ESMTP. В этом случае, в соответствии с описанием протокола, сервер должен в ответе перечислить поддерживаемые им расширения протокола. Полный перечень содержится в файле шаблона **EHLO.orig.pat.txt**, который в PigMail+PigProxy не используется и оставлен "к сведению". Реально используется шаблон **EHLO.pat.txt**, из которого исключены динамически подставляемые расширения **SIZE**, **CHUNKING**, **STARTTLS** и **PIPELINING**. Первое расширение либо подставляется, либо нет, в зависимости от действующего ограничения на размер письма, остальные - в зависимости от настроек сервера, заданных параметрами **SMTP[UseChunking]**, **SMTP[UseStartTLS]** и **SMTP[UsePipelining]**.

### *Шаблоны добавляемых заголовков писем*

Стандарт рекомендует, чтобы каждый почтовый сервер на пути прохождения письма поставил на нём свой "штемпель", - это позволяет проследить маршрут следования письма. Отметки добавляются в шапку письма в виде служебных полей-заголовков. Какими будут эти заголовки и какая информация будет в них записана, определяется целым набором шаблонов.

**Pop3ReceivedHeader.pat.txt** определяет содержимое заголовка **Received:** (стандарт требует обязательного добавления этого заголовка) при доставке письма из внешнего POP-ящика посредством загрузчика **Pop3Recv**.

**SmtpReceivedHeader.pat.txt** определяет содержимое заголовка **Received:** при стандартной доставке письма по протоколу SMTP.

**LocalReceivedHeader.pat.txt** определяет содержимое заголовка **Received:** при доставке письма в обход протокола SMTP сервисом локальной доставки.

**ReceivedLspHeader.pat.txt** определяет формат и содержимое дополнительного заголовка, в который записывается результат проверки локальных политик для отправителя.

**ReceivedSpfHeader.pat.txt** определяет формат и содержимое дополнительного заголовка, в который записывается результат проверки адреса отправителя на основании глобальных политик - посредством Sender Policy Framework.

**X-MailServerHeader.pat.txt** определяет формат и содержимое дополнительного необязательного так называемого X-заголовка - исходное содержимое шаблона добавляет сразу два таких заголовка. На самом деле этот шаблон не применяется: строка файла правил, задающая его использование, закомментирована.

Любой заголовок можно исключить, удалив содержимое соответствующего шаблона, - при этом файл шаблона будет иметь нулевой размер.

### *Шаблон извещения о доставке письма*

Почтовый клиент имеет возможность запросить подтверждение о доставке письма получателю. Для этого в поле заголовка письма **Return-Receipt-To** указывается адрес, по которому следует отправить подтверждение. Если установлен глобальный флаг **SMTP[SendReturnReceipts]**, сервер будет автоматически формировать письма-извещения для отправки на этот адрес. Шаблон для формирования такого извещения задаётся параметром **SMTP[ReturnReceiptsNotification]**, изначально он именуется **ReturnReceipt.pat.txt**.

### *Шаблоны индивидуальных автоответов*

Каждому локальному получателю можно при необходимости сопоставить автоответчик. Эта возможность полезна на случай отъезда или длительного отсутствия по другой причине, а также если время ответа может быть критично. Имя файла шаблона для каждого автоответчика задаётся индивидуально в списке ав-

тоответчиков. Пример такого шаблона именуется **AutoReplyVacation.pat.txt** - он как раз повествует о пребывании получателя в отпуске. Ещё один шаблон **DkTest.pat.txt** предназначен для удалённого тестрования настроек Yahoo Domain Keys - с его использованием робот-автоответчик передаёт отправителю подписанного письма результат проверки подписи и всю необходимую для поиска ошибок в настройках информацию.

### *Шаблоны индивидуальных извещений о поступлении почты*

При необходимости каждого локального получателя можно извещать (обычно отправкой сообщения на сотовый телефон) о поступлении нового письма. Эта возможность полезна для сотрудников, проводящих много времени в некотором отдалении от рабочего места, но тем не менее обязанных оперативно реагировать на все поступающие сообщения, - например, для системных администраторов. Имя файла шаблона извещения задаётся индивидуально в списке извещений. Пример такого шаблона именуется **SampleNotification.pat.txt**.

### *Шаблоны извещений о поимке вируса и сбоях в работе антивируса*

Обнаружение вируса в полученном письме - это событие, требующее быстрой реакции. Отправитель, если это не почтовый червь, рассылающий себя в обход стандартных путей, получит извещение от своего почтового клиента либо основного почтового сервера, поскольку SMTP-сервер откажется принять такое письмо. Остаётся выбор - извещать или нет о предотвращении атаки получателей и администратора сервера. Извещение для получателей формируется на основании шаблона, изначально именуемого **OnVirus.pat.txt** (это задаётся параметром **SMTP[OnVirusGeneralNotification]**), если установлен глобальный флаг **SMTP[SendVirusNotify]**. Для извещения администратора необходимо указать его адрес в параметре **SMTP[AdminVirusNotifyEmail]** и задать ненулевое значение параметра **SMTP[SendAdminVirusNotify]**, в этом случае извещение будет формироваться на основании шаблона, задаваемого параметром **SMTP[OnVirusAdminNotification]**; изначально он именуется **OnVirusAdmin.pat.txt**. Если вирус обнаружен противоспамными фильтрами, то для извещения получателей используется шаблон, определяемый параметром **Antispam[OnVirusGeneralNotification]** (изначально - **OnSpamVirus.pat.txt**), а для извещения администратора - шаблон, определяемый параметром **Antispam[OnVirusAdminNotification]** (изначально - **OnSpamVirusAdmin.pat.txt**).

Кроме обнаружения вирусов, иногда происходят и сбои в работе антивируса. Это столь же критическая ситуация, требующая максимально быстрого вмешательства. Извещение для получателей формируется на основании шаблона, изначально именуемого **OnVError.pat.txt** (это задаётся параметром **SMTP[OnVErrorGeneralNotification]**), если установлен глобальный флаг **SMTP[SendVirusNotify]**. Для извещения администратора необходимо указать его адрес в параметре **SMTP[AdminVirusNotifyEmail]** и задать ненулевое значение параметра **SMTP[SendAdminVirusNotify]**, в этом случае извещение будет формироваться на основании шаблона, задаваемого параметром **SMTP[OnVErrorAdminNotification]**; изначально он именуется **OnVErrorAdmin.pat.txt**.

Помимо основных шаблонов для формирования извещений также используются субшаблоны - механизм, позволяющий с минимальными усилиями включать в сообщения фрагменты, соответствующие актуальным настройкам сервера. Выбор включаемых субшаблонов осуществляется по специальному списку, расположение которого задаётся параметром **SMTP[InfectedFileNameAddOns]**. В качестве работающего примера в PigMail+PigProxy включены следующие субшаблоны:

| Имя файла | Назначение |
|---|---|
| **InfectedFileNameRcptKoi.pat.txt** | Подставляет имя сохранённого в карантине файла заражённого письма и необходимые пояснения в русскоязычную часть извещения, предназначенного для потенциальных получателей вируса. Главный шаблон **OnVirus.pat.txt** подготовлен в кодировке KOI-8R. |
| **FileDeletedRcptKoi.pat.txt** | Подставляет сообщение о том, что в соответствии с настройками сервера заражённое письмо удалено, в русскоязычную часть извещения, предназначенного для потенциальных получателей вируса. Главный шаблон **OnVirus.pat.txt** подготовлен в кодировке KOI-8R. |
| **InfectedFileNameRcptEng.pat.txt** | Подставляет имя сохранённого в карантине файла заражённого письма и необходимые пояснения в англоязычную часть извещения, предназначенного для потенциальных получателей вируса. |
| **FileDeletedRcptEng.pat.txt** | Подставляет сообщение о том, что в соответствии с настройками сервера заражённое письмо удалено, в англоязычную часть извещения, предназначенного для потенциальных получателей вируса. |

| | |
|---|---|
| **InfectedFileNameAdminWin.pat.txt** | Подставляет имя сохранённого в карантине файла заражённого письма и необходимые пояснения в извещение, предназначенное для администратора. Главный шаблон **OnVirusAdmin.pat.txt** подготовлен в кодировке Windows-1251. |
| **FileDeletedAdminWin.pat.txt** | Подставляет сообщение о том, что в соответствии с настройками сервера заражённое письмо удалено, в извещение, предназначенное для администратора. Главный шаблон **OnVirusAdmin.pat.txt** подготовлен в кодировке Windows-1251. |

### *Шаблон извещения о превышении квоты*

При необходимости получателей можно извещать о том, что их почтовые ящики неприлично распухли, превысив установленные ограничения на общий объём и количество писем, и часть почты в результате потеряна. Если установлен флаг **SMTP[QuotaExceedNotify]**, в почтовый ящик нерадивого получателя помещается специальное письмо-уведомление, формируемое на основании описываемого шаблона. Расположение шаблона задаётся параметром **SMTP[QuotaExceedNotification]**, изначально он именуется **QuotaExceeded.pat.txt**.

### *Шаблон административного оповещения о недоставке почты*

При необходимости администратора можно извещать о каждом случае недоставки почты по назначению - начиная от отказа в приёме подключения на основании IP-адреса клиента и заканчивая задержанием уже принятого письма различными фильтрами. Это извещение генерируется на основании описываемого шаблона. Расположение шаблона задаётся параметром **SMTP[OnAlertNotification]**, изначально он именуется **OnAlertNotification.pat.txt**. Для загрузчика внешней POP-почты Pop3Recv расположение задаётся параметром **Pop3Recv[OnAlertNotification]**, что при необходимости позволяет задать особый шаблон, но изначально используется тот же шаблон, что и для SMTP-сервиса.

## *Шаблоны расширенного сервиса доставки исходящей почты SmtpSend*

Шаблоны расширенного сервиса доставки исходящей почты SmtpSend изначально располагаются в каталоге **CONF\templates\smtpsend**, что определяется параметром **SmtpSend[Templates]**.

### *Шаблон письма-возврата*

Этот шаблон является основой для формирования извещения о фатальной невозможности доставки письма одному или нескольким адресатам. Изначально этот шаблон именуется **ReturnNotification.pat.txt**, что определяется параметром **SmtpSend[ReturnNotification]**.

### *Шаблон письма-предупреждения*

Этот шаблон является основой для формирования извещения о временной невозможности доставки письма одному или нескольким адресатам в течение времени, отведённого для нахождения письма в очереди повторной отправки. Изначально этот шаблон именуется **RetryNotification.pat.txt**, что определяется параметром **SmtpSend[RetryNotification]**.

## *Шаблоны POP-сервера*

Шаблоны POP-сервера изначально располагаются в каталоге **CONF\templates\pop**, что определяется параметром **POP[Templates]**.

### *Шаблон ответа сервера при подключении клиента*

Файл шаблона **OnThreadConnect.pat.txt** задаёт идентификатор сервера, подставляемый во все варианты положительных (означающих, что подключение принимается) ответов.

## *Шаблоны IMAP-сервера*

Шаблоны IMAP-сервера изначально располагаются в каталоге **CONF\templates\imap**, что определяется параметром **IMAP[Templates]**.

### *Шаблон ответа сервера при подключении клиента*

Файл шаблона **OnThreadConnect.pat.txt** задаёт идентификатор сервера, подставляемый во все варианты положительных (означающих, что подключение принимается) ответов.

## *Общие шаблоны прокси-сервера*

Для размещения шаблонов прокси-сервера изначально отведён базовый каталог **CONF\templates\proxy**, расположение которого задаётся параметром **PROXY[Templates]**. В настоящей версии общих для прокси-сервера в целом шаблонов нет. Шаблоны отдельных служб прокси-сервера изначально располагаются в подкаталогах базового каталога.

## *Шаблоны HTTP-прокси-сервера*

Шаблоны HTTP-прокси-сервера изначально располагаются в каталоге **CONF\templates\proxy\httpp**, что определяется параметром **HttpProxy[Templates]**.

### *Шаблоны стандартных ответов*

Эти шаблоны отвечают за формирование ответов сервера (в основном, в виде HTML-страниц), возвращаемых вместо запрошенных объектов при возникновении различных предусмотренных ситуаций. Ответы можно условно разделить на языкозависимые, то есть, содержащие текстовую информацию (неважно, в текстовом формате или в виде изображения), и нейтральные. Последние располагаются непосредственно в каталоге, предназначенном для размещения шаблонов. Для языкозависимых шаблонов предназначены подкаталоги, соответствующие языкам, которые поддерживаются прокси-сервером. Язык, на котором следует отвечать, определяется сервером на основании настроек клиента (браузера), передаваемых в запросе в виде дополнительной информации. Текущая версия распознаёт следующие языки:

- Английский. Подкаталог шаблонов - **en**. Это язык по умолчанию, он применяется, если сервер не может определить язык клиента или шаблон ответа на языке клиента отсутствует;
- Русский. Подкаталог шаблонов - **ru**;
- Немецкий. Подкаталог шаблонов - **de**;
- Французский. Подкаталог шаблонов - **fr**;
- Испанский. Подкаталог шаблонов - **es**;
- Итальянский. Подкаталог шаблонов - **it**.

В настоящее время в поставку входят шаблоны на русском и английском языках. В текущей версии предусмотрены следующие шаблоны:

| Имя файла | Назначение |
|---|---|
| **blank.gif** | Нейтральный шаблон. Прозрачное GIF-изображение размером 1x1 точку, передаваемое в качестве заменителя при блокировке рекламы. Это действие предусмотрено в списке стандартных ответов сервера (код **ADV_BLOCK**). Используется при активированном плагине поддержки списков управления доступом **acl**. |
| **empty.swf** | Нейтральный шаблон. Пустой ролик Macromedia Flash, передаваемый в качестве заменителя при блокировке рекламы, если запрашиваемый объект имеет расширение **.SWF**. Это действие предусмотрено в списке стандартных ответов сервера (код **ADVS_BLOCK**). Используется при активированном плагине поддержки списков управления доступом **acl**. |
| **adv_block.html** | Языкозависимый текстовый шаблон. Передаётся при блокировке рекламы, если используется туннельное подключение по методу CONNECT. Здесь подмена вывода невозможна, единственный вариант - передача HTML-страницы с текстом отказа. Это действие предусмотрено в списке стандартных ответов сервера (код **ADVC_BLOCK**). Используется при активированном плагине поддержки списков управления доступом **acl**. |
| **CanalKitBlocked2.html** | Языкозависимый текстовый шаблон. Передаётся при исчерпании выделенной пользователю квоты. Это действие не предусмотрено в списке стандартных ответов сервера, поэтому имя, формат и расположение шаблона не могут быть изменены. Используется при активированном плагине поддержки управления трафиком **TrafC**. |
| **connect_error2.html** | Языкозависимый текстовый шаблон. Передаётся при невозможности соединения с внешним сервером и содержит описание возникшей проблемы. Это действие не предусмотрено в списке стандартных ответов сервера, поэтому имя, формат и расположение шаблона не могут быть изменены. |
| **disabled.html** | Языкозависимый текстовый шаблон. Передаётся в ситуациях, когда доступ к прокси-серверу жёстко и безусловно запрещён. Это действие предусмотрено в списке стандартных ответов сервера (код **DISABLED**). |

| | |
|---|---|
| **forbidden.html** | Языкозависимый текстовый шаблон. Передаётся в ситуациях, когда доступ к прокси-серверу запрещён на основании списков управления доступом. Это действие предусмотрено в списке стандартных ответов сервера (код **TCP_DISABLED**). Используется при активированном плагине поддержки списков управления доступом **acl**. |
| **localredirect.html** | Языкозависимый текстовый шаблон. Передаётся при перенаправлении клиента на локально размещённую HTML-страницу (HTTP-прокси способен исполнять роль простейшего web-сервера). Это действие предусмотрено в списке стандартных ответов сервера (код **LOCAL-REDIRECT**). |
| **notfound.html** | Языкозависимый текстовый шаблон. Передаётся в ситуации, когда HTTP-прокси не обнаружил запрошенную локальную web-страницу. Это действие предусмотрено в списке стандартных ответов сервера (код **NOT-FOUND**). |
| **readheaders_error2.html** | Языкозависимый текстовый шаблон. Передаётся в ситуации, когда соединение с внешним сервером удалось, но при чтении заголовков ответа произошла ошибка. Содержит описание возникшей проблемы. Это действие не предусмотрено в списке стандартных ответов сервера, поэтому имя, формат и расположение шаблона не могут быть изменены. |
| **redirect.html** | Языкозависимый текстовый шаблон. Передаётся при перенаправлении клиента на внешний ресурс с использование алиасинга или обычного перенаправителя. Эти действия предусмотрены в списке стандартных ответов сервера (коды **HTTP-ALIAS** и **HTTP-REDIRECT**). Используется при активированных плагинах-перенаправителях **alias** и **redirect**. |
| **send_request_error2.html** | Языкозависимый текстовый шаблон. Передаётся в ситуации, когда соединение с внешним сервером удалось, но при передаче запроса произошла ошибка. Содержит описание возникшей проблемы. Это действие не предусмотрено в списке стандартных ответов сервера, поэтому имя, формат и расположение шаблона не могут быть изменены. |
| **tempdown.html** | Языкозависимый текстовый шаблон. Передаётся в ситуации, когда работа прокси-сервера временно заблокирована установкой параметра **HttpProxy[Active]** в ноль. Это действие не предусмотрено в списке стандартных ответов сервера, поэтому имя, формат и расположение шаблона не могут быть изменены. |
| **unauthorized.html** | Языкозависимый текстовый шаблон. Передаётся при запросе авторизации на прокси-сервере, если того потребуют списки управления доступом. Это действие предусмотрено в списке стандартных ответов сервера (код **TCP_DENIED**). Используется при активированном плагине поддержки списков управления доступом **acl**. |
| **unknown_method.html** | Языкозависимый текстовый шаблон. Передаётся в ситуации, когда клиент запросил операцию, не поддерживаемую прокси-сервером. Содержит описание проблемы и рекомендацию обратиться к разработчикам. Это действие предусмотрено в списке стандартных ответов сервера (код **UNKNOWN-METHOD**). |
| **unknown_protocol.html** | Языкозависимый текстовый шаблон. Передаётся в ситуации, когда клиент запросил доступ по протоколу, не поддерживаемому прокси-сервером. Содержит описание проблемы и рекомендацию обратиться к разработчикам. Это действие не предусмотрено в списке стандартных ответов сервера, поэтому имя, формат и расположение шаблона не могут быть изменены. |

### *Таблица HTML-стилей стандартных ответов*

К стандартным ответам относится также таблица HTML-стилей, по умолчанию включаемая в каждый ответ HTML-формата. Путём редактирования стилей можно легко изменять внешний вид ответов, не затрагивая их содержимого. Изначально файл таблицы стилей именуется **LocalReplyStyles.css** и располагается в каталоге **CONF\templates\proxy\httpp**, что определяется параметром **HttpProxy[LocalReplyStyles]**.

### *Шаблоны расшифровки ошибок WinSock*

Это специфический набор шаблонов, включаемых в некоторые стандартные ответы для пояснения сути зафиксированной сетевой ошибки. Эти шаблоны размещаются в подкаталоге **errors** каталога шаблонов HTTP-прокси - изначально это **CONF\templates\proxy\httpp\errors**. Все они являются языкозависимыми, поэтому распределены по дополнительным подкаталогам, соответствующим языкам, которые поддержива-

ются прокси-сервером. Язык, на котором следует отвечать, определяется сервером на основании настроек клиента (браузера), передаваемых в запросе в виде дополнительной информации. Текущая версия распознаёт следующие языки:

- Английский. Подкаталог шаблонов - **en**. Это язык по умолчанию, он применяется, если сервер не может определить язык клиента или шаблон ответа на языке клиента отсутствует;
- Русский. Подкаталог шаблонов - **ru**;
- Немецкий. Подкаталог шаблонов - **de**;
- Французский. Подкаталог шаблонов - **fr**;
- Испанский. Подкаталог шаблонов - **es**;
- Итальянский. Подкаталог шаблонов - **it**.

В настоящее время в поставку входят шаблоны на русском и английском языках. Имена файлов шаблонов имеют вид **nnnnn.html**, где **nnnnn** означает числовой код сетевой ошибки.

## *Шаблоны FTP-прокси-сервера*

Шаблоны FTP-прокси-сервера изначально располагаются в каталоге **CONF\templates\proxy\ftpp**, что определяется параметром **FtpProxy[Templates]**.

### *Шаблон ответа сервера при подключении клиента*

Файл шаблона **OnThreadConnect.pat.txt** задаёт идентификатор сервера, подставляемый во все варианты положительных (означающих, что подключение принимается) ответов.

## *Шаблоны POP3-прокси-сервера*

Шаблоны POP3-прокси-сервера изначально располагаются в каталоге **CONF\templates\proxy\pop3p**, что определяется параметром **Pop3Proxy[Templates]**.

### *Шаблон ответа сервера при подключении клиента*

Файл шаблона **OnThreadConnect.pat.txt** задаёт идентификатор сервера, подставляемый во все варианты положительных (означающих, что подключение принимается) ответов.

## *Шаблоны HTTP-сервера*

Шаблоны HTTP-сервера изначально располагаются в каталоге **CONF\templates\http**, что определяется параметром **HTTP[Templates]**.

### *Шаблоны стандартных ответов*

Эти шаблоны отвечают за формирование ответов сервера (в основном, в виде HTML-страниц), возвращаемых вместо запрошенных объектов при возникновении различных предусмотренных ситуаций. Ответы можно условно разделить на языкозависимые, то есть, содержащие текстовую информацию (неважно, в текстовом формате или в виде изображения), и нейтральные. Последние располагаются (пока чисто теоретически) непосредственно в каталоге, предназначенном для размещения шаблонов. Для языкозависимых шаблонов предназначены подкаталоги, соответствующие языкам, которые поддерживаются HTTP-сервером. Язык, на котором следует отвечать, определяется сервером на основании настроек клиента (браузера), передаваемых в запросе в виде дополнительной информации. Текущая версия распознаёт следующие языки:

- Английский. Подкаталог шаблонов - **en**. Это язык по умолчанию, он применяется, если сервер не может определить язык клиента или шаблон ответа на языке клиента отсутствует;
- Русский. Подкаталог шаблонов - **ru**;
- Немецкий. Подкаталог шаблонов - **de**;
- Французский. Подкаталог шаблонов - **fr**;
- Испанский. Подкаталог шаблонов - **es**;
- Итальянский. Подкаталог шаблонов - **it**.

В настоящее время в поставку входят шаблоны на русском и английском языках. В текущей версии предусмотрены следующие шаблоны:

| Имя файла | Назначение |
|---|---|
| **action_failed.html** | Языкозависимый текстовый шаблон. Передаётся при обработке ошибки выполнения запроса в результате неверной настройки сервера. Это действие предусмотрено в списке стандартных ответов сервера (код **ERR_EACTION**). |

| | |
|---|---|
| **config_error.html** | Языкозависимый текстовый шаблон. Передаётся при обработке ошибки предварительной обработки запроса в результате неверной настройки сервера. Это действие предусмотрено в списке стандартных ответов сервера (код **ERR_ONREQ**). |
| **disabled.html** | Языкозависимый текстовый шаблон. Передаётся в ситуациях, когда доступ к HTTP-серверу жёстко и безусловно запрещён. Это действие предусмотрено в списке стандартных ответов сервера (код **DISABLED**). |
| **filename_error.html** | Языкозависимый текстовый шаблон. Передаётся, когда в результате неверной настройки сервера не удалось выполнить преобразование логического пути в физический. Это действие предусмотрено в списке стандартных ответов сервера (код **ERR_FILE**). |
| **forbidden.html** | Языкозависимый текстовый шаблон. Передаётся в ситуациях, когда доступ к HTTP-серверу запрещён на основании списка управления доступом. Это действие предусмотрено в списке стандартных ответов сервера (код **FORBIDDEN**). Используется при активированном плагине поддержки списка управления доступом **acl**. |
| **notfound.html** | Языкозависимый текстовый шаблон. Передаётся в ситуации, когда HTTP-сервер не обнаружил запрошенный объект. Это действие предусмотрено в списке стандартных ответов сервера (код **NOT_FOUND**). |
| **overload.html** | Языкозависимый текстовый шаблон. Передаётся в случае недопустимо высокой нагрузки на сервер - при слишком большом числе одновременных обращений (код **UNAVAILABLE**). |
| **redirect.html** | Языкозависимый текстовый шаблон. Передаётся при перенаправлении клиента на другой локальный или внешний ресурс. Это действие предусмотрено в списке стандартных ответов сервера (код **REDIRECT**). |
| **tempdown.html** | Языкозависимый текстовый шаблон. Передаётся в ситуации, когда работа HTTP-сервера временно заблокирована установкой параметра **HTTP[Active]** в ноль. Это действие не предусмотрено в списке стандартных ответов сервера, поэтому имя, формат и расположение шаблона не могут быть изменены. |
| **unauthorized.html** | Языкозависимый текстовый шаблон. Передаётся при запросе авторизации на HTTP-сервере, если того потребуют список управления доступом или обращение к разделам web-интерфейса Eserv. Это действие предусмотрено в списке стандартных ответов сервера (код **UNAUTHORIZED**). |
| **unknown_action.html** | Языкозависимый текстовый шаблон. Передаётся, когда в результате неверной настройки сервера не удалось определить способ выполнения запроса. Это действие предусмотрено в списке стандартных ответов сервера (код **ERR_ACTION**). |
| **unknown_method.html** | Языкозависимый текстовый шаблон. Передаётся в ситуации, когда клиент запросил операцию, не поддерживаемую HTTP-сервером. Содержит описание проблемы и рекомендацию обратиться к разработчикам. Это действие предусмотрено в списке стандартных ответов сервера (код **UNKNOWN_METHOD**). |
| **unknown_root.html** | Языкозависимый текстовый шаблон. Передаётся, когда в результате неверной настройки сервера не удалось определить корневой каталог сайта. Это действие предусмотрено в списке стандартных ответов сервера (код **ERR_ROOT**). |

### *Таблица HTML-стилей стандартных ответов*

К стандартным ответам относится также таблица HTML-стилей, по умолчанию включаемая в каждый ответ HTML-формата. Путём редактирования стилей можно легко изменять внешний вид ответов, не затрагивая их содержимого. Изначально файл таблицы стилей именуется **LocalReplyStyles.css** и располагается в каталоге **CONF\templates\http**, что определяется параметром **HTTP[LocalReplyStyles]**.

## *Шаблоны FTP-сервера*

Шаблоны FTP-сервера изначально располагаются в каталоге **CONF\templates\ftp**, что определяется параметром **FTP[Templates]**.

### *Шаблон ответа сервера при подключении клиента*

Файл шаблона **OnThreadConnect.pat.txt** задаёт идентификатор сервера, подставляемый во все варианты положительных (означающих, что подключение принимается) ответов.

# Журналы и статистика

Журналы сервера подразделяются на оперативные и статистические. В оперативные журналы заносится информация, позволяющая восстановить последовательность событий. На основании статистических журналов можно оценивать объём платежей за пользование интернетом, эффективность работы фильтров.

Существует ещё основной журнал - он всегда располагается в том же каталоге, что и исполняемый файл сервера, и носит то же основное имя; в него записывается информация о запуске и остановке сервера, а также о различных нештатных ситуациях.

## *Оперативные журналы*

Предполагается, что оперативные журналы располагаются в каталоге **DATA\log** - это определяется параметрами **SMTP[Logs]**, **Pop3Recv[Logs]**, **POP[Logs]**, **IMAP[Logs]**, **PROXY[Logs]**, **HttpProxy[Logs]**, **FtpProxy[Logs]**, **SocksProxy[Logs]**, **TCPMAP[Logs]**, **UDPMAP[Logs]**, **Pop3Proxy[Logs]**, **HTTP[Logs]** и **FTP[Logs]** (соответственно, журналы каждого сервера и каждой службы прокси-сервера можно разместить в отдельном каталоге, изначально же используется значение, задаваемое базовым параметром **Dirs[Logs]**); расположение журналов статистики определяется параметром **Dirs[Stat]**, изначально это каталог **DATA\stat**. Содержимое журналов определяется управляющими файлами конфигурации, формат каждой строки задаётся специальным файлом **log.str.txt**, который находится в каталоге общих правил и плагинов **CommonPlugins**. В PigMail+PigProxy предусмотрена так называемая "ротация" журналов - формирование журнальных файлов в соответствии с текущей системной датой. Предусмотрено формирование следующих оперативных журналов (русскими буквами обозначены элементы даты - год, месяц, число):

| Имя файла | Назначение |
|---|---|
| **ггггммддSMTP.log** | Ежедневный основной оперативный журнал SMTP-сервера. |
| **ггггммддPOP3RECV.log** | Ежедневный основной оперативный журнал загрузчика внешней POP-почты **Pop3Recv**. |
| **ггггммддSMTPSEND.log** | Ежедневный основной оперативный журнал расширенного сервиса доставки исходящей почты **SmtpSend**. |
| **ггггммддPOP.log** | Ежедневный основной оперативный журнал POP-сервера. |
| **ггггммддIMAP.log** | Ежедневный основной оперативный журнал IMAP-сервера. |
| **ггггммддSCH.log** | Ежедневный оперативный журнал планировщика. |
| **ггггммддHTTPP.log** | Ежедневный основной оперативный журнал HTTP-прокси. |
| **ггггммддFTPP.log** | Ежедневный основной оперативный журнал FTP-прокси. |
| **ггггммддSOCKS.log** | Ежедневный основной оперативный журнал Socks-прокси. |
| **ггггммддTCPMAP.log** | Ежедневный основной оперативный журнал отображения портов TCP. |
| **ггггммддUDPMAP.log** | Ежедневный основной оперативный журнал отображения портов UDP. |
| **ггггммддPOP3PROXY.log** | Ежедневный основной оперативный журнал POP3-прокси. |
| **ггггммддHTTP.log** | Ежедневный основной оперативный журнал HTTP-сервера. |
| **ггггммддFTP.log** | Ежедневный основной оперативный журнал FTP-сервера. |
| **ггггммддSMTPErr.log** | Ежедневный журнал ошибок SMTP-сервера. |
| **ггггммддPOP3RECVErr.log** | Ежедневный журнал ошибок загрузчика внешней POP-почты **Pop3Recv**. |
| **ггггммддSMTPSENDErr.log** | Ежедневный журнал ошибок расширенного сервиса доставки исходящей почты **SmtpSend**. |
| **ггггммддPOPErr.log** | Ежедневный журнал ошибок POP-сервера. |
| **ггггммддIMAPErr.log** | Ежедневный журнал ошибок IMAP-сервера. |
| **ггггммддSCHErr.log** | Ежедневный журнал ошибок планировщика. |
| **ггггммддHTTPPErr.log** | Ежедневный журнал ошибок HTTP-прокси. |
| **ггггммддFTPPErr.log** | Ежедневный журнал ошибок FTP-прокси. |
| **ггггммддSOCKSErr.log** | Ежедневный журнал ошибок Socks-прокси. |

| | |
|---|---|
| **ггггммддTCPMAPErr.log** | Ежедневный журнал ошибок отображения портов TCP. |
| **ггггммддUDPMAPErr.log** | Ежедневный журнал ошибок отображения портов UDP. |
| **ггггммддPOP3PROXYErr.log** | Ежедневный журнал ошибок POP3-прокси. |
| **ггггммддHTTPErr.log** | Ежедневный журнал ошибок HTTP-сервера. |
| **ггггммддFTPErr.log** | Ежедневный журнал ошибок FTP-сервера. |
| **ггггммддSMTPDbg.log** | Ежедневный отладочный журнал SMTP-сервера. |
| **ггггммддPOP3RECVDbg.log** | Ежедневный отладочный журнал загрузчика внешней POP-почты **Pop3Recv**. |
| **ггггммддSMTPSENDDbg.log** | Ежедневный отладочный журнал расширенного сервиса доставки исходящей почты **SmtpSend**. |
| **ггггммддPOPDbg.log** | Ежедневный отладочный журнал POP-сервера. |
| **ггггммддIMAPDbg.log** | Ежедневный отладочный журнал IMAP-сервера. |
| **ггггммддHTTPPDbg.log** | Ежедневный отладочный журнал HTTP-прокси. |
| **ггггммддFTPPDbg.log** | Ежедневный отладочный журнал FTP-прокси. |
| **ггггммддSOCKSDbg.log** | Ежедневный отладочный журнал Socks-прокси. |
| **ггггммддTCPMAPDbg.log** | Ежедневный отладочный журнал отображения портов TCP. |
| **ггггммддUDPMAPDbg.log** | Ежедневный отладочный журнал отображения портов UDP. |
| **ггггммддPOP3PROXYDbg.log** | Ежедневный отладочный журнал POP3-прокси. |
| **ггггммддHTTPDbg.log** | Ежедневный отладочный журнал HTTP-сервера. |
| **ггггммддFTPDbg.log** | Ежедневный отладочный журнал FTP-сервера. |
| **ггггммддHTTPPacl.log** | Ежедневный журнал обработки списков прав доступа к HTTP-прокси. |
| **ггггммддHTTPPTrafC.log** | Ежедневный журнал обработки каналов управления трафиком HTTP-прокси. |
| **ггггммддFTPPacl.log** | Ежедневный журнал обработки списков прав доступа к FTP-прокси. |
| **ггггммддFTPPTrafC.log** | Ежедневный журнал обработки каналов управления трафиком FTP-прокси. |
| **ггггммддSOCKSacl.log** | Ежедневный журнал обработки списков прав доступа к Socks-прокси. |
| **ггггммддSOCKSTrafC.log** | Ежедневный журнал обработки каналов управления трафиком Socks-прокси. |
| **ггггммддHTTPacl.log** | Ежедневный журнал обработки списка прав доступа к HTTP-серверу. |
| **ггггммддFTPacl.log** | Ежедневный журнал обработки списка прав доступа к FTP-серверу. |
| **ггггммддSMTPav.log** | Ежедневный журнал антивирусной проверки почты, принятой SMTP-сервером. |
| **ггггммддPOP3RECVav.log** | Ежедневный журнал антивирусной проверки почты, принятой загрузчиком внешней POP-почты **Pop3Recv**. |
| **ггггммддHTTPPav.log** | Ежедневный журнал антивирусной проверки трафика HTTP-прокси. |
| **ггггммacSMTPav-r.log** | Ежемесячный журнал перезагрузки вирусных баз, выполняемой SMTP-сервером. |
| **ггггммEproxyav-r.log** | Ежемесячный журнал перезагрузки вирусных баз, выполняемой прокси-сервером. |

Выводимой в оперативные журналы информацией (и, соответственно, их объёмом) можно управлять, задавая уровень детализации. Уровень детализации для почтового сервера задаётся параметрами **SMTP[LogLevel]**, **POP[LogLevel]**, **IMAP[LogLevel]** (изначально наследующими значение глобального параметра **Server[LogLevel]**), а также **Pop3Recv[LogLevel]** и **SmtpSend[LogLevel]** (наследующих значение параметра **SMTP[LogLevel]**, поскольку загрузчик внешней POP-почты и расширенный сервис доставки исходящей почты являются компонентами SMTP-сервера). Уровень детализации для прокси-сервера задаётся параметрами **HttpProxy[LogLevel]**, **FtpProxy[LogLevel]**, **SocksProxy[LogLevel]**, **TCPMAP[LogLevel]**,

**UDPMAP[LogLevel]**, **Pop3Proxy[LogLevel]** (изначально наследующими значение общего для прокси-сервера параметра **PROXY[LogLevel]**, который, в свою очередь, наследует значение глобального параметра **Server[LogLevel]**). Для HTTP- и FTP-сервера уровень детализации задаётся соответственно параметрами **HTTP[LogLevel]** и **FTP[LogLevel]**, изначально наследующими значение глобального параметра **Server[LogLevel]**. Он может иметь значение от 1 до 9. Чем выше уровень детализации, тем больше подробностей пишется в оперативные журналы, включая информацию всех нижележащих уровней. Особый случай составляет нулевое значение - для совместимости с предыдущими версиями, в которых уровень детализации не задавался, оно соответствует максимальному уровню детализации.

### *Уровни детализации оперативных журналов SMTP-сервера*

1 Подключения и отключения клиентов, данные авторизации
2 Команды протокола
3 Реакция сервера на подключения и команды протокола, отметки о срабатывании различных фильтров
4 Трассировка доставки писем: обработка переадресации, раскрытие списков рассылки, перемещение писем в каталоги
5 Запуск агентов доставки (в том числе планировщиком)
6 Ответы SMTP-сервера
7 Отметки об успешном прохождении писем через фильтры и обработчики, подробный протокол работы планировщика, подробный протокол авторизации
8 Детальный протокол прохождения писем через контент-анализатор MContent

Всегда записывается:
- информация о технических проблемах во время приёма писем
- информация об обнаружении вирусов
- информация о действиях роботов-автоблокировщиков

### *Уровни детализации оперативных журналов загрузчика внешней POP-почты Pop3Recv*

1 Подключения загрузчика к внешнему POP-серверу и отключения, информация о проверке адресов отправителя и получателей
2 Команды загрузчика внешнему POP-серверу и ответы сервера
3 Результаты проверки адресов, отметки о срабатывании различных фильтров
4 Трассировка доставки писем: обработка переадресации, раскрытие списков рассылки, перемещение писем в каталоги
5 Запуск агентов доставки (в том числе планировщиком)
6 Расширенная диагностика проверки адресов и срабатывания фильтров
7 Отметки об успешном прохождении писем через фильтры и обработчики, подробный протокол работы планировщика
8 Детальный протокол прохождения писем через контент-анализатор MContent

Всегда записывается:
- информация о технических проблемах во время приёма писем
- информация об обнаружении вирусов

### *Уровни детализации оперативных журналов расширенного сервиса доставки исходящей почты SmtpSend*

1 Отметки о начале и завершении обработки файла письма, подключения сервиса к SMTP-серверу-получателю и отключения
2 Команды сервиса SMTP-серверу-получателю и ответы сервера
3 Результаты первичного анализа писем, отметки о дополнительной обработке адресов отправителей и получателей
4 Трассировка доставки извещений: обработка переадресации, раскрытие списков рассылки, перемещение в каталоги
5 Установка режимов доставки адресату
6 Зарезервировано
7 Отметки о запуске обработки каталогов очереди

Всегда записывается:
- информация о технических проблемах во время доставки писем

### *Уровни детализации оперативных журналов POP-сервера*

1 Подключения и отключения клиентов, данные авторизации
2 Команды протокола

3 Реакция сервера на подключения и команды протокола, отметки о срабатывании различных фильтров
4 Зарезервировано
5 Зарезервировано
6 Ответы сервера на команды протокола
7 Дополнительные строки многострочных ответов сервера на команды протокола, подробный протокол авторизации

Всегда записывается:
- информация о технических проблемах во время выполнения запросов

### *Уровни детализации оперативных журналов IMAP-сервера*

1 Подключения и отключения клиентов, данные авторизации
2 Команды протокола
3 Реакция сервера на подключения и команды протокола, отметки о срабатывании различных фильтров
4 Отметки о выборе действия, переклассификации и перепосылке писем
5 Зарезервировано
6 Ответы сервера на команды протокола
7 Дополнительные строки многострочных ответов сервера на команды протокола, подробный протокол авторизации

Всегда записывается:
- информация о технических проблемах во время выполнения запросов

### *Уровни детализации оперативных журналов HTTP-прокси*

1 Подключения и отключения клиентов, данные авторизации
2 Команды протокола, заглавные строки локальных ответов и ответов целевого сервера, результаты выполнения запросов
3 Реакция сервера на подключения и команды протокола, отметки о срабатывании различных фильтров
4 Зарезервировано
5 Отметки о работе дополнительных обработчиков, запись в журнал обработки списка прав доступа
6 Дополнительные заголовки запросов клиента, локальных ответов и ответов внешнего сервера
7 Отметки об успешных антивирусных проверках файлов в кэше прокси-сервера, подробный протокол авторизации

Всегда записывается:
- информация о технических проблемах во время выполнения запросов
- информация об обнаружении вирусов

### *Уровни детализации оперативных журналов FTP-прокси*

1 Подключения и отключения клиентов
2 Команды протокола - от клиента прокси-серверу и от прокси-сервера целевому серверу, ответы на команды
3 Реакция сервера на подключения и команды протокола, отметки о срабатывании различных фильтров
4 Зарезервировано
5 Отметки о работе дополнительных обработчиков, запись в журнал обработки списка прав доступа
6 Зарезервировано
7 Подробный протокол авторизации

Всегда записывается:
- информация о технических проблемах во время выполнения запросов

### *Уровни детализации оперативных журналов Socks-прокси*

1 Подключения и отключения клиентов, данные авторизации
2 Запросы и результаты их выполнения
3 Реакция сервера на подключения и запросы, отметки о срабатывании различных фильтров
4 Зарезервировано
5 Отметки о работе дополнительных обработчиков, запись в журнал обработки списка прав доступа
6 Зарезервировано
7 Подробный протокол авторизации

Всегда записывается:
- информация о технических проблемах во время выполнения запросов

### *Уровни детализации оперативных журналов POP3-прокси*

1 Подключения и отключения клиентов
2 Команды протокола и результаты их выполнения
3 Реакция сервера на подключения и команды протокола, отметки о срабатывании различных фильтров
4 Зарезервировано
5 Зарезервировано
6 Ответы прокси-сервера клиенту

Всегда записывается:
- информация о технических проблемах во время выполнения запросов

### *Уровни детализации оперативных журналов отображения портов TCP*

1 Подключения и отключения клиентов
2 Запросы и результаты их выполнения
3 Реакция сервера на подключения и запросы, отметки о срабатывании различных фильтров

Всегда записывается:
- информация о технических проблемах во время выполнения запросов

### *Уровни детализации оперативных журналов отображения портов UDP*

1 Подключения и отключения клиентов
2 Запросы и результаты их выполнения
3 Реакция сервера на подключения и запросы, отметки о срабатывании различных фильтров

Всегда записывается:
- информация о технических проблемах во время выполнения запросов

### *Уровни детализации оперативных журналов HTTP-сервера*

1 Подключения и отключения клиентов, данные авторизации
2 Команды протокола, заглавные строки ответов сервера и результаты выполнения запросов
3 Реакция сервера на подключения и команды протокола, отметки о срабатывании различных фильтров
4 Зарезервировано
5 Отметки о работе дополнительных обработчиков
6 Дополнительные заголовки запросов клиента и ответов сервера, информация о преобразовании логического пути к объекту в физический
7 Подробный протокол авторизации

Всегда записывается:
- информация о технических проблемах во время выполнения запросов

### *Уровни детализации оперативных журналов FTP-сервера*

1 Подключения и отключения клиентов, данные авторизации
2 Команды протокола и результаты выполнения запросов
3 Реакция сервера на подключения и команды протокола, отметки о срабатывании различных фильтров
4 Зарезервировано
5 Отметки о работе дополнительных обработчиков
6 Информация о преобразовании логического пути к объекту в физический
7 Подробный протокол авторизации

Всегда записывается:
- информация о технических проблемах во время выполнения запросов

## *Статистические журналы*

Статистические журналы также формируются с "ротацией". Поскольку возможен вывод одновременно в нескольких форматах, для каждого формата отведён отдельный специальный подкаталог в базовом каталоге статистических журналов. Изначально предполагается следующее распределение каталогов:

| Каталог | Параметр Eserv3.ini | Пояснение |
|---|---|---|
| **DATA\stat\estat\log** | **Dirs[Estat]** | Каталог для размещения статистических журналов в формате **Estat32** (**EPE Labs**). |
| **DATA\stat\advsoft** | **Dirs[AdvSoft]** | Каталог для размещения статистических журналов в формате **ProxyInspector** и **MailDetective** (**AdvSoft**). |

| | | |
|---|---|---|
| **DATA\stat\elog** | **Dirs[Elog]** | Каталог для размещения статистических журналов в формате **Elog** (**ЛЭНК**). |
| **DATA\stat\maillog** | **Dirs[Maillog]** | Каталог для размещения статистических журналов собственного текстового формата. Большинство журналов, включая статистику спам-фильтров, располагается в подкаталоге **SMTP**, журналы POP-сервера - в подкаталоге **POP3**, журналы IMAP-сервера - в подкаталоге **IMAP**, журналы HTTP-сервера - в подкаталоге **HTTP**, журналы FTP-сервера - в подкаталоге **FTP**. В самом базовом каталоге размещаются журналы, общие для всех серверов. |
| **DATA\stat\trafc** | **Dirs[TrafCStat]** | Каталог для размещения статистических журналов работы ограничителя трафика TrafC. |

Предусмотрено формирование следующих журналов:

| Формат | Имя файла | Назначение |
|---|---|---|
| **Estat32** | **ммддSTAT.log** | Ежедневный журнал статистики работы всех серверов - в соответствии с принятым в Eserv/2 стандартом. |
| **ProxyInspector** | **ггггммMAIL.log** | Ежемесячный журнал статистики работы всех почтовых серверов. |
| **ProxyInspector** | **ггггммPROXY.log** | Ежемесячный журнал статистики работы HTTP-прокси. |
| **ProxyInspector** | **ггггммFTPPROXY.log** | Ежемесячный журнал статистики работы FTP-прокси. |
| **ProxyInspector** | **ггггммMAP.log** | Ежемесячный журнал статистики работы служб "отображения" - Socks-прокси, POP3-прокси, отображений портов TCP и UDP. |
| **Elog** | **ггггммддSMTP.log** | Ежедневный журнал статистики работы SMTP-сервера. |
| **Elog** | **ггггммддPOP3RECV.log** | Ежедневный журнал статистики работы загрузчика внешней POP-почты **Pop3Recv**. |
| **Elog** | **ггггммддSMTPSEND.log** | Ежедневный журнал статистики работы агента отправки исходящей почты **smtpsend4** или расширенного сервиса доставки исходящей почты **SmtpSend**. |
| **Elog** | **ггггммддPOP.log** | Ежедневный журнал статистики работы POP-сервера. |
| **Elog** | **ггггммддIMAP.log** | Ежедневный журнал статистики работы IMAP-сервера. В настоящей версии статистика записывается интегрально по сеансам подключения. |
| **Elog** | **ггггммддHTTPP.log** | Ежедневный журнал статистики работы HTTP-прокси. |
| **Elog** | **ггггммддFTPP.log** | Ежедневный журнал статистики работы FTP-прокси. |
| **Elog** | **ггггммддSOCKS.log** | Ежедневный журнал статистики работы Socks-прокси. |
| **Elog** | **ггггммддPOP3PROXY.log** | Ежедневный журнал статистики работы POP3-прокси. |
| **Elog** | **ггггммддTCPMAP.log** | Ежедневный журнал статистики работы отображений портов TCP. |
| **Elog** | **ггггммддUDPMAP.log** | Ежедневный журнал статистики работы отображений портов UDP. |

| | | |
|---|---|---|
| **Elog** | **ггггммддHTTP.log** | Ежедневный журнал статистики работы HTTP-сервера. |
| **Elog** | **ггггммддFTP.log** | Ежедневный журнал статистики работы FTP-сервера. |
| **TrafC** | **ггггммддBANDS.log** | Ежедневный журнал статистики выделения Band-каналов ограничителя трафика TrafC. |
| **TrafC** | **ггггммддQUOTAS.log** | Ежедневный журнал статистики выделения Quota-каналов ограничителя трафика TrafC. |
| **Собственный** | **ггггммMAIL.txt** | Ежемесячный журнал статистики успешного приёма писем. |
| **Собственный** | **ггггммSMTPSEND.txt** | Ежемесячный журнал статистики работы агента отправки исходящей почты **smtpsend4** или расширенного сервиса доставки исходящей почты **SmtpSend**. |
| **Собственный** | **ггггммMAIL-REFUSED.txt** | Ежемесячный журнал статистики отказа в приёме писем. В этот журнал записывается информация обо всех отклонённых письмах, включая спам и письма с вирусами. |
| **Собственный** | **ггггммMAIL-SPAM.txt** | Ежемесячный журнал статистики блокировки спама. |
| **Собственный** | **ггггммMAIL-VIRUS.txt** | Ежемесячный журнал статистики блокировки писем с вирусами. |
| **Собственный** | **ггггммMAIL-AVERROR.txt** | Ежемесячный журнал статистики сбоев антивирусной проверки. |
| **Собственный** | **ггггммSPF.txt** | Ежемесячный журнал статистики проверки адреса отправителя с помощью Sender Policy Framework и MS Caller ID. |
| **Собственный** | **ггггммYDK.txt** | Ежемесячный журнал статистики проверки электронной подписи Yahoo Domain Keys. |
| **Собственный** | **ггггммPOPFILE_DEBUG.txt** | Ежемесячный отладочный статистический журнал работы спам-фильтра POPfile. |
| **Собственный** | **ггггммMAIL_SP.txt** | Ежемесячный отладочный статистический журнал совместной работы спам-фильтров POPfile и SpamProtexx, позволяющий оценивать совпадение их оценок. |
| **Собственный** | **ггггммMAIL_SD.txt** | Ежемесячный отладочный статистический журнал совместной работы спам-фильтров POPfile и/или SpamProtexx и LibSD, позволяющий оценивать совпадение их оценок. |
| **Собственный** | **ггггммRC.txt** | Ежемесячный журнал переклассификации писем в POPfile, SpamProtexx и/или LibSD. |
| **Собственный** | **ггггммPOPMAIL.txt** | Ежемесячный журнал статистики загрузки писем из ящиков POP-сервера. |
| **Собственный** | **ггггммIMAPMAIL.txt** | Ежемесячный журнал статистики сеансов работы пользователей с IMAP-сервером. |
| **Собственный** | **домен\хост_ггггмм.log** | Ежемесячный журнал статистики посещений HTTP-сервера. Для каждого виртуального сервера ведётся отдельный журнал. |
| **Собственный** | **домен\403_ггггмм.log** | Ежемесячный журнал статистики отказов в доступе к HTTP-серверу. Для каждого виртуального сервера ведётся отдельный журнал. |

| | | |
|---|---|---|
| **Собственный** | **downloads\ггггмм.txt** | Ежемесячный журнал статистики загрузок. Загрузкой считается запрос статического файла (не сценария) с расширением **.EXE**, **.RAR**, **.ZIP** или **.BIN** без указания границ фрагмента, то есть, целиком. |
| **Собственный** | **robots\домен\имя_хост_ггггмм.log** | Ежемесячный журнал статистики посещений HTTP-сервера поисковыми роботами. Для каждого виртуального сервера и робота ведётся отдельный журнал. |
| **Собственный** | **robots\robots_ггггмм.log** | Ежемесячный журнал статистики запросов файла **robots.txt**. По этому признаку определяются "правильные" поисковые роботы. |
| **Собственный** | **ггггммRC.txt** | Ежемесячный журнал статистики обмена данными (то есть, загрузки файлов в обе стороны и чтения оглавлений каталогов) с FTP-сервером. |
| **Собственный** | **ггггммAUTH.txt** | Ежемесячный журнал статистики авторизации на серверах комплекта Eserv/3. Это общий для всех серверов журнал, поэтому размещается в базовом каталоге статистических журналов собственного текстового формата. |
| **Собственный** | **ггггммSTAT.txt** | Ежемесячный журнал статистики использования трафика серверами комплекта Eserv/3. Это общий для всех серверов журнал, поэтому размещается в базовом каталоге статистических журналов собственного текстового формата. |
| **Собственный** | **ггггммAV.txt** | Ежемесячный журнал статистики антивирусной проверки трафика серверами комплекта Eserv/3. Это общий для всех серверов журнал, поэтому размещается в базовом каталоге статистических журналов собственного текстового формата. |

# Администрирование

Помимо контроля работы сервера по его журналам, необходимо регулярно следить за появлением файлов в следующих каталогах (предполагается, что структура каталогов оставлена без изменений):

- **DATA\mail\abuse**
- **DATA\mail\bounce**
- **DATA\mail\infected**
- **DATA\mail\loop**
- **DATA\mail\malformed**
- **DATA\mail\nonreadable**
- **DATA\mail\overquoted**
- **DATA\mail\quarantined**
- **DATA\mail\reclassify**
- **DATA\mail\spam**
- **DATA\mail\unchecked**
- **DATA\mail\undelivered**

Каждое вновь появившееся письмо следует внимательно изучить и при необходимости принять меры в соответствии с ситуацией.

Если файл письма надолго задерживается в каталоге **DATA\mail\out**, **DATA\mail\try** или **DATA\mail\retry**, или их подкаталоге, это означает наличие проблемы с отправкой исходящей почты. При этом следует внимательно изучить протоколы работы агента отправки, которые в соответствии с изначальными настройками располагаются в каталоге **DATA\temp**.

# Вопросы и ответы

**1. Я уже использую Eserv/3. Какие изменения в конфигурации мне надо выполнить при установке PigMail+PigProxy? Или всё заработает автоматически?**

К сожалению, нет. В некоторых ключевых моментах PigMail+PigProxy категорически не совместим со стандартной конфигурацией. В первую очередь Вам следует заполнить список локальных почтовых ящиков (**LocalDomainUsers**) - перечислить в нём все почтовые ящики, с которыми будет работать Ваш сервер. Без этого Вы не сможете ни отправить, ни принять ни одно сообщение. Далее, следует привести к новому формату список локальных доменов (**LocalDomains**) - он содержит ряд дополнительных параметров, - а также списки доверенных (**FromEmailWhiteList**) и запрещённых (**FromEmailBlackList**) отправителей - эти списки в силу исторических причин не совместимы по формату с аналогичными списками стандартной конфигурации. Отделите псевдонимы (алиасы) от списков рассылки - в PigMail+PigProxy это разные сущности, и перечень списков рассылки (**ToEmailMailLists**) по формату не совместим со списком псевдонимов (**ToEmailAliases**). Если Вы используете почтовых роботов, может потребоваться существенная переработка, поскольку в концепции PigMail+PigProxy все роботы считаются самодостаточными - доставку сообщений в почтовые ящики, если таковая требуется, они обязаны выполнять самостоятельно. Список почтовых роботов (**ToEmailRobots**) также следует привести к новому формату. Для работы POP/IMAP-сервера может потребоваться (это зависит от типа используемых Вами источников авторизации пользователей) заполнить список соответствия пользовательских учётных записей и почтовых ящиков (**UserMailBoxes**). Прочие списки также рекомендуется привести к формату PigMail+PigProxy, но это можно сделать и позже. Обязательно скопируйте образцы списков, отсутствующих в стандартной конфигурации.

Если Вы используете спам-фильтры, то скопируйте списки исключений. В стандартной конфигурации они хранятся вместе с управляющими списками SMTP-сервера - это **PopFileIpWhiteList**, **PopFileFromWhiteList** и **PopFileToWhiteList**. В составе PigMail+PigProxy эти списки располагаются в отдельном каталоге (по умолчанию это **CONF\lists\antispam**) и называются по-другому: **IpWhiteList** (список доверенных сетей), **FromEmailWhiteList** (список доверенных отправителей) и **ToEmailWhiteList** (список особых получателей).

Если Вы используете контент-анализатор MContent, сравните примеры пользовательских правил обработки для PigMail+PigProxy и стандартной конфигурации и внесите в свои правила необходимые изменения.

В силу исторических причин прокси-сервер Eserv/3 (Eproxy) настраивается и управляется иначе, нежели почтовая подсистема. Стандартная конфигурация предполагает изменение настроек в основном через редактирование файлов правил - либо ручное, либо через web-интерфейс. PigMail+PigProxy ориентируется на редактирование конфигурационного файла **PigMail2.ini** и множества управляющих списков. Общих элементов у них минимум - это список локальных доменов (**LocalDomains**), список источников авторизации (**AuthSources**) и списки пользователей, по которым выполняется авторизация. Без изменения переносятся списки каналов ограничителя трафика TrafC (**BandsList**, **QuotasList**, **UserCanalsList**). Совпадающие параметры конфигурационного файла PigMail2.ini также можно сосчитать по пальцам. Подавляющее большинство настроечных элементов PigMail+PigProxy аналога в стандартной конфигурации не имеет. Поэтому Вы, с одной стороны, не связаны грузом унаследованных настроек, а с другой стороны, вынуждены выстроить свою конфигурацию заново практически с нуля. Начинать надо с заполнения списка разрешённых сетевых интерфейсов (**MyIpList**). Поскольку PigMail+PigProxy не предусматривает первичную автонастройку разрешений, заполнение этого списка следует выполнить особо тщательно - благо количество имеющихся сетевых интерфейсов никогда не бывает слишком большим. При заполнении списков локальных (**LocalNetworks**) и доверенных (**IpWhiteList**) сетей следует определиться, необходима ли Вам авторизация на основании IP-адреса (или по сочетанию IP и MAC адресов с использованием списка **IpMacAuth**), не слишком ли либерально составлен общий список локальных сетей (возможно, будет разумным его игнорировать). Если используются отображения портов TCP или UDP, необходимо тщательно заполнить основные списки управления отображениями (**TcpMap** и **UdpMap**). Сложность может также представлять настройка списков доступа (**ACL**) для HTTP-, FTP- и Socks-прокси, особенно если Вас не устраивает предложенная в примере схема. В остальном же начальное заполнение списков вполне достаточно для первого запуска.

Изучите параметры конфигурационного файла **PigMail2.ini** и задайте им необходимые значения, если настройки по умолчанию не соответствуют Вашим требованиям.

**2. Списки локальных (LocalNetworks) и доверенных (IpWhiteList) сетей используются для авторизации пользователей. Это получается, что любой, кто подключился с одного из этих адресов, может отправлять почту куда угодно?**

Нет. Во-первых, авторизация на основе IP-адреса включается тогда и только тогда, когда отменено требование явной SMTP-авторизации - как для отправки всей почты и использования локального обратного адреса (эти требования по умолчанию отменены), так и для отправки почты наружу и скрытым локальным получателям (а эти требования по умолчанию действуют). Кроме того, необходимо, чтобы полученные таким образом имя учётной записи и домен авторизации пользователя совпали с требуемыми идентификаторами,

сопоставленными адресу отправителя в списке пользователей локальных доменов, а сам отправитель имел на это право - то есть, он в любом случае должен указать правильный обратный адрес.

Кроме того, отмена требования не запрещает клиентам авторизоваться явно - такая явная авторизация имеет приоритет над IP-авторизацией. Так что пользователям, авторизованным на основании IP-адреса, можно присвоить минимальные права, а пользователям с высокими полномочиями выдать имена учётных записей, которые не присваиваются автоматически.

**3. У меня на сервере выполняется программа, которая должна периодически отправлять отчёты по электронной почте. Почтовый сервер отказывается принимать от неё письма, если я указываю для неё в качестве SMTP-сервера localhost или 127.0.0.1. Как обойти этот запрет?**

На самом деле в PigMail+PigProxy жёстко запрещён приём подключений со всего loopback-диапазона 127.0.0.0 - 127.255.255.255. Это дополнительная мера защиты от спаморассыльщиков на случай, если они сумеют найти и использовать дыры в настройке прокси-сервера, - хотя, безусловно, чаще всего в таких случаях используется именно адрес 127.0.0.1. Рекомендуется назначить для внутреннего употребления один секретный IP-адрес (например, 127.5.33.198), записать его в список доверенных сетей для обхода запрета и прописать в настройках всех программ - отправителей почты. При этом не следует забывать smtpsend4, который таким же образом отсылает отправителям письма-возвраты. В примере, включённом в дистрибутив, в качестве особого везде использован адрес 127.0.0.10. Конечно, если какая-то программа упрямо желает отправлять письма только на localhost, придётся внести в белый список именно этот адрес.

**4. Мне необходимо вести архив почты таким образом, как раньше было настроено в Eserv/2, - пересылать всю проходящую через сервер почту на список рассылки. Это вообще реализуемо?**

Да. Правда, в PigMail+PigProxy отсутствует специальная настройка, которая отвечала бы за это. Но Вы можете подключить плагин **magicwords** и создать для него правило, сравнивающее, например, тему письма с универсальным шаблоном, состоящим из одной звёздочки *, и при успешном сравнении добавляющее в список получателей Ваш список рассылки. Если плагин уже используется, новое правило должно быть самым первым в списке "магических" слов; кроме того, оно не должно прерывать обработку списка.

**5. Проверка целостности управляющих списков пишет: "неизвестный формат, преобразование невозможно". Как это исправить?**

Пришлите мне файл, на который ругается утилита. Я дополню список возможных преобразований.

**6. У меня не работает доставка адресатам писем, переклассифицированных в чистые. В оперативном журнале SMTP-сервера после каждой попытки появляется сообщение "Auth wrong".**

Вероятно, Вы не настроили список получателей "чужих" доменов (**EmailSmtpForward**). В примере первая строка этого списка, содержащая в поле **EMAIL_MASK** значение ***(for returned mail only)***, отвечает именно за такую внутреннюю пересылку. Вам необходимо указать в этой строке учётную запись и пароль, соответствующие обратному адресу (по умолчанию - адресу администратора), от имени которого выполняются эти операции. Значения, указанные в примере, соответствуют (разумеется, в контексте примера) пользователю с правами администратора, которому разрешено использовать любой обратный адрес.

# Системные требования

Поскольку пакет PigMail+PigProxy основан на пакете Eserv/3+Eproxy/3, то и системные требования у него те же, что и у базового пакета. Желательная минимальная конфигурация:

- Процессор Celeron 1 ГГц;
- Объём оперативной памяти 512 МБ;
- Операционная система Windows XP.

Будет работать и на более слабых машинах, а на более старых Windows - 2000/NT4/9x - уже нет. Рекомендуемая конфигурация сильно зависит от числа пользователей, работающих с сервером. Поскольку PigMail+PigProxy активно работает с диском, регулярно перечитывая файл конфигурации и управляющие списки, крайне желательно применять жёсткий диск с высоким быстродействием. При использовании антивируса на прокси-сервере желательно использовать мощный процессор, чтобы вычислительные затраты на антивирусную проверку не снижали пропускную способность канала. Хорошие результаты показывает сервер на базе процессора Pentium IV 2 Ггц с объёмом оперативной памяти 1 ГБ и жёстким диском 160 ГБ, работающий под управлением Windows Server 2003.

Используемые в составе пакета компоненты Eserv/3 и Eproxy/3 совместимы с текущими версиями Windows Vista, Windows Server 2008 и Windows 7, в том числе с 64-разрядными версиями, а также с современными многоядерными процессорами.

Интернет-соединение может использоваться любое, в том числе с динамическим IP, но полноценное использование всех возможностей комплекта возможно только при использовании выделенного канала. Не имеет значения, как этот канал физически организован: если компьютер постоянно подключен к интернету, а не созванивается несколько раз в день, то будем считать такое подключение выделенным.

При установке PigMail+PigProxy на компьютер с включенным брандмауэром - например, входящим в Windows XP SP2/3 - необходимо разрешить в настройках брандмауэра входящие подключения к TCP-сервисам PigMail+PigProxy.

# Условия распространения

Пробный ключ, заказанный при загрузке дистрибутивного пакета, обеспечивает работоспособность Pig-Mail+PigProxy в течение 30 дней с момента генерации ключа. Для получения постоянного ключа следует оформить покупку на сайте **www.eserv.ru**.

# Благодарности

**Андрей Черезов** (ac) - идеолог и главный разработчик Eserv
**Рувим Пинка** (rvm) - соразработчик Eserv, автор модуля управления трафиком **TrafC**
**BigHarry** - разработчик почтового сервера **B-SMTP**, автор ряда идей
**Владимир Филиппов** (Unhurried) - участник тестирования, автор ряда идей
**Андрей Лавров** (A V L) - участник тестирования, автор ряда идей
**Андрей Матвеев** (Dandy) - разработчик почтового препроцессора **Mchecker** и контент-анализатора **MContent**, автор ряда идей
**Виталий Заикин** (vze) - активный пользователь, соавтор ряда идей
**Владимир Громухин** (leka) - активный пользователь бета-версий, автор ряда идей
**Андрей Трунов** (ant) - активный пользователь
**Blackman** - автор утилиты Advanced Password Generator
**Александр Перевозчиков** (alexandr) - активный пользователь
**Николай Дмитриев** (ND) - активный пользователь, соавтор ряда идей
**Станислав Сулименко** (grass_snake) - активный пользователь
**Владимир Ленцик** (Volodya_Lentsik) - активный пользователь и критик, автор ряда идей
И нижайше прошу прощения у тех, кого забыл упомянуть.

# Последние изменения

***17 июля 2012 года.*** **Версия 2.4**:

- SMTP-сервер: в загрузчике внешней POP-почты Pop3Recv исправлена ошибка некорректной конвертации базы данных
- Все серверы: изменено начальное значение внешнего IP-адреса (**Server[ExternIP]**)
- \+ SMTP-сервер: загрузчик внешней POP-почты Pop3Recv выводит в журнал отметку о невозможности определить отправителя в ситуации, когда пустой адрес отправителя запрещён настройками (спасибо **vmikhajlov**)
- Web-интерфейс: восстановлена работоспособность страницы переклассификации почты (спасибо **DAC**)
- IMAP-сервер: восстановлена работоспособность переклассификатора почты для спам-фильтров SpamProtexx и LibSD (спасибо **DAC**)

**Новые, изменённые и удалённые элементы настройки:**

| | Элемент | Тип | Расположение |
|---|---|---|---|
| * | **Server[ExternIP]** | INI-параметр | PigMail2.orig.ini |

**+** добавленный элемент/опция
***** изменённый элемент/опция
**-** удалённый элемент/опция
**!** критически важное изменение

# Обратная связь

Если обнаружатся ошибки или возникнут какие-либо пожелания, обращайтесь по адресу **pig.gy@mail.ru**. Отвечать не обещаю, но всё будет внимательно прочитано и обдумано.

**Игорь Панасенко** aka **pig**, ведущий программист Горного института Кольского научного центра РАН, Апатиты Мурманской области.

# Приложение 1. Права доступа к HTTP- и FTP-серверу

Объектом, для доступа к которому назначаются права доступа, является физический файл или каталог. Это сделано сознательно, поскольку при сложных правилах отображения логических путей на физические каталоги сервера вполне возможна множественность, когда одному и тому же физическому объекту соответствуют различные логические пути. В такой ситуации несложно при составлении списка доступа упустить из вида один из вариантов.

Следует, однако, учитывать, что при отображении путей сервер не выполняет их приведения к какому-либо единому стандартному формату. То есть, если выбранный в списке отображения базовый каталог определён относительно каталога запуска сервера (**..\CONF\pub\...**), то и полученный в результате преобразования путь будет соответствовать этому формату записи, и именно такого вида строки сервер будет искать в списке прав доступа. Если базовый каталог отсчитывается от корневого каталога диска, на котором размещён сервер (**\Eserv3\CONF\pub\...**), сервер будет искать строки этого формата. Если путь к базовому каталогу задан в полном формате с указанием буквы диска, то и в списке прав доступа сервер будет искать именно полные пути. Поэтому при планировании структуры сервера необходимо выбрать один из этих форматов в качестве стандарта и следовать ему - это позволит избежать множественности вариантов физических путей.

Права доступа наследуются вглубь иерархии каталогов до тех пор, пока не встретится каталог, для которого в списке доступа установлены другие права. Если путь отсутствует в списке (что на самом деле не рекомендуется - желательно все корневые каталоги описать явно), назначаются права доступа по умолчанию, определённые соответствующими параметрами (**HTTP[DefaultAccess]**, **FTP[DefaultAccess]**, **FTP[DefaultGuestAccess]**) конфигурационного файла **PigMail2.ini**.

Код права доступа, назначаемый пользователю при обращении к объекту, представляет собой целое число, каждый бит которого соответствует одному элементарному праву:

| Код | Право | Пояснение |
|---|---|---|
| 1 | выполнение | Это элементарное право, имеющее смысл для HTTP-сервера, определяет возможность выполнять сценарии непосредственно на сервере. Файлы, которым это право назначено явно, а также файлы, унаследовавшие это право от содержащих их каталогов, могут быть запущены как CGI-сценарии. |
| 2 | запись | Это элементарное право определяет возможность создания подкаталогов и файлов и перезаписи существующих файлов. |
| 4 | чтение | Это элементарное право определяет возможность чтения файлов. |
| 8 | оглавление | Это элементарное право определяет возможность чтения оглавления каталогов. |
| 16 | удаление | Это элементарное право определяет возможность удаления подкаталогов и файлов (а также самого каталога, которому назначено это право). |

Вместо числовых кодов можно указывать более наглядные символьные:

| Код | Число | Права |
|---|---|---|
| **ACCESS:EXEC** | 1 | выполнение |
| **ACCESS:WRITE** | 2 | запись |
| **ACCESS:READ** | 4 | чтение |
| **ACCESS:LIST** | 8 | оглавление |
| **ACCESS:DELETE** | 16 | удаление |
| **ACCESS:-** | 0 | доступ запрещён |
| **ACCESS:X** | 1 | выполнение |
| **ACCESS:W** | 2 | запись |
| **ACCESS:WX** | 3 | запись, выполнение |
| **ACCESS:R** | 4 | чтение |
| **ACCESS:RX** | 5 | чтение, выполнение |
| **ACCESS:RW** | 6 | чтение, запись |
| **ACCESS:RWX** | 7 | чтение, запись, выполнение |

| | | |
|---|---|---|
| **ACCESS:L** | 8 | оглавление |
| **ACCESS:LX** | 9 | оглавление, выполнение |
| **ACCESS:LW** | 10 | оглавление, запись |
| **ACCESS:LWX** | 11 | оглавление, запись, выполнение |
| **ACCESS:LR** | 12 | оглавление, чтение |
| **ACCESS:LRX** | 13 | оглавление, чтение, выполнение |
| **ACCESS:LRW** | 14 | оглавление, чтение, запись |
| **ACCESS:LRWX** | 15 | оглавление, чтение, запись, выполнение |
| **ACCESS:D** | 16 | удаление |
| **ACCESS:DX** | 17 | удаление, выполнение |
| **ACCESS:DW** | 18 | удаление, запись |
| **ACCESS:DWX** | 19 | удаление, запись, выполнение |
| **ACCESS:DR** | 20 | удаление, чтение |
| **ACCESS:DRX** | 21 | удаление, чтение, выполнение |
| **ACCESS:DRW** | 22 | удаление, чтение, запись |
| **ACCESS:DRWX** | 23 | удаление, чтение, запись, выполнение |
| **ACCESS:DL** | 24 | удаление, оглавление |
| **ACCESS:DLX** | 25 | удаление, оглавление, выполнение |
| **ACCESS:DLW** | 26 | удаление, оглавление, запись |
| **ACCESS:DLWX** | 27 | удаление, оглавление, запись, выполнение |
| **ACCESS:DLR** | 28 | удаление, оглавление, чтение |
| **ACCESS:DLRX** | 29 | удаление, оглавление, чтение, выполнение |
| **ACCESS:DLRW** | 30 | удаление, оглавление, чтение, запись |
| **ACCESS:DLRWX** | 31 | удаление, оглавление, чтение, запись, выполнение |
| **ACCESS:NONE** | 0 | доступ запрещён |
| **ACCESS:RUN** | 5 | чтение, выполнение |
| **ACCESS:PUT** | 6 | чтение, запись |
| **ACCESS:RETR** | 12 | оглавление, чтение |
| **ACCESS:GET** | 13 | оглавление, чтение, выполнение |
| **ACCESS:MOD** | 14 | оглавление, чтение, запись |
| **ACCESS:NOEXEC** | 30 | удаление, оглавление, чтение, запись |
| **ACCESS:ALL** | 31 | удаление, оглавление, чтение, запись, выполнение |

Для выполнения запросов протокола HTTP необходимы следующие права:

| Запрос | Действие | Права |
|---|---|---|
| **GET** | Вызов сценария<br>Чтение оглавления каталога<br>Чтение файла | выполнение<br>оглавление<br>чтение или выполнение |
| **HEAD** | Вызов сценария<br>Чтение параметров файла | выполнение<br>чтение или выполнение |
| **POST** | Вызов сценария<br>Чтение оглавления каталога<br>Чтение файла | выполнение<br>оглавление<br>чтение или выполнение |

| | | |
|---|---|---|
| **OPTIONS** | Запрос поддерживаемых опций сервера | не требуются |
| **PUT** | Запись файла | запись |
| **DELETE** | Удаление файла | удаление |
| **PROPFIND** | Чтение параметров файла или файлов | оглавление |
| **REPORT** | Чтение параметров файла или файлов | оглавление |
| **MKCOL** | Создание каталога | Оба права: оглавление и запись |
| **LOCK** | Блокировка файла или каталога | Любое из прав: чтение, запись |
| **UNLOCK** | Снятие блокировки файла или каталога | Любое из прав: чтение, запись |
| **MOVE** | Переименование файла или каталога | Три права: удаление, оглавление, запись. Права проверяются для исходного файла |

Для выполнения команд протокола FTP необходимы следующие права:

| Команда | Действие | Права |
|---|---|---|
| **LIST** | Чтение оглавления каталога | оглавление |
| **NLST** | Чтение оглавления каталога | оглавление |
| **RETR** | Чтение файла | чтение |
| **CWD** | Смена текущего каталога | Любое из прав: удаление, оглавление, чтение, запись |
| **CDUP** | Переход в родительский каталог | В текущей версии права не проверяются. Считается, что доступ в вышестоящий каталог всегда разрешён. |
| **SIZE** | Запрос размера файла | чтение |
| **MDTM** | Запрос даты-времени файла | чтение |
| **STOR** | Запись файла | запись |
| **APPE** | Дозапись файла | запись |
| **DELE** | Удаление файла | удаление |
| **RNFR** | Переименование, определяет исходное имя файла или каталога | Оба права: удаление и оглавление |
| **RNTO** | Переименование, определяет новое имя файла или каталога | Оба права: оглавление и запись |
| **MKD** | Создание подкаталога | Оба права: оглавление и запись |
| **RMD** | Удаление каталога | Оба права: удаление и оглавление. Права проверяются для удаляемого каталога, а не для родительского. |

# Приложение 2. Слова и выражения, употребимые в правилах*

Правила представляют собой интерпретируемые слово за словом программы на языке Форт (Forth - см. **http://www.forth.org.ru/**). Это язык, основу которого оставляет так называемый стек данных - структура, действующая по принципу LIFO (Last In - First Out; последним вошёл - первым вышел). Операторы, обычно называемые словами, помещают данные на стек и снимают их со стека. Синтаксические описания слов выглядят следующим образом:

**Слово ( значение1 значение2 -- значение3 )**

Такая запись означает примерно следующее: слово **Слово** снимает со стека два значения (на вершине стека при вызове слова находится **значение2**) и в качестве результата возвращает одно значение. Некоторые слова могут в качестве входных значений использовать следующий за ними фрагмент текста правил (это возможно, поскольку правила интерпретируются на лету слово за словом), что записывается так:

**Слово ( "строка" -- значение )**

Строки могут быть представлены двумя способами. Первый, классический - так называемые S-строки; для определения такой строки используются два значения - адрес строки и её длина (на вершину стека помещается длина). Второй способ - это так называемая STR-строка; она определяется одним значением, представляющим собой ссылку на специальную структуру данных, содержащую собственно текст строки и сведения о её длине. На основании STR-указателя с помощью специального слова можно получить ссылку на строку в S-формате. Обратное преобразование невозможно, зато возможно создать в памяти новую STR-строку, содержащую копию исходной S-строки.

Все слова регистрозависимы. В качестве разделителя между словами рекомендуется использовать пробел. Вообще-то интерпретатор в качестве разделителя принимает любые символы с кодом 32 (соответствующим пробелу) и меньше, но ряд слов, считывающих данные из текста правил, ориентируются только на пробел.

## *Контекстно-зависимые переменные*

Это слова-переменные, содержащие элементы контекста выполнения правила - такие, как переданные командами протокола адреса электронной почты, имя учётной записи и домен авторизации пользователя, компоненты web-запроса. Общим для них является то, что эти слова не используют и не снимают со стека никаких значений, они только возвращают значения - как правило, S-строку, хотя встречаются слова, возвращающие число или STR-указатель. Эти слова можно использовать не только при написании правил, но и в макроподстановках, генерирующих, например, уникальные имена каналов TrafC.

| Слово | Синтаксис | Действия |
|---|---|---|
| **Domain** | ( -- addr u ) | Результатом выполнения слова является S-строка, содержащая имя домена авторизации при последней попытке авторизации - независимо от успеха или неуспеха самой попытки. Если авторизация не выполнялась, возвращается строка нулевой длины. |
| **DomainLC** | ( -- addr u ) | Результатом выполнения слова является S-строка, содержащая приведённое к нижнему регистру имя домена авторизации при последней попытке авторизации - независимо от успеха или неуспеха самой попытки. Если авторизация не выполнялась, возвращается строка нулевой длины. |
| **DomainUC** | ( -- addr u ) | Результатом выполнения слова является S-строка, содержащая приведённое к верхнему регистру имя домена авторизации при последней попытке авторизации - независимо от успеха или неуспеха самой попытки. Если авторизация не выполнялась, возвращается строка нулевой длины. |
| **User** | ( -- addr u ) | Результатом выполнения слова является S-строка, содержащая имя учётной записи пользователя (логин) при последней попытке авторизации - независимо от успеха или неуспеха самой попытки. Если авторизация не выполнялась, возвращается строка нулевой длины. |

* *В основу раздела положен список, составленный Рувимом Пинкой*

| | | |
|---|---|---|
| **User-** | ( -- addr u ) | Результатом выполнения слова является S-строка, содержащая имя учётной записи пользователя (логин) при последней попытке авторизации. Если авторизация не выполнялась или попытка оказалась неудачной, возвращается строка из одного символа минуса **-**. |
| **UserEmail** | ( -- addr u ) | Результатом выполнения слова является S-строка, содержащая полное имя учётной записи пользователя в формате **логин@домен** при последней попытке авторизации - независимо от успеха или неуспеха самой попытки. Если авторизация не выполнялась, возвращается строка, состоящая из одного символа **@**. |
| **UserEmail-** | ( -- addr u ) | Результатом выполнения слова является S-строка, содержащая полное имя учётной записи пользователя в формате **логин@домен** при последней попытке авторизации. Если авторизация не выполнялась или попытка оказалась неудачной, возвращается строка из одного символа минуса **-**. |
| **UserLC** | ( -- addr u ) | Результатом выполнения слова является S-строка, содержащая приведённое к нижнему регистру имя учётной записи пользователя (логин) при последней попытке авторизации - независимо от успеха или неуспеха самой попытки. Если авторизация не выполнялась, возвращается строка нулевой длины. |
| **UserLC-** | ( -- addr u ) | Результатом выполнения слова является S-строка, содержащая приведённое к нижнему регистру имя учётной записи пользователя (логин) при последней попытке авторизации. Если авторизация не выполнялась или попытка оказалась неудачной, возвращается строка из одного символа минуса **-**. |
| **UserEmailLC** | ( -- addr u ) | Результатом выполнения слова является S-строка, содержащая приведённое к нижнему регистру полное имя учётной записи пользователя в формате **логин@домен** при последней попытке авторизации - независимо от успеха или неуспеха самой попытки. Если авторизация не выполнялась, возвращается строка, состоящая из одного символа **@**. |
| **UserEmailLC-** | ( -- addr u ) | Результатом выполнения слова является S-строка, содержащая приведённое к нижнему регистру полное имя учётной записи пользователя в формате **логин@домен** при последней попытке авторизации. Если авторизация не выполнялась или попытка оказалась неудачной, возвращается строка из одного символа минуса **-**. |
| **UserUC** | ( -- addr u ) | Результатом выполнения слова является S-строка, содержащая приведённое к верхнему регистру имя учётной записи пользователя (логин) при последней попытке авторизации - независимо от успеха или неуспеха самой попытки. Если авторизация не выполнялась, возвращается строка нулевой длины. |
| **UserUC-** | ( -- addr u ) | Результатом выполнения слова является S-строка, содержащая приведённое к верхнему регистру имя учётной записи пользователя (логин) при последней попытке авторизации. Если авторизация не выполнялась или попытка оказалась неудачной, возвращается строка из одного символа минуса **-**. |
| **UserEmailUC** | ( -- addr u ) | Результатом выполнения слова является S-строка, содержащая приведённое к верхнему регистру полное имя учётной записи пользователя в формате **логин@домен** при последней попытке авторизации - независимо от успеха или неуспеха самой попытки. Если авторизация не выполнялась, возвращается строка, состоящая из одного символа **@**. |

| | | |
|---|---|---|
| **UserEmailUC-** | ( -- addr u ) | Результатом выполнения слова является S-строка, содержащая приведённое к верхнему регистру полное имя учётной записи пользователя в формате **логин@домен** при последней попытке авторизации. Если авторизация не выполнялась или попытка оказалась неудачной, возвращается строка из одного символа минуса **-**. |
| **LUser** | ( -- addr u ) | Это слово определено в контексте прокси-сервера при активном плагине поддержки ограничителя трафика TrafC. Результатом выполнения слова является S-строка, содержащая приведённое к нижнему регистру имя учётной записи пользователя (логин) при последней попытке авторизации - независимо от успеха или неуспеха самой попытки. Если авторизация не выполнялась, возвращается строка нулевой длины. |
| **LUserEmail** | ( -- addr u ) | Это слово определено в контексте прокси-сервера при активном плагине поддержки ограничителя трафика TrafC. Результатом выполнения слова является S-строка, содержащая приведённое к нижнему регистру полное имя учётной записи пользователя в формате **логин@домен** при последней попытке авторизации - независимо от успеха или неуспеха самой попытки. Если авторизация не выполнялась, возвращается строка, состоящая из одного символа **@**. |
| **UUser** | ( -- addr u ) | Это слово определено в контексте прокси-сервера при активном плагине поддержки ограничителя трафика TrafC. Результатом выполнения слова является S-строка, содержащая приведённое к верхнему регистру имя учётной записи пользователя (логин) при последней попытке авторизации - независимо от успеха или неуспеха самой попытки. Если авторизация не выполнялась, возвращается строка нулевой длины. |
| **UUserEmail** | ( -- addr u ) | Это слово определено в контексте прокси-сервера при активном плагине поддержки ограничителя трафика TrafC. Результатом выполнения слова является S-строка, содержащая приведённое к верхнему регистру полное имя учётной записи пользователя в формате **логин@домен** при последней попытке авторизации - независимо от успеха или неуспеха самой попытки. Если авторизация не выполнялась, возвращается строка, состоящая из одного символа **@**. |
| **PeerIP** | ( – u ) | Результатом выполнения слова является число, содержащее IP-адрес клиента. Для его получения запрашивается текущее состояние подключения, поэтому после разрыва или штатного закрытия соединения результат не имеет смысла. |
| **vPeerIP** | ( – u ) | Результатом выполнения слова является число, содержащее IP-адрес клиента. Для его получения используется значение, запомненное при подключении клиента, поэтому результат имеет смысл и после разрыва или штатного закрытия соединения. |
| **CLIENT** | ( -- addr u ) | Результатом выполнения слова является S-строка, содержащая IP-адрес клиента. Для её получения запрашивается текущее состояние подключения, поэтому после разрыва или штатного закрытия соединения результат не имеет смысла. |
| **vCLIENT** | ( -- addr u ) | Результатом выполнения слова является S-строка, содержащая IP-адрес клиента. Для её получения используется значение, запомненное при подключении клиента, поэтому результат имеет смысл и после разрыва или штатного закрытия соединения. |

| | | |
|---|---|---|
| **PeerPort** | ( – u ) | Результатом выполнения слова является число, содержащее номер порта TCP, обслуживающего соединение со стороны клиента. Для его получения запрашивается текущее состояние подключения, поэтому после разрыва или штатного закрытия соединения результат не имеет смысла. |
| **vPeerPort** | ( – u ) | Результатом выполнения слова является число, содержащее номер порта TCP, обслуживающего соединение со стороны клиента. Для его получения используется значение, запомненное при подключении клиента, поэтому результат имеет смысл и после разрыва или штатного закрытия соединения. |
| **CLIENT_NAME** | ( -- addr u ) | Результатом выполнения слова является S-строка, содержащая DNS-имя клиента. Если имя установить не удаётся, то строка содержит IP-адрес клиента. Для её получения запрашивается текущее состояние подключения, поэтому после разрыва или штатного закрытия соединения результат не имеет смысла. |
| **CLIENT_MAC** | ( -- addr u ) | Результатом выполнения слова является S-строка, содержащая MAC-адрес клиента в виде последовательности из шести байтов, разделённых дефисом, в шестнадцатиричной нотации (например: **00-0C-6E-AD-29-58**). Если MAC-адрес определить не удаётся, строка содержит нули. Для её получения запрашивается текущее состояние подключения, поэтому после разрыва или штатного закрытия соединения результат не имеет смысла. |
| **IP** | ( – u ) | Результатом выполнения слова является число, содержащее IP-адрес активного сетевого интерфейса. Для его получения запрашивается текущее состояние подключения, поэтому после разрыва или штатного закрытия соединения результат не имеет смысла. |
| **vIP** | ( – u ) | Результатом выполнения слова является число, содержащее IP-адрес активного сетевого интерфейса. Для его получения используется значение, запомненное при подключении клиента, поэтому результат имеет смысл и после разрыва или штатного закрытия соединения. |
| **SERVER_IP** | ( -- addr u ) | Результатом выполнения слова является S-строка, содержащая IP-адрес активного сетевого интерфейса. Для её получения запрашивается текущее состояние подключения, поэтому после разрыва или штатного закрытия соединения результат не имеет смысла. |
| **vSERVER_IP** | ( -- addr u ) | Результатом выполнения слова является S-строка, содержащая IP-адрес активного сетевого интерфейса. Для её получения используется значение, запомненное при подключении клиента, поэтому результат имеет смысл и после разрыва или штатного закрытия соединения. |
| **Port** | ( – u ) | Результатом выполнения слова является число, содержащее номер порта TCP, обслуживающего соединение со стороны сервера. Для его получения запрашивается текущее состояние подключения, поэтому после разрыва или штатного закрытия соединения результат не имеет смысла. |
| **vPort** | ( – u ) | Результатом выполнения слова является число, содержащее номер порта TCP, обслуживающего соединение со стороны сервера. Для его получения используется значение, запомненное при подключении клиента, поэтому результат имеет смысл и после разрыва или штатного закрытия соединения. |

| | | |
|---|---|---|
| **SERVER_NAME** | ( -- addr u ) | Результатом выполнения слова является S-строка, содержащая DNS-имя активного сетевого интерфейса. Для её получения запрашивается текущее состояние подключения, поэтому после разрыва или штатного закрытия соединения результат не имеет смысла. |
| **COMMAND** | ( -- addr u ) | Результатом выполнения слова является S-строка, содержащая имя выполняемой команды протокола, преобразованное к верхнему регистру. Для HTTP-сервера и HTTP-прокси смысла не имеет, поскольку по стандарту протокола HTTP запрос является многострочным и исполняется по получении от клиента пустой строки, являющейся признаком-ограничителем. Таким образом, при исполнении запроса это слово возвращает строку нулевой длины. |
| **COMMANDLINE** | ( -- addr u ) | Результатом выполнения слова является S-строка, содержащая выполняемую командную строку со всеми переданными параметрами. Для HTTP-сервера и HTTP-прокси смысла не имеет; при исполнении запроса это слово возвращает строку нулевой длины. |
| **COMMANDLINE-** | ( -- addr u ) | Результатом выполнения слова является S-строка, содержащая выполняемую командную строку со всеми переданными параметрами. Если выполняемая команда содержит пароль, то пароль по соображениям секретности забит звёздочками. |
| **HTTP-COMMANDLINE** | ( -- addr u ) | Это слово определено в контексте прокси-сервера и имеет смысл только для HTTP-прокси. Результатом выполнения слова является S-строка, содержащая запрос, выполняемый HTTP-прокси. |
| **URL** | ( -- addr u ) | Это слово определено в контексте прокси-сервера и имеет смысл только для HTTP-прокси. Результатом выполнения слова является S-строка, содержащая запрошенную клиентом URL. |
| **METHOD** | ( -- addr u ) | Это слово определено в контексте прокси-сервера и имеет смысл только для HTTP-прокси. Результатом выполнения слова является S-строка, содержащая выполняемую команду протокола HTTP. |
| **TARGET-HOST** | ( -- addr u ) | Это слово определено в контексте прокси-сервера. Результатом выполнения слова является S-строка, содержащая имя целевого сервера. |
| **TARGET-PORT** | ( -- u ) | Это слово определено в контексте прокси-сервера. В результате выполнения слова на стек помещается номер порта целевого сервера. |
| **TARGET-PROT** | ( -- addr u ) | Это слово определено в контексте прокси-сервера. Результатом выполнения слова является S-строка, содержащая имя протокола или метода выполнения запроса. |
| **TARGET-URI** | ( -- addr u ) | Это слово определено в контексте прокси-сервера и имеет смысл только для HTTP-прокси. Результатом выполнения слова является S-строка, содержащая путь к объекту (URI) на целевом сервере. |
| **PIG.FTP-TARGET-FILE** | ( -- addr u ) | Это слово определено в контексте прокси-сервера и имеет смысл только для FTP-прокси. Результатом выполнения слова является S-строка, содержащая путь к объекту (URI) на целевом сервере. |
| **TargetIP** | ( – u ) | Это слово определено в контексте прокси-сервера. Результатом выполнения слова является число, содержащее IP-адрес целевого сервера. Для его получения запрашивается текущее состояние подключения, поэтому после разрыва или штатного закрытия соединения результат не имеет смысла. |

| | | |
|---|---|---|
| **IfaceIP** | ( – addr u ) | Это слово определено в контексте прокси-сервера. Результатом выполнения слова является S-строка, содержащая IP-адрес сетевого интерфейса, на котором открыто соединение с целевым сервером. Для её получения запрашивается текущее состояние подключения, поэтому после разрыва или штатного закрытия соединения результат не имеет смысла. |
| **IFACE** | ( – addr u ) | Это слово определено в контексте прокси-сервера. Результатом выполнения слова является S-строка, содержащая IP-адрес сетевого интерфейса, на котором открыто соединение с целевым сервером. Для её получения используется значение, запомненное при подключении к целевому серверу, поэтому результат имеет смысл и после разрыва или штатного закрытия соединения. |
| **INTERFACE-IP** | ( – addr u ) | Это слово определено в контексте прокси-сервера и имеет смысл только для FTP-прокси на этапе открытия пассивного сокета канала передачи данных. Результатом выполнения слова является S-строка, содержащая IP-адрес сетевого интерфейса, на котором открыто соединение. |
| **HOST-IP** | ( – addr u ) | Это слово определено в контексте прокси-сервера и имеет смысл только для FTP-прокси на этапе открытия пассивного сокета канала передачи данных. Результатом выполнения слова является S-строка, содержащая IP-адрес клиента или целевого сервера. |
| **REQUEST** | ( – addr u ) | Это слово определено в контексте HTTP-сервера. Результатом выполнения слова является S-строка, содержащая выполняемый сервером запрос. |
| **URI** | ( -- addr u ) | Это слово определено в контексте HTTP- и FTP-сервера. Результатом выполнения слова является S-строка, содержащая логический путь к запрашиваемому объекту. Её содержимое может отличаться от пути, реально переданного клиентом в запросе (для FTP-сервера отличается, как правило). |
| **QUERY_STRING** | ( -- addr u ) | Это слово определено в контексте HTTP-сервера. Результатом выполнения слова является S-строка, содержащая параметры CGI-запроса, выделенные из переданного в запросе URI. |
| **ROOT_DIR** | ( -- addr u ) | Это слово определено в контексте HTTP- и FTP-сервера. Результатом выполнения слова является S-строка, содержащая физический путь к назначенному корневому каталогу сайта. |
| **FILENAME** | ( -- addr u ) | Это слово определено в контексте HTTP- и FTP-сервера. Результатом выполнения слова является S-строка, содержащая физический путь к целевому файлу или каталогу. Для HTTP-сервера это слово имеет важную особенность - попытка использовать его на этапе анализа списка виртуальных каталогов может вызвать процедуру трансляции логического пути в физический и возможную модификацию самого логического пути. |
| **PIG.FILENAME** | ( -- addr u ) | Это слово определено в контексте HTTP-сервера. Результатом выполнения слова является S-строка, содержащая физический путь к целевому файлу или каталогу. Никаких побочных эффектов не имеет. |
| **PIG.STATIC-FILE** | ( -- addr u ) | Это слово определено в контексте HTTP-сервера. Результатом выполнения слова является S-строка, содержащая физический путь к целевому файлу или каталогу, вычисленный в предположении, что файл является статическим. |

| | | |
|---|---|---|
| **PIG.CGI-FILE** | ( -- addr u ) | Это слово определено в контексте HTTP-сервера. Результатом выполнения слова является S-строка, содержащая физический путь к целевому файлу или каталогу, вычисленный в предположении, что файл является сценарием. В этом режиме поддерживаются действительно виртуальные (не существующие на самом деле в физической иерархии сайта) каталоги. Несопоставленный остаток логического пути заносится в переменную **REAL_PATH_INFO**. |
| **PIG.DISCOVERED-PATH** | ( -- addr u ) | Это слово определено в контексте HTTP-сервера. Результатом выполнения слова является S-строка, содержащая сопоставленный с логическим физический путь. |
| **REAL_PATH_INFO** | ( -- addr u ) | Это слово определено в контексте HTTP-сервера. Результатом выполнения слова является S-строка, содержащая несопоставленный с физическим остаток логического пути к целевому объекту. |
| **Pig.IpAuthUser** | ( -- addr u ) | Это слово определено в контексте HTTP-сервера. Результатом выполнения слова является S-строка, содержащая полное имя учётной записи пользователя в формате **логин@домен**, назначенное в результате авторизации по IP или IP+MAC. |
| **CLIENT-URI** | ( -- addr u ) | Это слово определено в контексте FTP-сервера. Результатом выполнения слова является S-строка, содержащая исходно переданный в команде протокола логический путь к запрашиваемому объекту. |
| **PIG.ORIG-URI-** | ( -- addr u ) | Это слово определено в контексте FTP-сервера. Результатом выполнения слова является S-строка, содержащая исходно переданный в команде протокола логический путь к запрашиваемому объекту. Если пути в запросе не было, возвращается строка из одного символа минуса **-**. |
| **Pig.FtpUserEmail-** | ( -- addr u ) | Это слово определено в контексте FTP-сервера. Результатом выполнения слова является S-строка, содержащая имя учётной записи пользователя. Формат зависит от режима авторизации. Для гостевого режима возвращается просто имя пользователя. Для обычного режима возвращается полное имя в формате **логин@домен**. Если авторизация не выполнялась или попытка оказалась неудачной, возвращается строка из одного символа минуса **-**. |
| **PopFileActive?** | ( – flag ) | Это слово определено в контексте SMTP-сервера. В результате выполнения слова на стек будет помещено значение TRUE, если спам-фильтр POPfile загружен (точнее, загружен соответствующий плагин), и работа фильтра разрешена для текущего подключения. В противном случае на стек будет помещено значение FALSE. |
| **SpamProtexxActive?** | ( – flag ) | Это слово определено в контексте SMTP-сервера. В результате выполнения слова на стек будет помещено значение TRUE, если спам-фильтр SpamProtexx загружен, и работа фильтра разрешена для текущего подключения. В противном случае на стек будет помещено значение FALSE. |
| **LibSdActive?** | ( – flag ) | Это слово определено в контексте SMTP-сервера. В результате выполнения слова на стек будет помещено значение TRUE, если спам-фильтр LibSD загружен, и работа фильтра разрешена для текущего подключения. В противном случае на стек будет помещено значение FALSE. |

| | | |
|---|---|---|
| **BayesianAntispamActive?** | ( – flag ) | Это слово определено в контексте SMTP-сервера. В результате выполнения слова на стек будет помещено значение TRUE, если загружен и разрешён для текущего подключения хотя бы один из байсовых спам-фильтров POPfile, SpamProtexx, LibSD. В противном случае на стек будет помещено значение FALSE. |
| **ContentFilterActive?** | ( – flag ) | Это слово определено в контексте SMTP-сервера. В результате выполнения слова на стек будет помещено значение TRUE, если загружен упрощённый фильтр содержания, и его работа разрешена для текущего подключения. В противном случае на стек будет помещено значение FALSE. |
| **ContentTypeFilterActive?** | ( – flag ) | Это слово определено в контексте SMTP-сервера. В результате выполнения слова на стек будет помещено значение TRUE, если разрешена проверка по списку недопустимых типов содержимого. В противном случае на стек будет помещено значение FALSE. |
| **NobayesianAntispamActive?** | ( – flag ) | Это слово определено в контексте SMTP-сервера. В результате выполнения слова на стек будет помещено значение TRUE, если загружен и разрешён для текущего подключения упрощыннё фильтр содержания либо разрешена проверка по списку недопустимых типов содержимого. В противном случае на стек будет помещено значение FALSE. |
| **AntivirusActive?** | ( – flag ) | Это слово определено в контексте SMTP-сервера. В результате выполнения слова на стек будет помещено значение TRUE, если разрешена антивирусная проверка. В противном случае на стек будет помещено значение FALSE. |
| **Pig.NormalMode?** | ( – flag ) | Это слово определено в контексте SMTP-сервера. В результате выполнения слова на стек будет помещено значение TRUE, если письмо принято обычным образом по протоколу SMTP. В противном случае на стек будет помещено значение FALSE. |
| **Pig.Pop3Recv?** | ( – flag ) | Это слово определено в контексте SMTP-сервера. В результате выполнения слова на стек будет помещено значение TRUE, если письмо принято загрузчиком внешней POP-почты Pop2Smtp или Pop3Recv. В противном случае на стек будет помещено значение FALSE. |
| **Pig.LocalDelivery?** | ( – flag ) | Это слово определено в контексте SMTP-сервера. В результате выполнения слова на стек будет помещено значение TRUE, если письмо обрабатывается сервисом локальной доставки. В противном случае на стек будет помещено значение FALSE. |
| **Pig.SpecialMode?** | ( – flag ) | Это слово определено в контексте SMTP-сервера. В результате выполнения слова на стек будет помещено значение TRUE, если письмо принято загрузчиком внешней POP-почты Pop2Smtp или Pop3Recv либо обрабатывается сервисом локальной доставки. В противном случае на стек будет помещено значение FALSE. |
| **INCOMINGHOST** | ( -- addr u ) | Это слово определено в контексте SMTP-сервера. Результатом выполнения слова является S-строка, содержащая имя клиентского узла, переданное в протокольной команде HELO или EHLO. |
| **MAILFROM** | ( -- addr u ) | Это слово определено в контексте SMTP-сервера. Результатом выполнения слова является S-строка, содержащая адрес электронной почты отправителя. |

| | | |
|---|---|---|
| **MAILFROM-** | ( -- addr u ) | Это слово определено в контексте SMTP-сервера. Результатом выполнения слова является S-строка, содержащая адрес электронной почты отправителя. Если адрес пустой, возвращается строка из одного символа минуса **-**. |
| **PIG.MAILFROM** | ( -- addr u ) | Это слово определено в контексте SMTP-сервера. Результатом выполнения слова является S-строка, содержащая адрес электронной почты отправителя, в котором недопустимые с точки зрения файловой системы символы заменены символами подчёркивания. Поэтому возвращённую строку можно использовать для генерации пути к файлу. |
| **PIG.MAILFROM-** | ( -- addr u ) | Это слово определено в контексте SMTP-сервера. Результатом выполнения слова является S-строка, содержащая адрес электронной почты отправителя, в котором недопустимые с точки зрения файловой системы символы заменены символами подчёркивания. Поэтому возвращённую строку можно использовать для генерации пути к файлу. Если адрес пустой, возвращается строка из одного символа минуса **-**. |
| **PIG.SAVED-MAILFROM** | ( -- addr u ) | Это слово определено в контексте SMTP-сервера и имеет смысл на этапе формирования автоответа или извещения. Результатом выполнения слова является S-строка, содержащая адрес электронной почты отправителя исходного письма. |
| **PIG.SAVED-MAILFROM-** | ( -- addr u ) | Это слово определено в контексте SMTP-сервера и имеет смысл на этапе формирования автоответа или извещения. Результатом выполнения слова является S-строка, содержащая адрес электронной почты отправителя исходного письма. Если адрес пустой, возвращается строка из одного символа минуса **-**. |
| **RCPTTO** | ( -- addr u ) | Это слово определено в контексте SMTP-сервера. Результатом выполнения слова является S-строка, содержащая адрес электронной почты получателя письма. На этапе предварительно обработки адресов это адрес, переданный отправителем в команде протокола. На этапе доставки это адрес текущего получателя, определённый с учётом алиасов, переадресации и списков рассылки. |
| **PIG.REALRCPTTO** | ( -- addr u ) | Это слово определено в контексте SMTP-сервера. Результатом выполнения слова является S-строка, содержащая адрес электронной почты получателя письма. На этапе предварительно обработки адресов это адрес, определённый с учётом алиасов и переадресации. На этапе доставки это адрес текущего получателя, определённый с учётом алиасов, переадресации и списков рассылки, в котором недопустимые с точки зрения файловой системы символы заменены символами подчёркивания. Поэтому возвращённую строку можно использовать для генерации пути к файлу. |
| **H-MESSAGE-ID** | ( -- addr u ) | Это слово определено в контексте SMTP-сервера. Результатом выполнения слова является S-строка, содержащая заголовочное поле Message-ID - полностью, включая имя поля. Если поле в шапке принятого письма отсутствует, возвращается строка нулевой длины. |
| **MESSAGE-ID** | ( -- addr u ) | Это слово определено в контексте SMTP-сервера. Результатом выполнения слова является S-строка, содержащая заголовочное поле Message-ID - только само значение, не включая имя поля. Если поле в шапке принятого письма отсутствует либо отсутствует его значение, возвращается строка нулевой длины. |

| | | |
|---|---|---|
| **MESSAGE-ID-** | ( -- addr u ) | Это слово определено в контексте SMTP-сервера. Результатом выполнения слова является S-строка, содержащая заголовочное поле Message-ID - только само значение, не включая имя поля. Если поле в шапке принятого письма отсутствует либо отсутствует его значение, возвращается строка из одного символа минуса **-**. |
| **MESSAGE-ID-LOG** | ( -- addr u ) | Это слово определено в контексте SMTP-сервера. Результатом выполнения слова является S-строка, содержащая заголовочное поле Message-ID - только само значение, не включая имя поля. Символы точки с запятой, используемые в статистическом журнале собственного текстового формата в качестве разделителя полей, заменены символами подчёркивания. Если поле в шапке принятого письма отсутствует либо отсутствует его значение, возвращается строка нулевой длины. |
| **H-SAVED-MESSAGE-ID** | ( -- addr u ) | Это слово определено в контексте SMTP-сервера и имеет смысл на этапе формирования автоответа или извещения. Результатом выполнения слова является S-строка, содержащая заголовочное поле Message-ID исходного письма - полностью, включая имя поля. Если поле в шапке принятого письма отсутствует, возвращается строка нулевой длины. |
| **SAVED-MESSAGE-ID** | ( -- addr u ) | Это слово определено в контексте SMTP-сервера и имеет смысл на этапе формирования автоответа или извещения. Результатом выполнения слова является S-строка, содержащая заголовочное поле Message-ID исходного письма - только само значение, не включая имя поля. Если поле в шапке принятого письма отсутствует, возвращается строка нулевой длины. |
| **H-SUBJECT** | ( -- addr u ) | Это слово определено в контексте SMTP-сервера. Результатом выполнения слова является S-строка, содержащая заголовочное поле Subject (задающее тему письма) - полностью, включая имя поля. Если поле в шапке принятого письма отсутствует, возвращается строка нулевой длины. |
| **DECODED-SUBJECT** | ( -- addr u ) | Это слово определено в контексте SMTP-сервера. Результатом выполнения слова является S-строка, содержащая заголовочное поле Subject (задающее тему письма) - только само значение, не включая имя поля. Если поле в шапке принятого письма отсутствует, возвращается строка нулевой длины. |
| **DECODED-SUBJECT-LOG** | ( -- addr u ) | Это слово определено в контексте SMTP-сервера и имеет смысл на этапе формирования автоответа или извещения. Результатом выполнения слова является S-строка, содержащая заголовочное поле Subject (задающее тему письма) исходного письма - только само значение, не включая имя поля. Символы точки с запятой, используемые в статистическом журнале собственного текстового формата в качестве разделителя полей, заменены символами подчёркивания. Если поле в шапке принятого письма отсутствует, возвращается строка нулевой длины. |
| **REPLYFROM** | ( -- addr u ) | Это слово определено в контексте SMTP-сервера и имеет смысл на этапе формирования автоответа. Результатом выполнения слова является S-строка, содержащая адрес активного автоответчика. |
| **AUTOREPLYTO** | ( -- addr u ) | Это слово определено в контексте SMTP-сервера и имеет смысл на этапе формирования автоответа. Результатом выполнения слова является S-строка, содержащая адрес получателя автоответа. |

| | | |
|---|---|---|
| **REPLYURL** | ( -- addr u ) | Это слово определено в контексте SMTP-сервера и имеет смысл на этапе формирования автоответа. Результатом выполнения слова является S-строка, содержащая первый дополнительный параметр автоответа (обычно ссылку на HTML-страницу). |
| **REPLYNAME** | ( -- addr u ) | Это слово определено в контексте SMTP-сервера и имеет смысл на этапе формирования автоответа. Результатом выполнения слова является S-строка, содержащая второй дополнительный параметр автоответа (обычно имя автоответчика). |
| **SENT-FROM** | ( -- addr u ) | Это слово определено в контексте SMTP-сервера и имеет смысл на этапе формирования извещения. Результатом выполнения слова является S-строка, содержащая адрес робота-генератора извещения. |
| **NOTIFY-TO** | ( -- addr u ) | Это слово определено в контексте SMTP-сервера и имеет смысл на этапе формирования извещения. Результатом выполнения слова является S-строка, содержащая адрес получателя извещения. |
| **NOTE-PARAM1** | ( -- addr u ) | Это слово определено в контексте SMTP-сервера и имеет смысл на этапе формирования извещения. Результатом выполнения слова является S-строка, содержащая первый дополнительный параметр извещения. |
| **NOTE-PARAM2** | ( -- addr u ) | Это слово определено в контексте SMTP-сервера и имеет смысл на этапе формирования извещения. Результатом выполнения слова является S-строка, содержащая второй дополнительный параметр извещения. |
| **ROBOTFILENAME** | ( -- addr u ) | Это слово определено в контексте SMTP-сервера и имеет смысл на этапе обработки письма почтовым роботом. Результатом выполнения слова является S-строка, содержащая полный путь к копии файла письма, предназначенной для обработки роботом. |
| **ROBOTFILE** | ( -- addr u ) | Это слово определено в контексте SMTP-сервера и имеет смысл на этапе обработки письма почтовым роботом. Результатом выполнения слова является S-строка, содержащая полный путь к копии файла письма, предназначенной для обработки роботом. В отличие от **ROBOTFILENAME**, строка закавычена в соответствии с правилами написания длинных имён файлов. |
| **ClassifyDetails** | ( – str ) | Это слово определено в контексте SMTP-сервера при условии подключения (загрузки плагина) хотя бы одного из байсовых спам-фильтров POPfile, SpamProtexx, LibSD. Результатом выполнения слова является STR-строка, содержащая подробную информацию о работе каждого из активных фильтров. Если письмо не проверялось спам-фильтрами, возвращается нулевой указатель. |
| **CLASSIFY-DETAILS** | ( -- addr u ) | Это слово определено в контексте SMTP-сервера при условии подключения (загрузки плагина) хотя бы одного из байсовых спам-фильтров POPfile, SpamProtexx, LibSD. Результатом выполнения слова является S-строка, содержащая подробную информацию о работе каждого из активных фильтров. Если письмо не проверялось спам-фильтрами, возвращается пустая строка. |

| | | |
|---|---|---|
| **AV-DATABASE-INFO** | ( -- addr u ) | Это слово определено в контексте SMTP-сервера при условии подключения антивируса. Результатом выполнения слова является S-строка, содержащая информацию о типе и версии антивируса и текущем состоянии его баз в формате, пригодном для включения в текст письма-извещения. Если письмо не было проверено антивирусом по причине его временного отключения или в результате ошибки, возвращается пустая строка. |
| **X-AV-DATABASE-INFO** | ( -- addr u ) | Это слово определено в контексте SMTP-сервера при условии подключения антивируса. Результатом выполнения слова является S-строка, содержащая информацию о типе и версии антивируса и текущем состоянии его баз в формате, пригодном для включения в служебный заголовок проверенного письма. Если письмо не было проверено антивирусом по причине его временного отключения или в результате ошибки, возвращается пустая строка. |
| **SMTPSEND:NEW-BOUNDARY** | ( -- addr u ) | Это слово определено в контексте SMTP-сервера при активном сервисе расширенной доставки исходящей почты SmtpSend и предназначено для использования в шаблонах сообщений. Результатом выполнения слова является S-строка, содержащая уникальный разделитель MIME-секций письма. Строка также запоминается для последующего использования. Пример использования слова можно посмотреть в шаблонах расширенного сервиса доставки исходящей почты SmtpSend. |
| **SMTPSEND:BOUNDARY** | ( -- addr u ) | Это слово определено в контексте SMTP-сервера при активном сервисе расширенной доставки исходящей почты SmtpSend и предназначено для использования в шаблонах сообщений. Результатом выполнения слова является S-строка, содержащая разделитель MIME-секций письма, сгенерированный словом **SMTPSEND:NEW-BOUNDARY**. Пример использования слова можно посмотреть в шаблонах расширенного сервиса доставки исходящей почты SmtpSend. |
| **MSG-FOLDER** | ( -- addr u ) | Это слово определено в контексте POP/IMAP-сервера и имеет смысл только для IMAP-сервера. Результатом выполнения слова является S-строка, содержащая физический путь к папке IMAP, в которой находится письмо. Если выполняется перемещение письма, то это папка, в которую выполняется перемещение. |
| **MSG-FILE** | ( -- addr u ) | Это слово определено в контексте POP/IMAP-сервера и имеет смысл только для IMAP-сервера. Результатом выполнения слова является S-строка, содержащая физический путь к файлу обрабатываемого письма. |
| **TARGET-FOLDER** | ( -- addr u ) | Это слово определено в контексте POP/IMAP-сервера и имеет смысл только для IMAP-сервера. Результатом выполнения слова является S-строка, содержащая имя папки IMAP - без учёта иерархии, то есть, только имя папки самого нижнего уровня, - в которой находится письмо. Если выполняется перемещение письма, то это папка, в которую выполняется перемещение. |
| **TARGET-FOLDER-PATH** | ( -- addr u ) | Это слово определено в контексте POP/IMAP-сервера и имеет смысл только для IMAP-сервера. Результатом выполнения слова является S-строка, содержащая полный логический - от корня почтового ящика - путь к папке IMAP, в которой находится письмо. Если выполняется перемещение письма, то это папка, в которую выполняется перемещение. |

| | | |
|---|---|---|
| **TARGET-FILE** | ( -- addr u ) | Это слово определено в контексте POP/IMAP-сервера и имеет смысл только для IMAP-сервера. Результатом выполнения слова является S-строка, содержащая полный абсолютный физический путь к файлу обрабатываемого письма. |
| **TARGET-FILE-?WH** | ( -- addr u ) | Это слово определено в контексте POP/IMAP-сервера и имеет смысл только для IMAP-сервера. Результатом выполнения слова является S-строка, содержащая полный абсолютный физический путь к копии файла обрабатываемого письма, из которой удалены специфические заголовки, добавленные на этапе приёма письма по результатам его классификации антиспам-фильтрами. |
| **CURRENT-FOLDER** | ( -- addr u ) | Это слово определено в контексте POP/IMAP-сервера и имеет смысл только для IMAP-сервера. Результатом выполнения слова является S-строка, содержащая имя папки IMAP - без учёта иерархии, то есть, только имя папки самого нижнего уровня, - в которой письмо находилось до перемещения. |
| **CURRENT-FOLDER-PATH** | ( -- addr u ) | Это слово определено в контексте POP/IMAP-сервера и имеет смысл только для IMAP-сервера. Результатом выполнения слова является S-строка, содержащая полный логический - от корня почтового ящика - путь к папке IMAP, в которой письмо находилось до перемещения. |
| **PIG.USERMAILBOX** | ( -- addr u ) | Это слово определено в контексте POP/IMAP-сервера. Результатом выполнения слова является S-строка, содержащая полное имя почтового ящика (в формате **ящик@домен**) авторизовавшегося пользователя. Если почтовый ящик определить не удалось, возвращается строка нулевой длины. |
| **PIG.TARGET-BUCKET** | ( -- addr u ) | Это слово определено в контексте POP/IMAP-сервера и имеет смысл только для IMAP-сервера. Результатом выполнения слова является S-строка, содержащая целевую классификацию письма, назначенную для действия при перемещении письма между папками IMAP. Если класс не назначен, возвращается строка нулевой длины. |
| **RANDOM-ID** | ( -- addr u ) | Это слово определено в контексте SMTP- и POP/IMAP-сервера. Результатом выполнения слова является S-строка, содержащая уникальную последовательность символов. Эта строка может быть использована для генерации имён файлов. |
| **Pig.Reclassified?** | ( – flag ) | Это слово определено в контексте POP/IMAP-сервера и имеет смысл только для IMAP-сервера. Результатом выполнения слова является логическое значение, указывающее, производилась ли при перемещении письма между папками IMAP его переклассификация антиспам-фильтрами. |
| **Pig.OnReclassify** | ( – flag ) | Это слово определено в контексте POP/IMAP-сервера и имеет смысл только для IMAP-сервера. Результатом выполнения слова является логическое значение, указывающее, выполнять ли перепосылку письма после его перемещения между папками IMAP в зависимости или вне зависимости от факта его переклассификации. |

## *Слова для обработки данных*

Это слова, используемые для обработки значений, возвращаемых контекстно-зависимыми словами. За исключением нескольких констант (которые по определению не являются контекстно-зависимыми, хотя и ведут себя похожим образом), все они используют ранее помещённые на стек значения. Поэтому использование их в макроподстановках ограничено (хотя возможно) и требует повышенной осторожности.

| Слово | Синтаксис | Действия |
|---|---|---|

| | | |
|---|---|---|
| **TRUE** | ( -- flag ) | Константа, имеющая числовое значение -1 и интепретируемая как значение логической истины. Собственно, Форт в качестве истины воспринимает любое ненулевое значение, но попытки составить из таких "неполных" значений сложное логическое выражение могут дать на выходе совсем не соответствующий ожиданиям результат. |
| **FALSE** | ( -- flag ) | Константа, имеющая числовое значение 0 и интепретируемая как значение логической лжи. |
| **\|** | ( flag -- ) | Это слово используется в строках файла правил. Часть строки справа от \| выполняется, если условие (левая часть, которая должна поместить на стек одно значение) TRUE. |
| **[IF]** | ( flag -- ) | Это слово начинает блок условного выполнения. Слова, заключённые в этом блоке, выполняются, если на стеке находится значение TRUE. |
| **[ELSE]** | ( -- ) | Это слово начинает альтернативный блок условного выполнения. Слова, заключённые в этом блоке, выполняются, если при выполнении слова **[IF]** на стеке находилось значение FALSE. |
| **[THEN]** | ( -- ) | Это слово завершает блок условного выполнения. |
| **IP=** | ( "ip_address" -- flag ) | В результате выполнения слова на стек будет помещено значение TRUE, если клиентское подключение принято на сетевой интерфейс с указанным адресом. В противном случае на стек будет помещено значение FALSE. Пример: **IP= 10.0.0.1** |
| **Port=** | ( "port" -- flag ) | В результате выполнения слова на стек будет помещено значение TRUE, если клиентское подключение принято указанный порт сервера. В противном случае на стек будет помещено значение FALSE. Пример: **Port= 80** |
| **IP:Port=** | ( "ip_address:port" -- flag ) | В результате выполнения слова на стек будет помещено значение TRUE, если клиентское подключение принято на сетевой интерфейс с указанным адресом и на указанный порт. В противном случае на стек будет помещено значение FALSE. Пример: **IP:Port= 10.0.01:80** |
| **PeerIP=** | ( "ip_address" -- flag ) | В результате выполнения слова на стек будет помещено значение TRUE, если IP-адрес клиента равен указанному. В противном случае на стек будет помещено значение FALSE. Пример: **PeerIP= 10.0.0.1** |

| | | |
|---|---|---|
| **PeerPort=** | ( "port" -- flag ) | В результате выполнения слова на стек будет помещено значение TRUE, если порт клиента равен указанному (обычно такое условие смысла не имеет, поскольку порты для клиентских подключений назначаются динамически и достаточно произвольно, однако в ряде случаев именно порт на стороне клиента должен иметь вполне определённый номер). В противном случае на стек будет помещено значение FALSE. Пример: **PeerPort= 20** |
| **PeerIP:Port=** | ( "ip_address:port" -- flag ) | В результате выполнения слова на стек будет помещено значение TRUE, если IP-адрес и порт клиента равны указанным. В противном случае на стек будет помещено значение FALSE. Пример: **PeerIP:Port= 10.0.0.1:20** |
| **PeerIP:Mask=** | ( "ip_address:mask" -- flag ) | В результате выполнения слова на стек будет помещено значение TRUE, если IP-адрес клиента попадает в заданную базовым адресом и маской подсеть. В противном случае на стек будет помещено значение FALSE. Пример: **PeerIP:Mask= 10.0.0.1:255.255.255.0** |
| **DayOfWeek:** | ( "n1-n2" -- flag ) | В результате выполнения слова на стек будет помещено значение TRUE, если день недели укладывается в диапазон от n1 до n2. В противном случае на стек будет помещено значение FALSE. Дни недели нумеруются от 0 (воскресенье) до 6 (суббота). Пример: **DayOfWeek: 1-5** |
| **TimeInterval:** | ( "hh:mm-hh:mm" -- flag ) | В результате выполнения слова на стек будет помещено значение TRUE, если текущее время с точностью до минуты укладывается в заданный диапазон. В противном случае на стек будет помещено значение FALSE. Пример: **TimeInterval: 8:30-17:00** |
| **Time:** | ( "hh:mm" -- flag ) | В результате выполнения слова на стек будет помещено значение TRUE, если текущее время с точностью до минуты равно указанному. В противном случае на стек будет помещено значение FALSE. Пример: **Time: 8:30** |
| **Pop3Recv:SinceLastPoll:** | ( "[hh:]mm" -- flag ) | Это слово определено в контексте SMTP-сервера при активном загрузчике внешней POP-почты **Pop3Recv** и имеет смысл только для загрузчика. В результате выполнения слова на стек будет помещено значение TRUE, если с момента начала предыдущего опроса прошло больше указанного времени. В противном случае на стек будет помещено значение FALSE. При использовании слова в общем условии опроса за точку отсчёта принимается начало цикла опроса, при использовании в условии опроса ящика - начало опроса проверяемого ящика. Пример: **Pop3Recv:SinceLastPoll: 45** |

| | | |
|---|---|---|
| **EvalRules** | ( ... addr u -- ... ) | Выполняет правило, имя которого задаётся находящейся на стеке строкой. Правило может быть как встроенным (Форт-словом), так и внешним (файлом **имя.rules.txt**). Сначала производится поиск встроенного правила; при его отсутствии файл внешнего правила последовательно ищется в подкаталогах **myconf**, **..\CommonPlugins** и **conf**. Если правило не обнаруживается, генерируется ошибка. Количество и назначение величин, снимаемых со стека и помещаемых на стек, определяется правилом. |
| **EvalRules:** | ( ... "имя" - ... ) | Выполняет правило, имя которого задаётся в тексте выполняемого правила. Правило может быть как встроенным (Форт-словом), так и внешним (файлом **имя.rules.txt**). Сначала производится поиск встроенного правила; при его отсутствии файл внешнего правила последовательно ищется в подкаталогах **myconf**, **..\CommonPlugins** и **conf**. Если правило не обнаруживается, генерируется ошибка. Количество и назначение величин, снимаемых со стека и помещаемых на стек, определяется правилом. |
| **EvalRulesIfExists** | ( ... addr u -- ... ) | Выполняет правило, имя которого задаётся находящейся на стеке строкой. Отличается от **EvalRules** тем, что при необнаружении правила выполнение продолжается без ошибок. |
| **EvalRulesIfExists:** | ( ... "имя" - ... ) | Выполняет правило, имя которого задаётся в тексте выполняемого правила. Отличается от **EvalRules:** тем, что при необнаружении правила выполнение продолжается без ошибок. |
| **IsInFile** | ( addr1 u1 addr2 u2 -- flag ) | Выполняет поиск S-строки addr1 u1 в файле-списке, имя которого задано строкой addr2 u2. Поиск производится по первому полю, которое рассматривается как шаблон, могущий содержать символы групповой операции ***** и **?**. Раскрытие макроподстановок не выполняется. Если искомый образец найден, на стек помещается значение TRUE, при этом специальные слова **FIELD1**, **FIELD2** (и так далее, вплоть до **FIELD11**) заполняются значениями полей строки, в которой найдено совпадение. Если образец не найден, на стек помещается значение FALSE, а специальные слова возвращают строки нулевой длины. Подробнее о формате списков см. раздел **Назначение и формат управляющих списков**. |
| **IsInFile:** | ( addr u "имя" -- flag ) | Выполняет поиск S-строки addr u в файле-списке, имя которого задано в тексте выполняемого правила. Во всём остальном подобно слову **IsInFile**. |

| | | |
|---|---|---|
| **IsInFile2** | ( a1 u1 a2 u2 a3 u3 -- flag ) | Выполняет поиск S-строк a1 u1 и a2 u2 в файле-списке, имя которого задано строкой a3 u3. Поиск производится по первому и второму полям, которые рассматриваются как шаблоны, могущие содержать символы групповой операции ***** и **?**. Раскрытие макроподстановок не выполняется. Первая строка ищется в первом поле, вторая - во втором. При обнаружении одновременного совпадения на стек помещается значение TRUE, при этом заполняются специальные слова **FIELD1** - **FIELD11**. Если совпадение не обнаружено, на стек помещается значение FALSE, а специальные слова возвращают строки нулевой длины. |
| **IsInFile2:** | ( a1 u1 a2 u2 "имя" -- flag ) | Выполняет поиск S-строк a1 u1 и a2 u2 в файле-списке, имя которого задано в тексте выполняемого правила. Во всём остальном подобно слову **IsInFile2**. |
| **IsInFile3** | ( a1 u1 a2 u2 a3 u3 a4 u4 -- flag ) | Выполняет поиск S-строк a1 u1, a2 u2 и a3 u3 в файле-списке, имя которого задано строкой a4 u4. Поиск производится по первому, второму и третьему полям, которые рассматриваются как шаблоны, могущие содержать символы групповой операции ***** и **?**. Раскрытие макроподстановок не выполняется. Первая строка ищется в первом поле, вторая - во втором, третья - в третьем. При обнаружении одновременного совпадения на стек помещается значение TRUE, при этом заполняются специальные слова **FIELD1** - **FIELD11**. Если совпадение не обнаружено, на стек помещается значение FALSE, а специальные слова возвращают строки нулевой длины. |
| **IsInFile3:** | ( a1 u1 a2 u2 a3 u3 "имя" -- flag ) | Выполняет поиск S-строк a1 u1, a2 u2 и a3 u3 в файле-списке, имя которого задано в тексте выполняемого правила. Во всём остальном подобно слову **IsInFile3**. |
| **EvalForEachFileRecordRules** | ( a1 u1 a2 u2 -- ) | Выполняет правило, имя которого задано строкой a2 u2, для каждой строки списка, имя которого задано строкой a1 u1. При выполнении правила содержимое строки списка доступно путём обращения к специальным словам **FIELD1** - **FIELD11**. Выполняемое правило не должно изменять стек данных. |
| **EvalForEachFileRecordRules:** | ( "список" "правило" -- ) | Выполняет правило, имя которого задано в тексте выполняемого правила, для каждой строки списка, имя которого задано в тексте выполняемого правила. Во всём остальном подобно слову **EvalForEachFileRecordRules**. |

| | | |
|---|---|---|
| **EvalIsInFileRules** | ( a1 u1 a2 u2 -- flag ) | Выполняет правило, имя которого задано строкой a2 u2, для каждой строки списка, имя которого задано строкой a1 u1. При выполнении правила содержимое строки списка доступно путём обращения к специальным словам **FIELD1** - **FIELD11**. Выполняемое правило должно возвращать на стеке одно значение. Если это значение FALSE, анализ списка продолжается дальше, в противном случае анализ списка прерывается. Если анализ списка был прерван, на стек помещается значение TRUE, при этом специальные слова **FIELD1** - **FIELD11** имеют значения, соответствующие строке, на которой был прерван анализ. В противном случае на стек помещается значение FALSE, а специальные слова возвращают строки нулевой длины. |
| **EvalIsInFileRules:** | ( "список" "правило" -- flag ) | Выполняет правило, имя которого задано в тексте выполняемого правила, для каждой строки списка, имя которого задано в тексте выполняемого правила. Во всём остальном подобно слову **EvalIsInFileRules**. |
| **=~** | ( addr u "mask" -- flag ) | В результате выполнения слова на стек будет помещено значение TRUE, если находящаяся на стеке S-строка соответствует указанному шаблону сравнения. В противном случае на стек будет помещено значение FALSE. В шаблоне допустимы символы групповой операции ***** и **?**. Пример: **URL =~ http://*** |
| **~** | ( str "mask" -- flag ) | В результате выполнения слова на стек будет помещено значение TRUE, если находящаяся на стеке STR-строка соответствует указанному шаблону сравнения. В противном случае на стек будет помещено значение FALSE. В шаблоне допустимы символы групповой операции ***** и **?**. Пример: **MailFrom ~ *@rambler.ru** |
| **COMPARE** | ( a1 u1 a2 u2 -- flag ) | Выполняет посимвольное сравнение двух находящихся на стеке S-строк. Сравнение выполняется с учётом регистра символов по типовым правилам сравнения строк. Помещаемый на стек результат представляет собой число со знаком, определяющее результат сравнения - больше, меньше или равно. Если строки одинаковые, на стек помещается нулевое значение. |
| **COMPARE-U** | ( a1 u1 a2 u2 -- flag ) | Выполняет посимвольное сравнение двух находящихся на стеке S-строк без учёта регистра латинских символов (нелатинские сравниваются с учётом регистра). В остальном подобно слову **COMPARE**. |

| | | |
|---|---|---|
| **WildCMP-U** | ( a1 u1 a2 u2 -- flag ) | Выполняет сопоставление S-строки a1 u1 с шаблоном сравнения, представленным S-строкой a2 u2. Сопоставление производится без учёта регистра латинских символов (нелатинские сравниваются с учётом регистра). Результатом сопоставления является число со знаком, определяющее результат сопоставления - больше, меньше или равно. Если строка соответствует шаблону, на стек помещается нулевое значение. В шаблоне допустимы метасимволы групповой операции ***** и **?**. |
| **Match-U** | ( a1 u1 a2 u2 -- flag ) | Выполняет расширенное сопоставление S-строки a1 u1 с шаблоном сравнения, представленным S-строкой a2 u2. Сопоставление производится без учёта регистра латинских символов (нелатинские сравниваются с учётом регистра). Результатом сопоставления является число со знаком, определяющее результат сопоставления - больше, меньше или равно. Если строка соответствует шаблону, на стек помещается нулевое значение. Если сравнение выполняется слишком долго, возвращается специальное значение -2. В шаблоне допустимы метасимволы групповой операции, перечисленные в начале раздела **Назначение и формат управляющих списков**. |
| **STR@** | ( str -- addr u ) | Выполняет преобразование строки из STR-формата в S-формат. |
| **S@** | ( addr1 u1 -- addr2 u2 ) | Выполняет раскрытие макроподстановок (**{}**), содержащихся в исходной строке. При этом создаётся новая строка, параметры которой помещаются на стек. |
| **DUP** | ( x -- x x ) | Дублирует находящееся на стеке значение. |
| **2DUP** | ( x1 x2 -- x1 x2 x1 x2 ) | Дублирует находящуюся на стеке пару значений. |
| **DROP** | ( x -- ) | Снимает со стека одно значение. |
| **2DROP** | ( x1 x2 -- ) | Снимает со стека пару значений. |
| **SWAP** | ( x1 x2 -- x2 x1 ) | Меняет местами два верхних значения на стеке. |
| **2SWAP** | ( x1 x2 x3 x4 -- x3 x4 x1 x2 ) | Меняет местами две верхних пары значений на стеке. |
| **NIP** | ( x1 x2 -- x2 ) | Снимает со стека второе значение (эквивалентно **SWAP DROP**). |
| **0=** | ( x -- flag ) | В результате выполнения слова на стек будет помещено значение TRUE, если находящееся на стеке значение нулевое. В противном случае на стек будет помещено значение FALSE. |

| | | |
|---|---|---|
| **0<>** | ( x -- flag ) | В результате выполнения слова на стек будет помещено значение TRUE, если находящееся на стеке значение ненулевое. В противном случае на стек будет помещено значение FALSE. |
| **<** | ( n1 n2 -- flag ) | В результате выполнения слова на стек будет помещено значение TRUE, если n1 меньше, чем n2. В противном случае на стек будет помещено значение FALSE. При сравнении учитывается знак числа. |
| **>** | ( n1 n2 -- flag ) | В результате выполнения слова на стек будет помещено значение TRUE, если n1 больше, чем n2. В противном случае на стек будет помещено значение FALSE. При сравнении учитывается знак числа. |
| **U<** | ( u1 u2 -- flag ) | В результате выполнения слова на стек будет помещено значение TRUE, если u1 меньше, чем u2. В противном случае на стек будет помещено значение FALSE. Сравнение беззнаковое, то есть, сравниваемые значения считаются неотрицательными. |
| **U>** | ( u1 u2 -- flag ) | В результате выполнения слова на стек будет помещено значение TRUE, если u1 больше, чем u2. В противном случае на стек будет помещено значение FALSE. Сравнение беззнаковое, то есть, сравниваемые значения считаются неотрицательными. |
| **AND** | ( x1 x2 -- x3 ) | Вычисляет результат побитовой операции И над x1 и x2. |
| **OR** | ( x1 x2 -- x3 ) | Вычисляет результат побитовой операции ИЛИ над x1 и x2. |
| **XOR** | ( x1 x2 -- x3 ) | Вычисляет результат побитовой операции исключающего ИЛИ над x1 и x2. |
| **\EOF** | ( -- ) | Это слово прерывает выполнение текущего файла правил. |
| **NEW-MESSAGE-ID** | ( a1 u1 -- a2 u2 ) | Это слово определено в контексте SMTP-сервера для использования в шаблонах сообщений. Результатом выполнения слова является S-строка, содержащая заголовочное поле Message-ID с новым уникальным значением, включающим в себя исходно размешённую на стеке S-строку. Строка также заменяет значение, возвращаемое словом **H-MESSAGE-ID** и его производными. Пример использования слова можно посмотреть в шаблонах расширенного сервиса доставки исходящей почты SmtpSend. |

| | | |
|---|---|---|
| **NEW-SUBJECT:** | ( "текст" -- a u ) | Это слово определено в контексте SMTP-сервера для использования в шаблонах сообщений. Результатом выполнения слова является S-строка, содержащая заголовочное поле Subject, в содержимое которого включается весь остаток строки до завершающей фигурной скобки. Разумеется, сами фигурные скобки в текст включать нельзя, поэтому макроподстановки не поддерживаются. Строка также заменяет значение, возвращаемое словом **H-SUBJECT** и его производными. Пример использования слова можно посмотреть в шаблонах расширенного сервиса доставки исходящей почты SmtpSend. |

# Приложение 3. Предустановленные почтовые роботы

## *Список динамической общедоменной рассылки*

Расположение: **acSMTP\conf\smtp\robots\DomainLister**
Тип робота: **встроенный**
Команда запуска: **smtp\robots\DomainLister\RunRobot**
Индивидуальный плагин: **отсутствует**

Робот представляет собой специальное расширение стандартных списков рассылки. Источником адресов для робота является список локальных почтовых ящиков. Получив письмо, робот просматривает этот список в поиске почтовых ящиков, принадлежащих тому же домену, что и робот, и помеченных специальным флагом **L**. В эти ящики и будет выполнена окончательная доставка письма. Для обеспечения работы робота должна быть включена поддержка списков рассылки.

Никаких дополнительных проверок в отношении отправителя робот не выполняет.

## *Пополнение списков запрещённых и доверенных отправителей - явное указание адреса*

Расположение: **acSMTP\conf\smtp\robots\ListEmail**
Тип робота: **встроенный**
Команда запуска: **smtp\robots\ListEmail\RunRobot**
Индивидуальный плагин: **отсутствует**

Назначение робота - по запросам пользователей, не имеющих доступа к web-интерфейсу администратора, пополнять списки запрещённых и доверенных отправителей. Робот распознаёт и интерпретирует следующие команды, передаваемые в теме письма:

| Команда | Описание |
|---|---|
| **Blacklist xxx@yyy** | Адрес, являющийся параметром команды, заносится в список запрещённых отправителей. |
| **Whitelist xxx@yyy** | Адрес, являющийся параметром команды, заносится в список доверенных отправителей. |

Чтобы исключить дублирование и различные конфликты, робот проверяет наличие добавляемых адресов в пополняемых списках, а также в списке локальных почтовых ящиков. Синтаксическая правильность адресов роботом проверяется в минимальной степени.

Никаких дополнительных проверок в отношении отправителя робот не выполняет.

## *Пополнение списков запрещённых и доверенных отправителей - неявное указание адреса*

Расположение: **acSMTP\conf\smtp\robots\ListMailSender**
Тип робота: **встроенный**
Команда запуска: **smtp\robots\ListMailSender\RunRobot**
Индивидуальный плагин: **отсутствует**

Назначение робота - по запросам пользователей, не имеющих доступа к web-интерфейсу администратора, пополнять списки запрещённых и доверенных отправителей. Адреса для занесения в списки извлекаются из оригинальных почтовых сообщений, которые пересылаются роботу в виде вложений. В одном письме-конверте может быть несколько оригинальных сообщений. Для хранения адресов используется специальное служебное заголовочное поле X-E3-Mailfrom. Робот распознаёт и интерпретирует следующие команды, передаваемые в теме письма:

| Команда | Описание |
|---|---|
| **Blacklist domain** | Почтовый домен отправителя оригинального письма заносится в список запрещённых отправителей. |
| **Blacklist address** | Адрес отправителя оригинального письма как есть заносится в список запрещённых отправителей. |
| **Blacklist** | Адрес отправителя оригинального письма как есть заносится в список запрещённых отправителей. |

| | |
|---|---|
| **Whitelist** | Адрес отправителя оригинального письма как есть заносится в список доверенных отправителей. |

Чтобы исключить дублирование и различные конфликты, робот проверяет наличие добавляемых адресов в пополняемых списках, а также в списке локальных почтовых ящиков. Синтаксическая правильность адресов роботом проверяется в минимальной степени.

Для своей работы робот использует возможности контент-анализатора MContent.

Никаких дополнительных проверок в отношении отправителя робот не выполняет.

## *Переклассификация писем спам-фильтрами без использования протокола IMAP*

Расположение: **acSMTP\conf\smtp\robots\MailClassify**
Тип робота: **встроенный**
Команда запуска: **smtp\robots\MailClassify\RunRobot**
Индивидуальный плагин: **отсутствует**

Назначение робота - по запросам пользователей, не имеющих возможности использовать подключение по протоколу IMAP, выполнять переклассификацию писем байесовыми спам-фильтрами POPfile, SpamProtexx и LibSD. Оригинальные почтовые сообщения, подлежащие переклассификации, пересылаются роботу в виде вложений. В одном письме-конверте может быть несколько оригинальных сообщений. Требуемый класс для писем указывается в теме письма-конверта. Класс должен быть допустим хотя бы для одного из активных спам-фильтров.

Для своей работы робот использует возможности контент-анализатора MContent.

Никаких дополнительных проверок в отношении отправителя робот не выполняет.

# Приложение 4. История версий

## *2009 год*

***20 марта 2009 года.*** **Версия 2.0**:
- + Это первая версия PigMail+PigProxy, выпущенная в виде самодостаточного пакета

***21 марта 2009 года.*** **Версия 2.0a**:
- Исправлена ошибка в программе установки, приводившая к перезаписи файлов установленного расширения поддержки ведения статистики в базе данных MStat (спасибо **leka**)

***24 марта 2009 года.*** **Версия 2.0b**:
- Программа установки: реализовано корректное ожидание остановки и запуска служб (спасибо **leka**)
- Web-интерфейс: реализовано корректное ожидание остановки и запуска служб

***23 ноября 2009 года.*** **Версия 2.1**:
- + FTP-прокси: добавлена возможность задавать последовательность символов, используемую в качестве разделителя реквизитов авторизации на целевом сервере и на прокси (**FtpProxy[AuthDelimiter]**) (спасибо **grass_snake**)
- + HTTP-прокси: добавлена возможность автоматической авторизации пользователей на целевых HTTP-серверах (**HttpProxy[UseHttpAutoLogon]**, **HttpProxy[HttpAutoLogon]**) (идея **ND**)
- Web-интерфейс: исправлены замеченные ошибки отображения параметров в редакторе настроек и списков (спасибо **Volodya_Lentsik**)
- * SMTP-сервер: расширено начальное значение набора символов, запрещённых в адресе электронной почты (**SMTP[DenyLocalPartCharacters]**)
- Web-интерфейс: в обработчике встроенных отчётов исправлено некорректное сообщение об ошибке (спасибо **grass_snake**)
- Web-интерфейс: в редакторе настроек ослаблено слишком жёсткое ограничение на длину поля шаблона команды архивации вложений в настройках контент-анализатора **MContent** (спасибо **grass_snake**)
- + Web-интерфейс: в редакторе настроек и списков корректно обрабатываются параметры и поля, содержащие символы двойной кавычки **"**
- + Все серверы: обеспечена совместимость с изменениями в ядре Eserv версии 3.36
- + SMTP-сервер: в загрузчик внешней POP-почты **Pop3Recv** добавлена возможность работы с использованием защищённого (SSL) соединения (**Pop3Recv[Certificate]**, **Pop3Recv[SslVerifyServer]**). Изменился формат списка опрашиваемых почтовых ящиков (**Boxes**) (старый формат поддерживается для выполнения). При ручном обновлении версии необходимо выполнить проверку управляющих списков и шаблонов
- + SMTP-сервер: список опрашиваемых почтовых ящиков (**Boxes**) загрузчика внешней POP-почты **Pop3Recv** теперь доступен для редактирования не только во время паузы, но и в течение цикла опроса
- + SMTP-сервер: идентификаторы обработанных загрузчиком внешней POP-почты **Pop3Recv** писем теперь хранятся не в текстовом списке, а в базе данных (**Pop3Recv[Pop3RecvDB]**)
- + SMTP-сервер: загрузчик внешней POP-почты **Pop3Recv** позволяет в условии опроса указывать время, прошедшее с момента начала предыдущего опроса (слово **Pop3Recv:SinceLastPoll:**)
- SMTP-сервер: в сервисе расширенной доставки исходящей почты **SmtpSend** исправлено ошибочное увеличение предельного срока хранения письма в очереди на одну единицу измерения (час или день, в зависимости от очереди) (спасибо **Dandy**)
- Web-интерфейс: исправлена ошибка потери текста при редактировании файла SSL-сертификата для сервиса расширенной доставки исходящей почты **SmtpSend**
- Web-интерфейс: исправлены устаревшие ссылки в строке меню
- Web-интерфейс: исправлены обнаруженные ошибки в формировании некоторых встроенных отчётов
- + Программа установки: справка по начальным настройкам PigMail+PigProxy включена в дистрибутив
- + SMTP-сервер: небольшая оптимизация плагина MailRoll
- Все серверы: исправлена косметическая ошибка в плагине SNMP - отметка о запуске не выводилась в главный журнал
- + SMTP-сервер: сервис расширенной доставки исходящей почты **SmtpSend** больше не блокирует редактирование списка получателей "чужих" доменов (**EmailSmtpForward**) на время обработки очередей фиксированных маршрутов
- + SMTP-сервер: упрощённый фильтр содержания больше не блокирует редактирование списка шаблонов запрещённого содержимого тела письма (**BlackListBody**) на время анализа письма
- + Программа установки: реализован импорт настроек и данных из существующей установки PigMail+PigProxy версии 1

- + Прокси-сервер: добавлены новые параметры тонкой настройки производительности (**PROXY[PacketSize]**, **PROXY[MappingBufferSize]**) (спасибо **grass_snake** и **ac**)
- + SMTP-сервер: исключён ряд бесполезных проверок при работе загрузчика внешней POP-почты **Pop2Smtp**
- * SMTP-сервер: загрузчик внешней POP-почты **Pop3Recv** по умолчанию не принимает письма для локально не существующих адресатов многосерверного домена (спасибо **Alexander Zakharzhevskiy**). Поведение может быть изменено настройками (**SMTP[PopMultiSite]**)
- + SMTP-сервер, прокси-сервер: цикл проверки обновления вирусных баз антивируса KAV/KAVE не прерывается при ошибке загрузки. В этом случае через минуту предпринимается повторная попытка загрузить базы
- + SMTP-сервер: исходящий спам, передаваемый на обработку спам-администратору, не подвергается обработке контент-анализатором **MContent**
- + SMTP-сервер: плагин MailRoll не заносит в базу и не проверяет историю в случае пустого адреса отправителя. Уже имеющиеся записи с пустым адресом отправителя удаляются из базы при загрузке плагина. В процессе работы плагин производит очистку базы от случайных записей
- Web-интерфейс: исправлены ошибки на странице управления квотами
- Elog: исправлены ошибки в редакторе настроек
- + SMTP-сервер: идентификаторы обработанных спам-писем, принятых из внешних POP-ящиков, хранятся не в текстовом списке, а в базе данных (**Antispam[MessageIdDB]**)
- SMTP-сервер: исправлены замеченные ошибки в обработке некорректных адресов получателей
- + SMTP-сервер: добавлена возможность проверки адресов нелокальных получателей на целевом сервере (**SMTP[ValidateMultisiteRcpts]**, **SMTP[ValidateForwardedRcpts]**, **SMTP[ValidateExternRcpts]**)
- + FTP-сервер: ограничение числа попыток неуспешной авторизации действует также и на попытки гостевого входа в случае его запрета (спасибо **leka**)
- + HTTP-сервер: добавлена поддержка режима сценариев FastCGI
- + Все серверы: добавлена возможность автоматической блокировки атак подбора пароля (**Server[LockIntruders]**, **Server[IdsMemoDB]**, **Server[AuthFailCount]**, **Server[AuthFailPeriod]**, **SMTP[LockIntruders]**, **SMTP[AuthFailCount]**, **SMTP[AuthFailPeriod]**, **POP[LockIntruders]**, **POP[AuthFailCount]**, **POP[AuthFailPeriod]**, **IMAP[LockIntruders]**, **IMAP[AuthFailCount]**, **IMAP[AuthFailPeriod]**, **PROXY[LockIntruders]**, **PROXY[AuthFailCount]**, **PROXY[AuthFailPeriod]**, **HttpProxy[LockIntruders]**, **HttpProxy[AuthFailCount]**, **HttpProxy[AuthFailPeriod]**, **FtpProxy[LockIntruders]**, **FtpProxy[AuthFailCount]**, **FtpProxy[AuthFailPeriod]**, **SocksProxy[LockIntruders]**, **SocksProxy[AuthFailCount]**, **SocksProxy[AuthFailPeriod]**, **HTTP[LockIntruders]**, **HTTP[AuthFailCount]**, **HTTP[AuthFailPeriod]**, **FTP[LockIntruders]**, **FTP[AuthFailCount]**, **FTP[AuthFailPeriod]**)
- + HTTP-сервер, FTP-сервер, POP-сервер, IMAP-сервер, прокси-сервер: добавлена возможность использования "липучки" (задержки ответа) при выдаче отказов клиенту (**Server[UseTarpit]**, **Server[TarpitInterval]**, **POP[UseTarpit]**, **POP[TarpitInterval]**, **IMAP[UseTarpit]**, **IMAP[TarpitInterval]**, **PROXY[UseTarpit]**, **PROXY[TarpitInterval]**, **HttpProxy[UseTarpit]**, **HttpProxy[TarpitInterval]**, **FtpProxy[UseTarpit]**, **FtpProxy[TarpitInterval]**, **SocksProxy[UseTarpit]**, **SocksProxy[TarpitInterval]**, **Pop3Proxy[UseTarpit]**, **Pop3Proxy[TarpitInterval]**, **TCPMAP[UseTarpit]**, **TCPMAP[TarpitInterval]**, **HTTP[UseTarpit]**, **HTTP[TarpitInterval]**, **FTP[UseTarpit]**, **FTP[TarpitInterval]**)
- SMTP-сервер: изменён порядок загрузки писем загрузчиком внешней POP-почты **Pop3Recv** - теперь письма обрабатываются по возрастанию порядковых номеров во внешнем почтовом ящике (идея **grass_snake**)
- + SMTP-сервер: контент-анализатор **MContent** отмечает факт своей загрузки в основном журнале (спасибо **leka**)
- + Web-интерфейс, программа установки: контроль целостности распространён на шаблоны автоответчиков и извещений SMTP-сервера, а также на субшаблоны сообщений об обнаружении вирусов (идея **leka**)
- SMTP-сервер: исправлена ошибка обработки адресов получателей, принадлежащих многосерверному домену (спасибо **leka**)
- SMTP-сервер: исправлена ошибка "залипания" блокировки автоответа, проявлявшаяся при обработке нескольких писем в одной сессии, чаще всего при загрузке писем из внешнего POP-ящика (спасибо **Pg1**)
- + Web-интерфейс: в мастерах управления пользователями и почтовыми ящиками реализовано переименование, перемещение и удаление каталогов почтовых ящиков при их изменении и удалении
- + Web-интерфейс: улучшено управление почтовыми каталогами доменов в мастере управления доменами
- Все серверы: исправлена проверка параметров конфигурации при запуске серверов (спасибо **Dandy**)
- + Программа установки: в каталог установки записывается отладочный журнал (идея **leka**)

***Новые, изменённые и удалённые элементы настройки:***

| | Элемент | Тип | Расположение |
|---|---|---|---|
| + | **FtpProxy[AuthDelimiter]** | INI-параметр | PigMail2.orig.ini |
| + | **HttpProxy[UseHttpAutoLogon]** | INI-параметр | PigMail2.orig.ini |
| + | **HttpProxy[HttpAutoLogon]** | INI-параметр | PigMail2.orig.ini |
| * | **schema.ini** | файл формата | CONF\lists\proxy\httpp\ |
| + | **HttpAutoLogon.txt** | список | CONF\lists\proxy\httpp\ |
| * | **SMTP[DenyLocalPartCharacters]** | INI-параметр | PigMail2.orig.ini |
| + | **Pop3Recv[Certificate]** | INI-параметр | PigMail2.orig.ini |
| + | **Pop3Recv[SslVerifyServer]** | INI-параметр | PigMail2.orig.ini |
| * | **schema.ini** | файл формата | CONF\lists\pop3recv\ |
| * | **Boxes.txt** | список | CONF\lists\pop3recv\ |
| + | **SECURITY** | поле списка | CONF\lists\pop3recv\Boxes.txt |
| + | **SSL_CERT** | поле списка | CONF\lists\pop3recv\Boxes.txt |
| + | **SSL_VERIFY** | поле списка | CONF\lists\pop3recv\Boxes.txt |
| + | **Pop3Recv[Pop3RecvDB]** | INI-параметр | PigMail2.orig.ini |
| * | **Pop3Recv[MessageIdList]** | INI-параметр | PigMail2.orig.ini |
| + | **PROXY[PacketSize]** | INI-параметр | PigMail2.orig.ini |
| + | **PROXY[MappingBufferSize]** | INI-параметр | PigMail2.orig.ini |
| + | **SMTP[PopMultiSite]** | INI-параметр | PigMail2.orig.ini |
| + | **Antispam[MessageIdDB]** | INI-параметр | PigMail2.orig.ini |
| + | **SMTP[ValidateMultisiteRcpts]** | INI-параметр | PigMail2.orig.ini |
| + | **SMTP[ValidateForwardedRcpts]** | INI-параметр | PigMail2.orig.ini |
| + | **SMTP[ValidateExternRcpts]** | INI-параметр | PigMail2.orig.ini |
| + | **Server[LockIntruders]** | INI-параметр | PigMail2.orig.ini |
| + | **Server[IdsMemoDB]** | INI-параметр | PigMail2.orig.ini |
| + | **Server[AuthFailCount]** | INI-параметр | PigMail2.orig.ini |
| + | **Server[AuthFailPeriod]** | INI-параметр | PigMail2.orig.ini |
| + | **SMTP[LockIntruders]** | INI-параметр | PigMail2.orig.ini |
| + | **SMTP[AuthFailCount]** | INI-параметр | PigMail2.orig.ini |
| + | **SMTP[AuthFailPeriod]** | INI-параметр | PigMail2.orig.ini |
| + | **POP[LockIntruders]** | INI-параметр | PigMail2.orig.ini |
| + | **POP[AuthFailCount]** | INI-параметр | PigMail2.orig.ini |
| + | **POP[AuthFailPeriod]** | INI-параметр | PigMail2.orig.ini |
| + | **IMAP[LockIntruders]** | INI-параметр | PigMail2.orig.ini |
| + | **IMAP[AuthFailCount]** | INI-параметр | PigMail2.orig.ini |
| + | **IMAP[AuthFailPeriod]** | INI-параметр | PigMail2.orig.ini |
| + | **PROXY[LockIntruders]** | INI-параметр | PigMail2.orig.ini |
| + | **PROXY[AuthFailCount]** | INI-параметр | PigMail2.orig.ini |
| + | **PROXY[AuthFailPeriod]** | INI-параметр | PigMail2.orig.ini |
| + | **HttpProxy[LockIntruders]** | INI-параметр | PigMail2.orig.ini |

| | | | |
|---|---|---|---|
| + | **HttpProxy[AuthFailCount]** | INI-параметр | PigMail2.orig.ini |
| + | **HttpProxy[AuthFailPeriod]** | INI-параметр | PigMail2.orig.ini |
| + | **FtpProxy[LockIntruders]** | INI-параметр | PigMail2.orig.ini |
| + | **FtpProxy[AuthFailCount]** | INI-параметр | PigMail2.orig.ini |
| + | **FtpProxy[AuthFailPeriod]** | INI-параметр | PigMail2.orig.ini |
| + | **SocksProxy[LockIntruders]** | INI-параметр | PigMail2.orig.ini |
| + | **SocksProxy[AuthFailCount]** | INI-параметр | PigMail2.orig.ini |
| + | **SocksProxy[AuthFailPeriod]** | INI-параметр | PigMail2.orig.ini |
| + | **HTTP[LockIntruders]** | INI-параметр | PigMail2.orig.ini |
| + | **HTTP[AuthFailCount]** | INI-параметр | PigMail2.orig.ini |
| + | **HTTP[AuthFailPeriod]** | INI-параметр | PigMail2.orig.ini |
| + | **FTP[LockIntruders]** | INI-параметр | PigMail2.orig.ini |
| + | **FTP[AuthFailCount]** | INI-параметр | PigMail2.orig.ini |
| + | **FTP[AuthFailPeriod]** | INI-параметр | PigMail2.orig.ini |
| + | **Server[UseTarpit]** | INI-параметр | PigMail2.orig.ini |
| + | **Server[TarpitInterval]** | INI-параметр | PigMail2.orig.ini |
| + | **POP[UseTarpit]** | INI-параметр | PigMail2.orig.ini |
| + | **POP[TarpitInterval]** | INI-параметр | PigMail2.orig.ini |
| + | **IMAP[UseTarpit]** | INI-параметр | PigMail2.orig.ini |
| + | **IMAP[TarpitInterval]** | INI-параметр | PigMail2.orig.ini |
| + | **PROXY[UseTarpit]** | INI-параметр | PigMail2.orig.ini |
| + | **PROXY[TarpitInterval]** | INI-параметр | PigMail2.orig.ini |
| + | **HttpProxy[UseTarpit]** | INI-параметр | PigMail2.orig.ini |
| + | **HttpProxy[TarpitInterval]** | INI-параметр | PigMail2.orig.ini |
| + | **FtpProxy[UseTarpit]** | INI-параметр | PigMail2.orig.ini |
| + | **FtpProxy[TarpitInterval]** | INI-параметр | PigMail2.orig.ini |
| + | **SocksProxy[UseTarpit]** | INI-параметр | PigMail2.orig.ini |
| + | **SocksProxy[TarpitInterval]** | INI-параметр | PigMail2.orig.ini |
| + | **Pop3Proxy[UseTarpit]** | INI-параметр | PigMail2.orig.ini |
| + | **Pop3Proxy[TarpitInterval]** | INI-параметр | PigMail2.orig.ini |
| + | **TCPMAP[UseTarpit]** | INI-параметр | PigMail2.orig.ini |
| + | **TCPMAP[TarpitInterval]** | INI-параметр | PigMail2.orig.ini |
| + | **HTTP[UseTarpit]** | INI-параметр | PigMail2.orig.ini |
| + | **HTTP[TarpitInterval]** | INI-параметр | PigMail2.orig.ini |
| + | **FTP[UseTarpit]** | INI-параметр | PigMail2.orig.ini |
| + | **FTP[TarpitInterval]** | INI-параметр | PigMail2.orig.ini |
| * | **SMTP[UseTarpit]** | INI-параметр | PigMail2.orig.ini |
| * | **SMTP[TarpitInterval]** | INI-параметр | PigMail2.orig.ini |

***9 декабря 2009 года.*** **Версия 2.1a**:

- Все серверы: исправлена внутренняя ошибка, которая могла приводить к сбоям при создании или конвертации баз данных почтового реестра MailRoll, загрузчика внешней POP-почты Pop3Recv и блокиратора атак подбора пароля

***11 декабря 2009 года.*** **Версия 2.1b**:

- SMTP-сервер: в сервисе расширенной доставки исходящей почты SmtpSend и сервисе проверки адресов нелокальных получателей на целевом сервере исправлена ошибка анализа ответов целевого сервера

## *2010 год*

***10 июня 2010 года.*** **Версия 2.2**:

- + Все серверы: добавлена поддержка новых возможностей ядра Eserv, проведена оптимизация программного кода
- - Все серверы: исключены плагины, функциональность которых реализована в ядре Eserv
- + SMTP-север: добавлена возможность загрузки индивидуальных плагинов поддержки почтовых роботов без ручной правки файлов правил. Изменился формат списка почтовых роботов (**ToEmailRobots**) (старый формат поддерживается для выполнения). При ручном обновлении версии необходимо выполнить проверку управляющих списков и шаблонов
- + SMTP-сервер: добавлен почтовый робот, обеспечивающий автоматическую рассылку писем по всем почтовым ящикам заданного домена без необходимости ведения отдельного списка (идея **Dandy**)
- + Программа установки: в образец списка почтовых роботов (**ToEmailRobots**) внесены все включённые в дистрибутив PigMail+PigProxy готовые к применению почтовые роботы
- + Документация: добавлено приложение с описаниями всех готовых к применению почтовых роботов
- SMTP-сервер: служебный заголовок X-E3-Mailfrom, удаляемый при доставке исходящей почты, вынесен из подписываемой Yahoo Domain Keys части письма
- + SMTP-сервер: добавлена возможность задавать автоответчикам индивидуальные списки отправителей, которым разрешено отвечать (идея **Dandy**). Изменился формат списка автоответчиков (**AutoReply**) (старый формат поддерживается для выполнения). При ручном обновлении версии необходимо выполнить проверку управляющих списков и шаблонов
- + Программа установки: при восстановлении и обновлении версии автоматически восстанавливаются удалённые нештатным способом службы
- Все серверы: исправлена обработка INI-параметра **Server[ExternIP]**
- SMTP-сервер: исправлена ошибка проверки адресов перенаправляемых получателей на целевых серверах
- + SMTP-сервер: изменена схема доставки писем в общие (архивные) каталоги и очереди доставки. По возможности письмо помещается в такие каталоги в одном экземпляре с указанием списка адресатов, а не отдельными копиями для каждого адресата (идея **alex100474**). Исключение составляют случаи, когда письмо было изменено в результате индивидуальной обработки контент-анализатором MContent
- ! SMTP-сервер: обработка исходящей почты контент-анализатором MContent теперь выполняется не один раз для всех адресатов, а индивидуально для каждого. В связи с этим изменился смысл признаков IsInboundMail и IsOutboundMail. Подробности см. в комментариях к примерам в **acSMTP\conf\smtp\customrules\MContent.samples**
- + SMTP-сервер: сервис расширенной доставки исходящей почты SmtpSend проверяет первичную очередь не циклически, а по факту помещения письма в очередь
- ! SMTP-сервер: изменены правила подписывания исходящих писем с помощью Yahoo Domain Keys - подписывается всякое письмо, покидающее пределы сервера (включая перенаправления для "чужих" адресатов и для отсутствующих адресатов многосерверного домена) и отправленное с использованием обратного адреса, принадлежащего одному из локальных почтовых доменов. Если письмо уже содержит подпись Yahoo Domain Keys, то повторно оно не подписывается
- SMTP-сервер: исправлена ошибка в шаблоне общего автоответа о доставке письма (**ReturnReceipt**)
- SMTP-сервер: в шаблоны писем-извещений и автоответов внесены косметические изменения
- + SMTP-сервер: реализован специальный сервис локальной (внутренней) доставки писем (**SMTP[Local]**, **SMTP[UseLocalDelivery]**, секция **LocalDelivery**, шаблон **LocalReceivedHeader.pat.txt**)
- Прокси-сервер: устранена несовместимость автоматического коллектора списка пользовательских наборов каналов TrafC с новым механизмом управления памятью в ядре Eserv (спасибо **leka**)
- + Программа установки, web-интерфейс: мастер проверки целостности управляющих списков и шаблонов поддерживает обновление пользовательских шаблонов до новой версии, если они не редактировались на месте, а оставались в изначальном состоянии
- - SMTP-сервер: извещения о поступлении входящей почты не формируются для локальных автоответов
- + SMTP-сервер: извещения о поступлении входящей почты корректно формируются для служебных сообщений - административных оповещений о недоставке почты и писем-извещений сервиса расширенной доставки исходящей почты SmtpSend
- + SMTP-сервер: в сервисе расширенной доставки исходящей почты SmtpSend реализован режим групповой доставки - одна копия письма отправляется нескольким адресатам (**SmtpSend[GroupDelivery]**) (идея **alex100474**)

- SMTP-сервер: в сервисе расширенной доставки исходящей почты SmtpSend исправлена ошибка некорректного задания сертификата защищённого соединения и режима проверки подлинности целевого сервера при обработке очередей фиксированных маршрутов доставки
- ! SMTP-сервер: изменён формат списка получателей "чужих" доменов (**EmailSmtpForward**). При ручном обновлении версии необходимо выполнить проверку управляющих списков и шаблонов
- SMTP-сервер: в сервисе расширенной доставки исходящей почты SmtpSend и плагине проверки адресов нелокальных получателей на целевом сервере ликвидированы возможные утечки памяти
- SMTP-сервер: в плагине проверки адресов нелокальных получателей на целевом сервере исправлена ошибка определения списка целевых серверов
- SMTP-сервер: в загрузчике внешней POP-почты Pop3Recv исправлена ошибка некорректной записи в оперативный журнал в случае срабатывания контроля дубликатов (спасибо **grass_snake**)
- Web-интерфейс: исправлены ошибки отображения при редактировании сертификатов защищённого соединения в случае вызова из редактора списков
- + Elog: добавлена поддержка нового формата статистического журнала сервиса расширенной доставки исходящей почты SmtpSend в режиме групповой доставки
- + Программа установки, web-интерфейс: мастер проверки целостности управляющих списков и шаблонов воссоздаёт отсутствующие каталоги конфигурации и данных (идея **leka**)
- + Программа установки: предупреждение о запрете установки служб по причине наличия альтернативной установки Eserv выводится при любом варианте установки. При этом наличие альтернативной установки проверяется более тщательно, с учётом возможного наличия ключей реестра даже после полного удаления стандартной установки Eserv/3 (спасибо **alexandr**)
- + Программа установки: при первоначальной установке импорт настроек и данных из существующей установки PigMail+PigProxy версии 1 предлагается даже если сама установка не была обнаружена. Путь к каталогу-источнику отображается для контроля и может быть изменён вручную (спасибо **alexandr**)
- + Все серверы: добавлена поддержка дополнительных параметров тонкой настройки производительности (**SMTP[WriteSocketRetryDelay]**, **IMAP[WriteSocketRetryDelay]**, **PROXY[WriteSocketRetryDelay]**, **HTTP[WriteSocketRetryDelay]**, **FTP[WriteSocketRetryDelay]**, **PROXY[AuthCacheRefreshAge]**, **HTTP[AuthCacheRefreshAge]**, **HTTP[MaxFcgiCnt]**)
- + Прокси-сервер: ускорена работа за счёт изменения начальных настроек производительности (спасибо **pov** и **ac**)
- + HTTP-сервер: добавлена поддержка прав доступа для ряда методов WebDAV

***Новые, изменённые и удалённые элементы настройки:***

| | Элемент | Тип | Расположение |
|---|---|---|---|
| * | **schema.ini** | файл формата | CONF\lists\smtp\ |
| * | **ToEmailRobots.txt** | список | CONF\lists\smtp\ |
| + | **PLUGIN** | поле списка | CONF\lists\smtp\ToEmailRobots.txt |
| + | **SMTP[Autoresponders]** | INI-параметр | PigMail2.orig.ini |
| * | **AutoReply.txt** | список | CONF\lists\smtp\ |
| + | **REPLY_LIST** | поле списка | CONF\lists\smtp\AutoReply.txt |
| + | **autoresponders** | каталог конфигурации | CONF\lists\smtp\ |
| + | **schema.ini** | файл формата | CONF\lists\smtp\autoresponders\ |
| + | **SMTP[Local]** | INI-параметр | PigMail2.orig.ini |
| + | **SMTP[UseLocalDelivery]** | INI-параметр | PigMail2.orig.ini |
| * | **SMTP[ReturnPath]** | INI-параметр | PigMail2.orig.ini |
| * | **Antispam[ResendDir]** | INI-параметр | PigMail2.orig.ini |
| + | **LocalDelivery[Malformed]** | INI-параметр | PigMail2.orig.ini |
| + | **LocalDelivery[Undelivered]** | INI-параметр | PigMail2.orig.ini |
| + | **LocalDelivery[MaxMessageSize]** | INI-параметр | PigMail2.orig.ini |
| + | **LocalDelivery[MaxOutboundMessageSize]** | INI-параметр | PigMail2.orig.ini |
| + | **LocalDelivery[AllowOutboundMail]** | INI-параметр | PigMail2.orig.ini |
| + | **LocalDelivery[UseAlerter]** | INI-параметр | PigMail2.orig.ini |

| | | | |
|---|---|---|---|
| + | **LocalDelivery[OnAlertNotification]** | INI-параметр | PigMail2.orig.ini |
| + | **LocalDelivery[OnAlertNotifyFrom]** | INI-параметр | PigMail2.orig.ini |
| + | **LocalDelivery[OnAlertNotifyTo]** | INI-параметр | PigMail2.orig.ini |
| + | **LocalDelivery[Logs]** | INI-параметр | PigMail2.orig.ini |
| + | **LocalDelivery[LogLevel]** | INI-параметр | PigMail2.orig.ini |
| + | **LocalDelivery[LogToEStat]** | INI-параметр | PigMail2.orig.ini |
| + | **LocalDelivery[LogToAdvSoft]** | INI-параметр | PigMail2.orig.ini |
| + | **LocalDelivery[LogToElog]** | INI-параметр | PigMail2.orig.ini |
| + | **LocalDelivery[LogToMaillog]** | INI-параметр | PigMail2.orig.ini |
| + | **LocalDelivery[LogToMStat]** | INI-параметр | PigMail2.orig.ini |
| + | **LocalReceivedHeader.pat.txt** | шаблон | CONF\templates\smtp\ |
| * | **AutoReplyVacation.pat.txt** | шаблон | CONF\templates\smtp\ |
| * | **DkTest.pat.txt** | шаблон | CONF\templates\smtp\ |
| * | **OnAlertNotification.pat.txt** | шаблон | CONF\templates\smtp\ |
| * | **OnSpamVirus.pat.txt** | шаблон | CONF\templates\smtp\ |
| * | **OnSpamVirusAdmin.pat.txt** | шаблон | CONF\templates\smtp\ |
| * | **OnVError.pat.txt** | шаблон | CONF\templates\smtp\ |
| * | **OnVErrorAdmin.pat.txt** | шаблон | CONF\templates\smtp\ |
| * | **OnVirus.pat.txt** | шаблон | CONF\templates\smtp\ |
| * | **OnVirusAdmin.pat.txt** | шаблон | CONF\templates\smtp\ |
| * | **QuotaExceeded.pat.txt** | шаблон | CONF\templates\smtp\ |
| * | **ReturnReceipt.pat.txt** | шаблон | CONF\templates\smtp\ |
| * | **SampleNotification.pat.txt** | шаблон | CONF\templates\smtp\ |
| * | **RetryNotification.pat.txt** | шаблон | CONF\templates\smtpsend\ |
| * | **ReturnNotification.pat.txt** | шаблон | CONF\templates\smtpsend\ |
| + | **SmtpSend[GroupDelivery]** | INI-параметр | PigMail2.orig.ini |
| !* | **EmailSmtpForward.txt** | список | CONF\lists\smtp\ |
| + | **SSL_CERT** | поле списка | CONF\lists\smtp\EmailSmtpForward.txt |
| + | **SSL_VERIFY** | поле списка | CONF\lists\smtp\EmailSmtpForward.txt |
| + | **SMTP[WriteSocketRetryDelay]** | INI-параметр | PigMail2.orig.ini |
| + | **IMAP[WriteSocketRetryDelay]** | INI-параметр | PigMail2.orig.ini |
| + | **PROXY[WriteSocketRetryDelay]** | INI-параметр | PigMail2.orig.ini |
| + | **HTTP[WriteSocketRetryDelay]** | INI-параметр | PigMail2.orig.ini |
| + | **FTP[WriteSocketRetryDelay]** | INI-параметр | PigMail2.orig.ini |
| + | **PROXY[AuthCacheRefreshAge]** | INI-параметр | PigMail2.orig.ini |
| + | **HTTP[AuthCacheRefreshAge]** | INI-параметр | PigMail2.orig.ini |
| + | **HTTP[MaxFcgiCnt]** | INI-параметр | PigMail2.orig.ini |

## *2011 год*

***5 августа 2011 года.*** **Версия 2.3**:

- ! Все серверы: начиная с этой версии PigMail+PigProxy более не работает на Windows 2000 и более ранних версиях Windows

- + HTTP-сервер: добавлена поддержка прав доступа для дополнительных методов WebDAV
- HTTP-сервер: исправлена ошибка обработки запросов, когда в ряде случаев на стеке оставалось лишнее значение
- HTTP-сервер: исправлена ошибка, приводившая к ошибкам при выполнении ISAPI-сценариев (спасибо **leka**)
- IMAP-сервер: исправлена ошибка, приводившая к сбоям при попытке спам-переклассификации неверно отфроматированных писем, не содержащих в шапке ни одного заголовка Received (спасибо **Dandy**)
- + SMTP-север: служебные заголовки о результатах классификации письма добавляются при любом результате классификации. Также добавляются служебные заголовки о проверке письма антивирусом. Для писем, сгенерированных самим сервером, эти заголовки не добавляются
- + SMTP-сервер: добавлена возможность автоматической генерации опущенных отправителем заголовков Date и Message-ID (**SMTP[GenerateMissedHeaders]**)
- SMTP-сервер: в шаблонах извещений кириллические темы письма оформлены в закодированном виде. Доработан шаблон извещения о превышении квоты
- + SMTP-сервер: добавлены новые слова для использования в шаблонах писем (**AV-DATABASE-INFO**, **X-AV-DATABASE-INFO**, **ClassifyDetails**, **CLASSIFY-DETAILS**)
- SMTP-сервер: исправлена ошибка некорректной проверки существования адресата на целевом сервере в случае принадлежности адресата к домену из списка перенаправления
- SMTP-сервер: изменён режим кэширования параметра **SMTP[UseAntivirus]** - теперь его значение запоминается при инициализации почтовой сессии
- SMTP-сервер: исправлена ошибка доставки письма спам-администратору по умолчанию - адресат при этом не вычёркивался из списка
- SMTP-сервер: исправлена ошибка в загрузчике внешней POP-почты Pop3Recv - при переходе от ящика к ящику не сбрасывались настройки безопасности соединения (спасибо **figaro**)
- + SMTP-сервер: в загрузчике внешней POP-почты Pop3Recv и сервисе расширенной доставки исходящей почты SmtpSend реализован новый режим проверки сертификата защищённого соединения - без предъявления собственного клиентского сертификата (спасибо **ac**)
- SMTP-сервер: в загрузчике внешней POP-почты Pop3Recv и сервисе расширенной доставки исходящей почты SmtpSend для совместимости с OpenSSL используются синхронные сокеты (спасибо **figaro** и **ac**)
- !+ SMTP-сервер: выбор дополнительных серверов для доставки писем сервисом расширенной доставки исходящей почты SmtpSend можно осуществлять в зависимости от адреса отправителя, который будет использован в протокольной команде MAIL FROM (идея **figaro**). Изменился формат списка дополнительных транзитных серверов (**AltRelayList**). При ручном обновлении версии необходимо выполнить проверку управляющих списков и шаблонов
- Все серверы: проведены ревизия кода и объединение ряда плагинов, удалены неиспользуемые фрагменты
- + SMTP-сервер, IMAP-сервер: новые настройки модуля связи с байесовым спам-фильтом POPfile (**AntispamPopFile[Port]**, **AntispamPopFile[StartupTimeout]**, **AntispamPopFile[InitTimeout]**)
- SMTP-сервер: исправлена ошибка некорректной установки защищённого соединения (SSL) при проверке адресатов на целевом сервере
- POP-сервер: исправлен алгоритм определения класса отдаваемого клиенту письма
- + SMTP-сервер: добавлена поддержка тега h подписи Yahoo Domain Keys (спасибо **ac**)
- SMTP-сервер, POP-сервер: восстановлена работоспособность плагина callback
- + IMAP-сервер: реализован вывод ответов сервера в оперативный журнал
- HTTP-сервер: исправлена ошибка, из-за которой при наличии IP-авторизации некорректно обрабатывались ошибки протокольной авторизации (спасибо **ND**)
- Прокси-сервер: исправлена ошибка, приводившая к неработоспособности автоматического коллектора списка пользовательских наборов каналов TrafC (спасибо **ND**)
- SMTP-сервер: исправлена ошибка в алгоритме извлечения адресатов из шапки письма загрузчиком внешней POP-почты Pop3Recv, приводившая к аварийному завершению загрузки (спасибо **alexandr**)
- SMTP-сервер: исправлена ошибка в роботе DomainLister, из-за которой рассылка не работала (спасибо **alexandr**)
- + SMTP-сервер: загрузчик внешней POP-почты Pop3Recv защищён от некорректных манипуляций со стеком во время анализа, приёма и доставки писем (спасибо **alexandr**)
- SMTP-сервер: исправлена ошибка, из-за которой при архивировании исходящих писем на стеке оставались лишние данные (спасибо **alexandr**)
- Программа установки: восстановлена работоспособность сценария импорта настроек PigMail+PigProxy версии 1 (спасибо **alexandr**)
- + Программа установки: в процессе работы проверяется успешность импорта настроек PigMail+PigProxy версии 1 и проверки целостности управляющих списков и шаблонов (спасибо **alexandr**)

- Прокси-сервер: оптимизирован автоматический коллектор списка пользовательских наборов каналов TrafC - исключены обращения к ODBC-драйверу текстовых списков и уменьшено число файловых операций при обновлении списка (спасибо **ND** и **alexandr**)
- Прокси-сервер: исправлена ошибка, приводившая к сбоям при управлении квотами TrafC (спасибо **alexandr**, **rvm** и **ac**)

**Новые, изменённые и удалённые элементы настройки:**

| | Элемент | Тип | Расположение |
|---|---|---|---|
| + | **SMTP[GenerateMissedHeaders]** | INI-параметр | PigMail2.orig.ini |
| * | **OnAlertNotification.pat.txt** | шаблон | CONF\templates\smtp\ |
| * | **OnSpamVirusAdmin.pat.txt** | шаблон | CONF\templates\smtp\ |
| * | **OnVErrorAdmin.pat.txt** | шаблон | CONF\templates\smtp\ |
| * | **OnVirus.pat.txt** | шаблон | CONF\templates\smtp\ |
| * | **OnVirusAdmin.pat.txt** | шаблон | CONF\templates\smtp\ |
| * | **QuotaExceeded.pat.txt** | шаблон | CONF\templates\smtp\ |
| * | **RetryNotification.pat.txt** | шаблон | CONF\templates\smtpsend\ |
| * | **Pop3Recv[SslVerifyServer]** | INI-параметр | PigMail2.orig.ini |
| * | **SmtpSend[SslVerifyServer]** | INI-параметр | PigMail2.orig.ini |
| * | **EmailSmtpForward.txt** | список | CONF\lists\smtp\ |
| * | **SSL_VERIFY** | поле списка | CONF\lists\smtp\EmailSmtpForward.txt |
| * | **Boxes.txt** | список | CONF\lists\pop3recv\ |
| * | **SSL_VERIFY** | поле списка | CONF\lists\pop3recv\Boxes.txt |
| * | **TransferSecurityList.txt** | список | CONF\lists\smtpsend\ |
| * | **SSL_VERIFY** | поле списка | CONF\lists\smtpsend\TransferSecurityList.txt |
| * | **HeloIP.txt** | список | CONF\lists\smtpsend\ |
| * | **SSL_VERIFY** | поле списка | CONF\lists\smtpsend\HeloIP.txt |
| * | **schema.ini** | файл формата | CONF\lists\smtpsend\ |
| !* | **AltRelayList.txt** | список | CONF\lists\smtpsend\ |
| !+ | **SENDER_MASK** | поле списка | CONF\lists\smtpsend\AltRelayList.txt |
| + | **AntispamPopFile[Port]** | INI-параметр | PigMail2.orig.ini |
| + | **AntispamPopFile[StartupTimeout]** | INI-параметр | PigMail2.orig.ini |
| + | **AntispamPopFile[InitTimeout]** | INI-параметр | PigMail2.orig.ini |

Условные обозначения

**+** добавленный элемент/опция
***** изменённый элемент/опция
**-** удалённый элемент/опция
**!** критически важное изменение