Школьный сервер

Технологическая платформа для функционирования информационной системы автоматизации деятельности общеобразовательного учреждения. Руководство пользователя

Москва
2008

Оглавление

Глава 1

Общая информация

1.1 Что такое Школьный Сервер

Школьный Сервер — это простой в установке и удобный в работе серверный дистрибутив, специально предназначенный для использования в образовательных учреждениях и дающий возможность решать обычные задачи, не опасаясь вирусов и не затрачивая время на поиск нужных программ в сети Интернет и на полках магазинов.

Школьный Сервер представляет из себя современный комплекс программного обеспечения для создания информационного пространства общеобразовательного учреждения. В дистрибутив включены компоненты, автоматизирующие эту деятельность.

Объектно-ориентированная динамическая учебная среда Moodle
ориентирована на организацию взаимодействия между преподавателем и учениками а также для организации дистанционных курсов и поддержки очного обучения.

MediaWiki является управляемой web-средой для организации взаимодействия участников учебного процесса.

Школьный Сервер легко развёртывается и интегрируется в существующие сети. Этот дистрибутив выгодно отличается:

Улучшенной программой установки, ориентированной на автоматическое определение и настройку оборудования. В большинстве случаев для успешной установки пользователю достаточно нажимать кнопку "Далее разрешение технических вопросов можно оставить программе установки.

Оригинальной системой настройки (Центр управления системой),
основанной на платформе alterator. С её помощью и опытные, и неподготовленные пользователи могут легко решать типичные задачи по настройке и администрированию системы. При этом администрирование осуществляется через web-интерфейс, а значит всё, что нужно для настройки – это web-браузер.

Школьный Сервер может предоставлять самые разные службы. Всё необходимое программное обеспечение уже включено в дистрибутив:

- сервер файлов Samba;
- сервер службы каталогов OpenLDAP;
- сервер печати CUPS;
- сервер времени NTPD;
- система управления базами данных: MySQL, PostgreSQL (может быть дополнительно доустановлен с диска);
- ftp-сервер vsFTPd;
- web-сервер Apache 2.

1.1.1 Требования

Аппаратные требования дистрибутива:

- привод CD;
- процессор совместимой с Pentium III архитектуры от 500 МГц (рекомендуется тактовая частота не ниже 1 ГГц);
- объём оперативной памяти от 128 Мб (рекомендуется от 512 Мб). Если прланируется исползование Moodle и/или MediaWiki, то не менее 256 Мб.;
- свободное место на жёстком диске от 4 Гб (рекомендуется от 10 Гб). Необходимое место для хранения пользовательских данных, зеркал дистрибутивов и прочих потенциально объёмных данных может сильно варьироваться. Необходимо озаботиться наличием достаточного резерва вдобавок к указанным величинам;
- сетевой адаптер 10/100 Мбит (рекомендуется 1 Гбит);
- видеокарта необходима только на время установки.

Глава 2

Настройка системы

2.0.2 Центр управления системой

Центр управления системой — интегрированный набор инструментов для управления различными компонентами системы. Модули настройки сгруппированы по задачам. Выберите необходимый модуль настройки в меню, расположенном слева.

Практически каждый модуль настройки сопровождается встроенной справкой. Открыть справку можно, перейдя по ссылке «Справка» в верхней части страницы.

Интерфейс переведён на несколько языков:

- английский (en);
- русский (ru);
- украинский (uk).

Язык интерфейса определяется настройками браузера. Если после успешного соединения с Центром управления системой вы не увидели сообщений на родном языке, следует исправить настройки браузера или указать язык вручную, перейдя по ссылке с кодом языка в верхней части страницы.

2.1 Система

2.1.1 Информация о системе

Здесь отображается наиболее важная информация о системе:

- версия используемого ядра;
- информация о процессорах;
- использование памяти;
- использование дискового пространства.

2.1.2 Службы xinetd

Xinetd (демон Интернет-служб) принимает соединения на заданных портах и запускает соответствующие службы. В отличие от серверов, стартующих при загрузке системы и бездействующих в ожидании запросов, xinetd представляет собой только один процесс, чем экономит системные ресурсы.

Общие настройки (суммарное *количество запущенных процессов*, число процессов, обслуживающих *каждого клиента* и список допустимых *адресов*, с которых принимаются соединения) применяются ко всем службам, для которых соответствующие поля не заполнены. Если список допустимых адресов пуст, соединения будут приниматься со всех адресов.

Состояние службы определяет, будет ли обслуживаться соответствующий порт или нет.

Настройки каждого сервера содержат также имя *псевдо-пользователя* и *псевдо-группы*, от имени которых будет запущен процесс, путь к *исполняемому файлу сервера* и его *аргументы*. *Лимит адресного пространства* сервера может быть неограничен (`UNLIMITED`) или числом с суффиксом `K` (килобайт), `M` (мегабайт) или без суффикса.

Если не включён ни один из сервисов, xinetd не запускается. После настройки пройдите по ссылке `Запустить, остановить или перезапустить xinetd` и запустите его.

2.1.3 Системные службы

Системные службы, будучи запущенными, принимают соединения, предоставляя таким образом различные сервисы.

После выбора названия службы из списка отображается описание данной службы, а также текущее состояние: работает, остановлена, неизвестно.

Выпадающий список *Изменить состояние* позволяет остановить либо перезапустить работающую службу или запустить остановленную (после нажатия кнопки *Применить*). Изменение состояния службы действует только до перезагрузки. Если необходимо, чтобы служба запускалась автоматически при загрузке системы, отметьте соответствующий пункт *Запускать при загрузке системы*.

2.1.4 Системные журналы

Системные журналы позволяют отслеживать события, происходящие с системой. Эта информация может быть полезна при диагностике разного рода проблем.

Различные журналы могут быть выбраны из списка *Журналы*. Например:

Безопасность Этот журнал отображает важную информацию, связанную с безопасностью. Например, здесь можно посмотреть, какой конкретно пользователь и когда начал и закончил свою работу с системой.

Ядро Важные сообщения от ядра вашей системы. Сообщения этого журнала могут помочь при поиске неисправностей в работе оборудования.

Каждый журнал может содержать довольно большое количество сообщений. Уменьшить либо увеличить количество выводимых строк можно, выбрав нужное значение в списке *Показывать*.

При необходимости просмотра более старых/новых сообщений можно воспользоваться кнопками *Назад*/*Далее* соответственно.

Переход к самым старым и самым новым сообщениям осуществляется кнопками *Последняя страница* и *Первая страница*.

2.2 Программное обеспечение

2.2.1 Обновления

Обновления — это улучшения программ, установленных в вашей системе. Это могут быть как исправления, связанные с безопасностью, так и более свежие версии самих программ. Установка производится из источников, указанных в разделе *Источники обновлений*.

Установка обновлений производится в два этапа:

- Проверка наличия обновлений (кнопка *Проверить наличие обновлений*). Происходит проверка доступности новых обновлений для вашего дистрибутива. Обновления ищутся в источниках, указанных в разделе *Источники обновлений*. При этом может потребоваться соединение с сетью Интернет.
- Обновление системы (кнопка *Обновить систему*). Происходит загрузка доступных обновлений из настроенных источников и установка их в систему.

2.2.2 Источники обновлений

Источники обновлений, или *репозитории* — хранилища программ, специально подготовленных для установки в систему. Обычно используют репозитории, расположенные в сети Интернет, доступ к которым осуществляется по одному из протоколов: ftp, http, rsync. Можно выбрать репозиторий из списка *Адрес источника*. После выбора и нажатия кнопки *Изменить* репозиторий отобразится в окне *Репозитори* и будет использоваться в дальнейшем при установке и обновлении программ.

Если требуется указать репозиторий, отсутствующий в списке, можно воспользоваться кнопкой *Дополнительно* и добавить путь к новому репозиторию в поле *Новый источник*, после чего нажать кнопку *Добавить*.

2.2.3 Дополнительные диски

К дистрибутиву могут поставляться дополнительные диски с программным обеспечением.

Для того чтобы иметь возможность устанавливать это дополнительное ПО, необходимо добавить такие диски к списку доступных источников установки. Вставьте диск и нажмите *Добавить*. При помощи кнопки *Удалить* можно удалить добавленные ранее диски из списка.

Диск, с которого производилась установка, добавлять не требуется. Он добавляется автоматически при установке системы.

2.3 Дата и время

2.3.1 Дата и время

Системное время в Linux зависит от следующих факторов:

- **Часы в BIOS** — часы, встроенные в компьютер; они работают, даже если он выключен.
- **Системное время** — часы в ядре операционной системы. Во время работы системы все процессы пользуются именно этими часами.
- **Часовые пояса** — регионы Земли, в каждом из которых принято единое местное время.

При запуске системы происходит активация системных часов и их синхронизация с аппаратными, кроме того, в определённых случаях учитывается значение часового пояса. При завершении работы системы происходит обратный процесс.

Аппаратные часы компьютера не идеальны, минимум раз в год придётся их *подводить*. Но если у вас есть доступ к серверу точного времени, то рекомендуется им воспользоваться. Для этого достаточно отметить пункт «Получать точное время с NTP-сервера» и указать имя сервера.

В большинстве случаев вас устроит сервер pool.ntp.org. Тсть аналогичные серверы для целых регионов, например:

- ru.pool.ntp.org — для России
- ua.pool.ntp.org — для Украины

За более подробной информацией обращайтесь на сайт http://www.pool.ntp.org/.

Если синхронизация времени с NTP-сервером настроена, то ваш компьютер сможет сам работать как сервер точного времени. Для этого достаточно отметить соответствующий пункт *Работать как NTP-сервер*.

2.3.2 Часовой пояс

Время в Linux зависит от следующих факторов:

- **Часы в BIOS** — часы, встроенные в компьютер; они работают, даже если он выключен.
- **Системное время** — часы в ядре операционной системы. Во время работы системы все процессы пользуются именно этими часами.
- **Часовые пояса** — регионы Земли, в каждом из которых принято единое местное время.

При запуске системы происходит активация системных часов и их синхронизация с аппаратными, кроме того, в определённых случаях учитывается значение часового пояса. При завершении работы системы происходит обратный процесс.

Аппаратные часы могут быть выставлены или *по Гринвичу* или на *местное время* (параметр «Хранить время в BIOS по Гринвичу»).

Если вы хотите, чтобы происходил автоматический переход на летнее время и обратно — выберите первый вариант (*по Гринвичу*). Однако если на этом же компьютере установлена операционная система, которая также может автоматически переводить часы на летнее время, используйте второй вариант.

Для удобства поиска часовые пояса сгруппированы по странам.

2.4 Пользователи

2.4.1 Администратор системы

В любой системе Linux всегда присутствует один особый пользователь — администратор (он же суперпользователь), для которого зарезервировано неизменное системное имя — root.

Создав или сгенерировав пароль пользователя root, обязательно запишите или хорошо запомните его. Он потребуется, если вы решите изменить настройки системы, например добавить учётные записи пользователей, настроить сеть, установить дополнительное программное обеспечение.

Администратор отличается от всех прочих пользователей тем, что ему позволено производить любые изменения в системе. Каждый, кто сможет правильно ввести пароль администратора (узнав или подобрав), получит неограниченный доступ к системе. Даже ваши собственные неосторожные действия от имени пользователя root могут иметь необратимые и неочевидные для вас последствия. Поэтому повседневную работу в Linux следует выполнять от имени обычного пользователя.

2.4.2 Локальные учётные записи

Linux — многопользовательская система. Зарегистрировавшись — введя имя (login) и пароль — каждый пользователь, во-первых, приобретает возможность работать в удобном ему окружении, во-вторых, получает доступ к своим файлам, закрытым для других пользователей и просто посторонних.

В процессе установки предлагается создать только одну учётную запись обычного пользователя, чтобы от его имени администратор мог выполнять задачи, которые не требуют привилегий суперпользователя. Учётные записи для всех прочих пользователей можно будет создать в любой момент после установки системы.

2.4.2.1 Создание новой учётной записи

Новая учётная запись После ввода допустимого имени необходимо нажать *Создать*, после чего имя отобразится в списке слева. Для дополнительных настроек необходимо выделить добавленное имя либо, если необходимо изменить существующую учётную запись, выбрать её их списка.

Комментарий Произвольный комментарий к учётной записи. Часто здесь указывается реальные имя и фамилия пользователя.

Домашний каталог Каталог пользователя, в котором он будет иметь полные права. В случае регистрации в консоли работа начинается именно в этом каталоге. Обычно домашний каталог пользователя располагается в /home/имя_пользователя, где имя_пользователя — это имя учётной записи.

Интерпретатор команд Это командная оболочка, запускаемая по умолчанию при регистрации пользователя в текстовой консоли. По умолчанию используется /bin/bash.

Входит в группу администраторов При установленной отметке пользователь имеет возможность получить права администратора (root). Например, при помощи команды *su*. Естественно, для этого необходимо знать пароль администратора.

Пароль Пароль учётной записи может быть сгенерирован автоматически (*Создать автоматически*) либо создан самостоятельно. Во втором случае необходимо ввести его подтверждение.

2.4.3 Аутентификация

Традиционно операционные системы семейства *UNIX* настраиваются при помощи большого количества локальных текстовых файлов (*/etc/group*, */etc/hosts* и т. д.). С ростом количества компьютеров в сети растёт и количество локальных конфигурационных файлов, что сильно усложняет задачу администрирования, например, согласованного создания пользователя/группы на нескольких компьютерах.

Подсистема *Name Service Switch (NSS)* позволяет заменить разрозненные конфигурационные файлы одной или несколькими централизованными базами данных.

Pluggable Authentication Modules (PAM) — механизм, позволяющий тонко настроить схему аутентификации пользователей в системе. Данный модуль конфигуратора позволяет переключаться между заранее подготовленными схемами.

Для традиционной схемы работы (`локальная аутентификация и локальные конфигурационные файлы`) ничего дополнительно настраивать не требуется.

Для схемы `LDAP` требуется дополнительно заполнить следующие параметры:

- LDAP-сервер — местоположение сервера и протокол, например, `ldap://localhost.localdomain`.
- Базовый DN — точка привязки, например, `dc=example,dc=com`.

При использовании *LDAP* все локальные пользователи и группы остаются в силе и имеют приоритет. То есть если существует пользователь с одним и тем же именем и локально, и в *LDAP*, то будет отдано предпочтение локальному пользователю.

При аутентификации по этой схеме сначала происходит попытка аутентификации пользователя с использованием локальных баз данных. В случае если пользователь

не является системным (то есть UID больше определённого значения, по умолчанию — 500) и не прошёл аутентификацию локально, то делается повторная попытка с использованием данных из LDAP.

2.5 Сеть

2.5.1 Ethernet-интерфейсы

IP (Internet Protocol) — основа стека протоколов TCP/IP. `IP-адрес` и `Маска сети` — обязательные параметры каждого узла IP-сети. Первый параметр — уникальный идентификатор машины, от второго напрямую зависит, к каким машинам локальной сети данная машина будет иметь доступ. Если требуется выход во внешнюю сеть, то не забудьте про параметр `Шлюз по умолчанию`.

В случае наличия *DHCP-сервера* можно все вышеперечисленные параметры получить автоматически — просто включите `Использовать DHCP`.

Если в компьютере имеется несколько сетевых карт, то возможна ситуация, когда при очередной загрузке ядро присвоит имена интерфейсов (eth0, eth1) в другом порядке. В результате интерфейсы получат не свои настройки. Чтобы этого не происходило, вы можете привязать интерфейс к имени по его аппаратному адресу (MAC) или по местоположению на системной шине.

2.5.2 Общие сетевые настройки

Существует ряд общих сетевых параметров, не привязанных к какому либо конкретному интерфейсу.

`Имя компьютера` — имя компьютера, в формате *computer.domain*. Несмотря на то, что этот параметр никому из соседних компьютеров в сети не передаётся (в отличие, скажем, от имени компьютера в Windows-сети), значение этого параметра используют многие сетевые службы, например почтовый сервер.

При работе и настройке сетевых служб часто приходится использовать символьные имена других машин в сети. Чтобы система преобразовала их в *IP-адреса*, требуется либо перечислить соответствия файле */etc/hosts*, либо воспользоваться *DNS-сервером* (поле `DNS-серверы`).

Если в поле `Домены поиска` перечислить наиболее часто используемые домены (например *domain*), то можно пользоваться неполными именами машин *computer* вместо *computer.domain*).

2.5.3 PPTP-соединения

PPTP (Point-to-point tunneling protocol) — протокол для организации прямого соединения между двумя машинами в сети. Для создания нового соединения необходимо указать адрес удалённого PPTP-сервера, а также имя пользователя и пароль на этом сервере. Также необходимо выбрать, через какой *IP-интерфейс* будет происходить соединение — это требуется для корректной инициализации сетевой подсистемы.

Имена для PPTP-соединений принято назначать в формате *ppp[номер]*.

2.5.4 PPPoE-соединения

PPPoE (Point-to-point protocol over Ethernet) — протокол для организации прямого соединения между двумя машинами в сети. В основном используется xDSL-сетями. Для создания нового соединения необходимо указать *Ethernet-интерфейс*, через который будет производиться соединение, а также системное имя и пароль пользователя на PPPoE-сервере.

Имена для PPPoE-соединений принято назначать в формате *ppp[номер]*.

2.5.5 Брандмауэр

Брандмауэр — специальное программное обеспечение, с помощью которого вы можете:

- организовать выход компьютеров вашей сети в Интернет (либо другую подсеть) используя технологию NAT;
- ограничить или разрешить сетевой доступ к службам компьютера.

2.5.5.1 Общие параметры

Включить брандмауэр Глобальная настройка, включающая либо отключающая функции брандмауэра. При отключении все выставленные ниже установки не имеют силы. Внимание! При включении брандмауэра доступ к службам по умолчанию закрыт в том числе и для службы "System management center (www)". Если необходимо сохранить возможность использовать Центр управления системой, соединяясь с ним по сети, то следует включить к нему доступ.

Разрешить транзитные пакеты (forwarding) Если компьютер должен работать как шлюз (gateway), то необходимо выбрать данную опцию. Это позволит организовать совместный выход в Интернет для локальной сети, указанной в *Включить трансляцию сетевых адресов (NAT)*.

Включить трансляцию сетевых адресов (NAT) Указывается подсеть, для которой следует выполнять трансляцию сетевых адресов (NAT) и сетевой интерфейс, который связан с этой подсетью. Это позволит компьютерам указанной подсети соединяться с другими подсетями, например сетью Интернет, в случае, если сам шлюз имеет соответствующее подключение.

2.5.5.2 Разрешённые входящие соединения

Отметив либо сняв отметку, соответствующую определённой службе, можно включить либо отключить доступ к этой службе из сети. Особое внимание уделите службе «System management center (www)». Запретив доступ к ней, будет невозможно воспользоваться Центром управления системой по сети. Выпадающий список *Интерфейс* указывает имя интерфейса, по отношению. к которому настраиваются разрешения доступа.

2.6 Серверы

2.6.1 FTP-сервер

FTP (File Transfer Protocol) — старейший и самый распространённый протокол передачи данных в Сети. Шире всего он используется для организации файлового сервера с анонимным доступом. Возможность анонимного доступа управляется параметром `Разрешить вход анонимному пользователю`.

Менее распространённый вариант — сервер с возможностью загружать на него файлы, в том числе анонимными пользователями. Возможность загрузки включается параметрами `Разрешить запись` и `Разрешить закачку файлов`. Дополнительно настраиваются возможности создания каталогов, удаления и переименования файлов (параметры `Разрешить создание каталогов` и `Разрешить переименование/удаление файлов`. Анонимный пользователь не может производить запись файлов в произвольный каталог файлового сервера. Вы можете или создать свою структуру каталогов, или воспользоваться стандартным каталогом */incoming*. Последний автоматически создаётся, если включён параметр `Стандартный каталог для приёма файлов (/var/ftp/incoming)`.

Обратите внимание, что если вы позволяете анонимным пользователям закачивать файлы — стоит позаботиться о проблеме переполнения диска и не размещать каталог */var* в основном рабочем разделе.

И наконец, самый редкий вариант — сервер, позволяющий локальным пользователям скачивать и загружать файлы из своих домашних каталогов. Редкое использование такой конфигурации вызвано небезопасностью протокола *FTP*. Пароль пользователя передаётся по сети открытым текстом и может быть перехвачен злоумышленниками. Возможность работы с локальными пользователями управляется параметром `Разрешить вход локальных пользователей`.

По умолчанию сервер настроен таким образом, что пользователи могут только скачивать файлы. Чтобы они смогли загружать файлы, требуется включить уже знакомый параметр `Разрешить запись`. Разрешение на загрузку файлов можно настраивать индивидуально, добавляя пользователей, которым требуется такая возможность, в список.

2.6.2 Прокси-сервер

Пользователи корпоративных сетей обычно подключаются к сети Интернет через один общий канал. Если разместить на выходе (*шлюзе*) прокси-сервер, полученные через него страницы попадут в кеш, и при повторном обращении их скачивание уже не потребуется. Это существенно ускорит доступ к популярным сайтам и снизит потребляемый компанией *трафик*.

Добавьте адрес и порт, на которых серверу следует *принимать соединения*, и укажите их в настройках своего браузера. Если оставить адрес пустым, соединения будут приниматься на все доступные адреса.

Прокси-сервер также может использоваться для ограничения доступа пользователей к сети Интернет. Чтобы разрешить определённому сегменту сети пользоваться

сервером, добавьте к настройкам его *диапазон адресов*, например 192.168.1.0/24. Не входящие в диапазон клиенты допущены не будут.

В случае отказа пользователю будет выдана страница с описанием причины и контактная информация, в частности *Email* администратора сервера.

Можно не указывать *домен* локальных веб-сайтов, в этом случае он будет *добавлен* автоматически. Задайте домен в виде *.domain.org*. Локальными считаются сайты, чьё название не содержит точки.

Веб-сайты сомнительного содержания можно *заблокировать*, перечислив их в соответствующем списке.

Сразу после установки прокси-сервера он может оказаться не запущен. Запустить его (а также узнать его текущее состояние) можно, перейдя по ссылке *запустить, остановить или перезапустить службу*.

2.6.3 Сервер Samba

Samba предоставляет общий доступ к файлам и принтерам в локальной сети по протоколу *SMB/CIFS* (поддерживается в Microsoft® Windows™, OS/2, Linux и др.).

В этом модуле вы можете создавать или удалять общие папки и настраивать правда доступа к ним.

2.6.4 Сервер ИБП

В данном модуле вы можете регистрировать устройства бесперебойного питания. При регистрации устройству назначается символьное имя, указывается порт, к которому подсоединён управляющий кабель, а также драйвер. По каждому зарегистрированному устройству вы можете узнать состояние, заряд батарей и загруженность.

2.6.5 Сервер DHCP

Протокол DHCP позволяет клиенту самостоятельно получить IP-адрес из зарезервированного диапазона адресов, а также дополнительную информацию о локальной сети.

Обычно адрес предоставляется на ограниченный срок, по истечении которого может быть выдан другому клиенту.

Иногда бывает полезно выдавать клиенту один и тот же IP-адрес независимо от момента обращения. В этом случае он определяется по аппаратному адресу (*MAC-адресу*) сетевой карты клиента. Можете добавить свои значения в таблицу соответствия *статических адресов*.

2.7 Почта

2.7.1 SMTP-сервер

Служба postfix предназначена для передачи электронной почты от одного сервера к другому по протоколу SMTP (simple mail transfer protocol). Сервер назначения вы-

числяется по адресу получателя письма либо явно указывается в настройках (*шлюз для исходящей почты*).

Входящая почта складывается в ящики пользователей, *максимальный размер* которых можно принудительно ограничить. Значение 0 Мб снимает ограничение. Аналогично можно ограничить и размер отдельных сообщений.

С целью борьбы со спамом можно запретить приём писем со скомпроментировавших себя серверов. Их списки (*RBL*) поддерживаются некоторыми популярными компаниями.

Также можно непосредственно указать службе postfix:

- отвергать почту на определённые адреса email;
- отвергать почту с определённых адресов email;
- отвергать почту с определённых клиентов.

Включите нужный фильтр и добавьте свой вариант в соответствующий список.

Postfix позволяет добавлять реальным получателям корреспонденции псевдонимы. Почта, приходящая на адрес псевдонима, будет складываться в ящик настоящего пользователя. Добавьте необходимые значения в список.

SASL (Simple Authentication and Security Layer) — это инфраструктура, позволяющая добавить поддержку аутентификации к протоколам, ориентированным на соединение (POP3, IMAP4, SMTP и т. д.). В Postfix для аутентификации используются внешние службы — *dovecot* или *cirus*.

Сервер *postfix* по умолчанию не принимает входящую почту. Вы можете изменить режим, выбрав в поле `Состояние SMTP транспорта` один из нижеперечисленных вариантов:

- не принимать почту;
- принимать почту, но не фильтровать её;
- принимать почту и фильтровать её.

Последний режим полезен, когда *postfix* используется совместно с какой-либо системой обнаружения спама и/или антивирусом.

2.7.2 POP3/IMAP сервер

Сервер поддерживает несколько протоколов получения почты (`IMAP4`, `IMAP4 через TLS/SSL`, `POP3` и `POP3 через TLS/SSL`), а также несколько протоколов аутентификации пользователей (по умолчанию используется `PLAIN` — обычная аутентификация по имени и паролю).

Из соображений безопасности настоятельно рекомендуется включать и использовать *TLS/SSL*-версии протоколов получения почты.

2.7.3 Спам-фильтр

Для защиты от нежелательных сообщений (*спама*) можно использовать фильтр, встроенный в почтовый клиент. Однако ещё более эффективным решением является фильтр, размещённый сразу на почтовом сервере.

Возможны два варианта работы фильтра (поле `Режим спам-фильтра`): немедленное удаление спама и пометка писем с помощью специальных заголовков. Последний вариант — самый предпочтительный. С одной стороны, экономятся ресурсы машины (не запускается локальный фильтр), с другой — каждый пользователь может определять, что считать спамом и как с ним поступать.

Фильтр анализирует письмо по многим критериям и выставляет ему итоговую оценку. Чем она выше, тем больше вероятность, что это спам. Параметр `Пороговое значение` определяет, начиная с какого значения письмо будет признано спамом и, например, удалено. Критерии оценки писем можно задать самостоятельно, указав название правила и его очки.

`Баллы` формируются из одного или четырёх чисел.

```
RULE_NAME 0.5
RULE_NAME 0.5 0.6 0.5 0.5
RULE_NAME (0.2) (0.3) (0.2) (0.2)
```

Одно число соответствует окончательной оценке правила. Если указаны четыре числа, выбирается одно из них в зависимости от использования или неиспользования статистических (на основе алгоритма Байеса) и сетевых анализаторов.

		статистические	
		нет	есть
сетевые	нет	1-е	3-е
	есть	2-е	4-е

Если число указано в скобках, оно будет добавлено к уже начисленным очкам правила.

Белый список отправителей позволяет оценить их надёжность в долгосрочной перспективе.

2.8 Статистика

2.8.1 Прокси-сервер

Для просмотра статистики использования прокси-сервера выберите интересующий диапазон дат и нажмите *Показать*.

Данные сортируются по IP-адресу.

2.8.2 Сетевой трафик

Входящие и исходящие с сервера сетевые пакеты подсчитываются службой *ulogd*. Можно оценить итоговый объём полученных и переданных данных за всё время работы сервера, за определённый период времени (выберите начальную и конечную дату) и по каждой службе отдельно.

Из списка доступных сетевых интерфейсов выберите интересующий. Отметка *Сверять IP* помимо интерфейса учитывает и его IP-адрес в качестве получателя или отправителя пакетов.