Установка необходимого софта;

Устанавливаем mysql server, будем использовать 5.1, хотя не принципиально, там будут храниться данные о виртуальных пользователях, доменах и т.д.

#cd /usr/ports/databases/mysql51-server

#make install clean

Устанавливаем веб сервер apache22

#cd /usr/ports/www/apache22

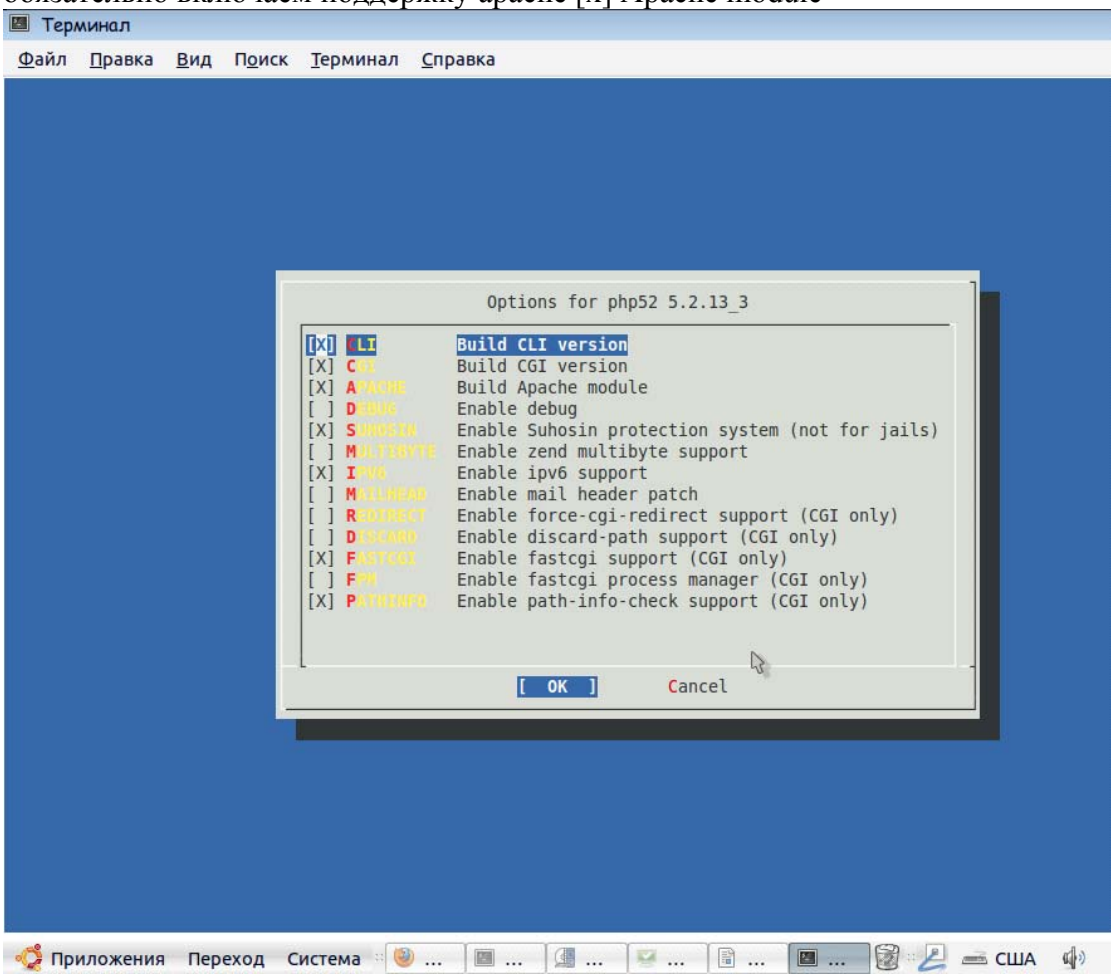
#make install clean

устанавливаем php52

#cd /usr/ports/lang/php52

#make install clean

обязательно включаем поддержку apache [x] Apache module



устанавливаем расширения php52 (необходимы для корректной работы postfixadmin)

#cd /usr/ports/lang/php52-extensions

#make install clean

включаем поддержку следующих модулей

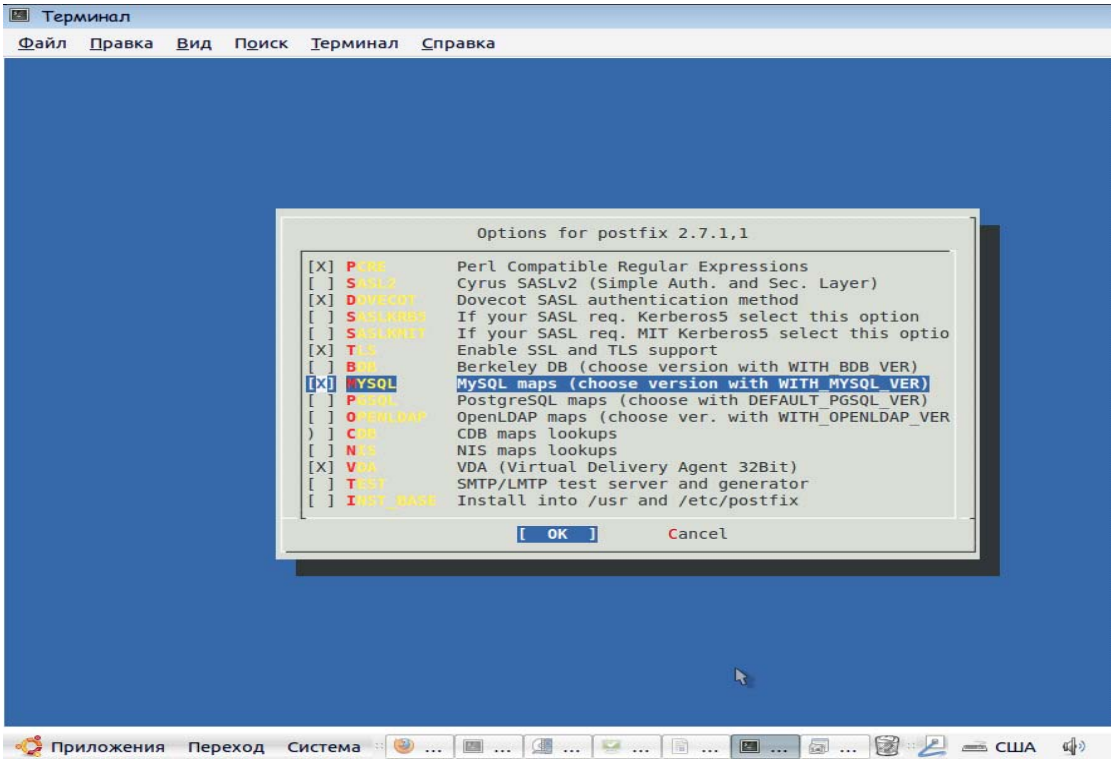
[x] BCMATH [x] GETTEXT [x] MCRYPT [x] MYSQLI [x]SESSION [x] SOCKETS

[x] WDDX

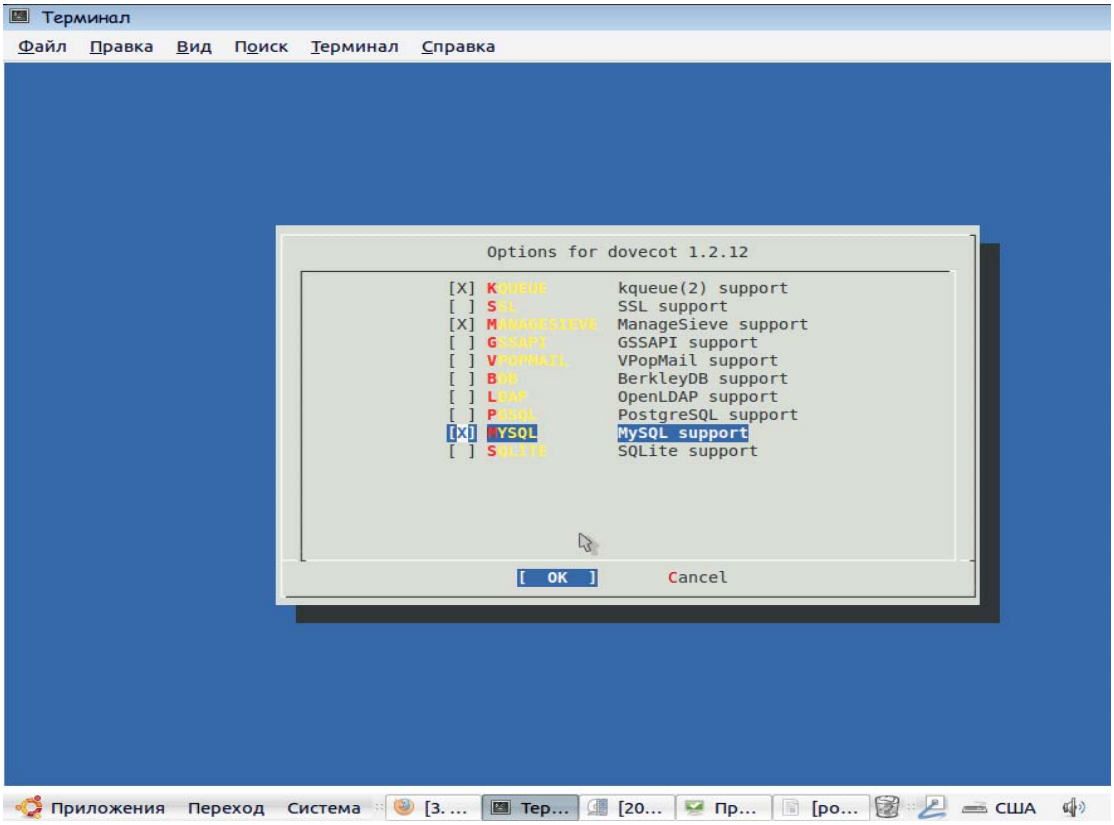
ставим postfixadmin

#cd /usr/ports/mail/postfixadmin

#make install clean
включаем обязательно поддержку MySQL 4.1+ [x] MYSQLI
устанавливаем phpmyadmin (не является обязательным для работы почтового сервера, но очень полезен при выявлении ошибок)
#cd /usr/ports/databases/phpmyadmin
#make install clean
устанавливаем postfix
#cd /usr/ports/mail/postfix
#make install clean



отмечаем [x] DOVECOT [x] MYSQL [x] VDA [x] TLS (этот модуль необязателен, используется для организации защищенных ssl соединений, можно отметить на перспективу)



postfix при установке потащит за собой и dovecot. Там включаем поддержку mysql [x] MYSQLв конце установки postfix спросит включить ли пользователя postfix. От имени которого будет работать демон в группу mail. Отвечаем утвердительно

Сначала настроим и опробуем наш apache сервер, он должен заработать с поддержкой php;
#ee /usr/local/etc/apache22/httpd.conf
ищем блок
<IfModule dir_module>
    DirectoryIndex index.html
</IfModule>
и меняем index.html на index.php

ищем блок
<IfModule mime_module>
            …
        AddType application/x-compress .Z
        AddType application/x-gzip .gz .tgz
добавляем
        AddType application/x-httpd-php .php
        AddType application/x-httpd-php-source .phps

далее можно поправить адрес электронной почты администратора, интерфейсы и навести другой внешний блеск.

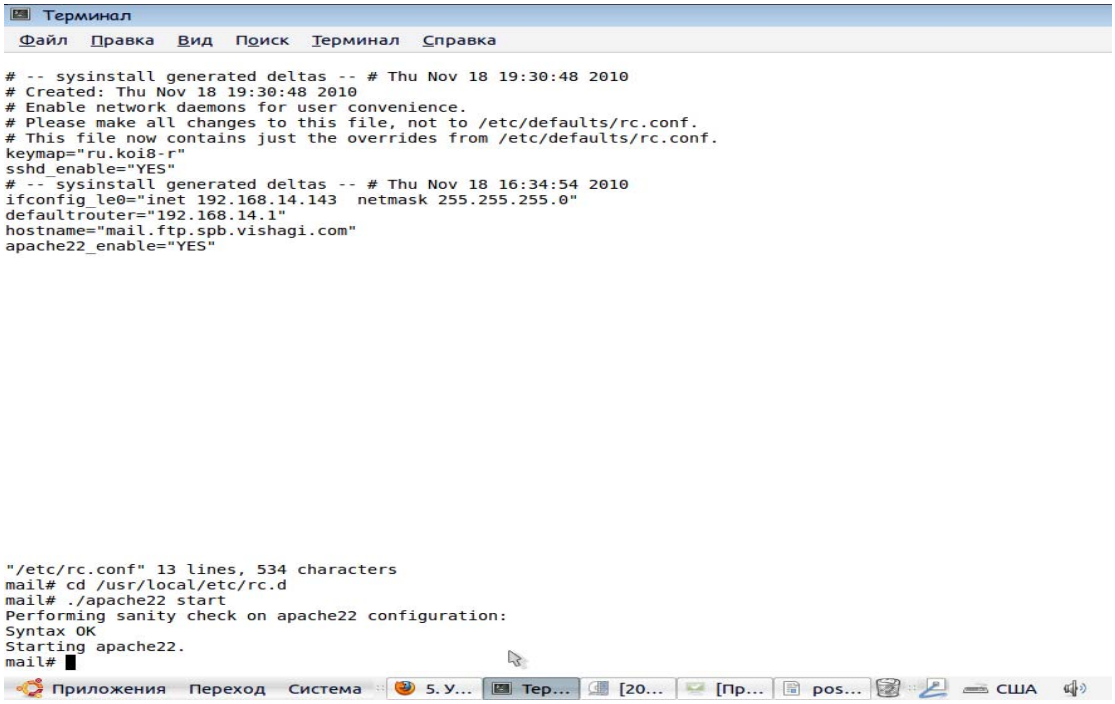
закрываем и не забываем сохранить

добавдяем строку apache22_enable="YES" в файл /etc/rc.conf (необходимо для запуска apache)

стартуем апач

#cd /usr/local/etc/rc.d

#./apache22 start



идем в папку /usr/local/www/apache22/data

создаем в ней файлик index.php

#ee index.php

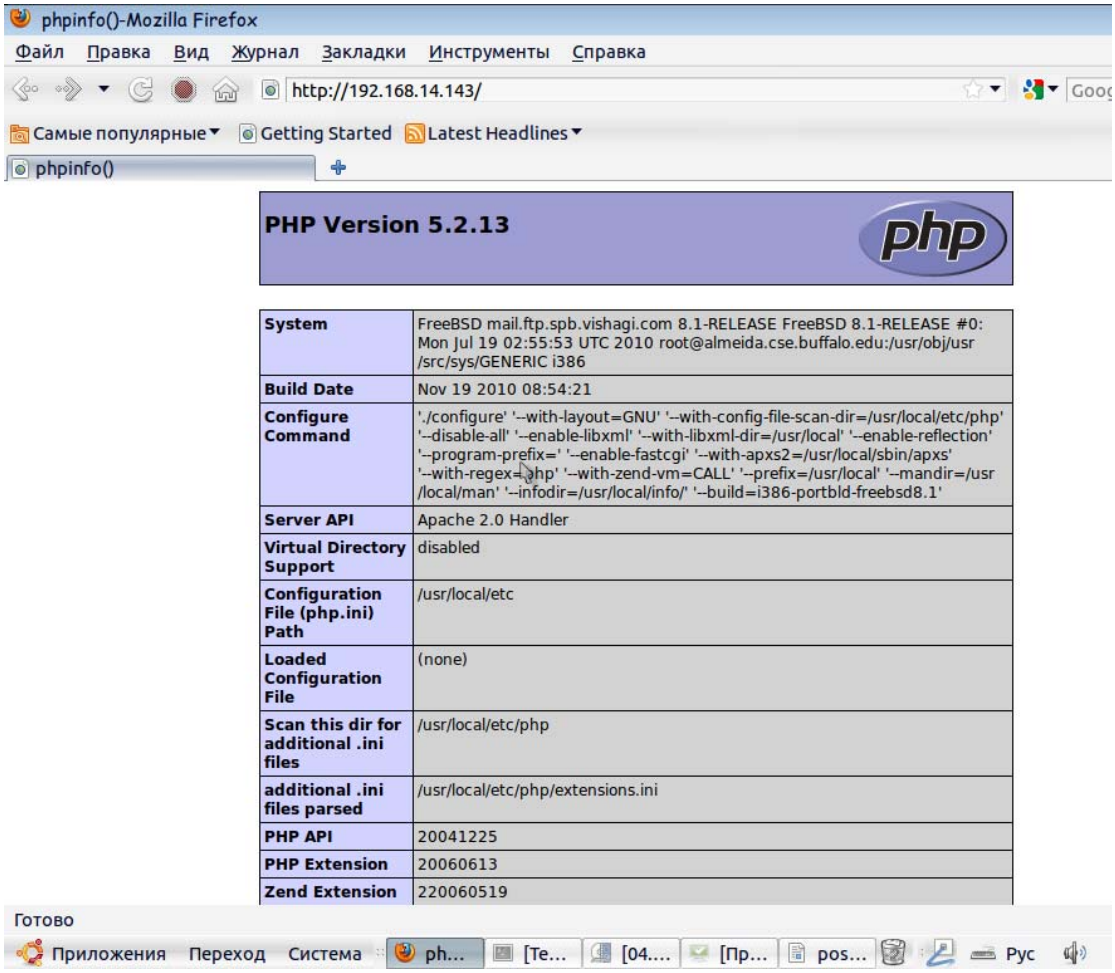
```
<?php

        phpinfo();

?>
```

заходим любым браузером на http://ip-сервера/

видим картинку типа

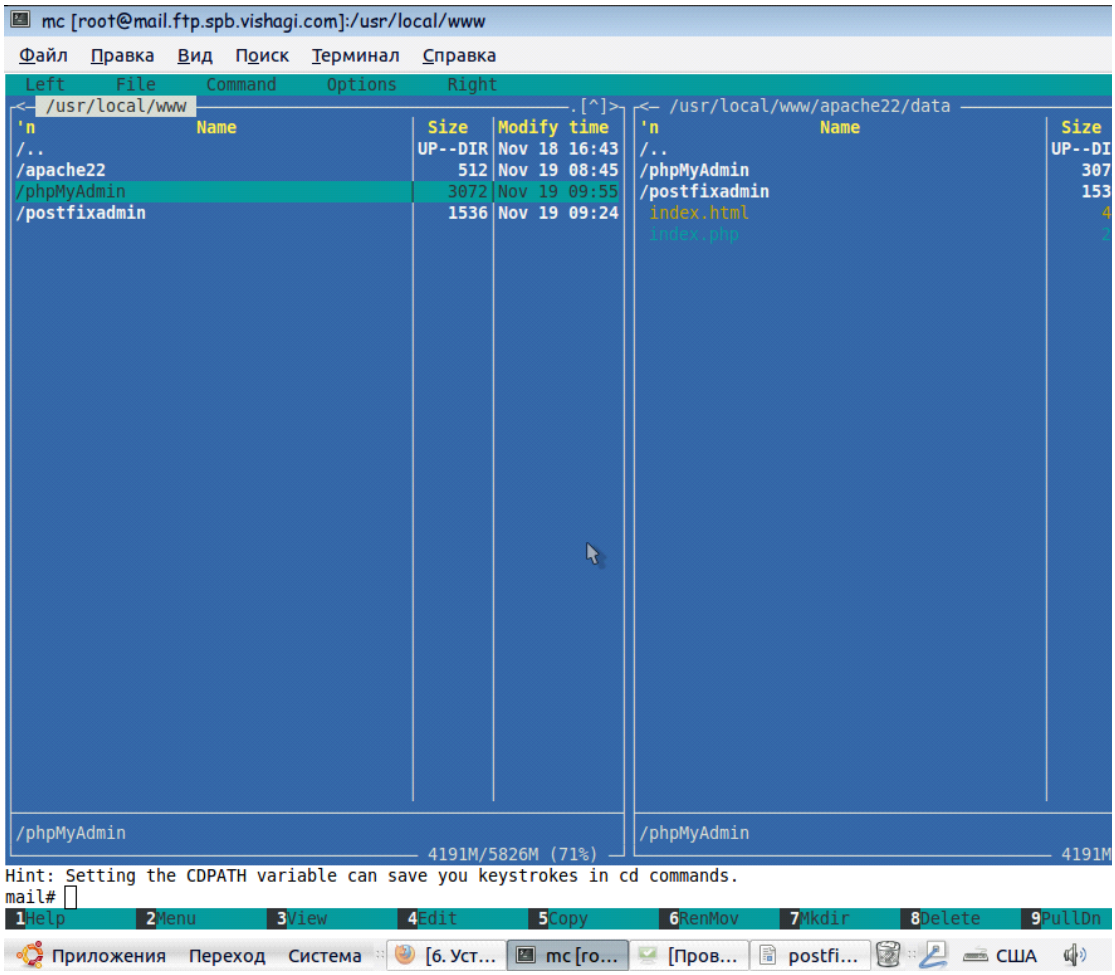


на этом этапе все ОК — двигаемся дальше, если что-то пошло не так смотрим лог /var/log/httpd-error.log.

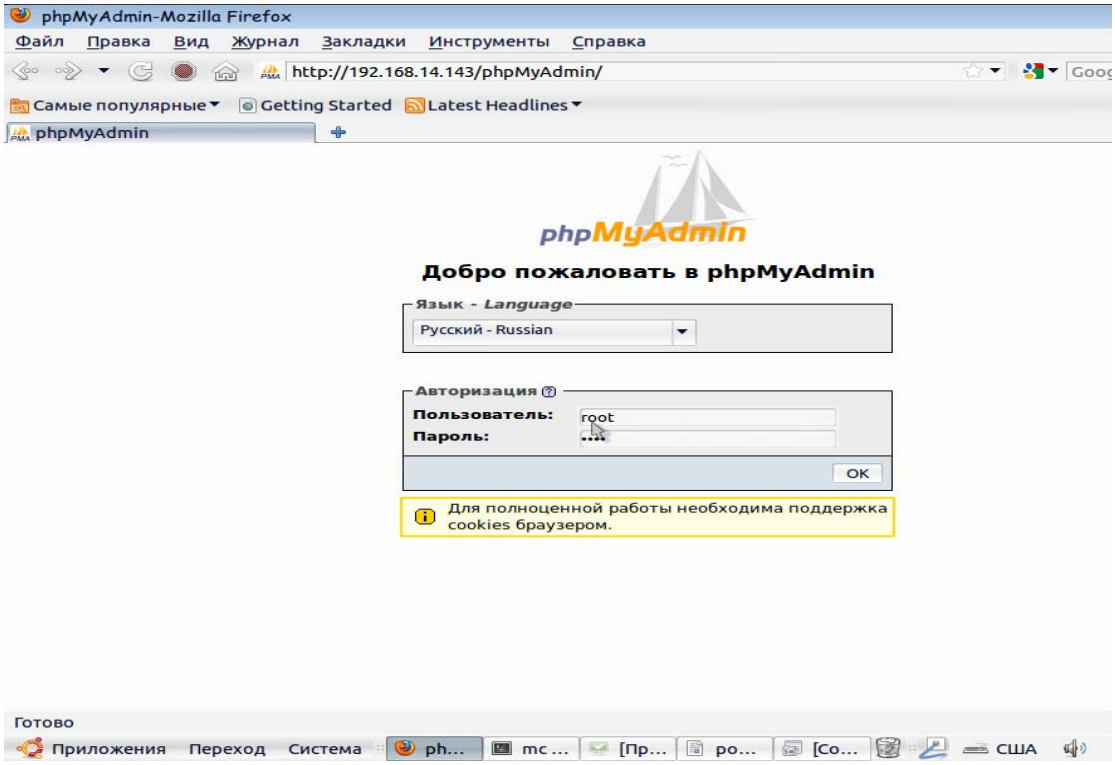
Запускаем сервер mysql
#echo 'mysql_enable="YES"' >> /etc/rc.conf
#/usr/local/etc/rc.d/mysql-server start
меняем пароль админа для mysql-server:
#mysqladmin -u root password toor(тут пароль)
Создаем базу для postfixadmin:
#mysql -u root -p
(Enter MySQL root password)
>CREATE DATABASE postfix;
>CREATE USER 'postfix'@'localhost' IDENTIFIED BY '**postfix(тут пароль)**';
>GRANT ALL PRIVILEGES ON `postfix` . * TO 'postfix'@'localhost';
>FLUSH PRIVILEGES;

чтобы не прописывать алиасы для веб сервера просто копируем папки /usr/local/www/postfixadmin и /usr/local/www/phpMyAdmin в папку /usr/local/www/apache22/data

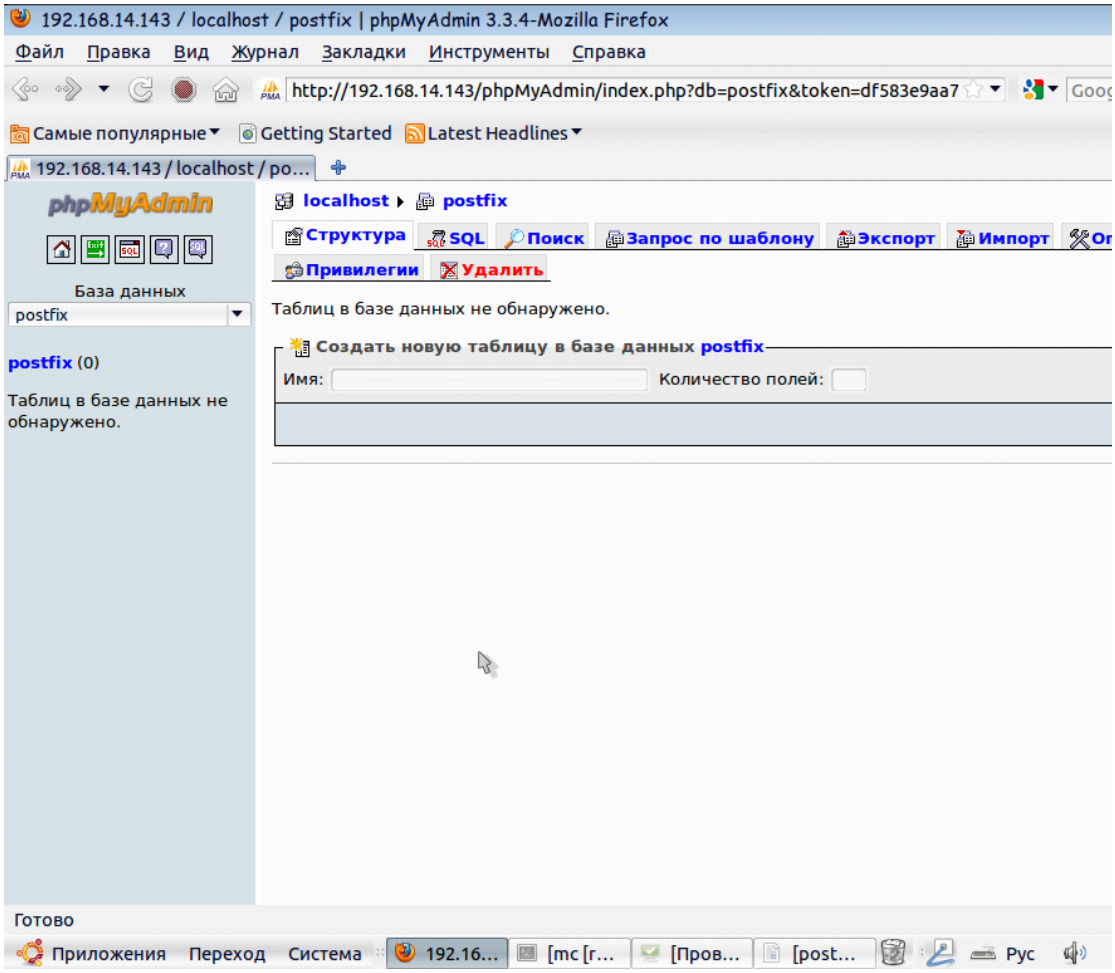
сделать можно при помощи mc или из командной строки



заходим браузером по адресу http://ip-сервера/phpMyAdmin



убеждаемся, что база postfix успешно создана



идем править конфигурационный файл /usr/local/www/apache22/data/postfixadmin/config.inc.php:

$CONF['configured'] = true;
$CONF['setup_password'] = ''; оставляем пока пустой

…

$CONF['database_type'] = 'mysqli'; для базы mysql 4.1+
$CONF['database_host'] = 'localhost'; база на этом же хосте
$CONF['database_user'] = 'postfix';
$CONF['database_password'] = 'postfix'; (тут ваш пароль пользователя postfix mysql)
$CONF['database_name'] = 'postfix';
$CONF['database_prefix'] = '';

…

$CONF['admin_email'] = 'admin@ftp.spb.vishagi.com';

…

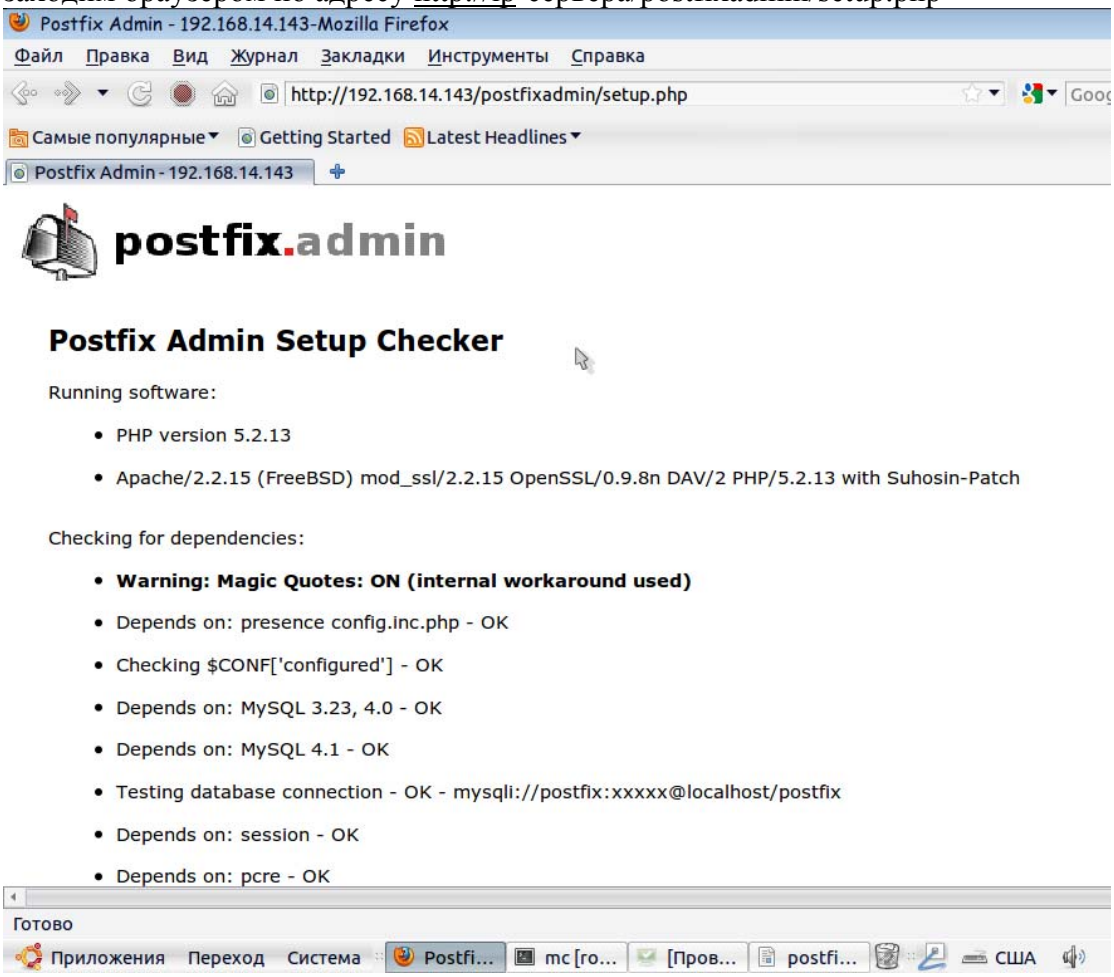
$CONF['encrypt'] = 'md5crypt'; шифровать пароли в mysql. Если вам это не нужно можно вставить cleartext

…

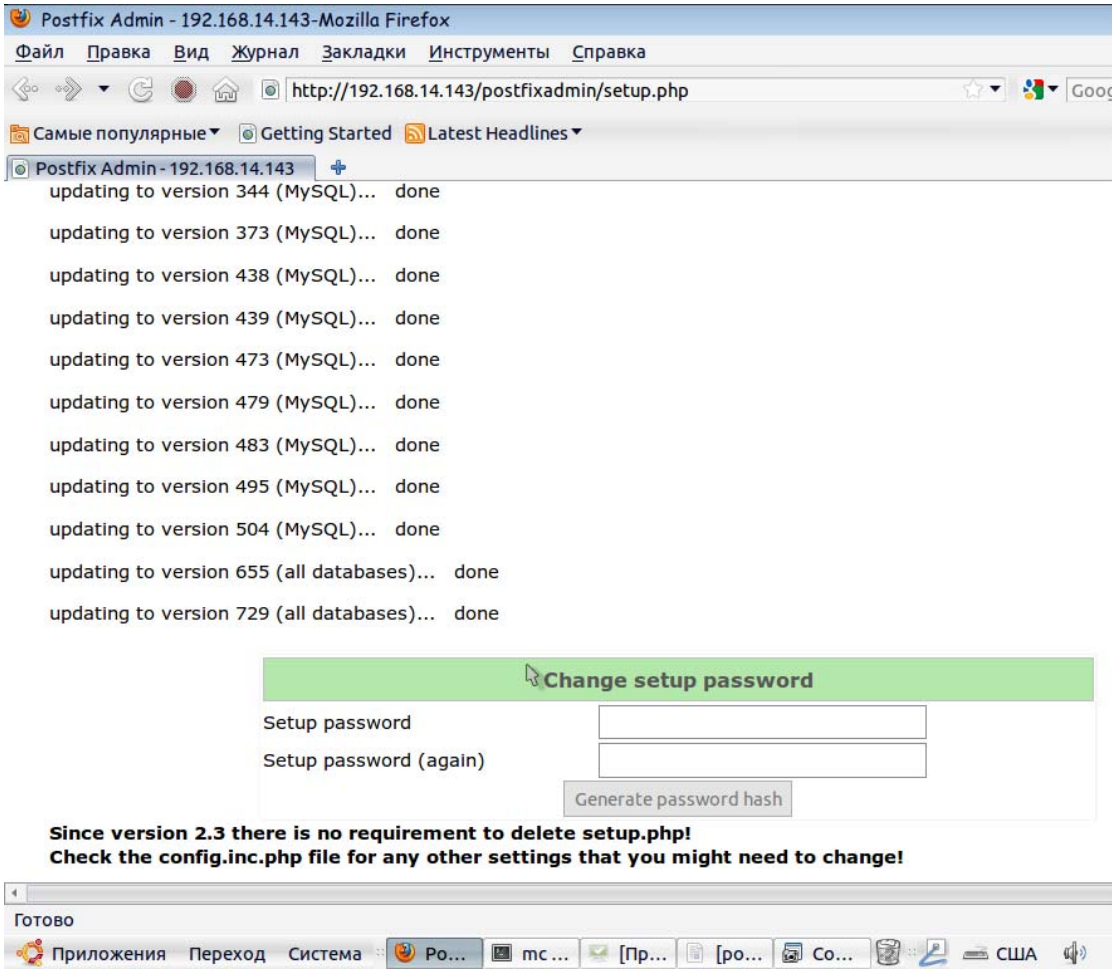
$CONF['authlib_default_flavor'] = 'md5';
$CONF['min_password_length'] = 0; минимальная длина пароля
$CONF['default_aliases'] = array (
    'abuse' => 'abuse@change-this-to-your.domain.tld',
    'hostmaster' => 'hostmaster@change-this-to-your.domain.tld',
    'postmaster' => 'postmaster@change-this-to-your.domain.tld',
    'webmaster' => 'webmaster@change-this-to-your.domain.tld'
); ставим свои

также там можно задать квоты почтовых ящиков, папки, создаваемые при создании почтового ящика и т. д.

заходим браузером по адресу http://ip-сервера/postfixadmin/setup.php



ниже будет предложено ввести пароль админа



вводим, кликаем СГЕНЕРИРОВАТЬ ХЭШ, получаем что-то типа

If you want to use the password you entered as setup password, edit config.inc.php and set

$CONF['setup_password'] =
'bfe2b9121bdb9d98d47a9a47a4eb4952:26a25c37ca2da60e32420745e98bf249fcd0c24b';

копируем строку в кавычках и вставляем её в файл
/usr/local/www/apache22/data/postfixadmin/config.inc.php

$CONF['setup_password'] =
'bfe2b9121bdb9d98d47a9a47a4eb4952:26a25c37ca2da60e32420745e98bf249fcd0c24b';

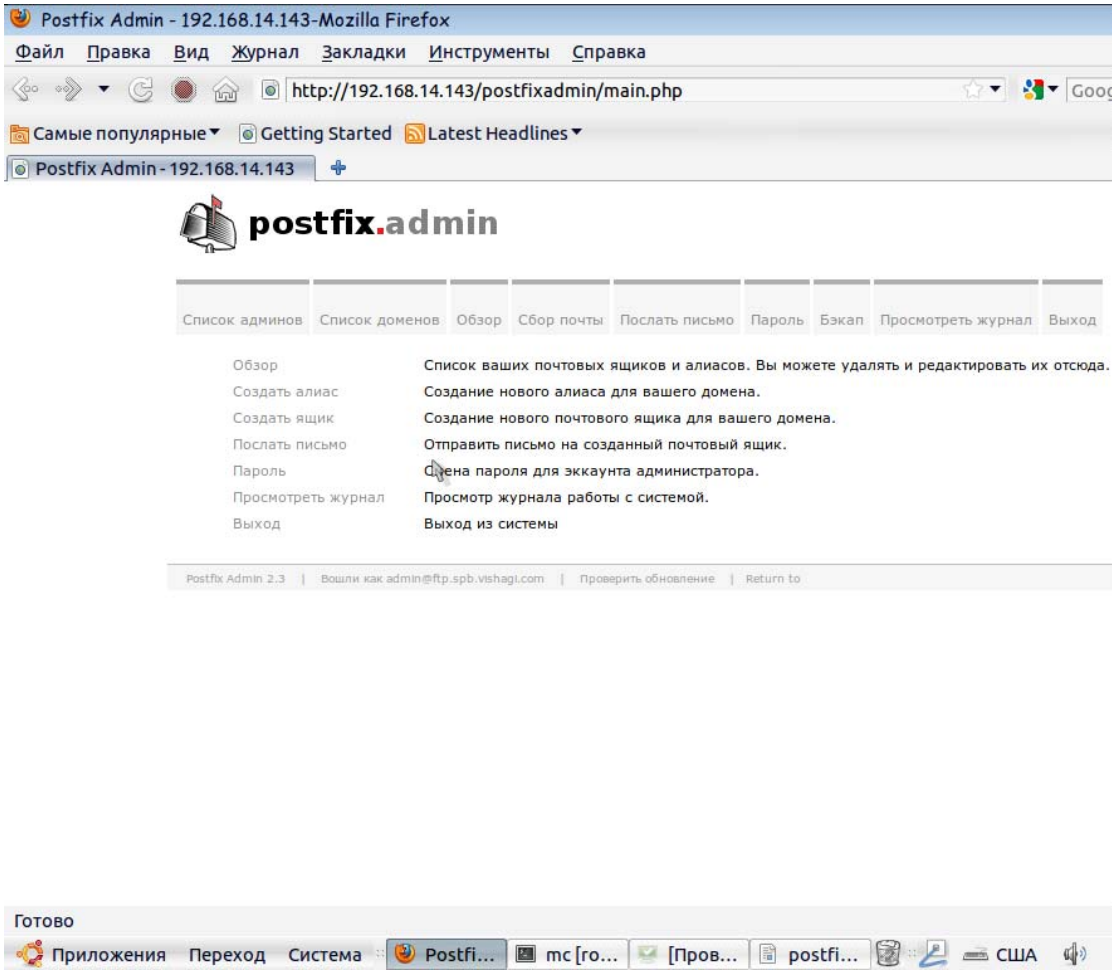
добавляем админа; Create superadmin account

получаем;

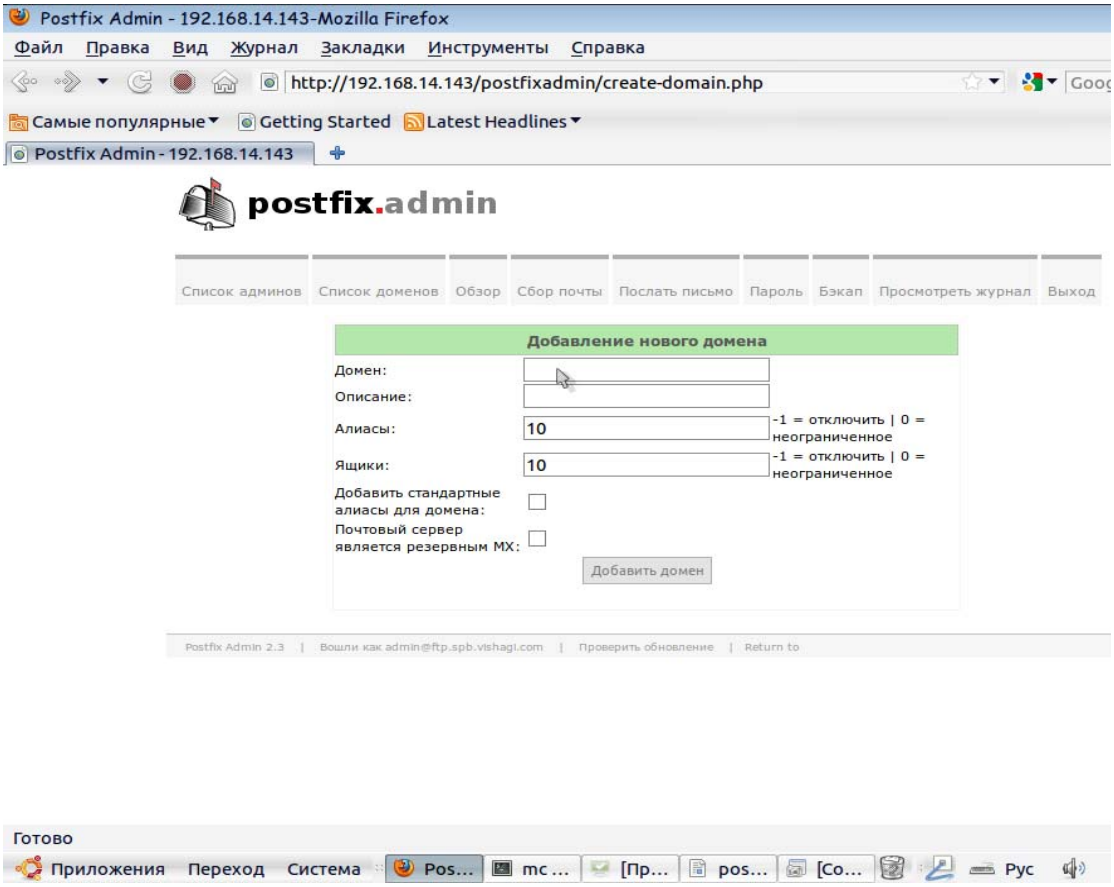
Администратор был добавлен!
(admin@ftp.spb.vishagi.com)

пробуем логиниться на http://ваш ip сервера/postfixadmin/login.php

получим



Ура! Все работает как надо.
Прописываем новый домен;



настроим постфикс на работу с виртуальными пользователями;
#ee /usr/local/etc/postfix/main.cf

…
myhostname = mail.ftp.spb.vishagi.com имя хоста, если не указано будет браться из /etc/rc.conf

…
mydomain = ftp.spb.vishagi.com домен

…
mynetworks = 192.168.14.0/24, 127.0.0.0/8 внутренняя сеть. Клиентам можно пересылать сообщения через почтовый сервер без всякой аутендификации.

…
alias_maps = hash:/etc/aliases

…
alias_database = hash:/etc/aliases

…
home_mailbox = Maildir/

…
smtpd_banner = $myhostname ESMTP $mail_name приветствие

virtual_alias_maps = mysql:/usr/local/etc/postfix/mysql_virtual_alias_maps.cf
virtual_gid_maps = static:125 (125 gid пользователя postfix)
virtual_mailbox_base = /var/mail
virtual_mailbox_domains =
mysql:/usr/local/etc/postfix/mysql_virtual_domains_maps.cf
virtual_mailbox_maps = mysql:/usr/local/etc/postfix/mysql_virtual_mailbox_maps.cf
virtual_minimum_uid = 125
virtual_transport = virtual
virtual_uid_maps = static:125

gid и uid пользователя постфикс можно узнать командой #id postfix

создадим файлы, о которых мы упомянули выше;

/usr/local/etc/postfix/mysql_virtual_alias_maps.cf
user = postfix
password = postfix пароль к базе
hosts = 127.0.0.1
dbname = postfix
table = alias
select_field = goto
where_field = address

/usr/local/etc/postfix/mysql_virtual_domains_maps.cf
user = postfix
password = postfix
hosts = 127.0.0.1
dbname = postfix
table = domain
select_field = domain
where_field = domain
additional_conditions = and backupmx = '0' and active = '1'

/usr/local/etc/postfix/mysql_virtual_mailbox_maps.cf
user = postfix
password = postfix
hosts = 127.0.0.1
dbname = postfix
table = mailbox
select_field = maildir
where_field = username

Отредактируем /etc/rc.conf для отключения Sendmail

```
sendmail_enable="NO"
sendmail_submit_enable="NO"
sendmail_outbound_enable="NO"
sendmail_msp_queue_enable="NO"
postfix_enable="YES"
```

Создадим и отредактируем файл /etc/periodic.conf

daily_clean_hoststat_enable="NO"

daily_status_mail_rejects_enable="NO"

daily_status_include_submit_mailq="NO"

daily_submit_queuerun="NO"

сворачиваем sendmail

#/etc/rc.d/sendmail forcestop

создадим базу алиасов:

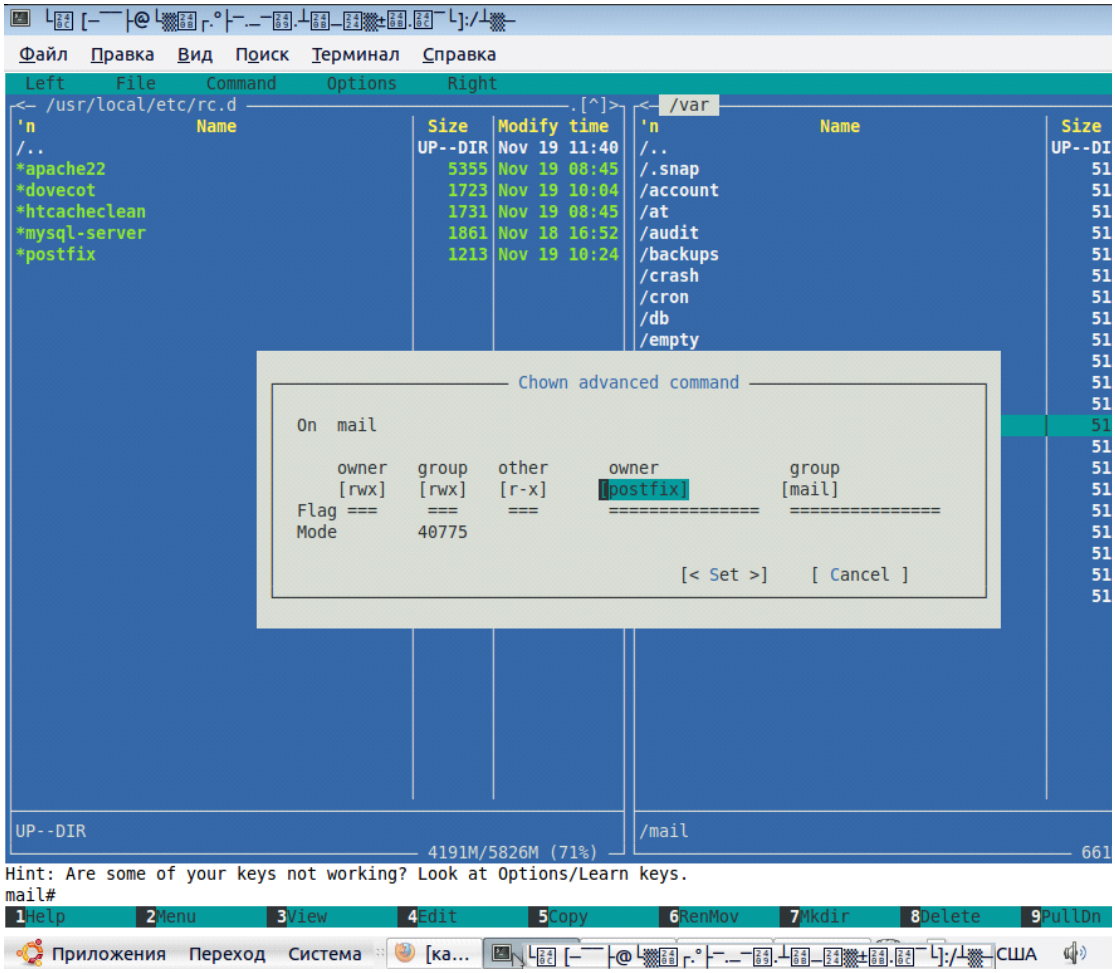
#/usr/bin/newaliases

стартуем postfix:

#cd /usr/local/etc/rc.d

#./postfix start

отдадим папку /var/mail пользователю postfix

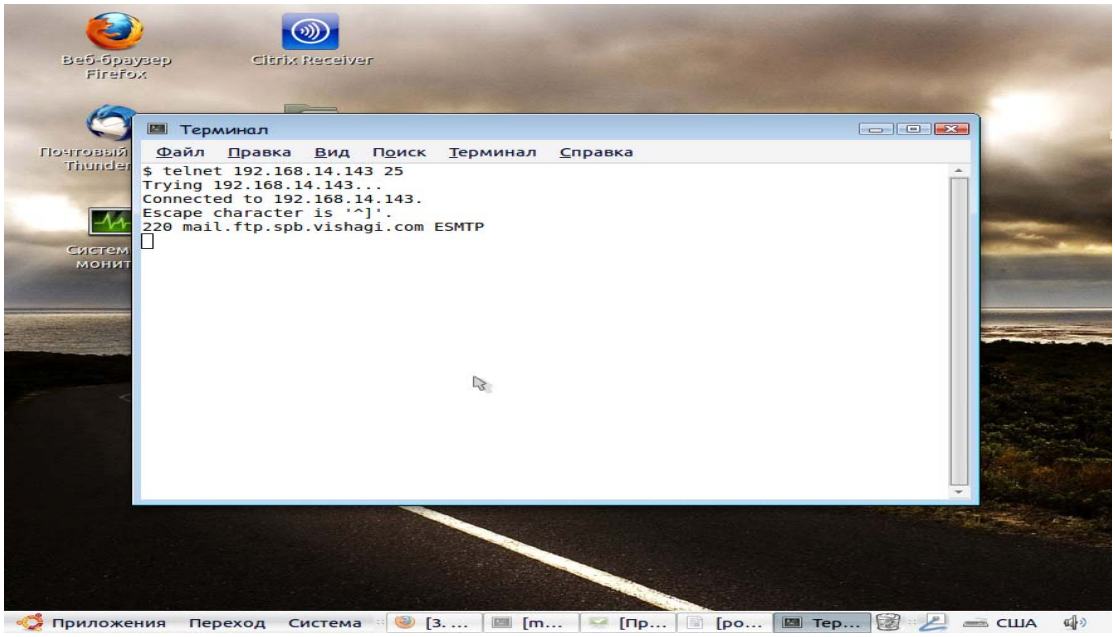


проверяем отсутствие ошибок в файлах /var/log/messages /var/log/maillog, там должно быть что-то типа;

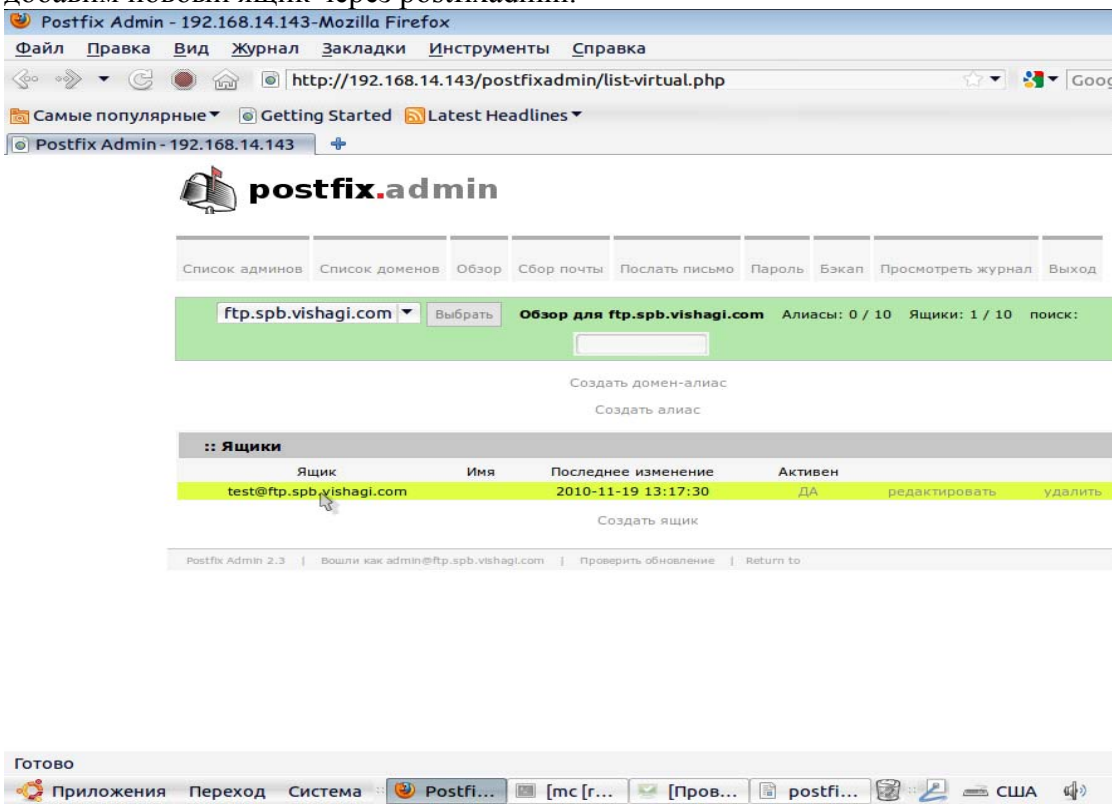
...daemon started... version … configuration file ...

проверяем работу postfix:

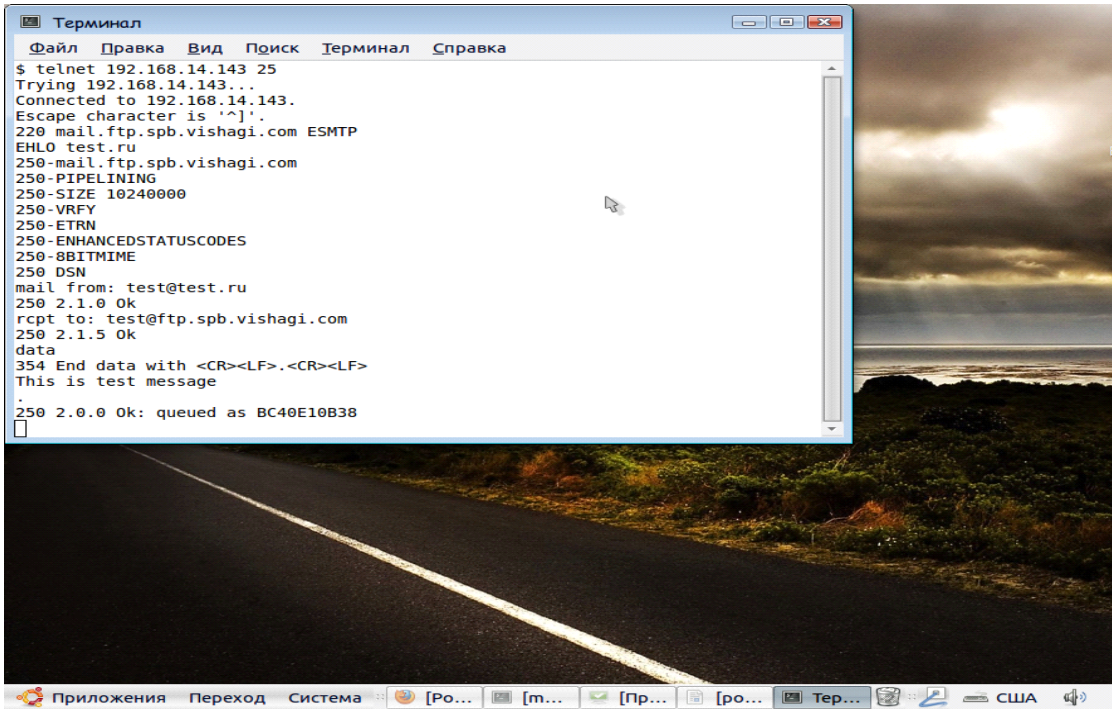
прицепимся telnet на 25 порт



сервер отвечает нам как и положено
добавим новоый ящик через postfixadmin:

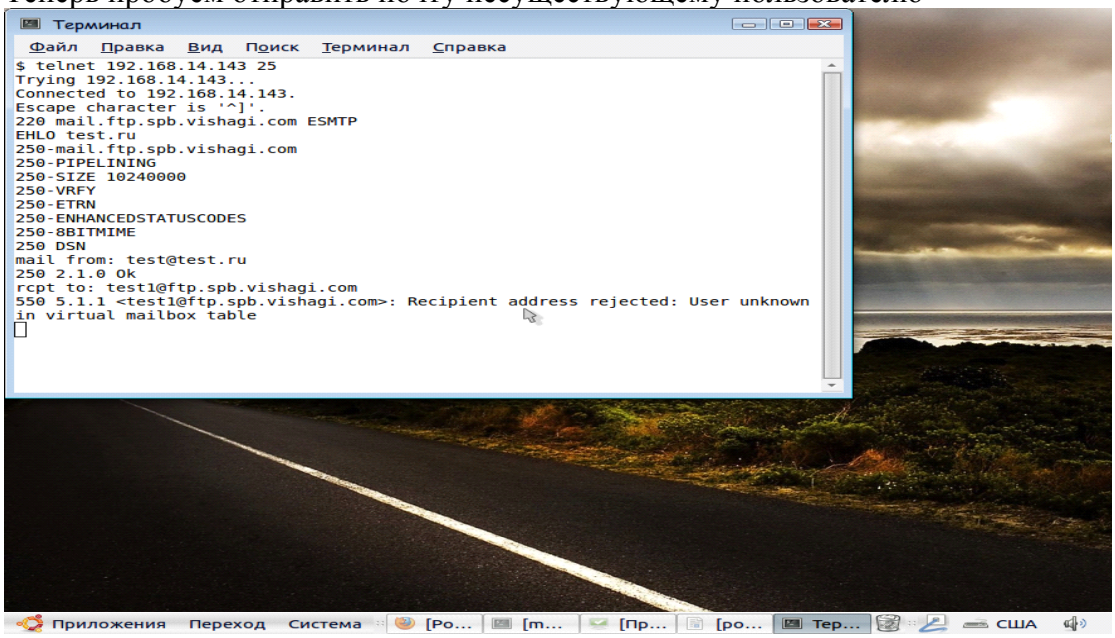


пробуем отправить ему почту через telnet



письмо ушло

Теперь пробуем отправить почту несуществующему пользователю



постфикс отпинывается сообщением Recipient address rejected: User unknown in virtual mailbox table , значит он корретно работает с пользователями из mysql, на этом задача настройки почтового сервера выполнена.

Теперь необходимл отдать почту пользователям, будем это делать по imap. В этом нам поможет dovecot

#ee /usr/local/etc/dovecot.conf

приводим к виду;

```
base_dir = /var/run/dovecot/
protocols = imap #убираем лишние, мне нужен только imap
listen = * #слушать на всех интерфейсах
disable_plaintext_auth = no #разрешаем plaintext логинов по non-SSL портам
log_path = /var/log/dovecot.log #куда складывать лог
info_log_path =/var/log/dovecot.log
ssl = no # отключаем ssl
login_greeting = Dovecot ready. # приветствие
mail_location = maildir:/var/mail/%u #где хранится почта
mail_privileged_group = mail
mail_full_filesystem_access = no
mail_debug = yes #работать в режиме отладки
dotlock_use_excl = yes
verbose_proctitle = yes
first_valid_uid = 125 #uid gid postfixa
last_valid_uid = 125
first_valid_gid = 125
last_valid_gid = 125
auth_debug_passwords=yes #тоже отладка логинов
maildir_copy_with_hardlinks = yes
protocol imap {
  imap_client_workarounds = delay-newmail netscape-eoh tb-extra-mailbox-sep
}
protocol lda {
  postmaster_address = shevtsov@ftp.spb.vishagi.com
}
auth_verbose = yes
auth default {
  mechanisms = plain login
  passdb sql {
    args = /usr/local/etc/dovecot-mysql.conf # авторизоваться в sql
  }
  userdb sql {
    # Path for SQL configuration file.
    # See /usr/local/share/examples/dovecot/dovecot-sql.conf
    args = /usr/local/etc/dovecot-mysql.conf
  }
  socket listen {
    master {
    }
    client {
      path = /var/run/dovecot/auth-client
      mode = 0660
    }
  }
}
dict {
```

}
plugin {
}

создадим вышеупомянутый файл dovecot-mysql.conf
#ee /usr/local/etc dovecot-mysql.conf

driver = mysql
connect = host=localhost port=3306 dbname=postfix user=postfix password=postfix
default_pass_scheme = MD5-CRYPT #для обращения к зашифрованным паролям
password_query = SELECT password FROM mailbox WHERE username = '%u'
user_query = SELECT maildir, 125 AS uid, 125 AS gid FROM mailbox WHERE username = '%u'

создаем файл лога dovecot

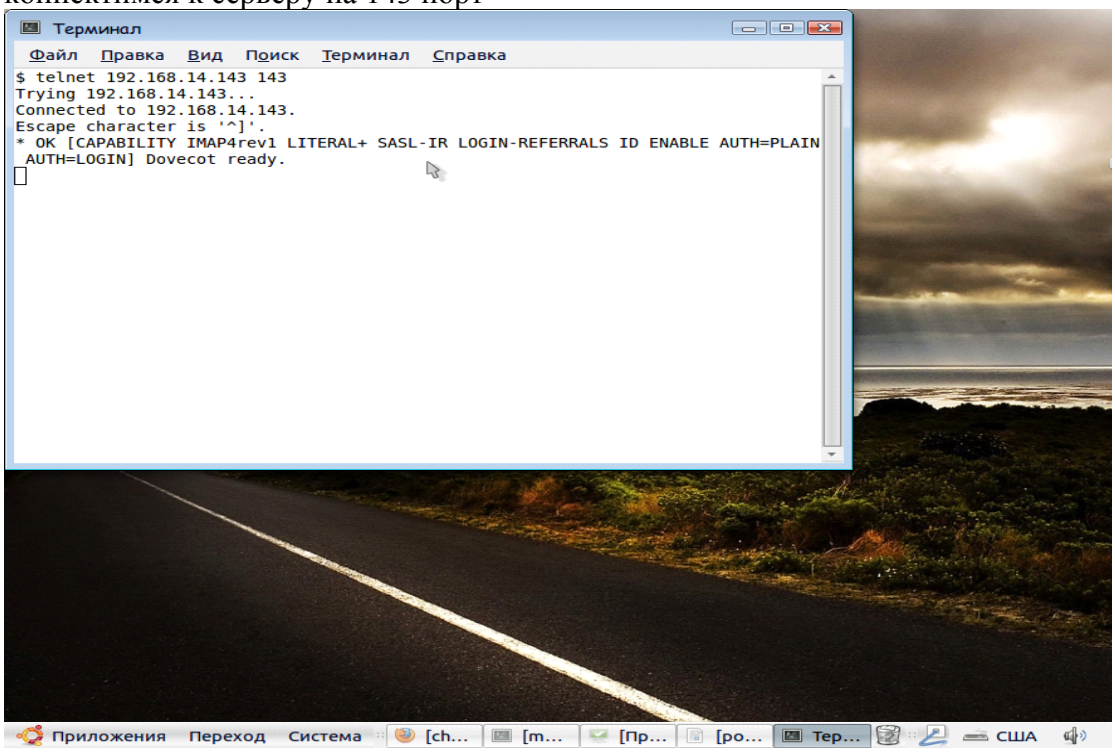
#touch /var/log/dovecot.log
#chmod 666 /var/log/dovecot.log

#echo 'dovecot_enable="YES"' >> /etc/rc.conf

запустим dovecot:
#cd /usr/local/etc/rc.d
#./dovecot start

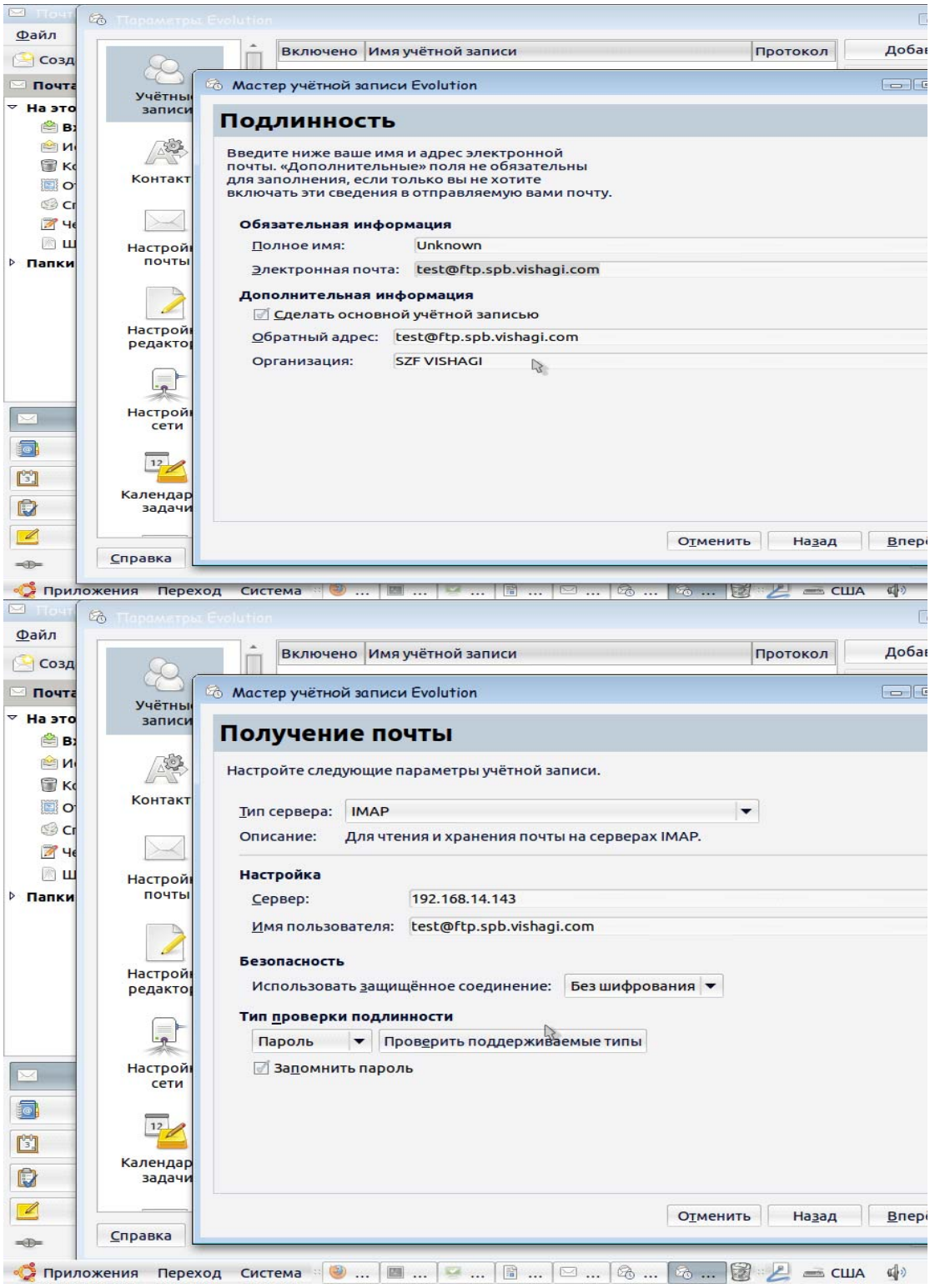
смотрим лог на отсутствие ошибок

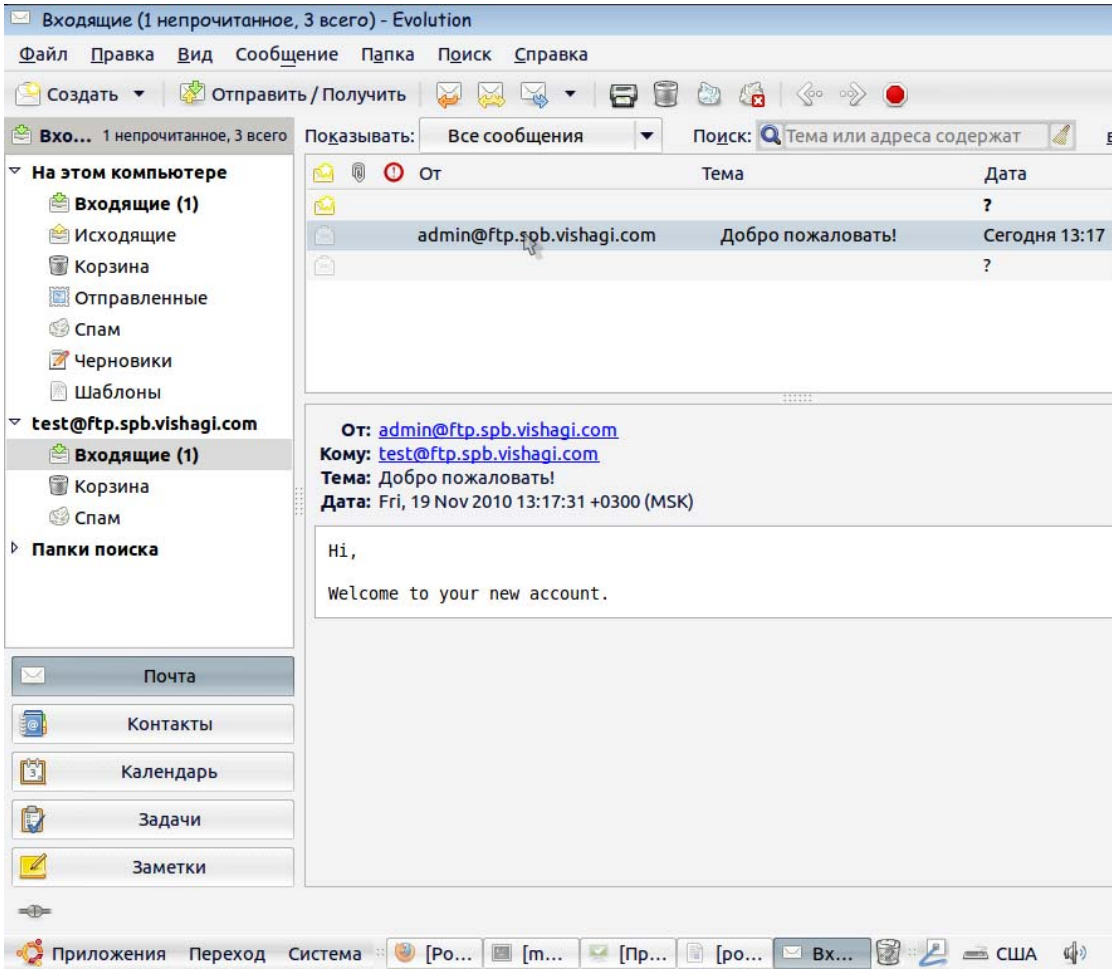
коннектимся к серверу на 143 порт

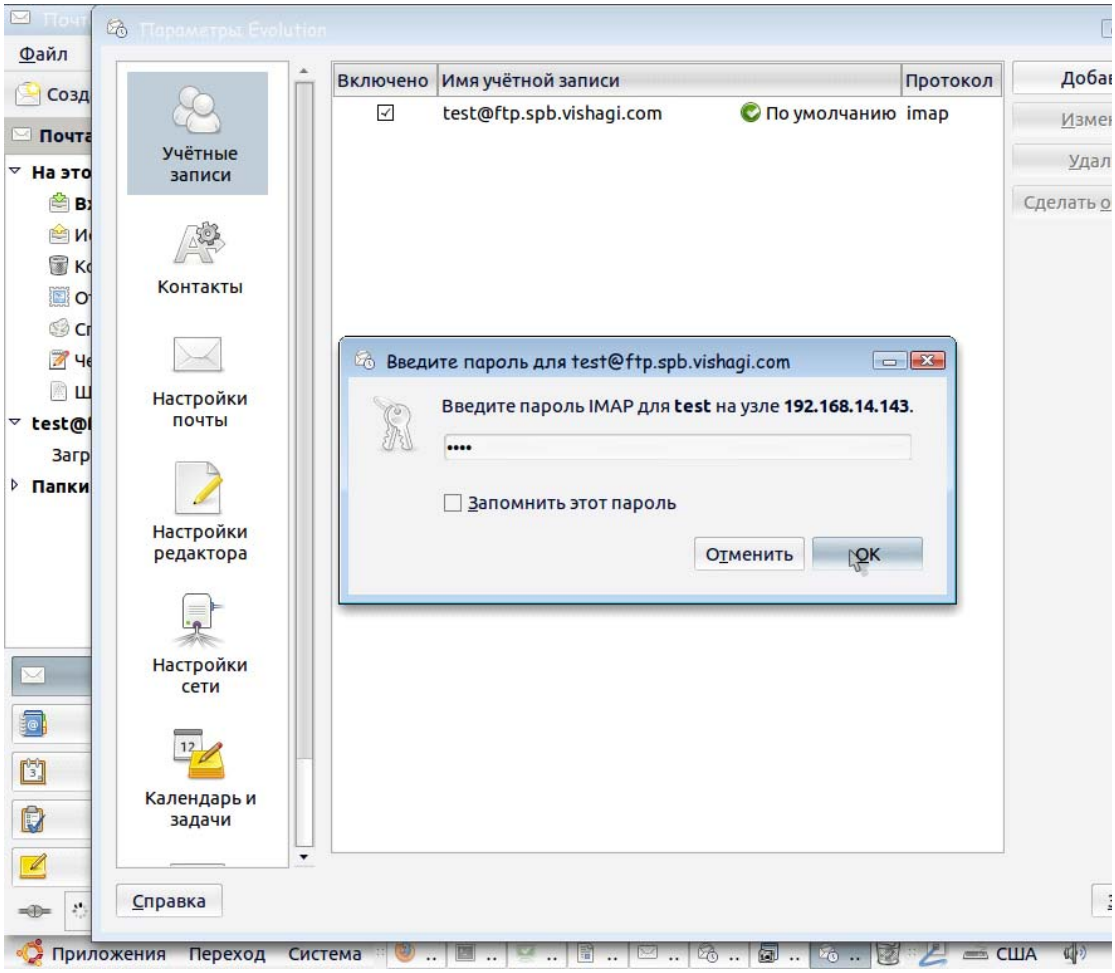


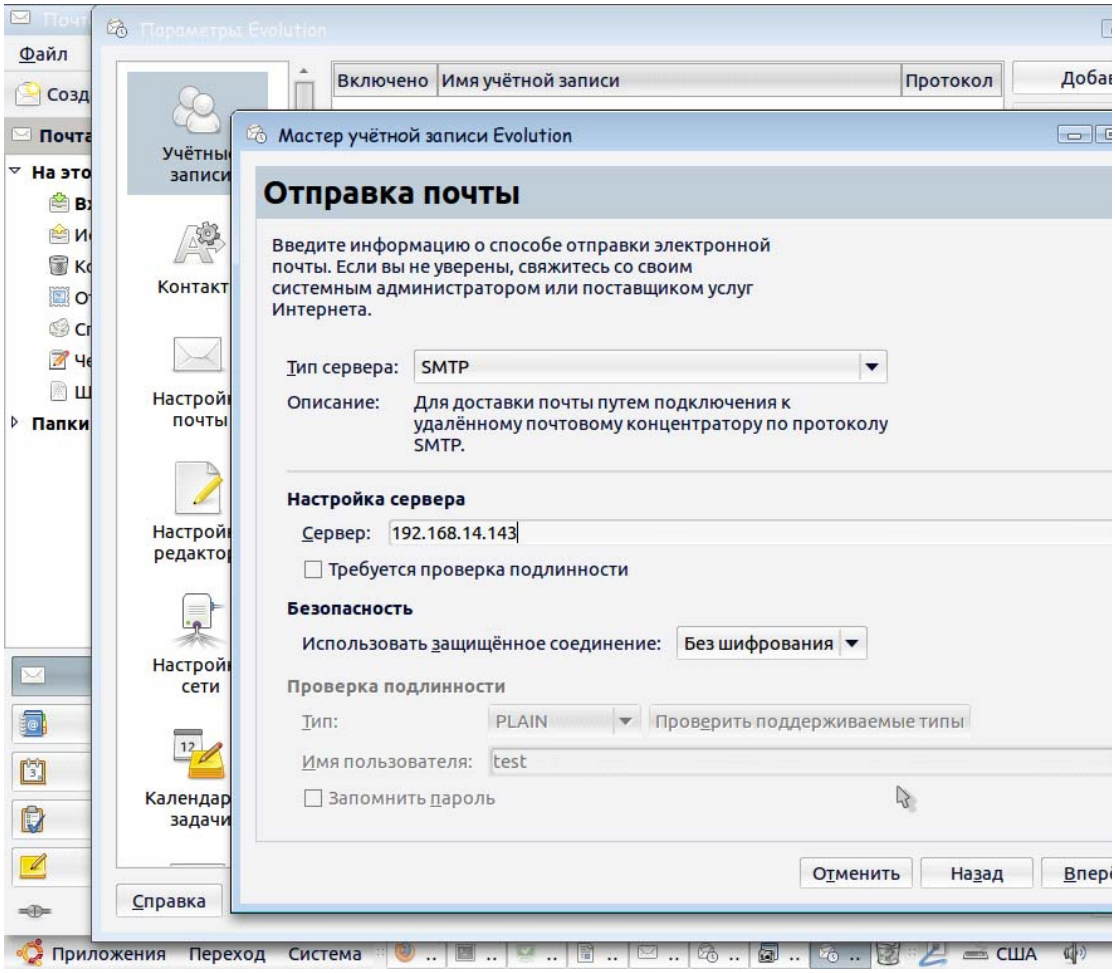
Dovecot отвечает как надо

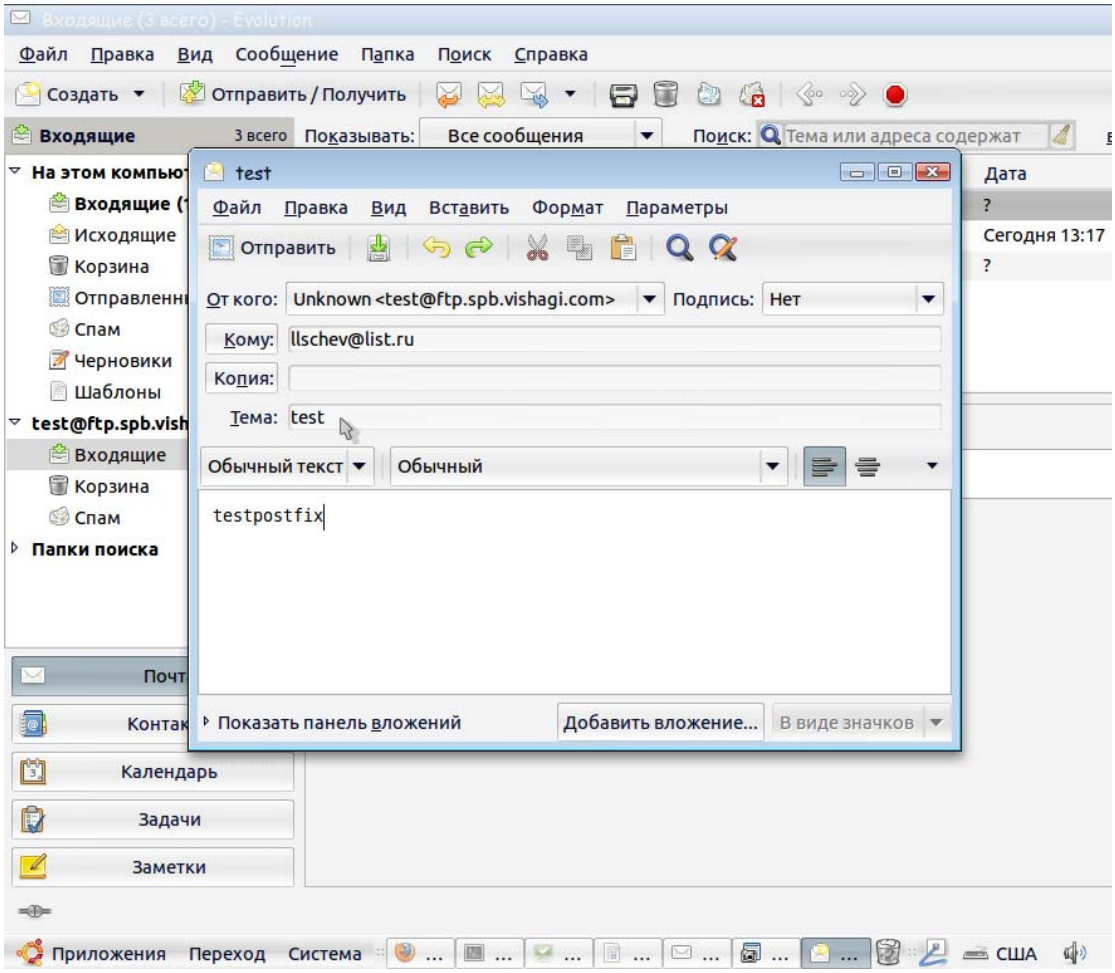
Тестим!

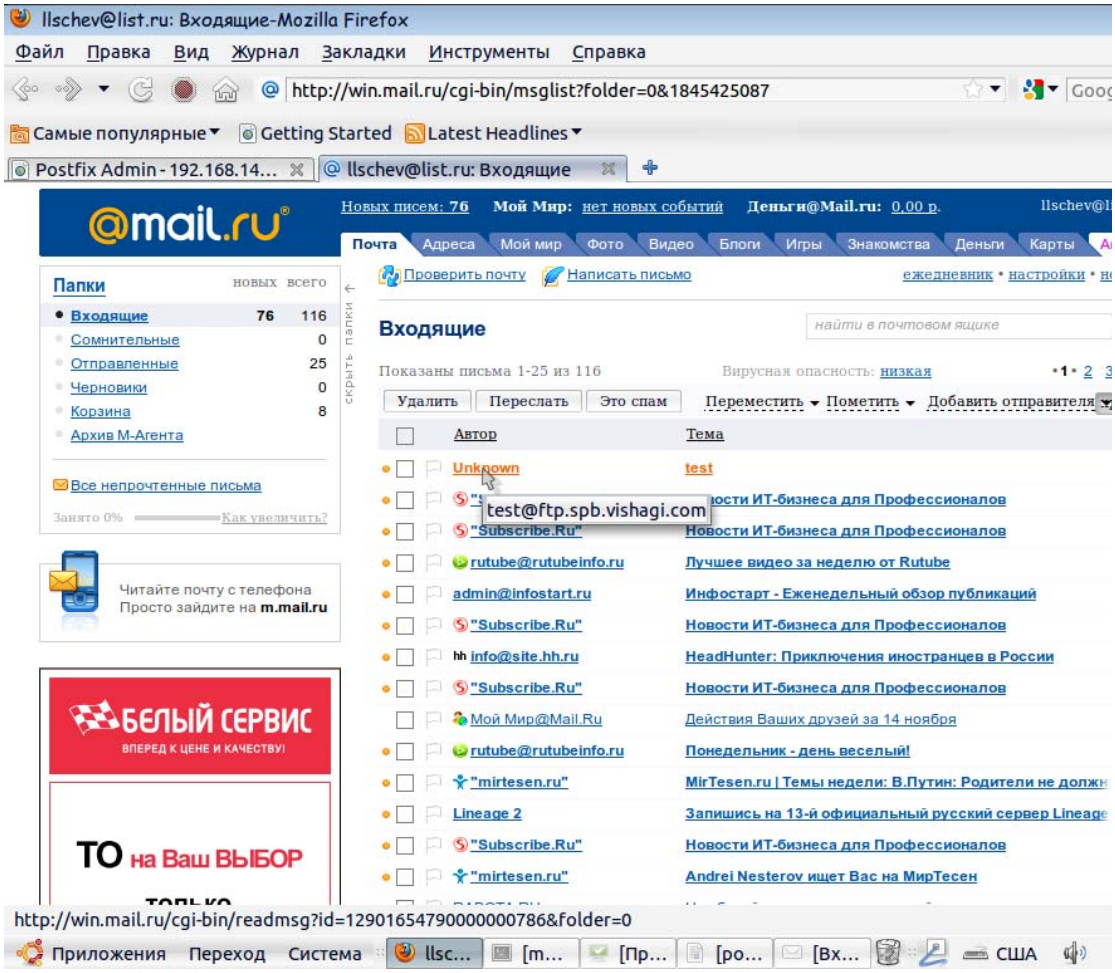


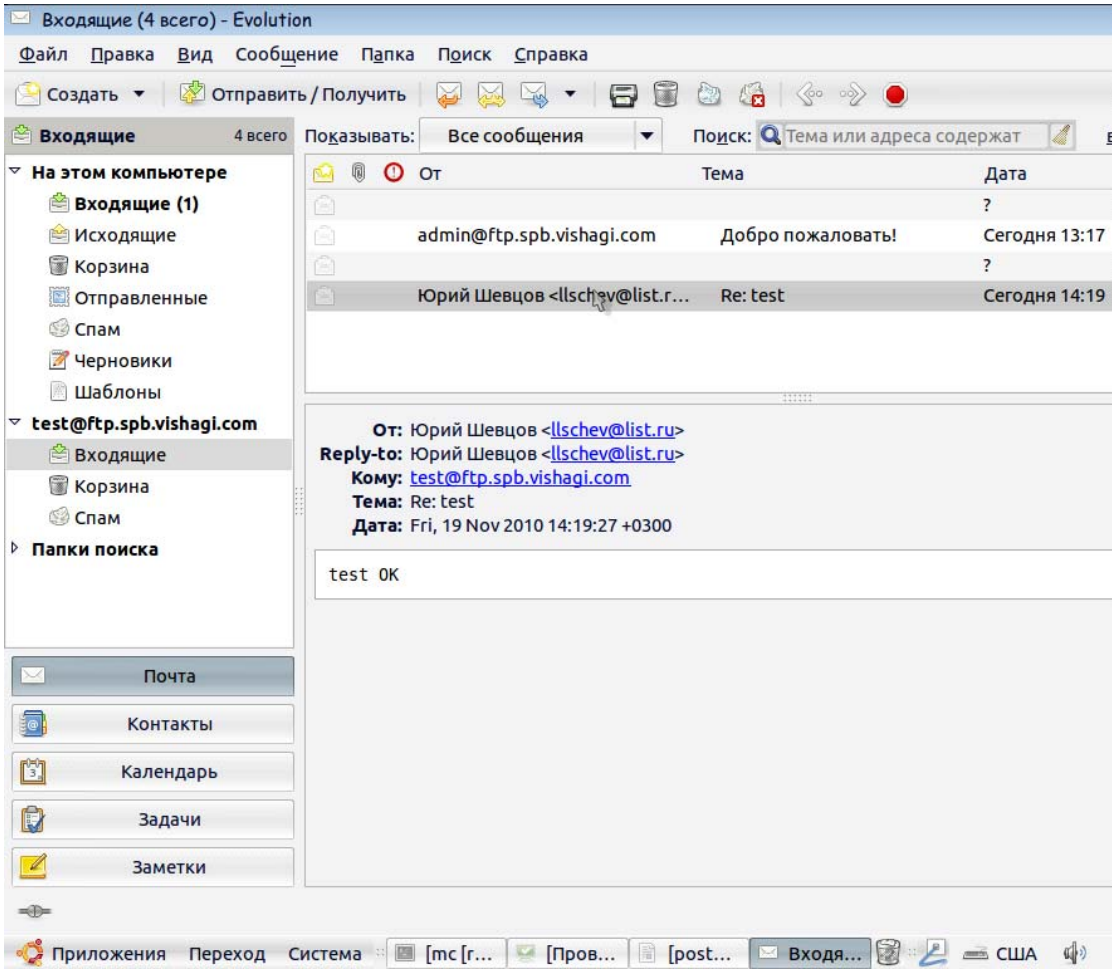

Входящие (1 непрочитанное, 3 всего) - Evolution
Файл Правка Вид Сообщение Папка Поиск Справка
Создать
Отправить / Получить
Вхо... 1 непрочитанное, 3 всего
Показывать:
Все сообщения
Поиск:
Тема или адреса содержат
На этом компьютере
Входящие (1)
Исходящие
Корзина
Отправленные
Спам
Черновики
Шаблоны
test@ftp.spb.vishagi.com
Входящие (1)
Корзина
Спам
Папки поиска
От
Тема
Дата
admin@ftp.spb.vishagi.com
Добро пожаловать!
Сегодня 13:17
От: admin@ftp.spb.vishagi.com
Кому: test@ftp.spb.vishagi.com
Тема: Добро пожаловать!
Дата: Fri, 19 Nov 2010 13:17:31 +0300 (MSK)
Hi,
Welcome to your new account.
Почта
Контакты
Календарь
Задачи
Заметки
Приложения Переход Система
США


Параметры Evolution
Учётные записи
Контакты
Настройки почты
Настройки редактора
Настройки сети
Календарь и задачи
Включено
Имя учётной записи
Протокол
test@ftp.spb.vishagi.com
По умолчанию
imap
Введите пароль для test@ftp.spb.vishagi.com
Введите пароль IMAP для test на узле 192.168.14.143.
Запомнить этот пароль
Отменить
OK
Справка
Приложения
Переход
Система
США


Параметры Evolution
Включено
Имя учётной записи
Протокол
Мастер учётной записи Evolution
Отправка почты
Введите информацию о способе отправки электронной почты. Если вы не уверены, свяжитесь со своим системным администратором или поставщиком услуг Интернета.
Тип сервера: SMTP
Описание: Для доставки почты путем подключения к удалённому почтовому концентратору по протоколу SMTP.
Настройка сервера
Сервер: 192.168.14.143
Требуется проверка подлинности
Безопасность
Использовать защищённое соединение: Без шифрования
Проверка подлинности
Тип: PLAIN
Проверить поддерживаемые типы
Имя пользователя: test
Запомнить пароль
Отменить
Назад
Справка
Приложения
Переход
Система
США

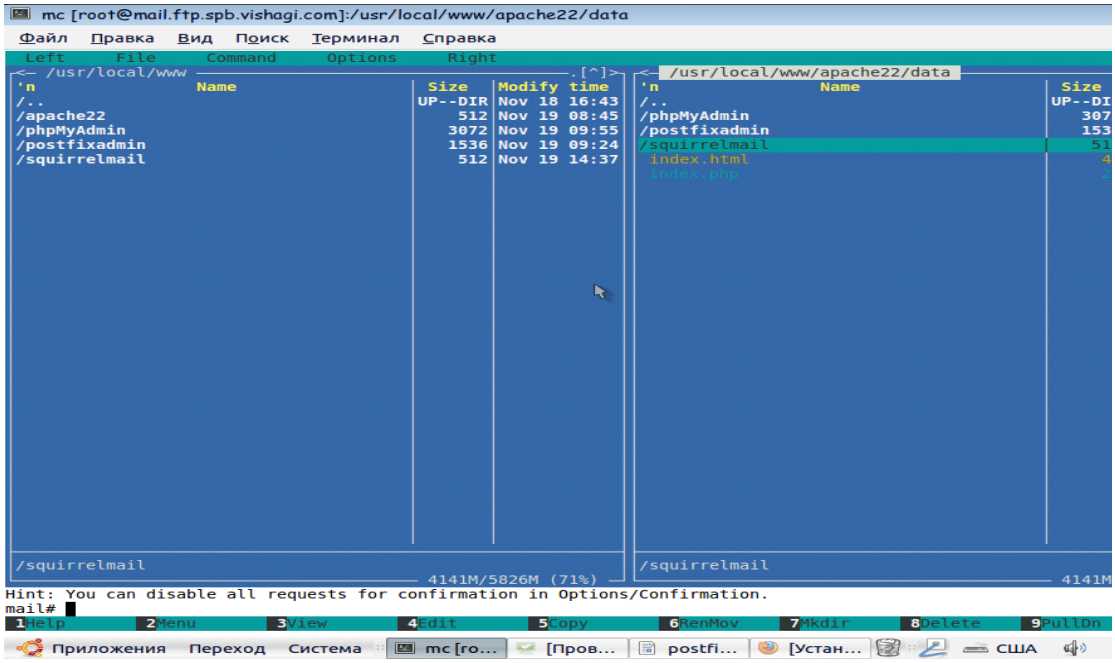

Входящие (3 всего) - Evolution
Файл Правка Вид Сообщение Папка Поиск Справка
Создать
Отправить / Получить
Входящие
3 всего
Показывать:
Все сообщения
Поиск:
Тема или адреса содержат
На этом компью
Входящие
Исходящие
Корзина
Спам
Черновики
Шаблоны
test@ftp.spb.vish
Входящие
Корзина
Спам
Папки поиска
Дата
?
Сегодня 13:17
?
test
Файл Правка Вид Вставить Формат Параметры
Отправить
От кого:
Unknown <test@ftp.spb.vishagi.com>
Подпись:
Нет
Кому:
llschev@list.ru
Копия:
Тема:
test
Обычный текст
Обычный
testpostfix
Показать панель вложений
Добавить вложение...
В виде значков
Почт
Контак
Календарь
Задачи
Заметки
Приложения
Переход
Система
США


llschev@list.ru: Входящие-Mozilla Firefox
Файл Правка Вид Журнал Закладки Инструменты Справка
http://win.mail.ru/cgi-bin/msglist?folder=0&1845425087
Самые популярные Getting Started Latest Headlines
Postfix Admin - 192.168.14...
llschev@list.ru: Входящие
@mail.ru
Новых писем: 76 Мой Мир: нет новых событий Деньги@Mail.ru: 0,00 р.
Почта Адреса Мой мир Фото Видео Блоги Игры Знакомства Деньги Карты
Папки новых всего
Входящие 76 116
Сомнительные 0
Отправленные 25
Черновики 0
Корзина 8
Архив М-Агента
Все непрочтенные письма
Занято 0% Как увеличить?
Проверить почту Написать письмо
ежедневник • настройки
Входящие
найти в почтовом ящике
Показаны письма 1-25 из 116 Вирусная опасность: низкая
Удалить Переслать Это спам Переместить Пометить Добавить отправителя
Автор Тема
Unknown test
test@ftp.spb.vishagi.com
"Subscribe.Ru" Новости ИТ-бизнеса для Профессионалов
rutube@rutubeinfo.ru Лучшее видео за неделю от Rutube
admin@infostart.ru Инфостарт - Еженедельный обзор публикаций
"Subscribe.Ru" Новости ИТ-бизнеса для Профессионалов
info@site.hh.ru HeadHunter: Приключения иностранцев в России
"Subscribe.Ru" Новости ИТ-бизнеса для Профессионалов
Мой Мир@Mail.Ru Действия Ваших друзей за 14 ноября
rutube@rutubeinfo.ru Понедельник - день веселый!
"mirtesen.ru" MirTesen.ru | Темы недели: В.Путин: Родители не должн
Lineage 2 Запишись на 13-й официальный русский сервер Lineage
"Subscribe.Ru" Новости ИТ-бизнеса для Профессионалов
"mirtesen.ru" Andrei Nesterov ищет Вас на МирТесен
Читайте почту с телефона
Просто зайдите на m.mail.ru
БЕЛЫЙ СЕРВИС
ВПЕРЕД К ЦЕНЕ И КАЧЕСТВУ!
ТО на Ваш ВЫБОР
http://win.mail.ru/cgi-bin/readmsg?id=12901654790000000786&folder=0
Приложения Переход Система
США

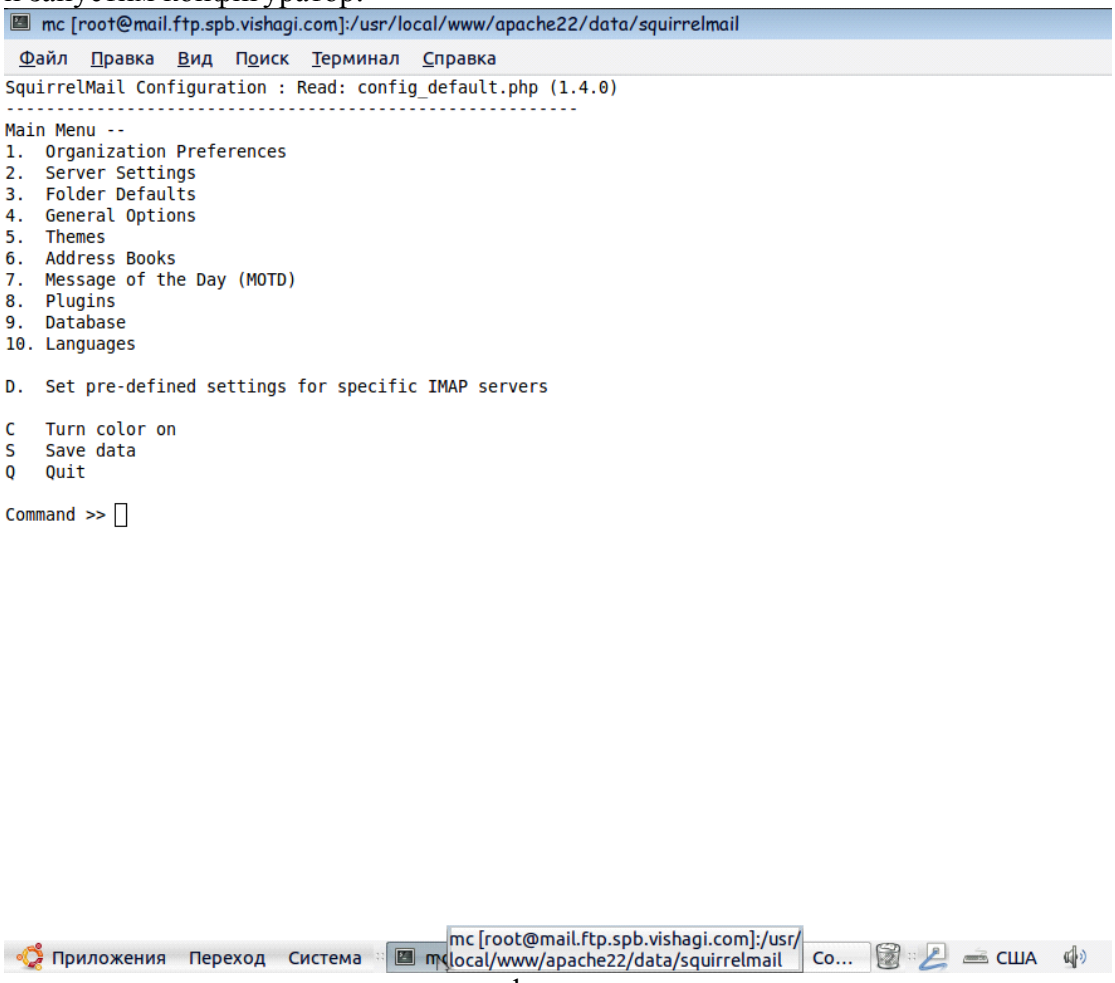


Веб сервер есть, установим веб мордочку к почте:

#cd /usr/ports/mail/squirrelmail
#make install clean

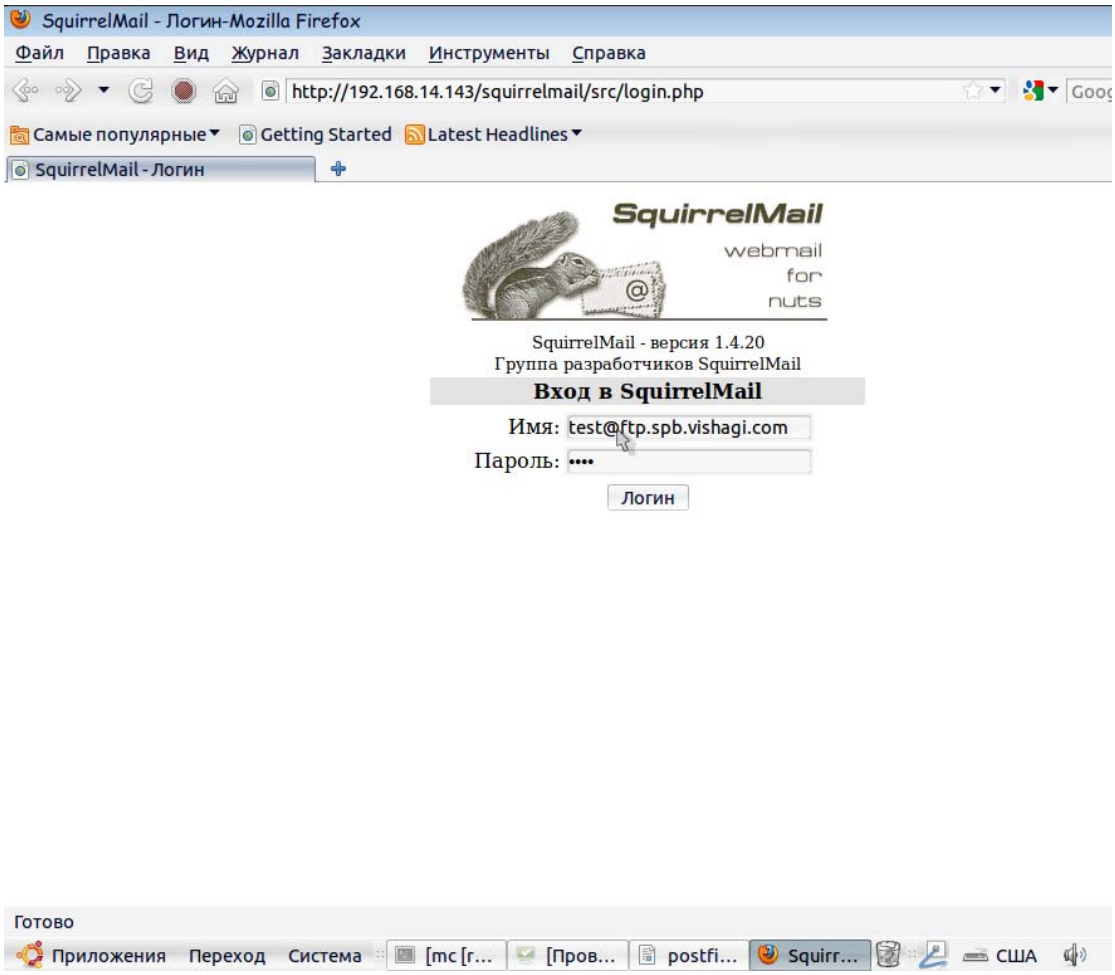


скопируем папку /usr/local/www/squirrelmail в /usr/local/www/apache22/data
и запустим конфигуратор:

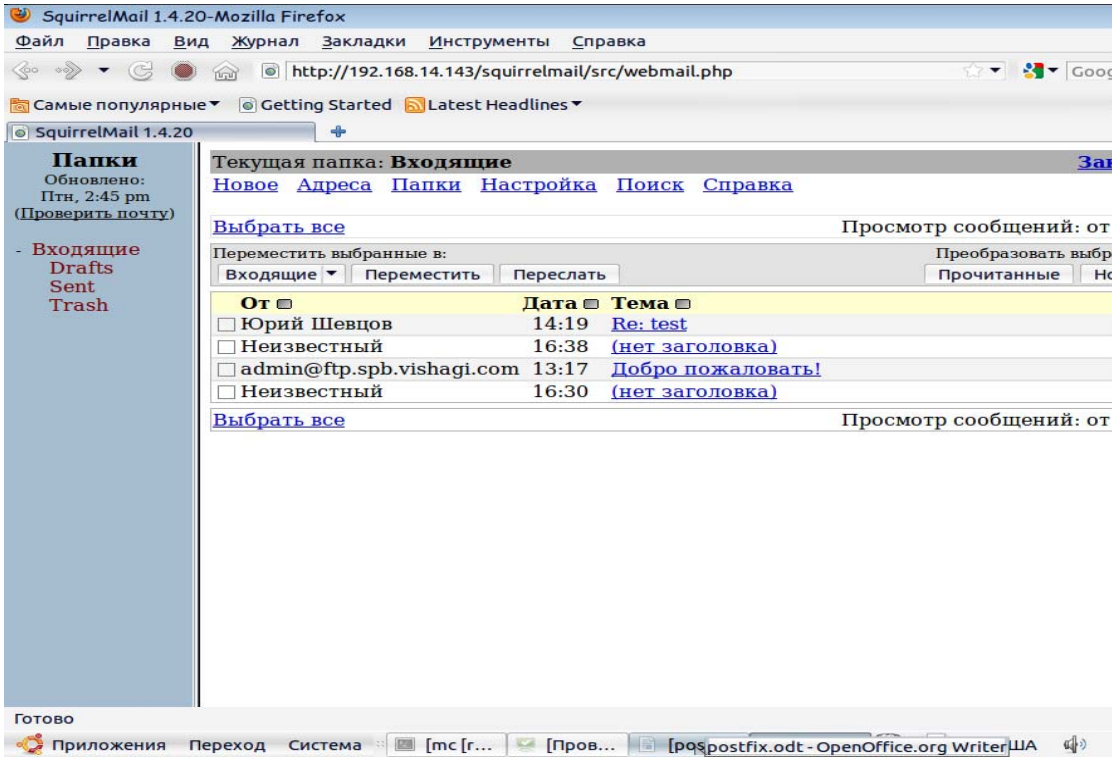


тут нужно указать домен, язык по дефолту и прочие приятные пустячки

тестим!



http://1ip сервера/squirrelmail/



- **установка и настройка ClamAV и spamAssassin**

```
# cd /usr/ports/security/clamav
# make install clean
```

Настраиваем запуск clamd и freshclam

```
# echo 'clamav_clamd_enable="YES"' >> /etc/rc.conf
# echo 'clamav_freshclam_enable="YES"' >> /etc/rc.conf
```

Настраиваем clamav

#ee /usr/local/etc/clamd.conf

```
##
## Example config file for the Clam AV daemon
## Please read the clamd.conf(5) manual before editing this file.
##
LogFile /var/log/clamav/clamd.log
LogFileMaxSize 0
PidFile /var/run/clamav/clamd.pid
DatabaseDirectory /var/db/clamav
LocalSocket /var/run/clamav/clamd.sock
FixStaleSocket yes
TCPSocket 3310
TCPAddr 127.0.0.1
User clamav
AllowSupplementaryGroups yes
ScanPDF yes
ScanMail yes
ScanPartialMessages yes
ScanHTML yes
```

```
ScanArchive yes
MaxScanSize 15M
```

запускаем

```
# /usr/local/etc/rc.d/clamav-clamd start
Starting clamav_clamd.
```

```
##
## Example config file for the Clam AV daemon
## Please read the clamd.conf(5) manual before editing this file.
##
LogFile /var/log/clamav/clamd.log
LogFileMaxSize 0
PidFile /var/run/clamav/clamd.pid
DatabaseDirectory /var/db/clamav
LocalSocket /var/run/clamav/clamd.sock
FixStaleSocket yes
TCPSocket 3310
TCPAddr 127.0.0.1
User clamav
AllowSupplementaryGroups yes
ScanPDF yes
ScanMail yes
ScanPartialMessages yes
ScanHTML yes
ScanArchive yes
MaxScanSize 15M
```

обновляем антивирус freshclam:

```
# /usr/local/etc/rc.d/clamav-freshclam start
Starting clamav_freshclam.
```

Устанавливаем spamassassin

```
# cd /usr/ports/mail/p5-Mail-SpamAssassin
# make install clean

# echo 'spamd_enable="YES"' >> /etc/rc.conf
```

#ee /usr/local/etc/mail/spamassassin/local.cf

```
# This is the right place to customize your installation of SpamAssassin.
#
# See 'perldoc Mail::SpamAssassin::Conf' for details of what can be
```

```
# tweaked.
#
# Only a small subset of options are listed below
#
###########################################################################
#
rewrite_header Subject *****SPAM*****
report_safe 1
# trusted_networks 212.17.35.
required_score 10.0
use_bayes 1
bayes_auto_learn 1
bayes_ignore_header X-Bogosity
bayes_ignore_header X-Spam-Flag
bayes_ignore_header X-Spam-Status
```

запускаем

```
# /usr/local/etc/rc.d/sa-spamd start
Starting spamd.
```

Устанавливаем amasind-new

```
# cd /usr/ports/security/amavisd-new
# make install clean
# echo 'amavisd_enable="YES"' >> /etc/rc.conf

# ee /usr/local/etc/amavisd.conf
```

```
use strict;
$max_servers = 2;            # num of pre-forked children (2..30 is common), -m
$daemon_user  = 'vscan';     # (no default;  customary: vscan or amavis), -u
$daemon_group = 'vscan';     # (no default;  customary: vscan or amavis), -g
$mydomain = 'ftp.spb.vishagi.com';   # a convenient default for other settings
$TEMPBASE = "$MYHOME/tmp";   # working directory, needs to exist, -T
$ENV{TMPDIR} = $TEMPBASE;    # environment variable TMPDIR, used by SA,
etc.
$QUARANTINEDIR = '/var/virusmails';  # -Q
$log_level = 0;              # verbosity 0..5, -d
$log_recip_templ = undef;    # disable by-recipient level-0 log entries
$DO_SYSLOG = 1;              # log via syslogd (preferred)
$syslog_facility = 'mail';   # Syslog facility as a string
$syslog_priority = 'debug';  # Syslog base (minimal) priority as a string,
$enable_db = 1;              # enable use of BerkeleyDB/libdb (SNMP and nanny)
$enable_global_cache = 1;    # enable use of libdb-based cache if $enable_db=1
$nanny_details_level = 2;    # nanny verbosity: 1: traditional, 2: detailed
```

```
$enable_dkim_verification = 1;  # enable DKIM signatures verification
$enable_dkim_signing = 1;    # load DKIM signing code, keys defined by dkim_key
@local_domains_maps = ( [".$mydomain"] );  # list of all local domains
@mynetworks = qw( 127.0.0.0/8 [::1] [FE80::]/10 [FEC0::]/10
                  10.0.0.0/8 192.168.14.0/24 192.168.0.0/16 );
$unix_socketname = "$MYHOME/amavisd.sock";  # amavisd-release or amavis-
milter
              # option(s) -p overrides $inet_socket_port and $unix_socketname
$inet_socket_port = 10024;   # listen on this local TCP port(s)
$policy_bank{'MYNETS'} = {   # mail originating from @mynetworks
  originating => 1,  # is true in MYNETS by default, but let's make it explicit
  os_fingerprint_method => undef,  # don't query p0f for internal clients
};
$interface_policy{'10026'} = 'ORIGINATING';
$policy_bank{'ORIGINATING'} = {  # mail supposedly originating from our users
  originating => 1,  # declare that mail was submitted by our smtp client
  allow_disclaimers => 1,  # enables disclaimer insertion if available
  # notify administrator of locally originating malware
  virus_admin_maps => ["virusalert\@$mydomain"],
  spam_admin_maps  => ["virusalert\@$mydomain"],
  warnbadhsender   => 1,
  # forward to a smtpd service providing DKIM signing service
  forward_method => 'smtp:[127.0.0.1]:10027',
  # force MTA conversion to 7-bit (e.g. before DKIM signing)
  smtpd_discard_ehlo_keywords => ['8BITMIME'],
  bypass_banned_checks_maps => [1],  # allow sending any file names and types
  terminate_dsn_on_notify_success => 0,  # don't remove NOTIFY=SUCCESS option
};

$interface_policy{'SOCK'} = 'AM.PDP-SOCK'; # only applies with
$unix_socketname
# Use with amavis-release over a socket or with Petr Rehor's amavis-milter.c
# (with amavis-milter.c from this package or old amavis.c client use 'AM.CL'):
$policy_bank{'AM.PDP-SOCK'} = {
```

```
  protocol => 'AM.PDP',
  auth_required_release => 0,  # do not require secret_id for amavisd-release
};
$sa_tag_level_deflt  = 2.0;  # add spam info headers if at, or above that level
$sa_tag2_level_deflt = 6.2;  # add 'spam detected' headers at that level
$sa_kill_level_deflt = 6.9;  # triggers spam evasive actions (e.g. blocks mail)
$sa_dsn_cutoff_level = 10;   # spam level beyond which a DSN is not sent
$sa_crediblefrom_dsn_cutoff_level = 18; # likewise, but for a likely valid From
# $sa_quarantine_cutoff_level = 25; # spam level beyond which quarantine is off
$penpals_bonus_score = 8;    # (no effect without a @storage_sql_dsn database)
$penpals_threshold_high = $sa_kill_level_deflt;  # don't waste time on hi spam
$bounce_killer_score = 100;  # spam score points to add for joe-jobbed bounces

$sa_mail_body_size_limit = 400*1024; # don't waste time on SA if mail is larger
$sa_local_tests_only = 0;    # only tests which do not require internet access?
$virus_admin               = "test\@$mydomain";  # notifications recip.

$mailfrom_notify_admin     = "virusalert\@$mydomain";  # notifications sender
$mailfrom_notify_recip     = "virusalert\@$mydomain";  # notifications sender
$mailfrom_notify_spamadmin = "spam.police\@$mydomain"; # notifications sender
$mailfrom_to_quarantine = ''; # null return path; uses original sender if undef

@addr_extension_virus_maps      = ('virus');
@addr_extension_banned_maps     = ('banned');
@addr_extension_spam_maps       = ('spam');
@addr_extension_bad_header_maps = ('badh');
$path = '/usr/local/sbin:/usr/local/bin:/usr/sbin:/sbin:/usr/bin:/bin';
$MAXLEVELS = 14;
$MAXFILES = 1500;
$MIN_EXPANSION_QUOTA =      100*1024;  # bytes  (default undef, not enforced)
$MAX_EXPANSION_QUOTA = 300*1024*1024;  # bytes  (default undef, not
enforced)
$sa_spam_subject_tag = '***SPAM*** ';
$defang_virus  = 1;  # MIME-wrap passed infected mail
```

```
$defang_banned = 1;  # MIME-wrap passed mail containing banned name
# for defanging bad headers only turn on certain minor contents categories:
$defang_by_ccat{+CC_BADH.",3"} = 1;  # NUL or CR character in header
$defang_by_ccat{+CC_BADH.",5"} = 1;  # header line longer than 998 characters
$defang_by_ccat{+CC_BADH.",6"} = 1;  # header field syntax error
$myhostname = 'mail.ftp.spb.vishagi.com';  # must be a fully-qualified domain name!
$notify_method  = 'smtp:[127.0.0.1]:10025';
$forward_method = 'smtp:[127.0.0.1]:10025';  # set to undef with milter!
$final_virus_destiny      = D_DISCARD;
$final_banned_destiny     = D_BOUNCE;
$final_spam_destiny       = D_BOUNCE;
$final_bad_header_destiny = D_PASS;
$bad_header_quarantine_method = undef;
@keep_decoded_original_maps = (new_RE(
  qr'^MAIL$',   # retain full original message for virus checking
  qr'^MAIL-UNDECIPHERABLE$', # recheck full mail if it contains undecipherables
  qr'^(ASCII(?! cpio)|text|uuencoded|xxencoded|binhex)'i,
# qr'^Zip archive data',     # don't trust Archive::Zip
));
$banned_filename_re = new_RE(
### BLOCKED ANYWHERE
# qr'^UNDECIPHERABLE$',  # is or contains any undecipherable components
  qr'^\.(exe-ms|dll)$',                 # banned file(1) types, rudimentary
# qr'^\.(exe|lha|tnef|cab|dll)$',         # banned file(1) types

### BLOCK THE FOLLOWING, EXCEPT WITHIN UNIX ARCHIVES:
# [ qr'^\.(gz|bz2)$'            => 0 ],  # allow any in gzip or bzip2
  [ qr'^\.(rpm|cpio|tar)$'      => 0 ],  # allow any in Unix-type archives

  qr'.\.(pif|scr)$'i,                   # banned extensions - rudimentary
# qr'^\.zip$',                          # block zip type

### BLOCK THE FOLLOWING, EXCEPT WITHIN ARCHIVES:
```

```
# [ qr'^\.(zip|rar|arc|arj|zoo)$'=> 0 ],  # allow any within these archives

  qr'^application/x-msdownload$'i,        # block these MIME types
  qr'^application/x-msdos-program$'i,
  qr'^application/hta$'i,

# qr'^message/partial$'i,         # rfc2046 MIME type
# qr'^message/external-body$'i,   # rfc2046 MIME type

# qr'^(application/x-msmetafile|image/x-wmf)$'i,  # Windows Metafile MIME type
# qr'^\.wmf$',                          # Windows Metafile file(1) type

  # block certain double extensions in filenames
  qr'\.[^./]*[A-Za-z][^./]*\.\s*(exe|vbs|pif|scr|bat|cmd|com|cpl|dll)[.\s]*$'i,

# qr'\{[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}\}?'i, # Class ID CLSID, strict
# qr'\{[0-9a-z]{4,}(-[0-9a-z]{4,}){0,7}\}?'i, # Class ID extension CLSID, loose

  qr'.\.(exe|vbs|pif|scr|cpl)$'i,             # banned extension - basic
);
@score_sender_maps = ({ # a by-recipient hash lookup table,
                        # results from all matching recipient tables are summed

  ## site-wide opinions about senders (the '.' matches any recipient)
  '.' => [  # the _first_ matching sender determines the score boost

    new_RE(  # regexp-type lookup table, just happens to be all soft-blacklist
      [qr'^(bulkmail|offers|cheapbenefits|earnmoney|foryou)@'i        => 5.0],
      [qr'^(greatcasino|investments|lose_weight_today|market\.alert)@'i=> 5.0],
      [qr'^(money2you|MyGreenCard|new\.tld\.registry|opt-out|opt-in)@'i=> 5.0],
      [qr'^(optin|saveonlsmoking2002k|specialoffer|specialoffers)@'i   => 5.0],
      [qr'^(stockalert|stopsnoring|wantsome|workathome|yesitsfree)@'i  => 5.0],
      [qr'^(your_friend|greatoffers)@'i                                => 5.0],
```

```
 [qr'^(inkjetplanet|marketopt|MakeMoney)\d*@'i                  => 5.0],
),
{ # a hash-type lookup table (associative array)
 'nobody@cert.org'                      => -3.0,
 'cert-advisory@us-cert.gov'              => -3.0,
 'owner-alert@iss.net'                  => -3.0,
 'slashdot@slashdot.org'                 => -3.0,
 'securityfocus.com'                    => -3.0,
 'ntbugtraq@listserv.ntbugtraq.com'       => -3.0,
 'security-alerts@linuxsecurity.com'      => -3.0,
 'mailman-announce-admin@python.org'      => -3.0,
 'amavis-user-admin@lists.sourceforge.net'=> -3.0,
 'amavis-user-bounces@lists.sourceforge.net' => -3.0,
 'spamassassin.apache.org'              => -3.0,
 'notification-return@lists.sophos.com'   => -3.0,
 'owner-postfix-users@postfix.org'        => -3.0,
 'owner-postfix-announce@postfix.org'     => -3.0,
 'owner-sendmail-announce@lists.sendmail.org'   => -3.0,
 'sendmail-announce-request@lists.sendmail.org' => -3.0,
 'donotreply@sendmail.org'              => -3.0,
 'ca+envelope@sendmail.org'               => -3.0,
 'noreply@freshmeat.net'                => -3.0,
 'owner-technews@postel.acm.org'          => -3.0,
 'ietf-123-owner@loki.ietf.org'           => -3.0,
 'cvs-commits-list-admin@gnome.org'       => -3.0,
 'rt-users-admin@lists.fsck.com'          => -3.0,
 'clp-request@comp.nus.edu.sg'            => -3.0,
 'surveys-errors@lists.nua.ie'            => -3.0,
 'emailnews@genomeweb.com'                => -5.0,
 'yahoo-dev-null@yahoo-inc.com'           => -3.0,
 'returns.groups.yahoo.com'               => -3.0,
 'clusternews@linuxnetworx.com'           => -3.0,
 lc('lvs-users-admin@LinuxVirtualServer.org')    => -3.0,
```

```
    lc('owner-textbreakingnews@CNNIMAIL12.CNN.COM') => -5.0,

    # soft-blacklisting (positive score)
    'sender@example.net'                => 3.0,
    '.example.net'                      => 1.0,

  },
 ],  # end of site-wide tables
});


@decoders = (
 ['mail', \&do_mime_decode],
 ['asc',  \&do_ascii],
 ['uue',  \&do_ascii],
 ['hqx',  \&do_ascii],
 ['ync',  \&do_ascii],
 ['F',    \&do_uncompress, ['unfreeze','freeze -d','melt','fcat'] ],
 ['Z',    \&do_uncompress, ['uncompress','gzip -d','zcat'] ],
 ['gz',   \&do_uncompress,  'gzip -d'],
 ['gz',   \&do_gunzip],
 ['bz2',  \&do_uncompress,  'bzip2 -d'],
 ['lzo',  \&do_uncompress,  'lzop -d'],
 ['rpm',  \&do_uncompress, ['rpm2cpio.pl','rpm2cpio'] ],
 ['cpio', \&do_pax_cpio,   ['pax','gcpio','cpio'] ],
 ['tar',  \&do_pax_cpio,   ['pax','gcpio','cpio'] ],
 ['deb',  \&do_ar,          'ar'],
# ['a',    \&do_ar,          'ar'],  # unpacking .a seems an overkill
 ['zip',  \&do_unzip],
 ['7z',   \&do_7zip,       ['7zr','7za','7z'] ],
 ['rar',  \&do_unrar,      ['rar','unrar'] ],
 ['arj',  \&do_unarj,      ['arj','unarj'] ],
 ['arc',  \&do_arc,        ['nomarch','arc'] ],
```

```
  ['zoo',  \&do_zoo,        ['zoo','unzoo'] ],
  ['lha',  \&do_lha,        'lha'],
# ['doc',  \&do_ole,         'ripole'],
  ['cab',  \&do_cabextract,  'cabextract'],
  ['tnef', \&do_tnef_ext,    'tnef'],
  ['tnef', \&do_tnef],
# ['sit',  \&do_unstuff,     'unstuff'],  # broken/unsafe decoder
  ['exe',  \&do_executable, ['rar','unrar'], 'lha', ['arj','unarj'] ],
);


@av_scanners = (

# ### http://www.clamav.net/
 ['ClamAV-clamd',
   \&ask_daemon, ["CONTSCAN {}\n", "/var/run/clamav/clamd.sock"],
   qr/\bOK$/m, qr/\bFOUND$/m,
   qr/^.*?: (?!Infected Archive)(.*) FOUND$/m ],
# # NOTE: run clamd under the same user as amavisd, or run it under its own
# #   uid such as clamav, add user clamav to the amavis group, and then add
# #   AllowSupplementaryGroups to clamd.conf;
# # NOTE: match socket name (LocalSocket) in clamav.conf to the socket name in
# #   this entry; when running chrooted one may prefer socket "$MYHOME/clamd".

@av_scanners_backup = (

  ### http://www.clamav.net/   - backs up clamd or Mail::ClamAV
  ['ClamAV-clamscan', 'clamscan',
    "--stdout --no-summary -r --tempdir=$TEMPBASE {}",
    [0], qr/:.*\sFOUND$/m, qr/^.*?: (?!Infected Archive)(.*) FOUND$/m ],


);
```

```
1;  # insure a defined return value
```

дописываем в файл /usr/local/etc/postfix/main.cf следующую строку, чтобы сообщения передавались на проверку

content_filter=smtp-amavis:[127.0.0.1]:10024

Теперь внесем изменения в файл master.cf.

```
smtp-amavis unix - - n - 2 smtp
    -o smtp_data_done_timeout=1200
    -o smtp_send_xforward_command=yes
    -o disable_dns_lookups=yes
    -o max_use=20
127.0.0.1:10025 inet n - n - - smtpd
    -o content_filter=
    -o local_recipient_maps=
    -o relay_recipient_maps=
    -o smtpd_restriction_classes=
    -o smtpd_delay_reject=no
    -o smtpd_client_restrictions=permit_mynetworks,reject
    -o smtpd_helo_restrictions=
    -o smtpd_sender_restrictions=
    -o smtpd_recipient_restrictions=permit_mynetworks,reject
    -o mynetworks_style=host
    -o mynetworks=127.0.0.0/8
    -o strict_rfc821_envelopes=yes
    -o smtpd_error_sleep_time=0
    -o smtpd_soft_error_limit=1001
    -o smtpd_hard_error_limit=1000
    -o smtpd_client_connection_count_limit=0
    -o smtpd_client_connection_rate_limit=0
    -o
receive_override_options=no_header_body_checks,no_unknown_recipient_checks
```

#ee /etc/group

находим строчку vscan:*:110: и добавляем в неё clamav – vscan:*:110:clamav, или если там уже есть пользователи то добавляем через запятую (vscan: *:110:someuser,clamav)

Перезапускаем сервер.

Сигнатура для проверки антивируса
***
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X