

ПАСПОРТ

Сервис Электронной почты

08.03.2018

№ б/н

Калуга

ОПИСАНИЕ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ СИСТЕМЫ

СЕРВИС ЭЛЕКТРОННОЙ ПОЧТЫ

Оглавление

1. АННОТАЦИЯ.....	2
2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ.....	3
3. ТЕХНОЛОГИЧЕСКОЕ ОБЕСПЕЧЕНИЕ.....	4
4. ФУНКЦИОНАЛЬНОЕ ОБЕСПЕЧЕНИЕ.....	5
4.1 Web интерфейс пользователя.....	5
4.2 Подключение почтовых программ IMAP4/SMTP.....	7
4.3 Шифрование сообщений.....	7
4.4 Дублирование корреспонденции на системный ящик.....	7
4.5 Фильтрация SPAM.....	8
4.6 Общие папки.....	8

_____ / Петров А.В. /

1. АННОТАЦИЯ

Цель сервиса электронной почты получение/отправка/маршрутизация электронной корреспонденции между локальными пользователями системы и внешними абонентами.

Безопасность передачи данных на канальном уровне обеспечивается применением технологий SSL/TLS.

Безопасность передачи данных на прикладном уровне обеспечивается возможностью шифрования электронного письма средствами программного обеспечения PGP для шифрования и цифровой подписи сообщений.

Работа пользователя с сервисом обеспечивается использованием:

- Web интерфейса пользователя;
- Протоколов связи IMAP4/SMTP.

В процессе функционирования сервис обучается, в том числе опираясь на мнение пользователей, работе с нежелательной корреспонденцией.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Термин	Определение
Сервис электронной почты	Комплексное решение представляющее собой совокупность программно-аппаратного обеспечения для целей осуществления процессов управления хранением и обеспечения процессов приема/отправки электронной корреспонденции.

3. ТЕХНОЛОГИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

Технология	Назначение/Описание
Apache2	HTTP сервер. Обеспечение работы Web интерфейса к почтовому ящику пользователей
Roundcube	Web ориентированный интерфейс к почтовому ящику пользователя
Roundcube Enigma	Плагин для Web интерфейса пользователя для шифрование отправляемых сообщений и дешифровки полученных
Postfix	Агент передачи почты (MTA — mail transfer agent)
Dovecot	IMAP- и POP3-сервер
Fail2Ban	Служба анализа журналов сервисов. Блокировка подозрительной сетевой деятельности.
MySQL	SQL сервер. Обеспечивающий хранение маршрутов почты, пользователей и групп пользователей
Spamassassin	Средство для фильтрации спама, основанное на взаимодействии ключевых компонентов — оценочного сервиса, транспортного агента и базы шаблонов писем
PHP	Препроцессор гипертекста. Скриптовый язык общего назначения
PGP	Компьютерная программа, также библиотека функций, позволяющая выполнять операции шифрования и цифровой подписи сообщений, файлов и другой информации, представленной в электронном виде.

4. ФУНКЦИОНАЛЬНОЕ ОБЕСПЕЧЕНИЕ

4.1 Web интерфейс пользователя

Внешний вид

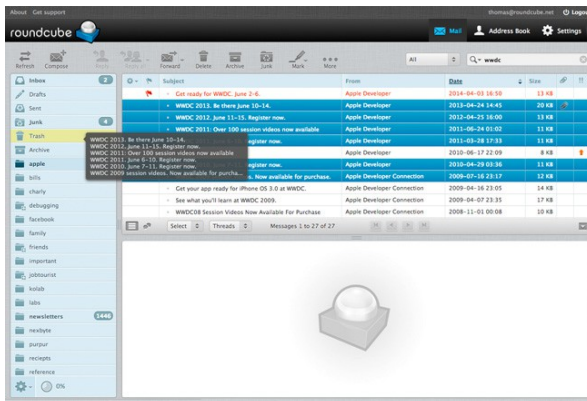


Иллюстрация 1: Основной экран

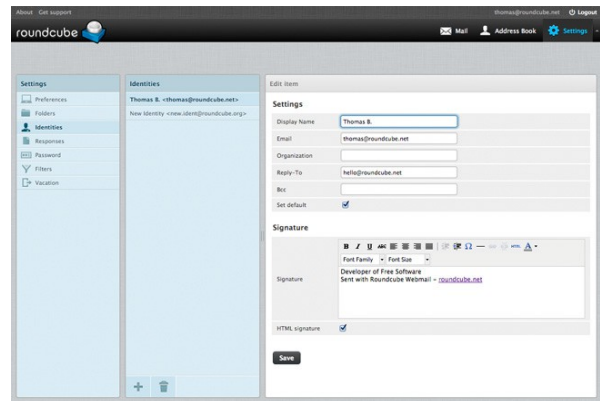


Иллюстрация 2: Управление подписью

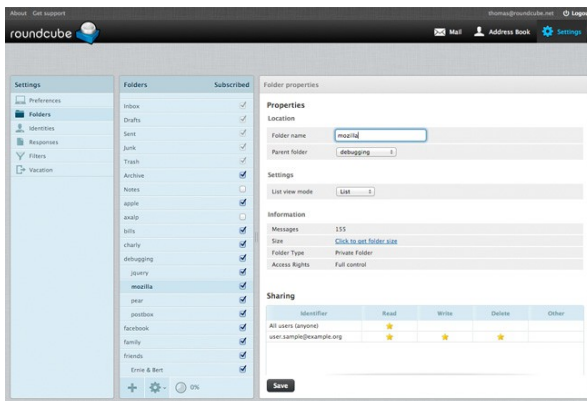


Иллюстрация 3: Управление папками

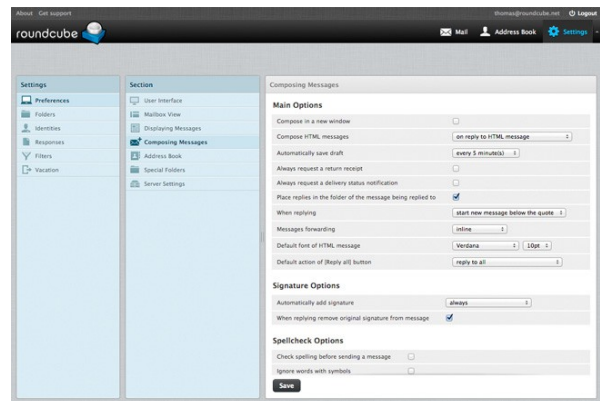


Иллюстрация 4: Управление созданием сообщений

Функциональные возможности

- Доступно на более чем 70 языках
- Управление сообщениями «Перетаскивание»
- Полная поддержка сообщений MIME и HTML
- Сложная защита конфиденциальности

- Создание сообщений с прикрепленными файлами
- Несколько идентификаторов отправителя
- Полнофункциональная адресная книга с группами и разъемами LDAP
- Интеграция адресной книги типа «поиск по типу»
- Создание Richtext / HTML-сообщений
- Пересылка сообщений с вложениями
- Поиск сообщений и контактов
- Список потоковых сообщений
- Поддержка IDNA
- Проверка орфографии
- Конкретные шаблоны ответов
- Управление папками IMAP
- Общие / глобальные папки IMAP
- Поддержка внешнего SMTP-сервера
- Поддержка списков контроля доступа (ACL)
- Встроенное кэширование для быстрого доступа к почтовому ящику
- Неограниченные пользователи и сообщения
- Функции импорта / экспорта
- Шаблонная система для пользовательских скинов
- Plug-in API для гибких расширений

- Поддержка шифрования PGP
- Просмотр трех столбцов

4.2 Подключение почтовых программ IMAP4/SMTP

К сервису электронной почты могут быть подключены приложения Outlook Express, The Bat, Mozilla Thunderbird и другие использующие для работы с сервисом протоколы IMAP4/SMTP и шифрование связи SSL/TLS.

4.3 Шифрование сообщений

Шифрование PGP осуществляется последовательно хешированием, сжатием данных, шифрованием с симметричным ключом, и, наконец, шифрованием с открытым ключом, причём каждый этап может осуществляться одним из нескольких поддерживаемых алгоритмов. Симметричное шифрование производится с использованием одного из семи симметричных алгоритмов (AES, CAST5, 3DES, IDEA, Twofish, Blowfish, Camellia) на сеансовом ключе. Сеансовый ключ генерируется с использованием криптографически стойкого генератора псевдослучайных чисел. Сеансовый ключ зашифровывается открытым ключом получателя с использованием алгоритмов RSA или Elgamal (в зависимости от типа ключа получателя). Каждый открытый ключ соответствует имени пользователя или адресу электронной почты.

4.4 Дублирование корреспонденции на системный ящик

Вся полученная/отправленная корреспонденция дублируется на системный ящик.

4.5 Фильтрация SPAM

В сервисе применяется эффективное средство SpamAssassin для фильтрации

спама, основанное на взаимодействии ключевых компонентов - оценочного сервиса, транспортного агента и базы шаблонов писем.

SpamAssassin использует Байесовскую фильтрацию, обработку DNSBL, Sender Policy Framework, DomainKeys, DKIM, Razor и другие методы распознавания спама. Является проектом верхнего уровня в Apache Software Foundation.

4.6 Общие папки

Общие папки позволяют пользователям почтового сервиса получать доступ к общим почтовым папкам для чтения и хранения сообщений. Эта функция отлично подходит для уведомления о проблемах системы (или улучшениях), а также предлагает пользователям возможность обмениваться информацией.