Подпись и	
Инв. №	
Взам.	
Подпись и	
Инв. №	

СИСТЕМА ДИСПЕТЧЕРИЗАЦИИ ВХОДЯЩИХ И ИСХОДЯЩИХ РАССЫЛОК ЭЛЕКТРОННОЙ ПОЧТЫ БОЛЬШИХ ОБЪЁМОВ

Программа для ЭВМ «MAIL DISPATCHER»

Руководство системного администратора

Лист утверждения

RU. 68061970.00001-01 32 01-ЛУ

2019

УТВЕРЖДЕНО

RU. 68061970.00001-01 32 01-ЛУ

СИСТЕМА ДИСПЕТЧЕРИЗАЦИИ ВХОДЯЩИХ И ИСХОДЯЩИХ РАССЫЛОК ЭЛЕКТРОННОЙ ПОЧТЫ БОЛЬШИХ ОБЪЁМОВ

Программа для ЭВМ «MAIL DISPATCHER»

Руководство системного администратора

Лист утверждения

RU. 68061970.00001-01 32 01-ЛУ

Листов____

2019

АННОТАЦИЯ

В данном программном документе приведено руководство системного администратора по развертыванию, настройке, применению и эксплуатации программы для ЭВМ «MAIL DISPATCHER» - программного обеспечения для диспетчеризации входящих и исходящих рассылок электронной почты больших объемов.

В первом разделе «Общие сведения о программном обеспечении» изложены сведения о назначении программного обеспечения, области применения, характеристиках, приведена информация достаточная для понимания функций программы и ее эксплуатации, требования к техническому обеспечению.

Во втором разделе «Архитектура программного обеспечения и основные характеристики» представлена архитектура программного обеспечения, рассмотрены подсистемы, реализованные в программном обеспечении.

В третьем разделе «Функционал «MAIL DISPATCHER»» рассмотрен основной функционал системы: вход в систему, обзор элементов графического интерфейса, детально рассмотрен функционал модулей и подсистем.

В четвертом разделе «Текущая работа администратора/оператора системы MAIL DISPATCHER» детально изложена схема работы с Заявками Пользователей системы.

Оформление программного документа «Руководство системного администратора» произведено по требованиям ЕСПД (ГОСТ 19.101-77[1], ГОСТ 19.103-77[2], ГОСТ 19.104-78*[3], ГОСТ 19.105-78*[4], ГОСТ 19.106-78*[5], ГОСТ 19.505-79*[6], ГОСТ 19.503-78*[7] ГОСТ 19.604-78*[8]).

1) ГОСТ 19.101-77 ЕСПД. Виды программ и программных документов
2) ГОСТ 19.103-77 ЕСПД. Обозначение программ и программных документов
3) ГОСТ 19.104-78* ЕСПД. Основные надписи
4) ГОСТ 19.105-78* ЕСПД. Общие требования к программным документам
5) ГОСТ 19.106-78* ЕСПД. Общие требования к программным документам, выполненным печатным способом
6) ГОСТ 19.505-79* ЕСПД. Руководство оператора. Требования к содержанию и оформлению
7) ГОСТ 19.503-79* ЕСПД. Руководство системного программиста. Требования к содержанию и оформлению
8) ГОСТ 19.604-78* ЕСПД. Правила внесения изменений в программные документы, выполненные печатным способом

Оглавление

1 ОБЩИЕ СВЕДЕНИЯ О ПРОГРАММЕ «MAIL DISPATCHER»

1.1 Обозначение и наименование

- Система диспетчеризации корпоративной почты;
- Программа для ЭВМ «MAIL DISPATCHER» (MD).

1.2 Назначение и области использования

Программное обеспечение – ПО «MAIL DISPATCHER» - интегрированное инновационное решение, оптимизирующее работу электронной почты, повышающее эффективность и скорость получения, доставки почтовых сообщений, реализующая высокопроизводительные современные технологии обработки и защиты электронной почты от широкого спектра угроз.

Программное обеспечение предназначено для почтовых серверов, реализовано в варианте - выделенный сервер, виртуальная машина.

Модули программы используют элементы искусственного интеллекта, машинного обучения, эвристический анализ, и другие передовые технологии для интенсификации обработки сообщений и защиты электронной почты.

Программное обеспечение разработано под операционную систему Linux.

Программное обеспечение предназначено для работы в режиме реального времени.

Решение достаточно эффективно интегрируется с различными почтовыми системами, и может быть легко включено в почтовую систему небольших, средних и крупных компаний.

1.3 Функции, реализуемые программой

Программное обеспечение реализует широкий спектр функций по оптимизации работы почты:

- Ранжирование IP-адресов отправителей (machine-learned ranking, MLR);
- Оптимизацию доставки почтовых сообщений в одном соединении (spooling);
- Функция защиты входящих и исходящих почтовых соединений STARTTLS;
- Электронные подписи исходящей почты по протоколам (DKIM);

Проверки:

- контента письма (классификатором Байеса и др.);
- нейросетью (SVM-метод);

и другие;

Программа позволяет:

- определять и блокировать спам, вирусы, фишинг-,фарминг-, скамминг- и bounce-сообщения;
- защищать от атак на SMTP, в том числе атак типа zero-day, DoS, ботнет;
- определять и блокировать вредоносные коды во вложениях писем, в том числе не известные вирусы и черви;
- блокировать вредоносный код внутри прикрепленных файлов различных типов;
- корректно обрабатывать большинство известных типов архивов, в том числе многотомные и самораскрывающиеся;
- изолировать зараженные объекты и спам в карантине;
- вести статистику, учитывающую аспекты работы системы;
- логировать почтовые сообщения по требованию клиента;
- информировать клиентов об инцидентах.

1.4 Основные характеристики «MAIL DISPATCHER»

- Модули многоуровневой защиты:
  - *блокирует фишинговые атаки, спам и серую рассылку с помощью различных методов защиты, таких как проверка репутации отправителя, анализ содержимого и изображений, машинное обучение и т. д. ;*
- Двух-этапная фильтрация:
  - ***«Легкая» фильтрация – валидация подключения:***
    - ✓ *STARTTLS - использование протокола TLS/SSL на базе STARTTLS. TLS и SSL используют асимметричное шифрование для аутентификации, симметричное шифрование для конфиденциальности и коды аутентичности сообщений для сохранения целостности сообщений;*
    - ✓ *Репутация адресов - осуществляется проверку email-адреса/email-домена/IP-адреса в репутационных базах, формируются белые и чёрные списки доменов и пользователей;*
    - ✓ *Валидация получателей - технология проверки получателей с помощью установления дополнительного SMTP-соединения;*
    - ✓ *Валидация отправителей - проверка подлинности отправителей используя SPF,DKIM, DMARC-проверок, на основании которых выставляется спам-рейтинг письма;*
    - ✓ *Greylisting – «серые списки», временная задержка сообщения, запрос повторной отправки более одного раза в зависимости от репутации IP-адреса;*
    - ✓ *RBL-проверка - механизм фильтрации спама на основе DNS (DNSBL, SURBL);*
  - ***«Тяжелая» фильтрация – фильтрация контента:***
    - ✓ *Лингвистический анализ;*
    - ✓ *Эвристический анализ;*
    - ✓ *URL-фильтр - динамически обновляемую базу данных URL-адресов;*
    - ✓ *Анализ по известным IoC;*
    - ✓ *Защита от эксплойтов в документах: обнаружение комплексного вредоносного ПО и эксплойтов в документах PDF, Microsoft Office и других форматах с использованием статической и эвристической логики для обнаружения и анализа аномалий;*
    - ✓ *Проверка вложений (в том числе формата – ZIP, RAR, TGZ, 7z, *.exe, *.doc и т.д.);*
- Механизм фильтрации основан на статистическом методе Байеса классификации документов по категориям. Реализована динамическая подстройка системы к изменяющемуся потоку спам сообщений;
- Технология фильтров является уникальной и обеспечивает до 99,99% распознавание спама;
- Многоуровневый модуль проверки вложений на вирусы, включает как лицензионные, так и свободно распространяемые пакеты:
  - ✓ AVAST;
  - ✓ Clam AV;
  - ✓ Dr Web;
  - ✓ ESET Nod32;
  - ✓ Kaspersky Antivirus;

- Обновление антивирусных баз осуществляется автоматически по заданному временному периоду;
- Транспортная подсистема — осуществляет доставку писем получателю. В случае если сервер получателя недоступен, сообщения будут размещены в очереди и будут пересылаться на почтовый сервер получателя, как только он становится доступен;
- Подсистема карантина — помещает сообщения, которые распознаны как “вероятно спам” или содержащие вредоносный код в карантин;
- Модуль отчетов и статистики;
- Модуль логирования почтовых сообщений;
- Личный кабинет пользователя. Доступ через web- интерфейс.

1.5 Режимы включения

В зависимости от выбранного пакета обслуживания, клиент получает услугу фильтрации электронной почты в следующих режимах:

- в режиме SaaS на выделенном персонально для клиента сервере в дата-центре;
- установка системы фильтрации «MAIL DISPATCHER» непосредственно в дата-центре клиента.

1.6 Преимущества

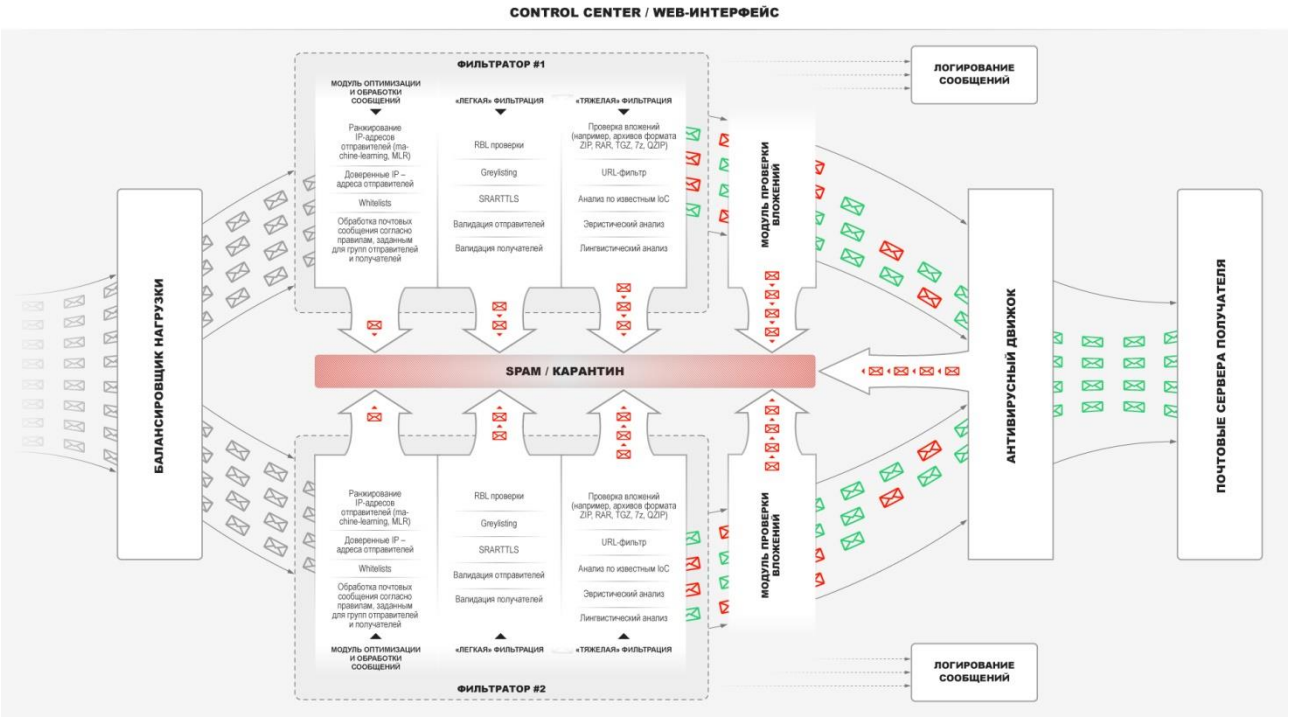
- Высокое качество защиты электронной почты;
- Уровень распознавания спама 99,99% -
  - *Обеспечивается благодаря уникальным технологиям фильтрации, модулям многоуровневой защиты от спама (несколько сотен алгоритмов, сотни тысяч признаков спама), мощной антивирусной системе, встроенной «Песочницы» и системе предотвращения атак;*
- Отдельное решение, программно-аппаратный комплекс, легко интегрирующийся с любыми почтовыми системами Заказчика;
- Наличие возможности горизонтального масштабирования системы для случая роста объемов почтовых сообщений:
  - *Возможность подключения неограниченного количества почтовых ящиков и доменов;*
- Решение возможно развернуть как на отдельном компьютере, так и на виртуальной машине VMWare ESXi;
- Масштабируемость:
  - *Решение способно удовлетворить как запросы небольшой компании, имеющей один почтовый сервер, так и потребности по фильтрации почтового трафика Интернет или хостинг провайдера.*
- Высокая производительность и стабильность работы:
  - *Благодаря многопоточной архитектуре, «MAIL DISPATCHER» способен одновременно обрабатывать значительный объем почтовых сообщений.*
- Отказоустойчивость системы реализуется возможностью распределенного развертывания системы. Компоненты системы – Web-интерфейс, База данных настроек, База данных журнала сообщений(логи), Фильтраторы могут быть размещены как в целом, так и каждый на отдельных, как физических так виртуальных машинах:

  - *Модульная архитектура делает выведение «MAIL DISPATCHER» из строя, в том числе путем атаки, практически невозможным;*
- Подключение по выбору Заказчика – SaaS, дата-центр Заказчика;
- Доступность подключения в схеме SaaS:
  - *Перенаправление почты для обработки осуществляется с помощью изменения MX-записи домена организации;*
  - *Не требуется никаких других изменений в конфигурации почтового сервера клиента или изменения настроек в почтовых программах сотрудников организации;*
- Для обработки данных используется СУБД с открытым кодом ClickHouse;
- Возможность балансировка нагрузки обработки почтовых сообщений;
- Повышение эффективности обработки почтовых сообщений ~40-50%;
- Увеличение скорости доставки сообщений ~30-40%;
- Встроенная «Песочница»;
- Гибкость настроек и удобство администрирования:
  - *Система имеет гибкую систему настроек, позволяющую выполнить практически любой возможный набор правил;*
  - *Доступ к личному кабинету пользователя осуществляется через web-интерфейс;*
- Прозрачный трэкинг сообщений (мониторинг):
  - *Модуль отчетов и статистики, а так же возможность логирования почтовых сообщений позволяют контролировать процесс фильтрации;*
  - *Логирование сообщений осуществляется исключительно по требованию клиента. Прозрачность системы мониторинга позволяет отследить любое сообщение и его состояние, что позволяет контролировать статус каждого сообщения;*
- Приватность и надежность:
  - *Технологии, реализованные в «MAIL DISPATCHER», позволяют обеспечить конфиденциальность и сохранность почтовой переписки клиентов. При установке системы в дата-центре клиента, клиент получает возможность полного контроля над системой.*

2 АРХИТЕКТУРА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

2.1 Архитектура системы

Архитектура «MAIL DISPATCHER» приведена ниже:



В системе MAIL DISPATCHER реализована, на основе анализа лучших мировых практик, модель параллельной обработки сообщений.
Типовая стандартная архитектура включает:

- Подсистему – **«Балансировщик нагрузки»**;
- Подсистемы **«Фильтратор»;**
- Подсистему **«Антивирусный движок»**;
  - **«Модули проверки вложений»**;
- Подсистемы **«Логирования сообщений»;**
- Подсистему **«Логирование сообщений»;**
- Подсистему **«Карантин»;**
- Подсистему **«Control Center/Web-Интерфейс»**;

2.1.1 *Подсистема «Балансировщик нагрузки»*

Подсистема позволяет реализовать механизм динамической балансировки (выравнивания) нагрузки (load balancing) при параллельной обработке значительного объема почтовых сообщений. В стандартном варианте в системе разворачиваются не менее двух однотипных линий (кластеров) фильтраторов. Почтовые сообщения обрабатываются в отдельных потоках. Балансировка нагрузки или выравнивание нагрузки (load balancing) - метод распределения заданий между несколькими устройствами (фильтраторами) с целью оптимизации использования ресурсов, сокращения времени обслуживания запросов,

горизонтального масштабирования кластера (динамическое добавление/удаление устройств), а также обеспечения отказоустойчивости (резервирования).

Балансировка распределения сообщений реализуется на основе анализа и приоритета записи MX (от англ. mail exchanger) — тип DNS-записи, предназначенный для маршрутизации электронной почты с использованием протокола SMTP.

2.1.2 *Подсистема «Фильтратор».*

Модули многоуровневой защиты от спама (несколько сотен алгоритмов, сотни тысяч признаков спама). Технология фильтров является уникальной и обеспечивает до 99,99% распознавание спама.

В системе реализован механизм динамического многоярусного распараллеливания обработки сообщений. Первый ярус – использование в системе нескольких однотипных модулей фильтраторов. Количество фильтраторов в системе определяется рядом параметров – планируемым потоком сообщений, планируемыми техническими ресурсами, ограничением операционной системы на количество стеков памяти для каждого потока.

Второй ярус – распределение обработки сообщений в отдельных потоках непосредственно на фильтраторах. В системе используется структура независимых очередей, система поддерживает отдельную очередь для каждого домена (IP-адреса), вводится ограничение на количество потоков с одного IP-адреса.

Подсистема типового **«Фильтратора»** включает ряд модулей:

- *Модуль оптимизации обработки сообщений;*
- ***Структуру двухэтапной фильтрации:***
  - *Подсистема «легкой» фильтрации;*
  - *Подсистема «тяжелой» фильтрации;*

Подсистемы фильтрации реализуют ряд механизмов. Так в частности подсистема *«Тяжелой» фильтрации*, включает модуль *«Антивирусный движок»* с встроенным механизмом проверки вложений в сообщениях. Модули многоуровневой защиты от спама (несколько сотен алгоритмов, сотни тысяч признаков спама). Технология фильтров является уникальной и обеспечивает до 99,99% распознавание спама.

2.1.2.1 *Модуль оптимизации обработки сообщений*

Включает следующие механизмы:

- *Ранжирование IP-адресов отправителей (machine-learning, MLR);*
- *Доверенные IP – адреса отправителей;*
- *Whitelists;*
- *Обработка почтовых сообщения согласно правилам, заданным для групп отправителей и получателей;*

2.1.2.2 *Двухэтапная фильтрация*

«Легкая» фильтрация

Валидация подключения

- ***RBL проверки***
  - Для обработки входящих сообщений поддерживается механизм фильтрации спама на основе DNS (DNSBL,

SURBL). Проверки осуществляются с помощью внешних сетевых сервисов:

- DNSBL (DNS blacklist или DNS blocklist) - на серверах хранятся списки IP-адресов, которые были замечены в спам-рассылке;
- SURBL на серверах хранятся списки веб-адресов,которые были замечены в нежелательных или фишигновых письмах.

- **Greylisting** - применяется технология Greylisting («серые списки»), основанная на временной задержке сообщения. Классическая реализация основана на запоминании троек (e-mail отправителя, e-mail получателя, ip адрес сервера отправителя) при каждом получении письма. Если тройка встречается впервые, то сервер отвечает временным отказом (как если бы сервер временно не работал) и запоминает тройку. Протокол SMTP предусматривает возврат писем отправителю с ошибкой «временно отклонено». Авторитетные SMTP серверы повторяют отправку по умолчанию каждые 15 минут снова и снова. Из стандарта RFC 5321 следует, что отправитель должен делать паузу перед повторной попыткой отправить сообщение адресату после неудачи. MAIL DISPATCHER может запросить повторную отправку более одного раза в зависимости от репутации IP-адреса.

- **SRARTTLS**

  MAIL DISPATCHER поддерживает использование протокола TLS/SSL на базе STARTTLS. TLS и SSL используют асимметричное шифрование для аутентификации, симметричное шифрование для конфиденциальности и коды аутентичности сообщений для сохранения целостности сообщений.

- **Репутация адресов**

  В основе технология проверки email-адреса/email-домена/IP-адреса в репутационных базах. Формирование белых и чёрных списков.

  - Белый список - адреса отправителей, находящиеся в списке, являются доверенными, а отправленные ими сообщения пропускаются. В белый список можно добавить как email-адреса, так и домены.
  - Черный список - адреса отправителей, находящиеся в данном списке, являются нежелательными, отправленные ими сообщения блокируются. В черный список можно добавить как email адреса, так и домены.

- **Валидация отправителей**

  Проверка подлинности отправителей обеспечивается за счет SPF, DKIM, DMARC-проверок, на основании которых выставляется спам-рейтинг письма.

- DKIM-проверка является одним из механизмов определения легитимности отправителя, данная технология добавляет к электронному сообщению цифровую подпись, связанную с доменом компании;
- SPF-проверка позволяет определить легитимность отправителя, путём сопоставления IP-адреса почтового сервера отправителя с информацией в TXT-записи домена, которую указал владелец домена.
- После прохождения DKIM- и SPF-проверок осуществляется DMARC-проверка – проверяется, действительно ли сообщение было отправлено из указанного домена

- **Валидация получателей**

  Технология проверки получателей функционирует с помощью установления дополнительного SMTP-соединения, в рамках которого в поле rcpt to указывает соответствующий адрес получателя, а в случае если адрес не существует, то конечный SMTP-сервер вернет ошибку.

«Тяжелая» фильтрация

- **Проверка вложений (в т.ч., архивов формата ZIP, RAR, TGZ, 7z, QZIP)**

  Проверка вложений вынесена в отдельный блок «*Антивирусный движок»,* реализующий весь комплекс проверки сообщений на вирусы, в том числе включающий *«Модуль проверки вложений»*.

  Встроенный антивирусный движок использует несколько современных эффективных антивирусных систем:

  - ✓ AVAST;
  - ✓ ClamAV;
  - ✓ DrWeb;
  - ✓ ESET Nod32;
  - ✓ Kaspersky Antivirus;

  Используется лицензионное ПО, антивирусные базы постоянно обновляются согласно регламентам поставщиков, как правило, ежедневно.

  Функционал позволяет блокировать и отправлять в карантин, в режиме реального времени электронные письма, содержащие вредоносные вложения.

- **Эвристический анализ**

  Функционал реализуется используемым антивирусным движком. Используется сложная высокоинтеллектуальная технология эмпирического анализа всех частей сообщения: поля заголовка, тела сообщения и т.д. Анализируется не только само сообщение, но и, в случае наличия, вложение к нему. Эвристический анализатор постоянно совершенствуется, к нему

непрерывно добавляются новые правила. Он работает «на опережение» и позволяет распознавать еще неизвестные разновидности спама нового поколения до выпуска соответствующего обновления.

- **URL-фильтр**

  MAIL DISPATCHER имеет динамически обновляемую базу данных URL-адресов, на основе которых определяется спам-рейтинг сообщения. Письма, в которых содержатся URL-адреса, ведущие на фишинговые сайты и/или вредоносное ПО, классифицируются как спам.

- **Анализ по известным IoC**
  - Домены (FQDN);
  - Хэши (MD5, SHA1);
  - Адреса IPv4;
  - URL;
  - Транзакционные (MTA, User-Agent);
  - Значение реестра;
  - Имя файла/путь;
  - Mutex;
  - Имена пользователей;
  - Адреса E-mail;

  Ежедневно система получает множество образцов реальных фишинговых сообщений от своих партнеров, в том числе SOC и CERT, и использует их в механизмах фильтрации.

  Механизм фильтрации использует данные по IoC, содержащую информацию о потенциальных угрозах безопасности, которая используется для многокритериальной оценки легитимности каждого сообщения.

- **Лингвистический анализ**

  Лингвистический анализ определяет язык сообщения, и позволяет увеличивать спам-рейтинг письма на определенном языке в зависимости от региональной специфики. Осуществляется классификация сообщений по частоте встречающихся ключевых слов методом Байеса. Слова и словосочетания в сообщениях сравниваются с типичной для спама лексикой. Сравнение производится по словарной базе данных, анализу подвергаются как видимые, так и скрытые специальными техническими уловками слова, выражения и символы. Байесовский фильтр, встроенный в MAIL DISPATCHER, обучается на входящей и исходящей почте, создавая признаки писем специфичных для каждой отдельной компании

Подсистема фильтров является многоуровневой. Решение "спам" или "не спам" принимается по совокупности всех признаков после обработки сообщения всеми фильтрами. После проверки, в зависимости от результатов анализа для каждого сообщения определяются баллы, выставляются флаги, определяется тип дальнейшего действия.

2.1.3 *Подсистемы «Логирование сообщений»*

Для детального анализа и мониторинга обработки сообщений используется «Журнал сообщений», база данных лог-файлов по каждому сообщению. Используется СУБД с открытым кодом ClickHouse (v 19.8.3), позволяющая выполнять аналитические запросы в режиме реального времени на структурированных больших данных.

Журнал сообщений позволяет контролировать статус обработки каждого сообщения, (входящего и исходящего) проходящего через MAIL DISPATCHER. Детально подсистема рассмотрена в разделе ***Функционал системы – СООБЩЕНИЯ***.

2.1.4 *Подсистема «Антивирусный движок»*

Встроенный антивирусный движок использует не менее пяти современных эффективных антивирусных систем:

- ✓ AVAST;
- ✓ ClamAV;
- ✓ DrWeb;
- ✓ ESET Nod32;
- ✓ Kaspersky Antivirus;

Используется лицензионное ПО, антивирусные базы постоянно обновляются согласно регламентам поставщиков, как правило, ежедневно.

Функционал позволяет анализировать сообщения на наличие вирусов в режиме реального времени, блокировать и отправлять в карантин электронные письма, содержащие вирусы, вредоносные вложения и др.

Подсистема проверяет и блокирует вредоносные коды, в том числе не известные вирусы, во вложениях писем.

Антивирусный движок реализует:

- блокировку вредоносного кода внутри прикрепленных файлов различных типов;
- встроенную поддержку всех форматов почтовых файлов;
- встроенную поддержку выполняемых файлов ELF и Portable Executable, сжатых UPX, FSG, Petite, NsPack, wwpack32, MEW, Upack и замаскированных SUE, Y0da Cryptor и другими;
- корректно обработку большинства известных типов архивов, в том числе многотомные и самораскрывающиеся (Zip, RAR, Tar, Gzip, Bzip2, OLE2, Cabinet, CHM, BinHex, SIS и другие);
- встроенную поддержку общераспространённых форматов документов, включая файлы MS Office и MacOffice, HTML, RTF и PDF;
- изоляцию зараженных объектов и спама в карантине.

В случае если хотя бы один из 5 антивирусов определит возможное наличие вируса, вредоносное вложение то сообщение направляется в карантин, а вредоносное вложение в зависимости от действий администратора либо удаляется (блокируется), либо отправляется в «Песочницу», специальную систему проводящую анализ вредоносного вложения в изолированной среде.

2.1.5 Подсистема *«Карантин»*

В подсистему помещаются сообщения, которые распознаны как "вероятно спам". Подсистема обеспечивает ведение карантина для каждого подключившегося клиента, как по входящим, так и исходящим сообщениям. Сообщения, хранящиеся на карантине, могут быть проанализированы или очищены позднее администратором системы.

Пользователям системы, ежедневно рассылаются сообщения, с данными по сообщениям, попавшим в карантин. В зависимости от состояния сообщения, причины отправки в карантин, сообщения могут быть проанализированы либо пользователем, либо при наличии опасных вложений или подозрений на наличие вирусов – администратором . В зависимости от

2.1.6 Подсистема *«Control Center/Web-Интерфейс»*

Управление MAILDISPATCHER осуществляется с использованием специальной подсистемы «Control Center/Web-Интерфейс». Детально подсистема рассмотрена далее.

2.2 Песочница

Для раскрытия поведения и обнаружения неизвестных сложных угроз и целенаправленных атак в системе «MAIL DISPATCHER» дополнительно разворачивается сетевое устройство безопасности, реализующее система эмуляции кода в изолированной защищенной среде («Песочница»).

«Песочница» – это выделенная аппаратная или аппаратно-программная среда для исполнения файлов программ.

Возможно решение на базе аппаратной платформы или решение на базе облачного сервиса. Первая схема предусматривает размещение специализированного аппаратного устройства в инфраструктуре Заказчика и реализацию выделенной среды эмуляции на этой аппаратной платформе. Вся обработка файлов проводится на мощностях данного устройства, а обращение к внешним источникам осуществляется только для обновления сигнатурных механизмов обнаружения вредоносного кода.

Для оценки угрозы исполняемых файлов, сжатых файлов (ZIP-файлов) и широкого набора файлов приложений (таких как Adobe Flash, Adobe PDF, JavaScript и т. д.) используются виртуальные машины, оснащенные инструментами, эмулирующими типичную рабочую среду (операционные системы и программное обеспечение).

Общая схема приведена на следующем рисунке.

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ:

- Анализ и выявление потенциальных и неизвестных сложных угроз;
- Выявление целенаправленных атак;
- Эмуляция собственной рабочей среды и кода в изолированной защищённой среде;
- Предварительная фильтрация подозрительных файлов;
- Оценка угроз исполняемых файлов, архивов (ZIP) и широкого набора файлов приложений (Adobe Flash, Adobe PDF, JavaScript и т. д.);
- Подробные отчеты о перехваченных пакетах, исходных файлах, логах трассировки и скриншотах;

ПЕРЕЧЕНЬ ТИПОВ ФАЙЛОВ ВОЗМОЖНЫХ ДЛЯ АНАЛИЗА:

- **Исполняемые:** BAT, CMD, DLL, EXE, JAR, MSI, PS1, UPX, WSF и VBS;
- **Архивные**: 7Z, ARB, BZIP, BZIP2, CAB, EML, GZIP, LZW, RAR, TAR, XZ и т. д.
- **Скриптовые**: JavaScript/HTML, Batch Script, Power Shell, VBS;
- **Microsoft Office**: Word, Excel, PowerPoint, Outlook и т.д.;
- **Adobe**: PDF, SWF, Flash;
- **Статические веб-файлы:** HTML, JS, URL, LNK;
- **Файлы ОС:** Android APK;
- **И другие;**

3 ФУНКЦИОНАЛ «MAIL DISPATCHER»

3.1 Общее описание

Доступ к системе «MAIL DISPATCHER» (MD) реализован с использованием графического интерфейса (веб-интерфейса) для администратора/оператора.

Доступ к веб-интерфейсу системы создается администратором системы – задается логин, пароль, права доступа.

Функционал системы Mail Dispatcher позволяет администратору/оператору осуществлять следующие действия:

- Настраивать систему;
- Управлять (вводить/удалять) организациями, подразделениями, подключенными к системе;
- Управлять (вводить/удалять) почтовые домены в разрезе организаций, подразделений, фирм;
- Управлять (вводить/удалять) администраторов/операторов системы;
- Настраивать групповые политики, права доступа администраторов / операторов;
- Просматривать, контролировать и анализировать данные по входящим и исходящим сообщениям;
- Просматривать широкий спектр параметров статистики входящих и исходящих сообщений;
- Настраивать и управлять Черными и Белыми списками фильтрации почты;
- Настраивать и управлять Группами фильтрации почты;
- Осуществлять поиск входящих и исходящих сообщений;
- Контролировать и анализировать сообщения попавшие в «Карантин» и «Спам»;

и т.д.

3.2 Вход в систему

Для доступа к системе MD необходимо осуществить вход, используя браузер, указав в строке ввода адрес системы, используя hostname или IP-адрес:

- **https://hostname.xxx/**
- **https://xxx.xxx.xxx.xxx/**

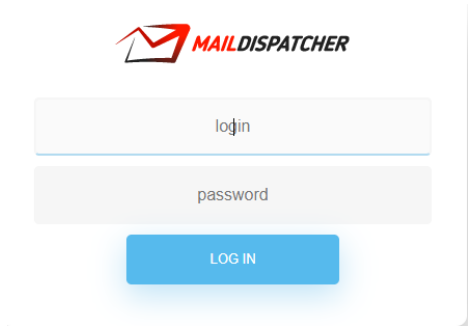


Рис. 3.2.1. Пример учетной записи для входа в систему MD.

Указываем, полученный от администратора логин и пароль. Переходим в веб-интерфейс MD.

Общий экран веб-интерфейса системы:

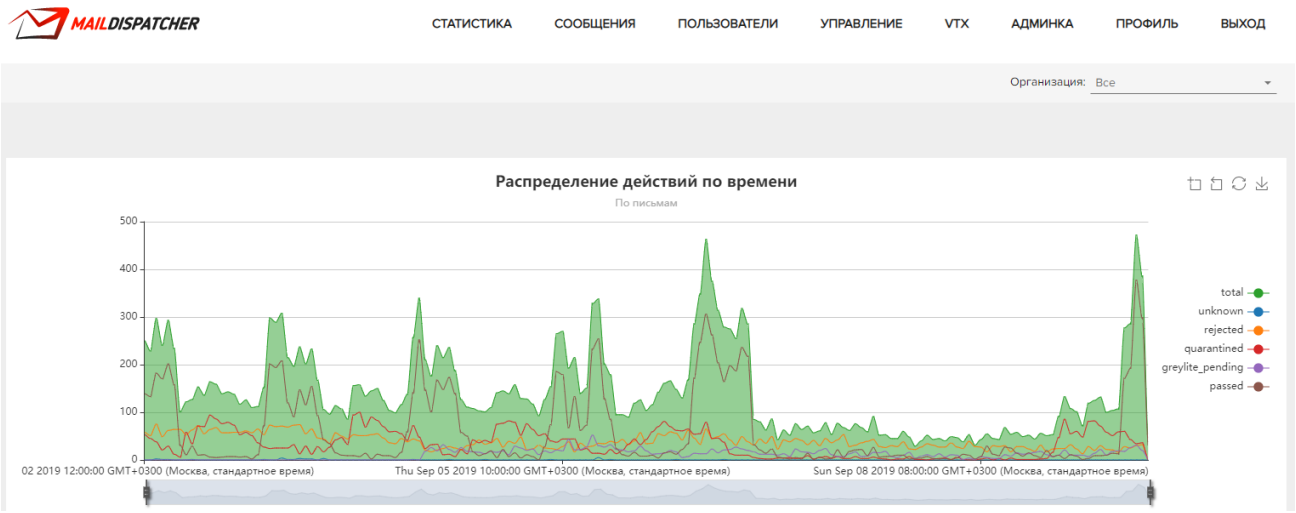


Рис. 3.2.2. Веб-интерфейс системы.

Веб-интерфейс - система меню верхнего уровня (***Статистика, Сообщения, Пользователи, Управление*** и т.д.) с выпадающей структурой подменю. Меню и подменю реализуют иерархическую структуру выбора функциональных возможностей приложения. Назначение элементов меню и подменю интуитивно понятны.

Система меню и подменю включает:

- **Статистика**
  - *Сводка;*
  - *Отправители;*
  - *Получатели;*
  - *Дополнительно;*
  - *Дневная;*
- **Сообщения**
  - *Журнал сообщений;*
  - *Информация о сообщении;*
  - *Действия по дайджестам;*
- **Пользователи**
  - *Учетные записи;*
  - *Права доступа;*
- **Управление**
  - *Организации;*
  - *Управление черными/белыми списками;*
  - *Группы фильтрации;*
  - *Домены, адреса;*
- **VTX**
  - *Песочница;*
- **Профиль;**
- **Выход;**

Основной функционал системы «MAIL DISPATCHER» - диспетчеризация входящих и исходящих рассылок электронной почты, анализ, контроль и настройка правил входящей и исходящей почты, работа с почтовыми сообщениями.

Функционал системы реализован для работы как с одной организацией, так и несколькими структурами в одной организации или несколькими отдельными организациями. Выбор осуществляется, используя элемент ***Организация,*** основного окна графического интерфейса.

3.3 Обзор элементов меню графического интерфейса

Рассмотрим основные элементы, назначение и функционал меню и подменю веб-интерфейса MD.

3.3.1 Основное меню - СТАТИСТИКА

Включает подменю:

- ***Сводка;***
- ***Отправители;***
- ***Получатели;***
- ***Дополнительно;***
- ***Дневная;***

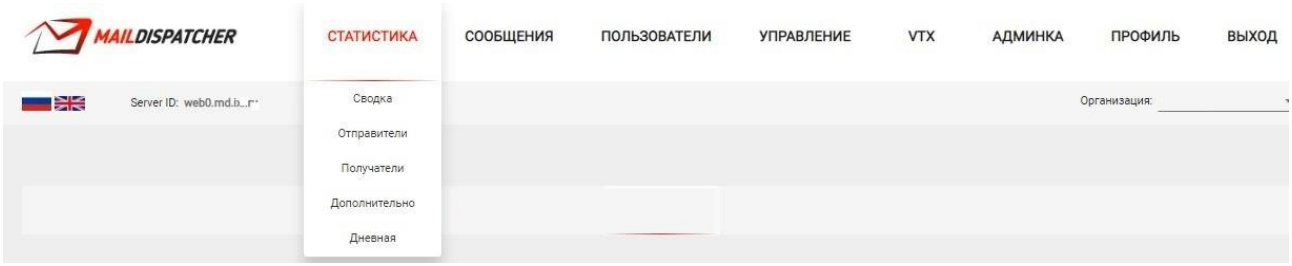


Рис. 3.3.1. Веб-интерфейс СТАТИСТИКА

Меню ***Статистика*** позволяет получить широкий спектр детальной информации по статистике входящей и исходящей почты, детализацию почасовой статистки сообщений за последние двое суток. Для обработки данных используется СУБД с открытым кодом ClickHouse.

3.3.2 *Основное меню - СООБЩЕНИЯ*

Включает подменю:

- *Журнал сообщений;*
- *Информация о сообщении;*
- *Действия по дайджестам;*

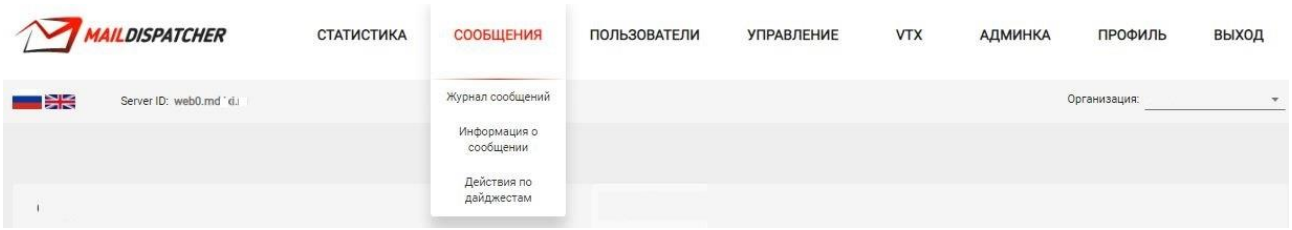


Рис. 3.3.2. Веб-интерфейс СООБЩЕНИЯ

Подменю ***Журнал сообщений*** содержит полную информацию по входящим сообщениям (время получения, отправитель, получатель, тема и т.д.). Функционал Журнала

сообщений позволяет провести детальный анализ, осуществить контроль и настроить правила получения входящей корреспонденции.

Подменю ***Информация о сообщении*** позволяет получить детальную информацию о сообщении по известному CID или MSGID.

Подменю ***Действия по дайджестам*** позволяет получить информацию по сообщениям самими Пользователями доставленными из карантина.

3.3.3 *Основное меню - ПОЛЬЗОВАТЕЛИ*

Включает подменю:

- *Учетные записи;*
- *Права доступа;*

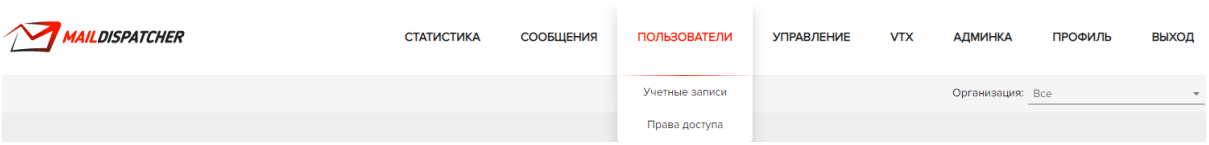


Рис. 3.3.3. Веб-интерфейс ПОЛЬЗОВАТЕЛИ

Функционал подменю ***Учетные записи*** позволяет просматривать, добавлять, удалять, модифицировать учетные записи пользователей (операторов, администраторов) системы.

Функционал подменю ***Права доступа*** определяет права доступа оператора/администратора в системе – доступ к элементам меню и подменю, возможность просмотра и редактирования, доступ к настройкам фильтрации.

3.3.4 *Основное меню - УПРАВЛЕНИЕ*

Включает подменю:

- *Организации;*
- *Управление черными/белыми списками;*
- *Группы фильтрации;*
- *Домены, адреса;*

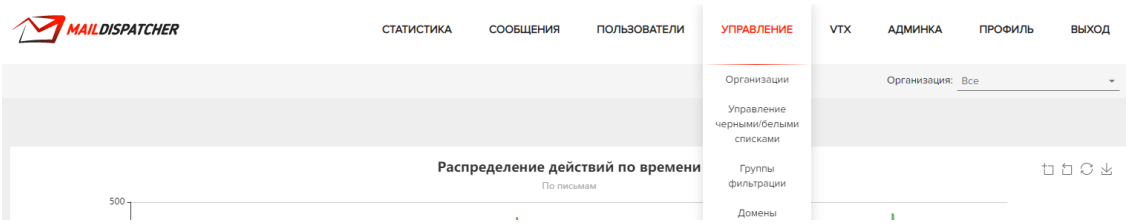


Рис. 3.3.4. Веб-интерфейс УПРАВЛЕНИЕ

Доступ к меню УПРАВЛЕНИЕ имеют только пользователи с правами администратора.

Функционал системы подменю детально рассмотрен далее.

3.3.5 *Основное меню - VTX*

Включает подменю:

- *Песочница;*

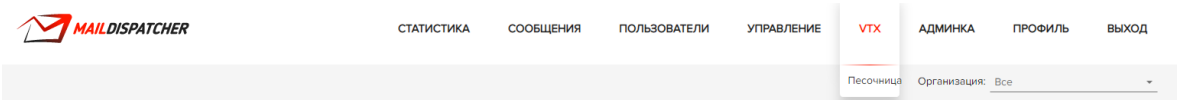


Рис. 3.3.5. Веб-интерфейс VTX

Доступ к меню VTX имеют только пользователи с правами администратора.

Примечание: *«Песочница» не является встроенным модулем «MAIL DISPATCHER». Вопрос поставки, установки, настройки «Песочницы» решается в индивидуальном порядке с Заказчиком. В этом документе функционал не рассматривается.*

3.3.6 *Основное меню - ВЫХОД*

Выход из системы.

3.4 Функционал системы - СООБЩЕНИЯ.

Функционал меню **СООБЩЕНИЯ** включает просмотр, контроль, поиск, анализ, настройка фильтрации Входящих и Исходящих сообщений по организации (-ям).

Детальная информация по сообщениям приведена в Журнале сообщений.

Для просмотра *Сообщений:*

Меню → *СООБЩЕНИЯ*

→ *Журнал сообщений*

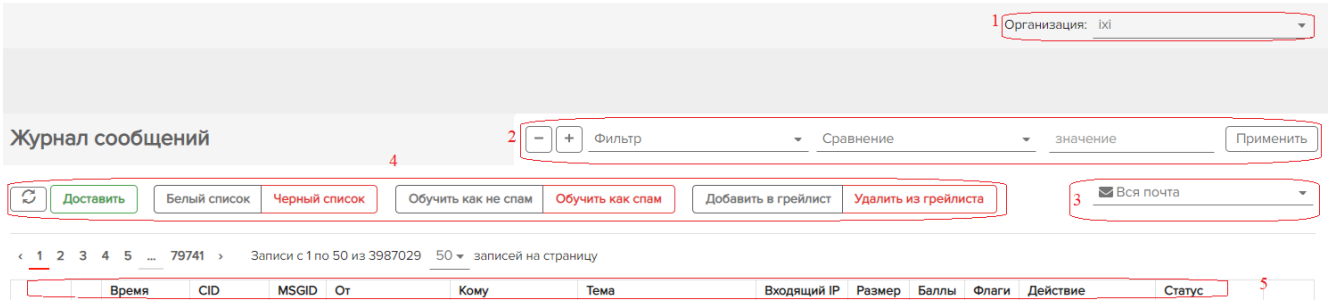


Рис.3.4.1. Веб-интерфейс – Журнал сообщений

Основные элементы Журнала сообщений:

1 - элемент выбора организации – выпадающий список;
2 – многоуровневый фильтр, настройки рассмотрены далее;
3 – выбор почты – выпадающий список;
4 – активные элементы работы с почтовыми сообщениями;
5 – параметры Журнала почтовых сообщений;

3.4.1 *Журнал входящих сообщений*

Для работы с входящей почтой используется широкий функционал системы.

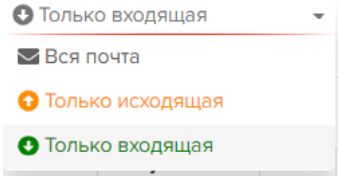
3.4.1.1 *Просмотр входящей почты*

Для просмотра *Входящей почты*:

Меню → *СООБЩЕНИЯ*

→ *Журнал сообщений*

→ Выборка сообщений



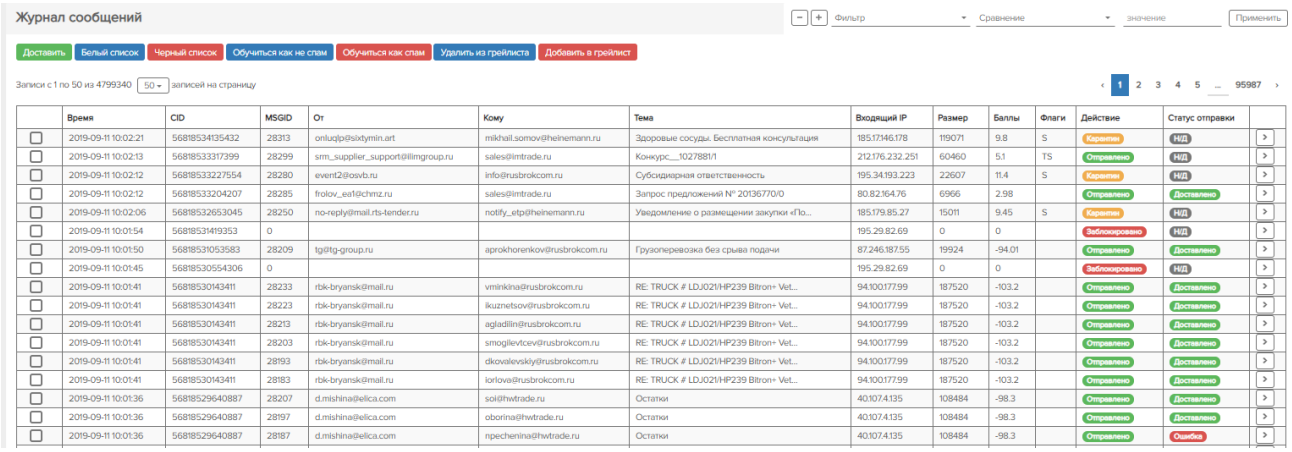


Рис. 3.4.2. Веб-интерфейс – Журнал сообщений входящей почты

В верхней части журнала входящих сообщений элементы интерфейса:

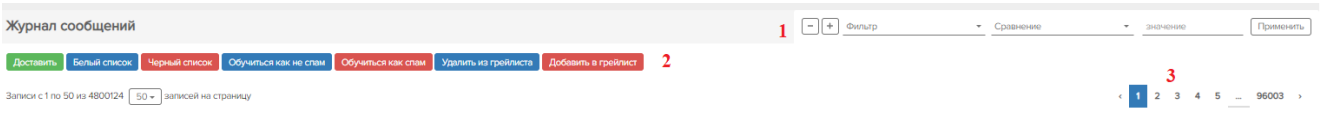


Рис. 3.4.3. Журнал сообщений входящей почты – элементы интерфейса

1 - многоуровневый фильтр;
2 – элементы управления сообщениями;
3 – переход по страницам;
▢ - выбор строк (сообщений);

Журнал входящих сообщений содержит детальную информацию по полученным сообщениям:

- **Время** - дата и время получения сообщения;
- **CID** – идентификатор сообщения;
- **MSGID** – уникальный идентификатор сообщения. Позволяет отслеживать рассылки сообщений от одного отправителя разным получателям;
- **От** - E-mail отправителя;
- **Кому** – E-mail получателя;
- **Тема** - тема сообщения;
- **Входящий IP** - IP адрес отправителя;
- **Размер** – размер сообщения в байтах;
- **Баллы** - параметр, вычисляемый системой при прохождении фильтров, в процессе анализа, в относительных единицах. Чем выше спамрейтинг, тем вероятнее сообщение относиться к спаму;
- **Флаги –** флаг сообщения, отображается буквами. При наведении стрелки, выводится расшифровка:
    - **T** - Помечено;
    - **Z** - Зомби;
    - **F** - Спуфинг;
    - **V** - Вирус;
    - **S** - Спам;

- **Р -** Фишинг;

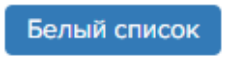
- **Действие -** информация по состоянию сообщения:
  - Отправлено;
  - Карантин – помещено в карантин;
  - Заблокировано – заблокировано политикой системы;
  - Н/Д – не доставлено;
  - Грейлистинг – помещено в «серый» список;
- **Статус отправки –** состояние сообщения:
  - Доставлено ;
  - Н/Д – не доставлено;
  - Отложено – отправка отложена;
  - Ошибка – ошибка отправки;
  - Ожидает доставки;
  - Доставляется;
  - Доставлено из карантина;

> **Спец.символ**, позволяющий получить детальную информацию о сообщении (см.далее);

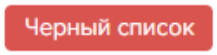
Элементы управления сообщениями включают:

 - Выбор строки (строк);

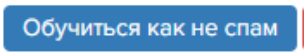
- Доставить сообщение;



- Добавить выбранные адреса отправителей в белый список;



- Добавить выбранные адреса отправителей в черный список;



- Доставить выбранные сообщения и обучиться на них как не спам – сообщения;

- Обучиться на выбранных сообщениях как спам-сообщения;

- Удалить выбранные адреса отправителей в грейлиста;

- Добавить выбранные адреса отправителей в грейлист;

3.4.1.2 *Селекция (выборка) входящих сообщений.*

В интерфейсе ***Журнала сообщений*** реализован, достаточно гибкий, многоуровневый механизм фильтрации сообщений.

Настройка фильтров расположена в правой верхней части ***Журнала сообщений*:**

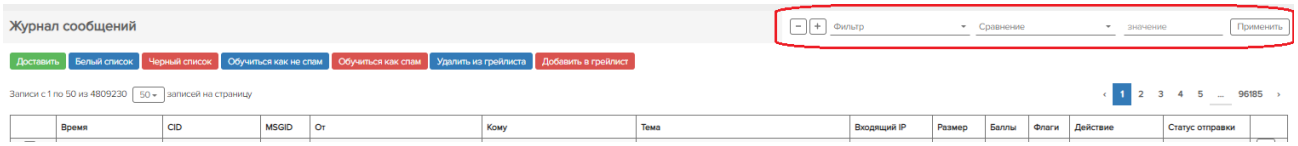


Рис. 3.4.4. Журнал сообщений входящей почты – Фильтр

Селекция сообщений определяются количеством фильтров (знаки: **+** добавить, **-** удалить) и параметрами фильтрации, выбором фильтра из выпадающего меню:

Рис.6. 4.5. Журнал сообщений входящей почты – Фильтр – Меню выбора типа

Выпадающий список включает опции: ***От; Кому; Действие; Статус отправки; Сервер; Входящий IP; Тема; Время; Баллы; CID; Greilite Проверено; Контентный анализ; SMTP анализ; Размер;…….. и т д.***

Далее определяется операция сравнения и указывается значение:

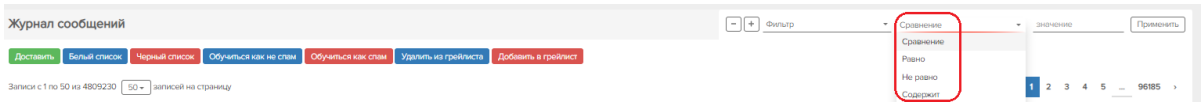


Рис.3.5.6. Журнал сообщений входящей почты – Фильтр – Пример выбора

Пример многоуровневого фильтра:

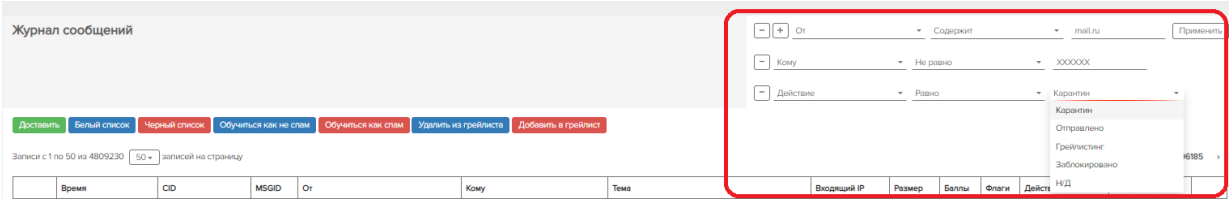


Рис. 3.4.7. Журнал сообщений входящей почты – Многоуровневый фильтр

Применение многоуровневых фильтров позволяет реализовать выборку по широкому спектру критериев.

3.4.1.3 *Просмотр детальной информации о сообщении.*

При обработке и анализе сообщений в ряде случаев возникает необходимость детального просмотра информации по сообщению. В частности при анализе сообщений попавших в карантин, спам, заблокированных т.д.

Для просмотра информации по сообщению активируем элементы меню:

→ **Общее**

→***Журнал сообщений.***

При необходимости, используя фильтрацию, находим сообщение. Далее активируем элемент > крайний правый столбик ***Журнала сообщений*** строки сообщения.

Переходим к экранному интерфейсу, открывается в отдельном экране детальная информация по сообщению – лог фильтрации:

Информация о сообщении

Лог фильтрации

Время	2019-09-13 09:36:27
CID:MSGID	56835658733724:7325
Сервер	12 - flt0.md.
Тема	Новогодние музыкально-цирковое шоу для всей семьи
От	@lavkadedamoroza.ru
К	de.ru
Баллы	19.23
Действие	Карантин
Помечено	Нет
Зомби	Нет
Спуфинг	Нет
Вирус	Нет
Спам	Да
Фишинг	Нет
Greylite проверено	Да
Greylite попытки	0/0
Входящий IP	8 .187.171
Баллы Clamd	0
Баллы VTX	0
Баллы Oktopoda	0
Баллы LTI	0
Контентный анализ	Score:19.23;req_hits=4.5;quarantine=6.5;delete=199; Results for file: stdin (5.072 seconds) Symbol: DCC_CHECK (3.2) Symbol: ARC_NA (0.00) Symbol: ASN (0.00)[asn:12578, ipnet:87.246.160.0/19, country:LV] Symbol: BAD_REP_POLICIES (0.10) Symbol: BAYES_SPAM (4.74)[99.08%] Symbol: CTYPE_MIXED_BOGUS (1.00) Symbol: DKIM_TRACE (0.00)[justeml.com:+, topeml.com:+] Symbol: DMARC_NA (0.00)[lavkadedamoroza.ru] Symbol: FROM_EQ_ENVFROM (0.00) Symbol: FROM_HAS_DN (0.00) Symbol: HAS_LIST_UNSUB (-0.01) Symbol: MANY_INVISIBLE_PARTS (1.00)[10] Symbol: MIME_GOOD (-0.10)[multipart/mixed, multipart/alternative, text/plain] Symbol: MIME_TRACE (0.00)[0:+, 1:+, 2:+, 3:^] Symbol: MX_GOOD (-0.30)[mx.yandex.net, mx.yandex.net, mx.yandex.net, mx.yandex.net, mx.yandex.net] Symbol: OMOGRAPH_URL (0.01)[:] Symbol: PRECEDENCE_BULK (0.00) Symbol: PREVIOUSLY_DELIVERED (0.00)[andrey@imtrade.ru]

Рис. 3.4.8. Журнал сообщений входящей почты – Детальная информация по сообщению

На экран выводится поля данных. Наиболее значимые поля:

- CID (Connection ID) – идентификатор TCP соединения, через которое пришло письмо;
- MSGID (Message ID) – уникальный идентификатор почтового сообщения, внутри TCP соединения;
- От - E-mail - отправитель сообщения;
- К – E-mail получателя сообщения;
- Баллы - параметр, вычисляемый системой при прохождении фильтров, в процессе анализа, в относительных единицах. Чем выше спамрейтинг, тем вероятнее сообщение относиться к спаму;
- Действие - статус отправки сообщения;

  Приведен детальный анализ параметров сообщения:

  ✓ Greylite;
  ✓ Баллы Clamd; VTX; LTI;
  ✓ Контентный анализ сообщения;
  ✓ SMTP анализ;

3.4.2 *Журнал исходящих сообщений.*

Для работы с исходящей почтой используется тот же функционал системы, рассмотренный ранее для входящей почты с определенными изменениями.

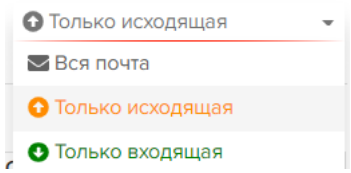
3.4.2.1 *Просмотр исходящей почты.*

Для просмотра *Исходящей почты*:

Меню → *Исходящая почта*

→ *Журнал сообщений*

→ Выборка сообщений



Переходим в экранный интерфейс:

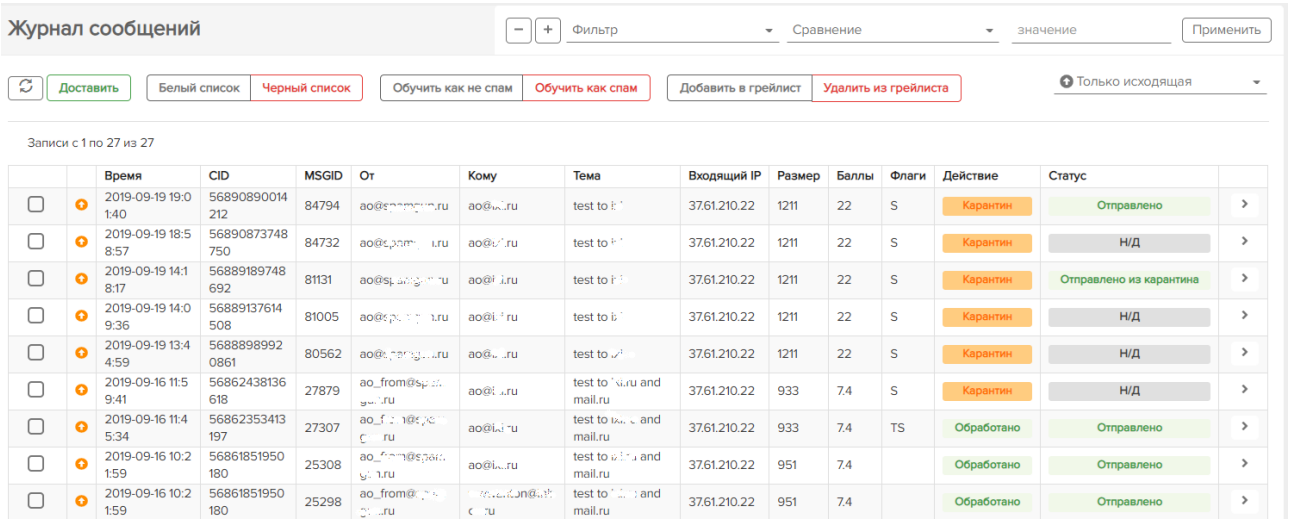


Рис. 3.4.9. Журнал сообщений исходящей почты

Работа с Журналом сообщений Исходящей почты идентична схеме работы с Журналом Входящей почты (см. п.3.1.1 – 3.1.3).

3.5 Функционал системы - ПОЛЬЗОВАТЕЛИ

Функционал меню **ПОЛЬЗОВАТЕЛИ** позволяет просматривать, изменять, добавлять, удалять учетные записи, управлять правами доступа ***администраторов и операторов системы.***

Экранный интерфейс меню, включает подменю *Учетные записи, Права доступа:*

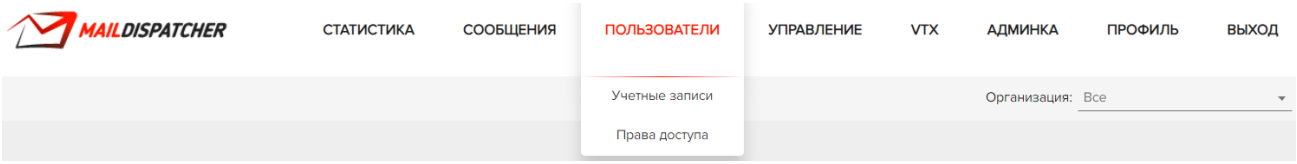


Рис.3.5.1. Графический интерфейс меню ПОЛЬЗОВАТЕЛИ

3.5.1 *Просмотр пользователей (администраторов, операторов)*

Для просмотра имеющихся Пользователей активируем

Меню → *ПОЛЬЗОВАТЕЛИ*

→Учетные записи

Переходим в экранный интерфейс:

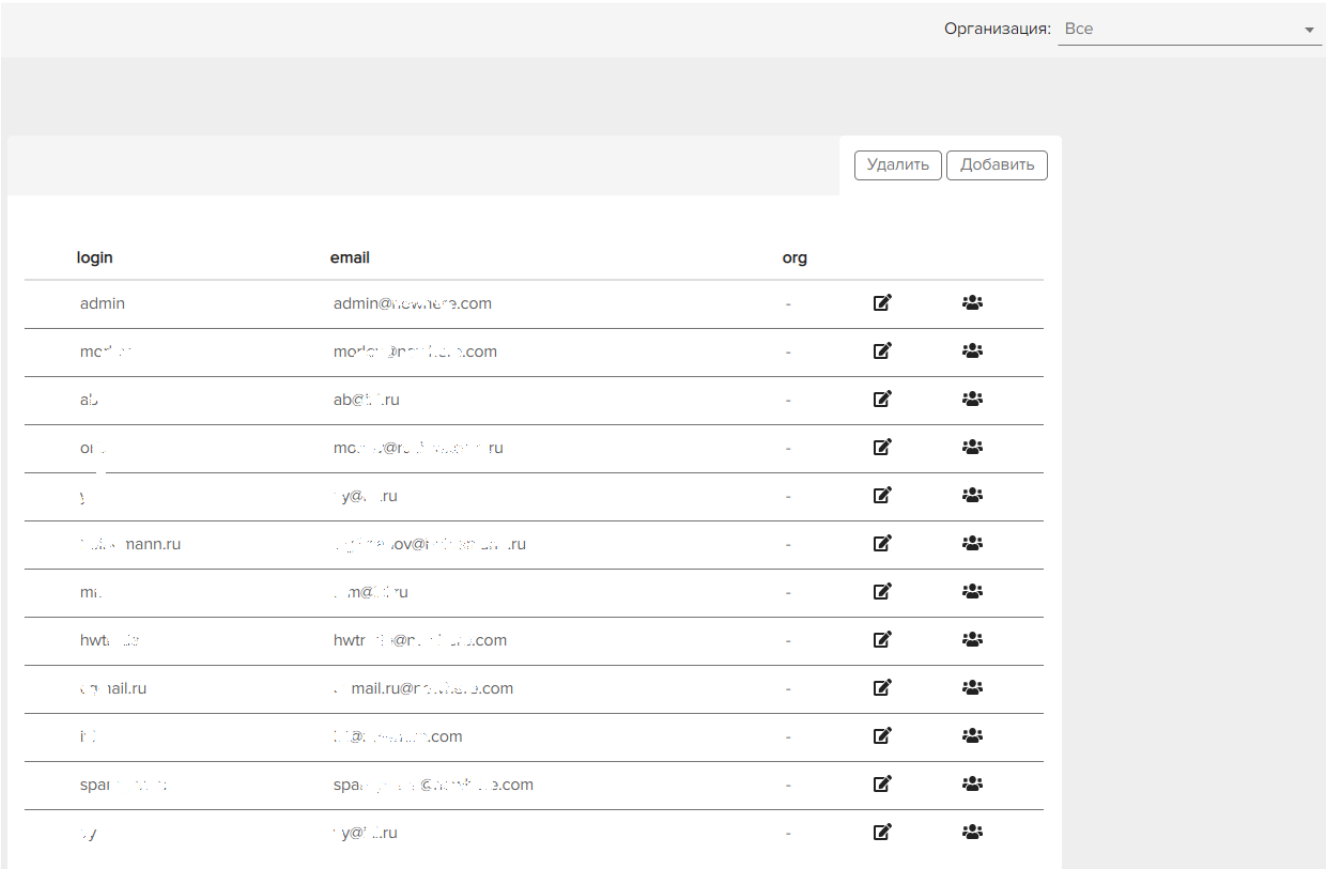


Рис.3.5.2. Журнал - Учетные записи пользователей

Таблица данных содержит данные по учетным записям пользователей – ***операторов и администраторов*** системы.

Поля таблицы:

- login - имя пользователя;
- email - почта пользователя в стандартном формате E-mail;
- org - организация (подразделение) к которому относится пользователь;
- - редактирование данных пользователя;
- - определение прав доступа пользователя (оператора, администратора);

Элементы интерфейса позволяют выбрать пользователей конкретной организации (подразделения) - выпадающее меню ***Организация.***

В верхней части экрана расположены элементы интерфейса:

- Удалить – удаление Пользователей из системы;
- Добавить – ввод новых Пользователей в систему;

3.5.2 *Редактирование пользователей (администраторов, операторов)*

Редактирование пользователей (данные, права) возможно только с правами ***администратора***.

Для редактирования имеющихся Пользователей активируем:

Меню → *ПОЛЬЗОВАТЕЛИ*

→Учетные записи

Переходим в экранный интерфейс учетных записей пользователя. По конкретному пользователю активируем элемент редактирования . Переходим в экранный интерфейс:

Рис. 3.5.3. Пользователь – учетные данные

По Пользователю возможно изменение:

- Основной организации;
- Логина;
- Пароля;
- E-mail;
- Token активации имеет два состояния *Подключен (Enabled)/ Отключен*;

По окончанию ввода изменения необходимо активировать - ***Сохранить***.

В ***Журнале учетных записей*** возможно редактирование ***Прав доступа*** пользователя (оператора, администратора).

Для редактирования прав Пользователей активируем:

Меню → *ПОЛЬЗОВАТЕЛИ*

→Учетные записи

Переходим в экранный интерфейс учетных записей пользователя. По конкретному пользователю активируем элемент редактирования прав . Переходим в экранный интерфейс:

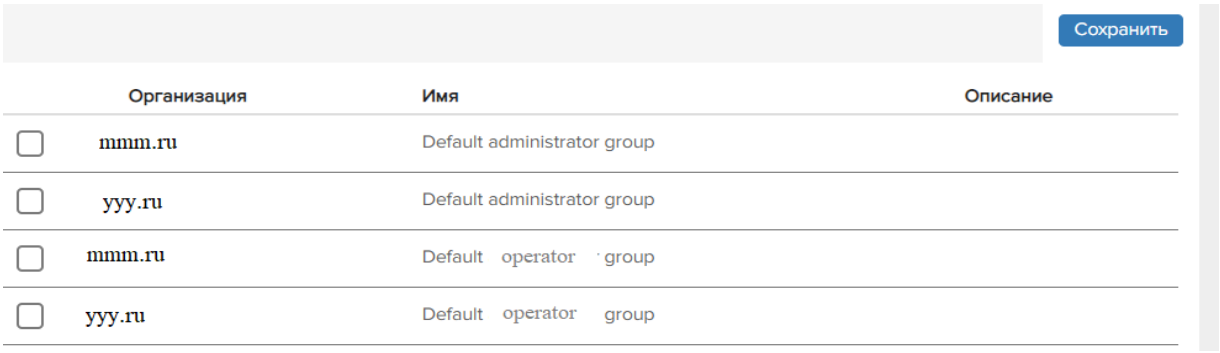


Рис. 3.5.4. Пользователь – права доступа

Для операторов и администраторов каждой организации (подразделения) возможно создание групп доступа с разными правами, более детально данный вопрос рассматривается в разделе ***Права доступа***. Как правило, для организации (подразделения) создаются по меньшей мере две группы доступа «Default administrator group», «Default operator group». Для конкретного администратора (оператора) права доступа должны быть подключены, используя элемент .

Завершение определения прав доступа → ***Сохранить***.

3.5.3 *Ввод новых пользователей (администраторов, операторов)*

Для ввода новых пользователей необходимы права ***администратора***.

Активируем:

Меню → *ПОЛЬЗОВАТЕЛИ*

→Учетные записи

Переходим в экранный интерфейс учетных записей пользователя.

Активируем элемент интерфейса **Добавить** в верхней части экрана.

Экранный интерфейс ввода Пользователей (операторов, администраторов):

Рис. 3.4.5. Пользователь – ввод нового

Заполняем поля:

- Основная организация – выбор из выпадающего списка;
- Логин – произвольная комбинация символов;
- Пароль – произвольная комбинация символов;
- E-mail – электронная почта пользователя в стандартном формате;
- Token – подключить/не подключить – API (Application Programming Interface) доступ к системе;

Рис. 3.5.6. Пользователь – тестовые данные

Активируем Сохранить

Переходим к учетным записям пользователей. В списке добавился введенный пользователь.

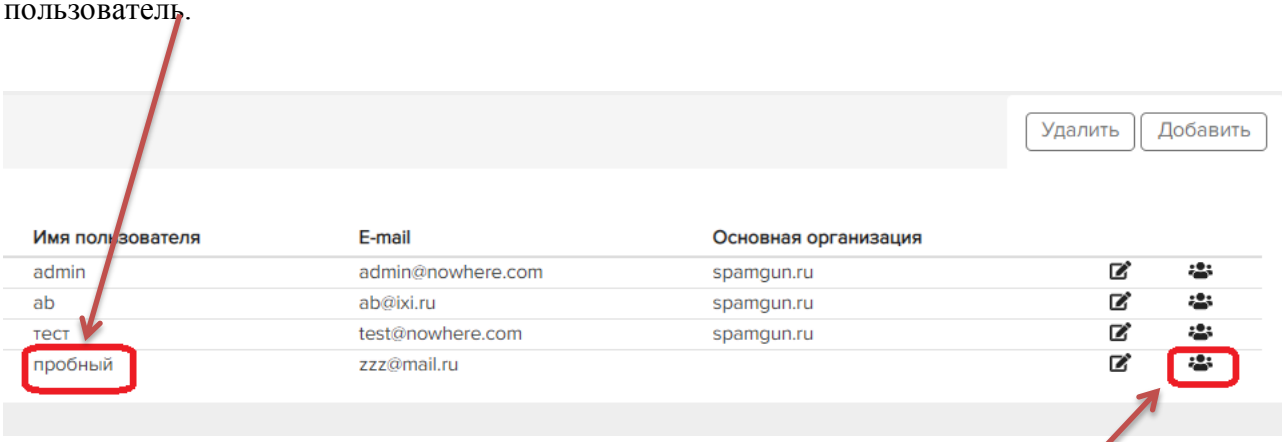


Рис. 3.5.7. Пользователь – вновь введенный

Определяем права доступа пользователя. Активируем элемент

Переходим к журналу групп доступа, выбираем группу (администратор или оператор):

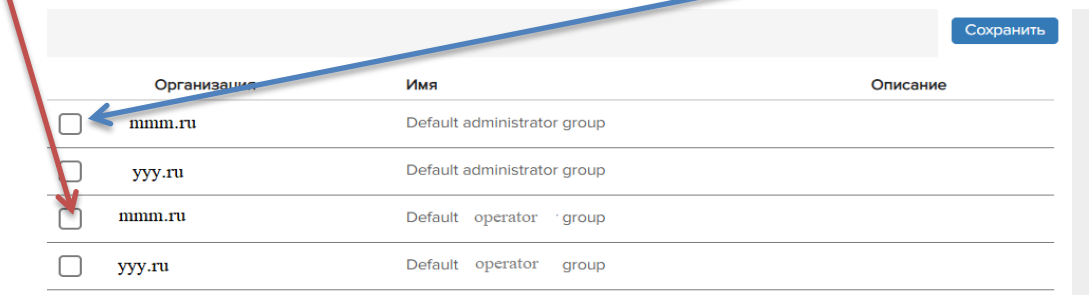


Рис. 3.5.8. Пользователь – определение прав

Далее активируем Сохранить

Ввод нового пользователя с соответствующими правами завершен.

3.5.4 *Права доступа*

Для работы с правами доступа необходимы права ***администратора.***

В системе реализована схема разграничения прав доступа пользователей.

Для каждой организации (подразделения) создаются ***Группы*** с соответствующими правами доступа к ресурсам системы. При создании или редактировании пользователей возможно подключение и переподключение пользователя в соответствующую группы прав доступа.

Для работы с правами (группами) доступа:

Активируем:

Меню → *ПОЛЬЗОВАТЕЛИ*

→*Права доступа*

Переходим в экранный интерфейс:

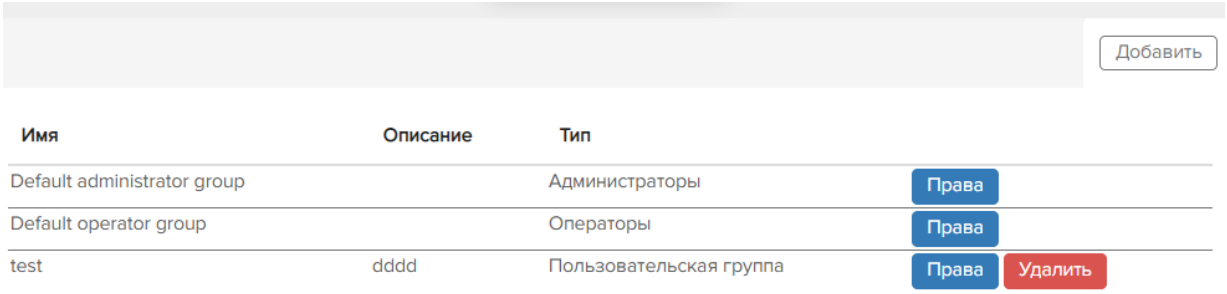


Рис.3.5.9. Права (группы) доступа

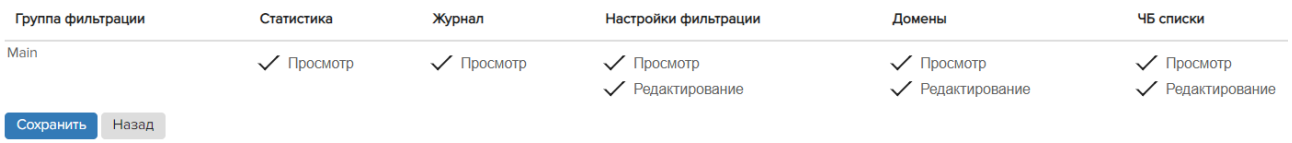
По умолчанию в системе для каждой организации (подразделения) создается две группы с разными правами доступа:

- Default administrator group;
- Default operator group;

Для просмотра или изменения прав по конкретной группе необходимо активировать элемент меню Права .

Для *Administrator group* экранный интерфейс с правами доступа:

Рис.3.5.10. Права доступа - *Default administrator group*



Для *Operator group* экранный интерфейс с правами доступа:

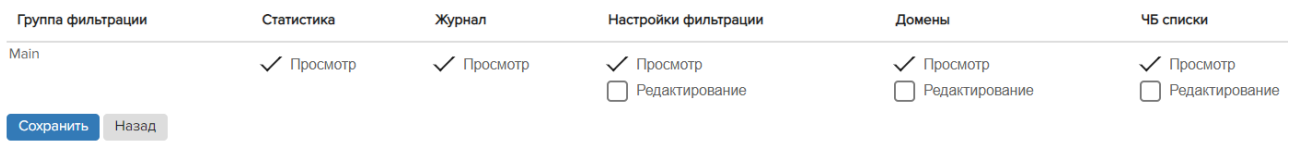


Рис. 3.5.11. Права доступа - *Default operator group*

Назначение прав для соответствующих групп интуитивно понятно. При необходимости соответствующие права можно как отключить, так и включать. После внесения изменений необходимо активировать элемент Сохранить.

Возможно создание Групп с специальными правами доступа. Для этого активируется элемент *«Добавить»* в основном интерфейсе (Рис.4.8). Переходим в интерфейс создания новой группы прав:

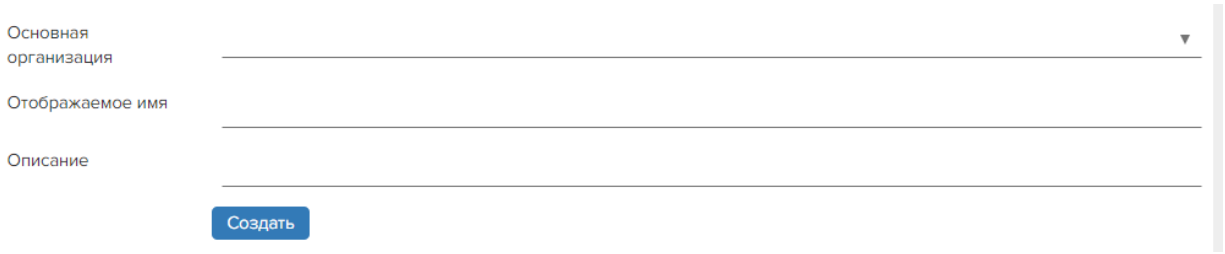


Рис.3.5.12. Права доступа – создание группы

Из выпадающего списка (*Основная организация*) выбираем организацию (подразделение) для которой создаем группу доступа. Заполняем остальные поля:

Рис. 3.5.13. Права доступа – создание группы – определение полей

Активируем *Создать*. Группа создана:

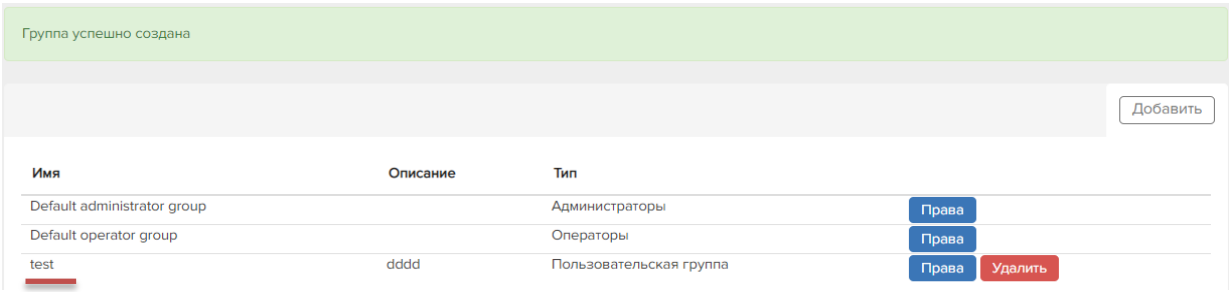


Рис. 3.5.14. Права доступа – создание группы

Тип - устанавливается по умолчанию – *Пользовательская группа*.

Определяем права группы – активируем элемент *Права*, переходим в интерфейс:

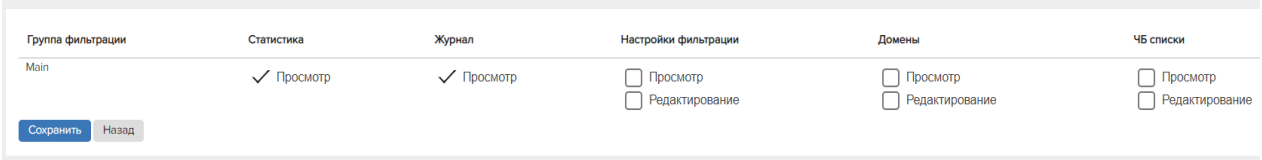


Рис.3.5.15. Права доступа – создание группы – определение прав

Определяем необходимые права группы *test,* активируем *Сохранить*, создание *Пользовательской группы* завершено. Пользовательская группа можно удалить, в отличии от групп по умолчанию, активируя элемент *Удалить* (Рис.3.5.13.).

3.6 Функционал системы - УПРАВЛЕНИЕ

Функционал меню **УПРАВЛЕНИЕ** позволяет просматривать, изменять, добавлять, удалять ***Организации, Группы фильтрации, Домены,адреса, Черные/Белые списки***.

Экранный интерфейс меню, включает подменю*:*

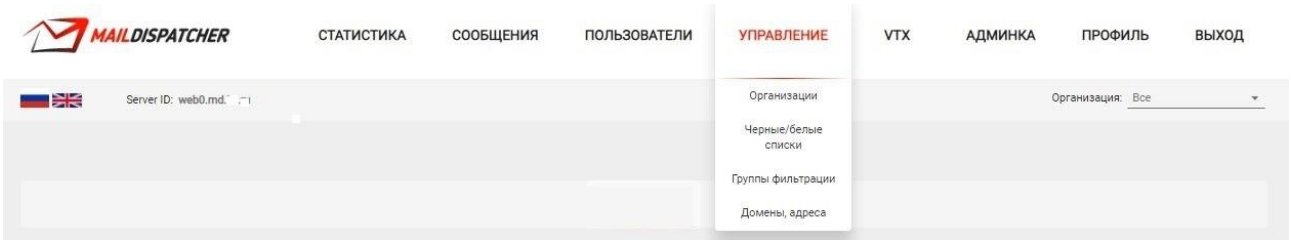


Рис.3.6.1. Экранный интерфейс (меню, подменю) - УПРАВЛЕНИЕ

3.6.1 *УПРАВЛЕНИЕ – подменю* Организации

Система «MAIL DISPATCHER» позволяет работать со значительным количеством организаций или подразделениями одной организации – функционал подменю *Организации.* Функционал подменю *Организации* позволяет реализовать права доступа пользователей (операторов, администраторов) по работе только с заданными структурами.

Активируем:

Меню → *УПРАВЛЕНИЕ*

→*Организации*

Переходим в экранный интерфейс:

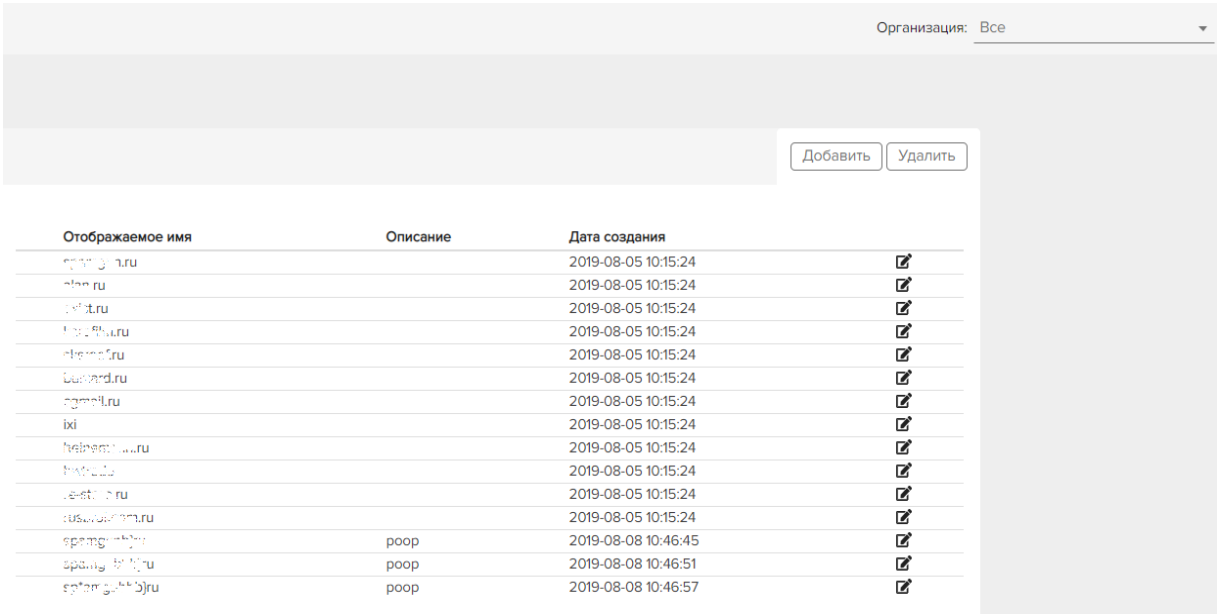


Рис. 3.6.2. Экранный интерфейс подменю - *Организации*

Функционал Журнала *Организации* стандартно позволяет добавлять, удалять, редактировать. Наименование полей таблицы интуитивно понятны.

3.6.2 *УПРАВЛЕНИЕ – подменю* Группы фильтрации

Обработка потока сообщений для каждой организации определяется Группами фильтрации. Группа фильтрации использует пороги баллов для отнесения сообщения к определенной категории. (*Балл - параметр, вычисляемый системой при прохождении фильтров, в процессе анализа, в относительных единицах. Чем выше спамрейтинг, тем вероятнее сообщение относиться к спаму.*)

Для перехода к функционалу Группы фильтрации активируем:

Меню → *УПРАВЛЕНИЕ*

→*Группы фильтрации*

Переходим в экранный интерфейс:

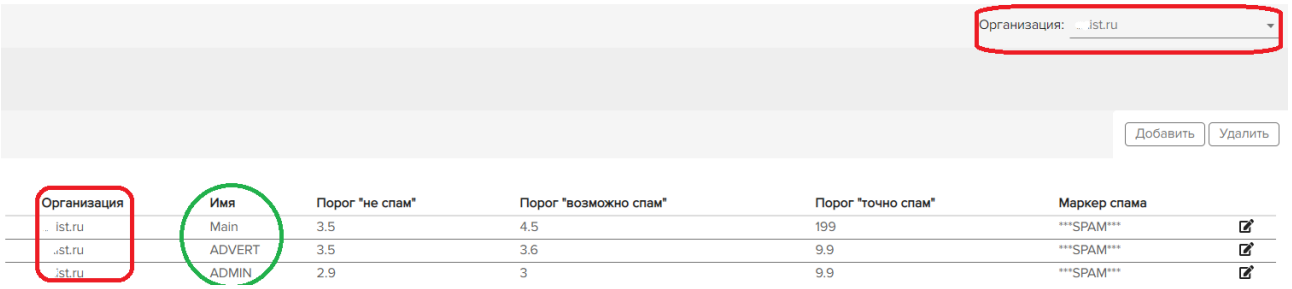


Рис. 3.6.3. Экранный интерфейс подменю – *Группы фильтрации*

Из выпадающего списка *«Организация»* выбираем конкретную организацию. В интерфейсе выводятся *Группы фильтрации* для данной организации. Как видно из приведенных данных у организации три группы фильтрации (Main, ADVERT, ADMIN), различающихся порогами (баллами).

Для Группы фильтрации ***Main***:

- Порог «Не спам» - если параметр (балл) сообщения вычисляемый системой при прохождении фильтров <3.5 то сообщения доставляется Получателю;
- Порог «Возможно спам» - если параметр (балл) сообщения вычисляемый системой при прохождении фильтров > 3.5 но <4.5, сообщение доставляется Получателю с пометкой ***SPAM***;
- Порог «Точно спам»:
  - ✓ если параметр (балл) сообщения вычисляемый системой при прохождении фильтров > 4.5 но <199, сообщение отправляется в *«Карантин»;*
  - ✓ если параметр (балл) сообщения вычисляемый системой при прохождении фильтров > 199 , сообщение определяется как СПАМ и удаляется*;*

Пользователи с правами *Администраторов,* имеют возможность «Добавить», «Удалить», «Редактировать» ( ) как *Группы фильтрации*, так и параметры конкретной группы.

3.6.3 *УПРАВЛЕНИЕ – подменю* Домены,адреса

Для перехода к функционалу Домены активируем:

Меню → *УПРАВЛЕНИЕ*

→*Домены,адреса*

Переходим в экранный интерфейс:

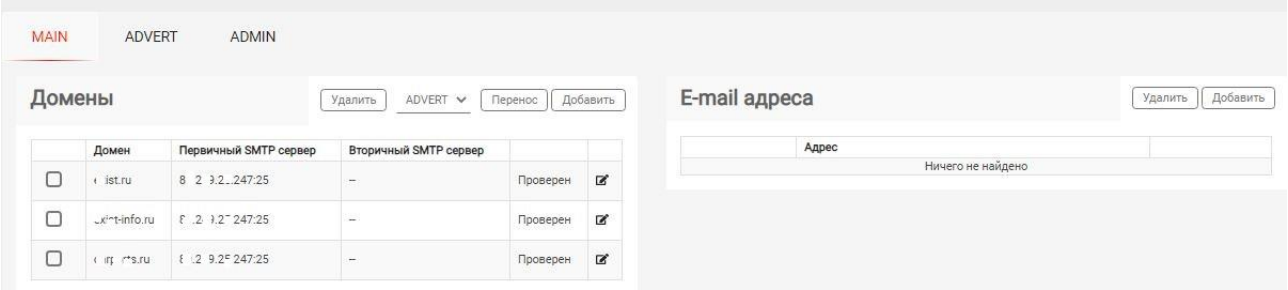


Рис.3.6.4. Экранный интерфейс подменю – *Домены*

Функционал подменю ***Домены*** позволяет добавить, изменить, удалить, перенести почтовые домены организации в соответствующую Группу Фильтрации. Как видно из данных приведенных на рис.3.6.4. Группу Фильтрации – ***Main***, включены 3 почтовых сервера. Как отмечено в п.3.6.2. Группы Фильтрации отличаются параметрами (баллами, порогами) фильтрации.

Для включения нового почтового сервера организации в конкретную Группу фильтрации, необходимо активировать соответствующую Группу, в данном случае выбрать одну из трех Групп (***MAIN, ADVERT, ADMIN***) и активировать элемент Добавить.

Переходим к экранному интерфейсу:

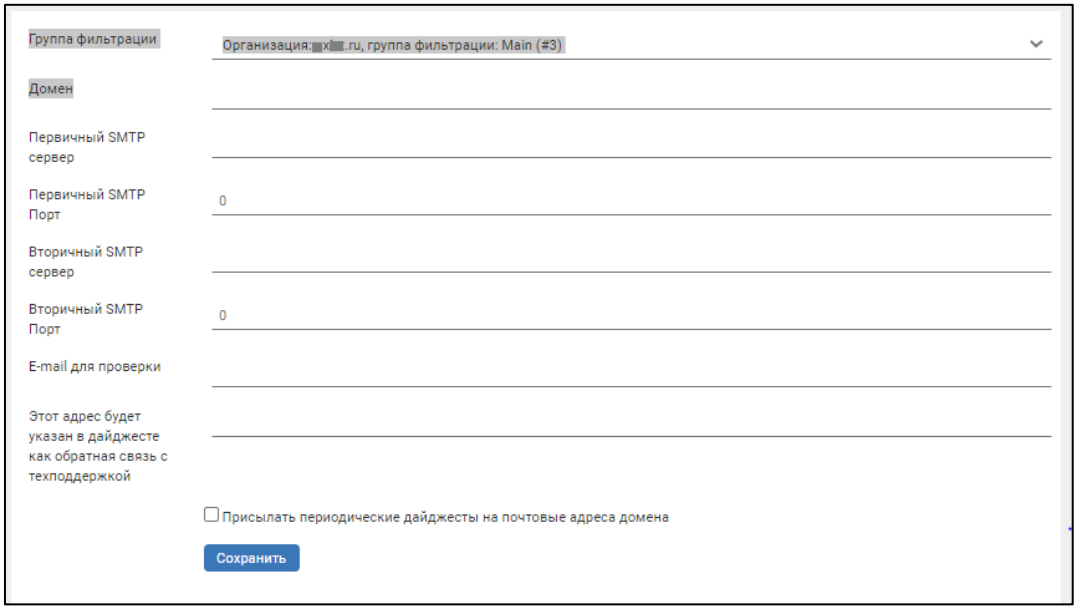


Рис.3.6.5. Ввод Домена в Группу Фильтрации

В экранной форме стандартно заполняются требуемые поля.

Поле- *E-mail для проверки* с адресацией данного домена необходим для проверки состояния.

Поле *Присылать периодические дайджесты на почтовые адреса домена*, при активации ☑ реализует отправку Пользователям домена дайджест писем попавшим в карантин за прошедший день.

По заполнению полей стандартно активируется *Сохранить* .

Для переноса почтового домена из одной Группы фильтрации в другую необходимо выбрать строку домена в исходной группе (☐), из выпадающего списка Групп – Группу в которую необходимо перенести (например ADVERT) и активировать *Перенос* .

Пример дайджеста писем попавших в карантин по Пользователю:

MAILDISPATCHER

ОПОВЕЩЕНИЕ О ПИСЬМАХ В КАРАНТИНЕ:

Время	От	Кому	Тема	Баллы	Ссылка для отправки	
2020-07-15 10:34:20	info@prommashtest.ru	vcx@proba.ru	Испытания продукции в системе РОСАТОМ	13.62	Доставить	Доставить администратору
2020-07-15 08:12:12	ohzipvz@volansky.network	vcx@proba.ru	Оптом маски и респираторы по ценам от производителя.	30.94	Доставить	Доставить администратору
2020-07-15 07:52:11	icfizjy@galasym.nl	vcx@proba.ru	Стильные платья за 1890 руб	31.98	Доставить	Доставить администратору
2020-07-15 07:51:06	orjydqh@gimages.nl	vcx@proba.ru	Мужская поясная сумка + Подарок	18.58	Доставить	Доставить администратору
2020-07-15 07:32:47	info@probsu.ru	vcx@proba.ru	Нужны кассеты и поворотные столы для формования сборного железобетона? ᴇ Испанская компания MoldTech решит задачу любой сложности!!!	9.24	Доставить	Доставить администратору
2020-07-15 07:32:19	efremova@werug.ru	vcx@proba.ru	Ультрафиолетовые светильники для дезинфекции.	35.7	Доставить	Доставить администратору
2020-07-15 06:14:47	ymbicpb@golfasert.nl	vcx@proba.ru	Робот-мойщик окон Hobot	20.24	Доставить	Доставить администратору

Рис.3.6.6. Дайджест писем попавших в карантин

Пользователь имеет возможность активировать:

- *Доставить* – письмо будет доставлено Пользователю;
- *Доставить администратору* – письмо будет отправлено Администратору почты для дальнейшего анализа;

3.6.4 *УПРАВЛЕНИЕ – подменю Черные/белые списки*

Для перехода к функционалу *Черные/белые списки* активируем:

Меню → *УПРАВЛЕНИЕ*

→ *Черные/белые списки*

Переходим в экранный интерфейс:

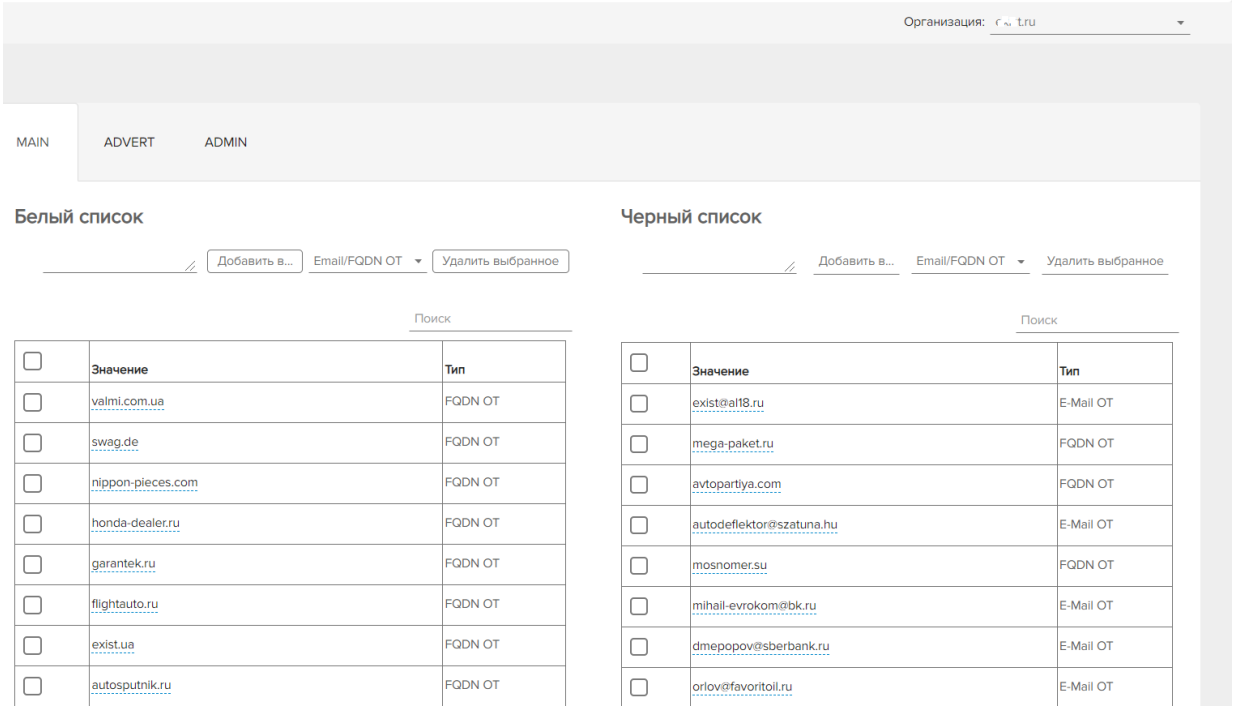


Рис. 3.5.6. Журнал *Черные/белые списки*

В системе «MAIL DISPATCHER» для фильтрации сообщений используется известный функционал ***Черные/Белые списки***. Непосредственно списки создаются по организации и Группе фильтрации. Черные и белые списки заполняются пользователем с правами администратора.

Списки формируются по категориям:

- по домену (xxxxxx.zz) – метка FQDN OT;
- по E-mail (yyy@xxxx.zz) –метка E-mail OT;
- по IP-адресу (zzz.vvv.yyy.xxx) домена - метка FQDN OT;
- по хэш-функции (SHA256) сообщения - метка файл;

Функционал позволяет:

- «Добавить» - добавить данные в соответствующую категорию Черного/Белого списка. В строку можно добавлять несколько элементов, разделив запятой.
- «Удалить выбранное» - удалить данные из соответствующей категории и Группы фильтрации Черного/Белого списка. Предварительно необходимо выделить элемент или элементы списка (☐).
- «Поиск» - осуществить поиск в соответствующем списке;

Предварительно:

- Выбираем организацию – элемент интерфейса ***Организация*** выпадающий

список;

- При наличии нескольких ***Групп фильтрации*** – выбираем необходимую Группу;

Списки могут занимать несколько страниц, как показано в нижней части интерфейса:

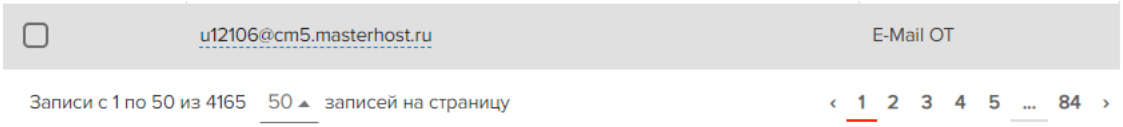


Рис. 3.5.7. Журнал *Черные/белые списки – страницы*

3.7 Функционал системы - СТАТИСТИКА

Функционал ***СТАТИСТИКА*** позволяет получить информацию по широкому спектру параметров полученных сообщений.

3.7.1 *СТАТИСТИКА - Сводка*

Для перехода к данным *Сводка* активируем:

Меню → *СТАТИСТИКА*

→ *Сводка*

Переходим в экранный интерфейс.

Определяем «Организацию» из выпадающего списка, выводится ряд графиков, таблиц и диаграмм с данными по статистике распределения сообщений:

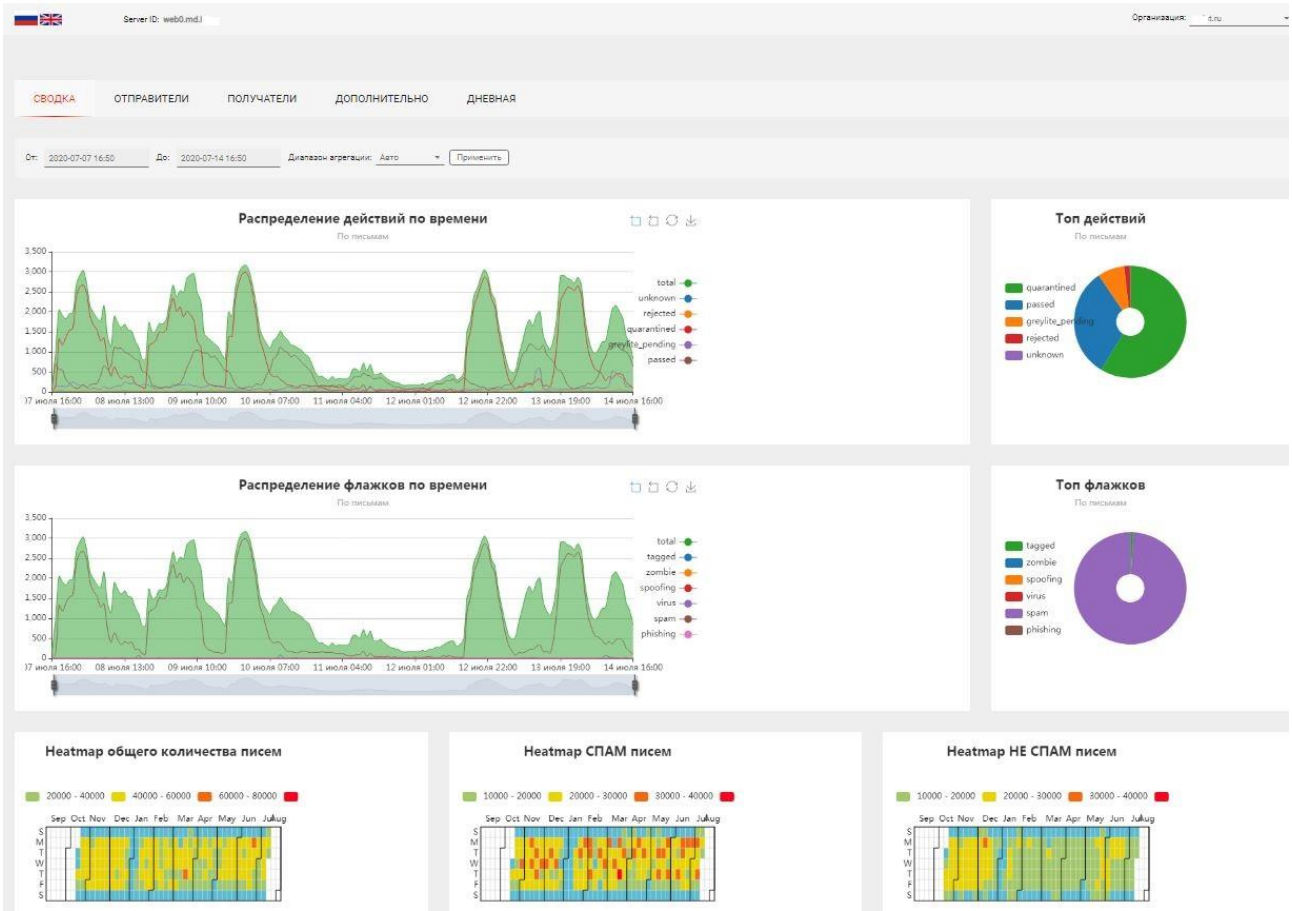


Рис. 3.7.1. Графики статистики

Данные по сообщениям на графиках, диаграммах и в таблицах позволяют получить детальную информацию в широком диапазоне.

Система «MAIL DISPATCHER» позволяет обрабатывать сообщения одновременно с большого количества почтовых доменов (серверов), как одной организации, так и нескольких организаций (подразделений). Разграничение доступа к данным пользователей (операторов, администраторов) осуществляется на уровне прав доступа. Для просмотра данных статистики по конкретному домену (организации) используется элемент ***Организация*** - представляющий выпадающий список.

Используется ряд фильтров и параметров

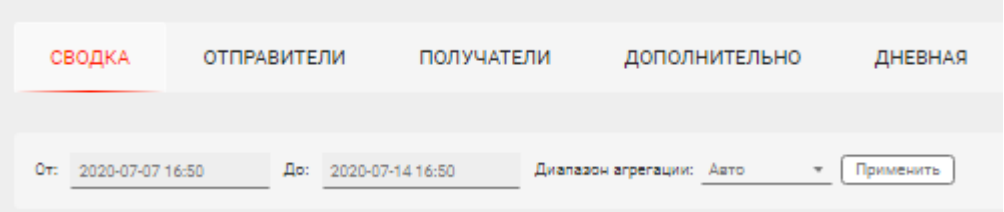


Рис. 3.7.2. Фильтры

По *периоду От*_____*До*_____. Задается *Диапазон агрегации*: 5 мин – 1 неделя.

Рассмотрим детальнее некоторые графики данных. Данные приведенные на графиках, диаграммах и в таблицах интуитивно понятны, включают общепринятые величины и параметры.

3.7.2 *СТАТИСТИКА - распределение сообщений по критериям*

3.7.2.1 *Распределение действий по времени*

Типовой график приведен на рисунке:

Рис. 3.7.3. Распределение действий над сообщениями по времени

По осям приведены следующие данные:

- Ось Y – динамически изменяемая временная шкала в часах (от 1 часа до недели);
- Ось X – Количество сообщений в единицу времени (за 1 час);

В правой части графика приведена расшифровка выборки действий над сообщениями:

- total - всего сообщений;
- unknown - неизвестный тип сообщения;
- rejected - отброшенное (удаленное) сообщение (явный СПАМ);
- quarantined – сообщение, помещенное в карантин (возможный СПАМ);
- greylite_pending – обрабатываемое (проверяемое) сообщение;
- passed - доставленные сообщения;

Временной интервал на шкале (ось Y) динамически выбирается перемещением ползунков (нижняя часть графика).

График позволяет анализировать распределение получения сообщений по времени, выделять временные аномалии, пиковые периоды и т.д.

При наведении курсора на конкретное время, на экран выводится детальная расшифровка действий по сообщениям для данного момента времени:

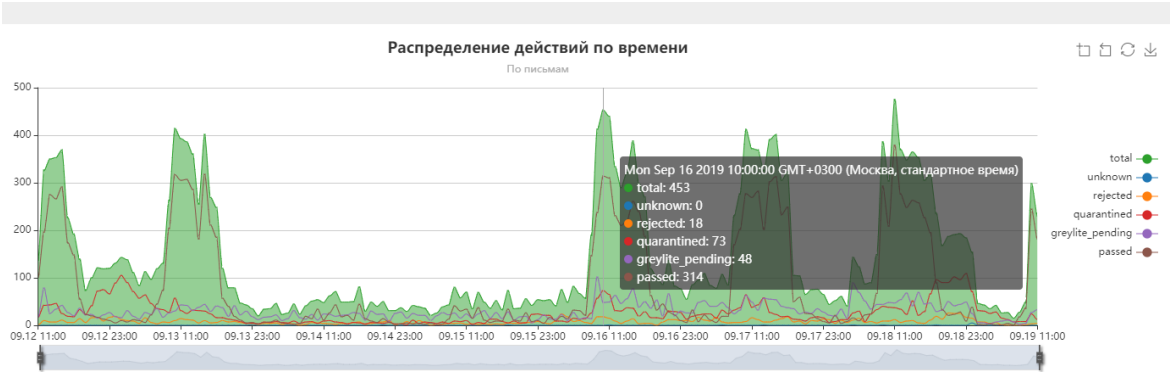


Рис. 3.7.4. Детализация данных по времени

На большей части графиков используются активные элементы - 

Элементы позволяют провести ряд операций над графиком – *Увеличить, Уменьшить, Обновить, Скачать.*

Используя курсор, возможно, варьировать данные выводимые на графике. Активирую курсором цветовой элемент можно отключать (включать) данные на графике. На следующем графике приведены данные при отключенном элементе – ***total***.

Рис. 3.7.5. Данные без вывода общего количества сообщений (total)

3.7.2.2 *Распределение флажков по времени*

Типовой график приведен на рисунке:

Рис. 3.7.6. Детализация распределения данных сообщений по времени

По осям приведены данные:

- Ось Y – динамически изменяемая временная шкала в часах (от 1 часа до недели);
- Ось X – Количество сообщений в единицу времени (за 1 час);

В правой части графика приведена расшифровка выборки классификации (флажков) сообщений:

- total - всего сообщений;

Классифицированные как:

- tagged - сообщение доставлено, но помечено как возможно «СПАМ»;
- zombie - классифицированные, как зомби;
- spoofing – классифицированные, как спуфинг;
- virus – классифицированные, как содержащие вирус;
- spam - классифицированные, как спам;
- phishing - классифицированные, как фишинг;

Временной интервал на шкале (ось Y) динамически выбирается перемещением ползунков.

График позволяет анализировать распределение получения сообщений по времени, выделять временные аномалии, пиковые периоды и т.д.

При наведении курсора на конкретное время, на экран выводится детальная расшифровка действий по сообщениям для данного момента времени.

Используя курсор, возможно, варьировать данные выводимые на графике. Активирую курсором цветовой элемент можно отключать (включать) данные на графике, как и на большинстве, остальных графиков.

3.7.3 *СТАТИСТИКА - Отправители*

Для перехода к данным *Отправители* активируем:

Меню → *СТАТИСТИКА*

→ *Отправители*

Определяем «***Организацию***» из выпадающего списка в правой верхней части экрана, выводится ряд графиков, таблиц и диаграмм с данными по статистике распределения сообщений по ***Отправителям***.

Рис. 3.7.7. Детализация распределения данных сообщений по Отправителям

Данные приведенные на графиках, диаграмме и таблице интуитивно понятны.
Функционал элементов позволяющих детализировать данные, описан выше.

3.7.4 *СТАТИСТИКА - Получатели*

Для перехода к данным *Получатели* активируем:

Меню → *СТАТИСТИКА*

→ *Получатели*

Определяем «***Организацию***» из выпадающего списка в правой верхней части экрана, выводится ряд графиков, таблиц с данными по статистике распределения сообщений по ***Получателям***.

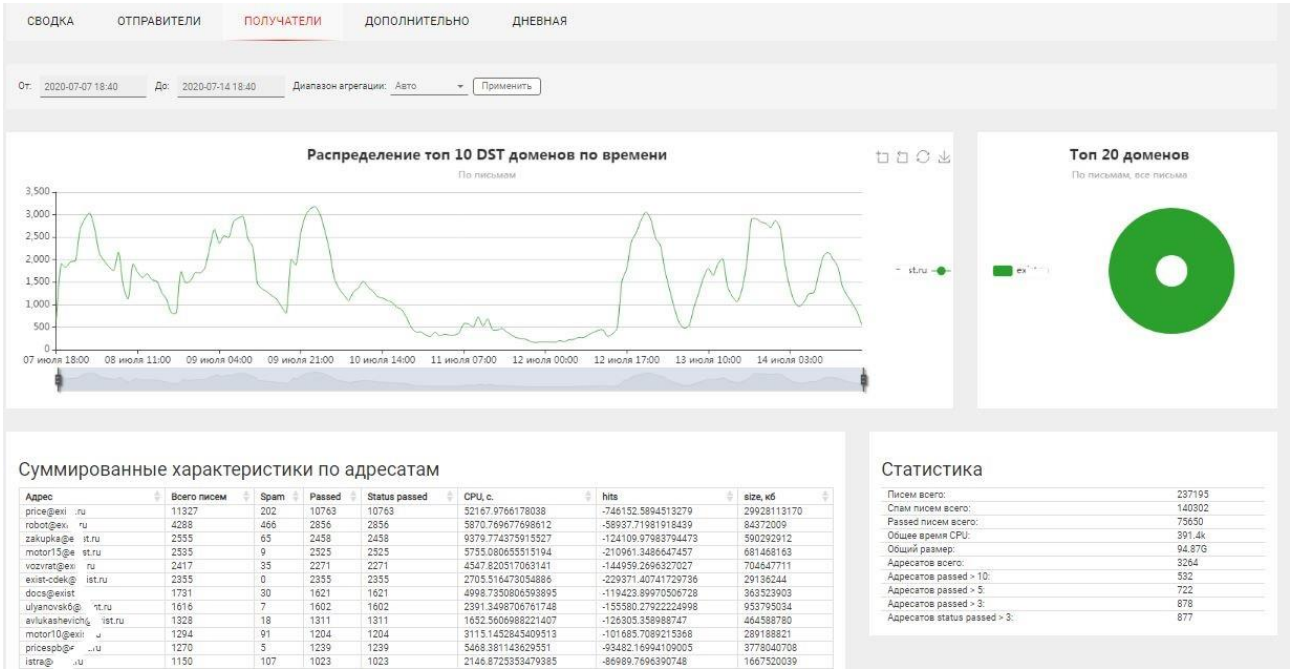


Рис. 3.7.8. Детализация распределения данных сообщений по Получателям

Данные приведенные на графиках, диаграмме и таблице интуитивно понятны.
Функционал элементов позволяющих детализировать данные, описан выше.

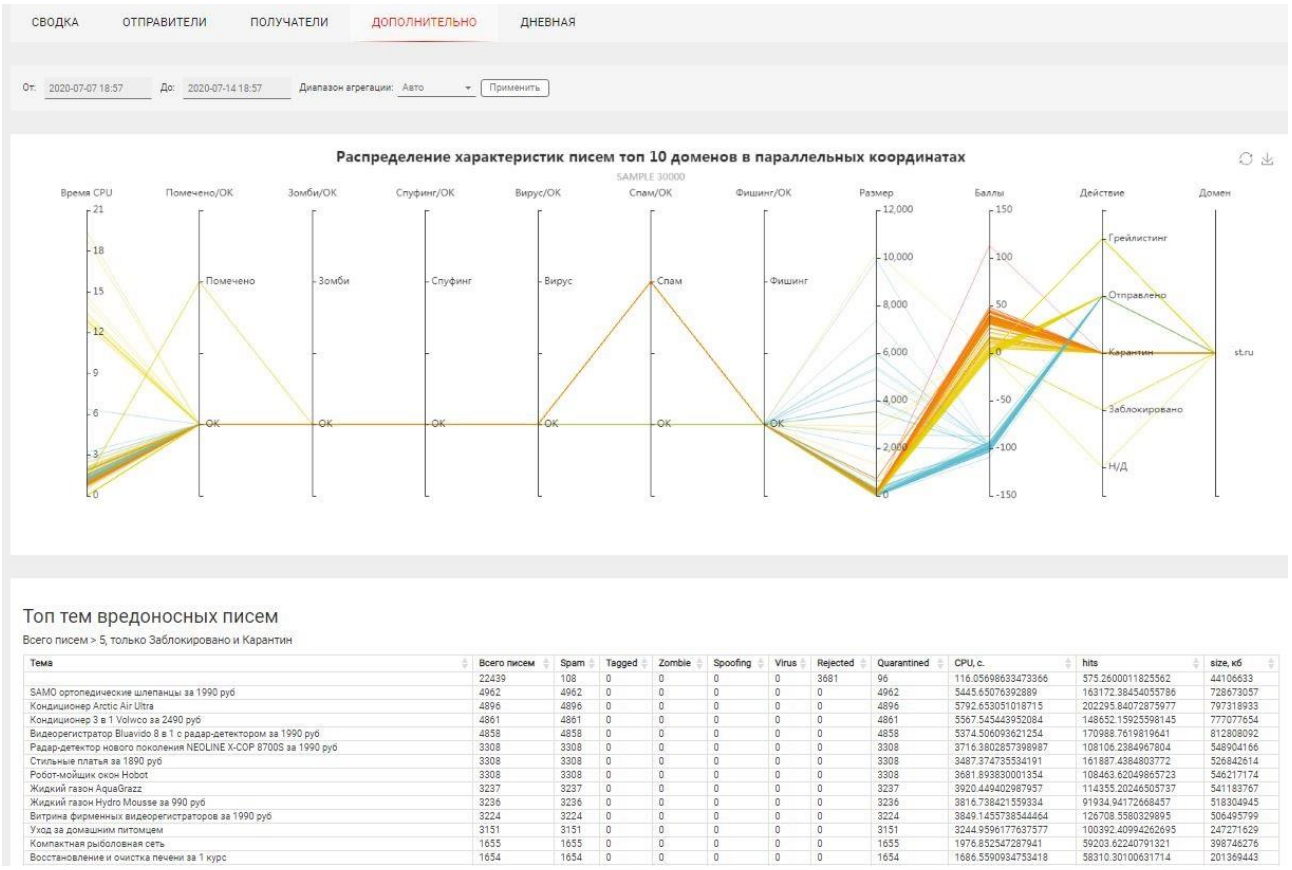
3.7.5 *СТАТИСТИКА - Дополнительно*

Для перехода к данным *Дополнительно* активируем:

Меню → *СТАТИСТИКА*

→ *Дополнительно*

Определяем «***Организацию***» из выпадающего списка в правой верхней части экрана, выводится ряд графиков, таблиц с данными по статистике распределения сообщений по дополнительным параметрам.



Топ тем вредоносных писем

Всего писем > 5, только Заблокировано и Карантин

Тема	Всего писем	Spam	Tagged	Zombie	Spoofing	Virus	Rejected	Quarantined	CPU, c.	hits	size, кб
	22439	108	0	0	0	0	3681	96	116.05698633473366	575.2600011825562	44106633
SAMO ортопедические шлепанцы за 1990 руб	4962	4962	0	0	0	0	0	4962	5445.65076392889	163172.38454055786	728673057
Кондиционер Arctic Air Ultra	4896	4896	0	0	0	0	0	4896	5792.653051018715	202295.84072875977	797318933
Кондиционер 3 в 1 Volvco за 2490 руб	4861	4861	0	0	0	0	0	4861	5567.545443952084	148652.15925598145	777077654
Видеорегистратор Bluavido 8 в 1 с радар-детектором за 1990 руб	4858	4858	0	0	0	0	0	4858	5374.506093621254	170988.7619819641	812808092
Радар-детектор нового поколения NEOLINE X-COP 8700S за 1990 руб	3308	3308	0	0	0	0	0	3308	3716.3802857398987	108106.2384967804	548904166
Стильные платья за 1890 руб	3308	3308	0	0	0	0	0	3308	3487.374735534191	161887.4384803772	526842614
Робот-мойщик окон Hobot	3308	3308	0	0	0	0	0	3308	3681.893830001354	108463.62049865723	546217174
Жидкий газон AquaGrazz	3237	3237	0	0	0	0	0	3237	3920.449402987957	114355.20246505737	541183767
Жидкий газон Hydro Mousse за 990 руб	3236	3236	0	0	0	0	0	3236	3816.738421559334	91934.94172668457	518304945
Витрина фирменных видеорегистраторов за 1990 руб	3224	3224	0	0	0	0	0	3224	3849.1455738544464	126708.5580329895	506495799
Уход за домашним питомцем	3151	3151	0	0	0	0	0	3151	3244.9596177637577	100392.40994262695	247271629
Компактная рыболовная сеть	1655	1655	0	0	0	0	0	1655	1976.852547287941	59203.62240791321	398746276
Восстановление и очистка печени за 1 курс	1654	1654	0	0	0	0	0	1654	1686.5590934753418	58310.30100631714	201369443

Рис. 3.7.9. Детализация распределения данных сообщений по параметрам

Данные приведенные на графиках, диаграмме и таблице интуитивно понятны.
Функционал элементов позволяющих детализировать данные, описан выше.

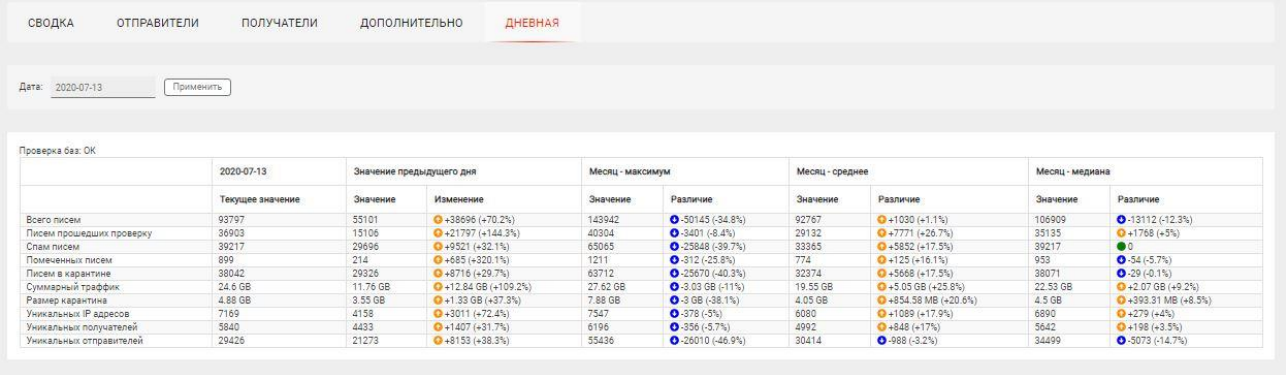
3.7.6 *СТАТИСТИКА - Дневная*

Для перехода к данным *Дневным* активируем:

Меню → *СТАТИСТИКА*

→ *Дневная*

Определяем «***Организацию***» из выпадающего списка в правой верхней части экрана, выводится ряд графиков, таблиц с данными по статистике распределения сообщений по дополнительным параметрам.



	2020-07-13	Значение предыдущего дня		Месяц - максимум		Месяц - среднее		Месяц - медиана	
	Текущее значение	Значение	Изменение	Значение	Различие	Значение	Различие	Значение	Различие
Всего писем	93797	55101	+38696 (+70.2%)	143942	-50145 (-34.8%)	92767	+1030 (+1.1%)	106909	-13112 (-12.3%)
Писем прошедших проверку	36903	15106	+21797 (+144.3%)	40304	-3401 (-8.4%)	29132	+7771 (+26.7%)	35135	+1768 (+5%)
Спам писем	39217	29696	+9521 (+32.1%)	65065	-25848 (-39.7%)	33365	+5852 (+17.5%)	39217	0
Помеченных писем	899	214	+685 (+320.1%)	1211	-312 (-25.8%)	774	+125 (+16.1%)	953	-54 (-5.7%)
Писем в карантине	38042	29326	+8716 (+29.7%)	63712	-25670 (-40.3%)	32374	+5668 (+17.5%)	38071	-29 (-0.1%)
Суммарный траффик	24.6 GB	11.76 GB	+12.84 GB (+109.2%)	27.62 GB	-3.03 GB (-11%)	19.55 GB	+5.05 GB (+25.8%)	22.53 GB	+2.07 GB (+9.2%)
Размер карантина	4.88 GB	3.55 GB	+1.33 GB (+37.3%)	7.88 GB	-3 GB (-38.1%)	4.05 GB	+854.58 MB (+20.6%)	4.5 GB	+393.31 MB (+8.5%)
Уникальных IP адресов	7169	4158	+3011 (+72.4%)	7547	-378 (-5%)	6080	+1089 (+17.9%)	6890	+279 (+4%)
Уникальных получателей	5840	4433	+1407 (+31.7%)	6196	-356 (-5.7%)	4992	+848 (+17%)	5642	+198 (+3.5%)
Уникальных отправителей	29426	21273	+8153 (+38.3%)	55436	-26010 (-46.9%)	30414	-988 (-3.2%)	34499	-5073 (-14.7%)

Рис. 3.7.10. Детализация распределения данных сообщений за день и текущий месяц

Данные приведенные в таблице интуитивно понятны.
Функционал элементов позволяющих детализировать данные, описан выше.

4 ТЕКУЩАЯ РАБОТА АДМИНИСТРТОРА/ОПЕРАТОРА СИСТЕМЫ MD.

Основная деятельность администратора/оператора системы MD заключается в ежедневном постоянном контроле состояния входящих и исходящих сообщений, работе с Заявками Пользователей, настройке Черных и Белых списков, анализе аномалий, контроле сообщений попавших в карантин, спам, заблокированных и т.д.

1.1. Обработка Заявок Пользователей почтовой системы.

Пользователи системы, в зависимости от настройки, получают ежедневно детальную информацию (время сообщения, от кого, тема сообщения и т.д.) о недоставленных сообщениях помещенных в «Карантин».

Пользователь имеет возможность, в зависимости от типа сообщения, наличия вложения, результатов анализа проведенного системой, анализа характеристик сообщения проведенного пользователем, либо получить сообщение из карантина, выбрав «Доставить», либо отправить сообщение для дополнительного анализа администратору системы.

В ряде случаев, неполучение сообщения, задержке и т.д. пользователь имеет возможность написать и отправить Заявку с изложением проблемы. Виды Заявок рассмотрены далее.

4.1 Заявка Пользователя о неполучении сообщения.

При прохождении сообщения в системе MD возможно, в очень редких случаях, «ложное» срабатывание. Сообщение может быть отправлено в карантин, спам, заблокировано и т.д. В ряде случае, при некорректной настройки фильтрации, возможно прохождение спам - сообщения.

Схема обработки Заявок пользователей почтовой системы следующая:

1) При получении заявки пользователя системы о неполучении сообщения, необходимо получить детальную информацию о дате и времени отправки, E-mail отправителя и т.д.;
2) Открываем ***Журнал сообщений*** входящей почты – ***Меню→Общее→Журнал сообщений***. Используя фильтры, находим требуемое сообщение.
3) Если сообщение найдено в ***Журнале Сообщений***, проводим предварительный анализ найденного сообщения. Определяем по полям ***Действие и Причина*** состояние сообщения (Заблокировано, Спам, Карантин, Доставлено из карантина, Ошибка доставки из карантина, Ошибка доставки, Вирус и т.д.).

Для случая ***нормального сообщения*** заблокированного системой рассмотрим основные варианты действия:

Состояние поля *«Действие»*	**Причина**	**Действие**
Карантин	Письмо не прошло систему фильтрации и отправлено в карантин.	Три возможных варианта. 1. Отмечаем письмо в журнале. В ***Журнале сообщений*** активируем кнопку «*Доставить*» в элементе интерфейса.

		2. Отмечаем письмо в журнале. В ***Журнале сообщений*** активируем кнопку «*Обучиться*» в элементе интерфейса. Письмо будет доставлено получателю. Аналогичные письма не будут попадать в карантин. 3. Отмечаем письмо в журнале. В ***Журнале сообщений*** активируем кнопку «*Не спам*» в элементе интерфейса. Письмо будет доставлено получателю. IP-адрес получателя будет добавлен в Белый список.
Спам	Сообщение удалено, как спам-сообщение. В информации о сообщении в поле Rules указано Policy: Greylisted_Block.NDR. В связи с тем что последнее время участились случаи отправки спам-сообщений с использованием NDR, сообщения не соответствующие критериям блокируются как спам.	Сообщаем администратору системы MD.
Заблокировано	Сервер отправителя не отвечает требованиям стандарта протокола SMTP.	Сообщаем администратору системы MD.

4.2 Заявка Пользователя о получении спам - сообщения.

В системе MD возможно, в ряде случае, при некорректной настройки фильтрации, прохождение спам - сообщения.

Схема обработки Заявки Пользователя почтовой системы стандартна:

1) При получении заявки Пользователя системы о получении спам-сообщения, необходимо получить детальную информацию о дате и времени отправки, E-mail отправителя, CID, MSGID и т.д.;
2) Открываем ***Журнал сообщений*** исходящей почты – ***Меню→Исходящая почта → Журнал сообщений.*** Используя фильтры, находим требуемое сообщение.
3) Проводим предварительный анализ найденного сообщения. Определяем по полям ***Действие и Причина*** состояние сообщения (*Доставлено, Помечено).*

Для случая ***спам - сообщения*** полученного Пользователем, рассмотрим варианты возможных действий:

Состояние поля *«Действие»*	**Причина**	**Действие**
Доставлено	В системе MD возможно, в ряде случае, при некорректной настройки фильтрации, прохождение спам - сообщения.	В случае если проведенный анализ сообщения (***Помечено***) подтвердил, что это спам, то для предотвращения повторного получения спама, E-mail отправителя необходимо добавить в Черный список. Выделяем сообщение → ***Спам.***
Помечено		Для случая сообщения (***Помечено)***, информацию о сообщении необходимо передать администратору системы MD, для анализа и возможной коррекции настроек фильтрации.

4.3 Заявка Пользователя о проверке наличия сообщения в Журнале и задержке получения сообщения.

В системе MD возможно, в ряде случае, задержка прохождение сообщения, в связи с обработкой системой фильтрации.

Схема обработки Заявки Пользователя почтовой системы стандартна:

1) При получении заявки Пользователя системы о проверки наличия сообщения, либо его задержки, необходимо получить детальную информацию о дате и времени отправки, E-mail отправителя, CID, MSGID и т.д.;
2) Открываем ***Журнал сообщений*** исходящей почты – ***Меню→Исходящая почта → Журнал сообщений.*** Используя фильтры, находим требуемое сообщение.
3) Проводим предварительный анализ найденного сообщения. Определяем по полям ***Действие и Причина*** состояние сообщения. Варианты – [Заблокировано, Спам, Карантин, Ошибка доставки, Вирус] . Рассмотрим вариант, когда в поле «*Действие*» → *Ожидание.*

Состояние поля *«Действие»*	**Причина**	**Действие**
Ожидание (кол-во попыток из N)	Почтовый сервер отправителя не имеет репутации или репутация достаточно низкая. Согласно стандартам SMTP сервер отправителя должен повторно отправить сообщение через определенный интервал времени.	Ждем некоторое время. Сообщаем Пользователю о состоянии сообщения. При необходимости, после проверки отправителя и сообщения, для ускоренной отправки сообщения, возможно включить IP адрес отправителя в Greylite ***→Выделяем***

		сообщение→Добавить в greylite. В этом случае исключаются запросы на повторную отправку, но фильтрация сообщения не отменяется. В случае если сообщение не проходит, сообщаем администратору системы MD.

4.4 Заявка Пользователя по исходящему письму.

В системе MD проводится фильтрация, как входящей, так и исходящей почты. При наличии спама исходящее письмо также может быть *Заблокировано*, помещено в *Карантин,*
Схема обработки Заявки Пользователя почтовой системы стандартна:

1) При получении заявки Пользователя системы о проверки наличия сообщения, либо его задержки, необходимо получить детальную информацию о дате и времени отправки, E-mail получателя и т.д.;
2) Открываем ***Журнал сообщений*** исходящей почты – ***Меню→Исходящая почта → Журнал сообщений.*** Используя фильтры, находим требуемое сообщение.
3) Проводим предварительный анализ найденного сообщения. Определяем по полям ***Действие и Причина*** состояние сообщения. Варианты – [Заблокировано, Спам, Карантин, *Ожидание*].

Состояние поля *«Действие»*	**Причина**	**Действие**
Ожидание (кол-во попыток из N)	Почтовый сервер получателя не имеет репутации или репутация достаточно низкая. Согласно стандартам SMTP сервер отправителя должен повторно отправить сообщение через определенный интервал времени.	Ждем некоторое время. Сообщаем Пользователю о состоянии сообщения. При необходимости, после проверки отправителя и сообщения, для ускоренной отправки сообщения ***→Выделяем сообщение → Доставить.*** В этом случае исключаются запросы на повторную отправку, но фильтрация сообщения не отменяется. В случае если сообщение не проходит, сообщаем администратору системы MD.
Карантин	Исходящее сообщение не прошло фильтрацию в системе MD,	Сообщаем Пользователю о состоянии сообщения.

	помещено в Карантин.	При необходимости, после проверки отправителя и сообщения, для отправки сообщения ***→Выделяем сообщение → Доставить.***
СПАМ	Исходящее сообщение не прошло фильтрацию в системе MD, помещено в *СПАМ*.	Сообщаем администратору системы MD.

Лист регистрации изменений									
Номера листов (страниц)					Всего листов (страниц) в докум.	№ документа	Входящий № сопроводи- тельного документа и дата	Подпись.	Дата
Изм	Изменен- ных	Заменен -ных	Новых	Аннулиро ванных					