

SPAMOREZ

Mail Security Platform

Защита корпоративной почты от спама, вирусов и фишинга

 В облаке

 У себя

 Офлайн

 В наших ДЦ

 Под ключ

3 млн писем заблокировано в сутки · 99,9% точность

Первые 14 дней — бесплатно



Свидетельство Роспатент

№ 2018665525



Реестр российского ПО

Запись № 15099 · 07.10.2022

С чем сталкивается бизнес

Почта остаётся главным каналом атак — и главным источником потерь времени



Спам отнимает время

- ✓ Сотрудники разбирают нежелательные письма вручную
- ✓ Рассылки и мусор прячут важные письма



Вирусы и фишинг

- ✓ Вредоносные вложения приходят по обычной почте
- ✓ Поддельные ссылки выглядят как настоящие



Пропавшие письма

- ✓ Нужное письмо не дошло — и непонятно, почему
- ✓ Лишние блокировки срывают сделки



Зависимость и сложность

- ✓ Зарубежные сервисы и данные за пределами страны
- ✓ Настройка требует отдельного администратора



Что нужно на самом деле

Защита, которая работает сразу, прозрачна для администратора и оставляет данные под вашим контролем.

ПРЕИМУЩЕСТВА

Почему SPAMOREZ

Российская платформа защиты почты: от спама, вирусов и фишинга



Точность

- ✓ 99,9% точность фильтрации
- ✓ 3 млн писем блокируется в сутки



Любой формат

- ✓ В облаке, у себя, офлайн или в наших ДЦ
- ✓ Подключение в облаке за 5 минут



Прозрачность

- ✓ Трекер: путь любого письма за секунды
- ✓ Карантин с выпуском в один клик
- ✓ Link Shield проверяет ссылки при клике



Российское ПО

- ✓ Реестр российского ПО, запись № 15099
- ✓ Свидетельство Роспатент № 2018665525



Попробуйте бесплатно

Первые 14 дней — бесплатно. Одна панель управления для всех вариантов подключения.

Варианты подключения

Выберите удобный формат — один продукт, пять способов



В облаке

- ✓ Смена MX-записи — готово
- ✓ Подключение за 5 минут
- ✓ Без сервера и администратора
- ✓ SLA 99,9%



SPZGate у себя

- ✓ На вашем Linux-сервере
- ✓ Docker, одна команда
- ✓ Данные только у вас
- ✓ SIEM-интеграция, REST API



Офлайн-установка

- ✓ Архив ~625 МБ — всё внутри
- ✓ Без apt-get и docker pull
- ✓ SHA-256 верификация
- ✓ Госсектор, банки, ОПК



В наших ДЦ

- ✓ 5 датацентров: МСК, СПб, Новосибирск, Екб, Франкфурт
- ✓ Выделенная VM, доступ только у вас
- ✓ Бэкап AES-256 ежедневно



Под ключ

- ✓ Наши инженеры — удалённо
- ✓ Настройка доменов и правил
- ✓ Обучение администратора
- ✓ Закрывающие документы

Все варианты работают с одной и той же панелью управления — карантин, белые/чёрные списки, правила, трекер

Быстрый старт без установки

SaaS · Подключение за 5 минут · Работает с любым почтовым сервером



Подключение за 5 минут

Смените MX-запись домена — и вся входящая почта идёт через Спаморез. Никакого сервера.



Очередь писем до 10 суток

Если ваш сервер недоступен — письма накапливаются и доставляются автоматически.



Панель управления

Карантин, белые/чёрные списки, правила, трекер доставки — всё в браузере.



SLA 99,9%

Распределённая инфраструктура в нескольких датацентрах. Мониторинг 24/7.



Оплата за ящики

Платите только за активные ящики. От 140 ₽/ящик в месяц. Первые 14 дней бесплатно.



Без администратора

Не нужен выделенный IT-специалист — настройка через веб-панель без знания Linux.

Как подключиться:

1

Зарегистрируйтесь

my.spamorez.ru — форма занимает 2 минуты

2

Добавьте домен

Введите ваш почтовый домен в панели управления

3

Смените MX-запись

Укажите mx.spamorez.ru вместо текущего сервера

4

Готово

Изменения вступают в силу за 5–60 минут

Exchange · Office 365 · Яндекс Почта · Google · Postfix · Exim · любой SMTP
14 дней бесплатно · без карты · настройка 5 минут · my.spamorez.ru

SPZGate в наших датацентрах

Выделенная VM · Данные только у вас · 5 городов



Москва

DataLine · M9 · Tier III+
пинг <5 мс



Санкт-Петербург

Selectel · Tier III
пинг <15 мс из МСК



Новосибирск

DataPro · Tier II+
для Сибири и ДВ



Екатеринбург

UTC · Tier II+
для Урала и Зап. Сибири



Франкфурт

Hetzner · EU · Tier III
GDPR

Конфигурация выделенной VM:

2 vCPU

Процессор

4 ГБ

RAM

50 ГБ SSD

NVMe

Белый IP

PTR + rDNS

- ✓ Бэкап конфигурации AES-256 ежедневно, хранение 30 дней
- ✓ Доступ только у вас — мы не имеем доступа к вашим письмам
- ✓ Договор, акт выполненных работ, все закрывающие документы

Как начать:



Оставьте заявку

Менеджер свяжется за 1 час



Разворачиваем VM + SPZGate

За 1 рабочий день



Передаём доступы, меняем MX

Вы сразу работаете

Одна и та же панель управления, что в облаке · SPZGate на вашей VM · support@spamorez.ru

Установим SPZGate у вас — под ключ



Удалённая установка

Нужен только SSH-доступ к серверу. Инженер подключается и разворачивает SPZGate.



Настройка под вас

Домены, ящики, правила фильтрации, белые/чёрные списки — всё настроим за вас.



Обучение администратора

Показываем панель управления, объясняем карантин, правила и трекер доставки.



Закрывающие документы

Договор, акт выполненных работ, счёт-фактура. Всё официально.



Поддержка после запуска

Вопросы по настройке — отвечаем в рабочее время. Telegram и email.



Данные остаются у вас

SPZGate устанавливается на ваш сервер. Письма не покидают вашу сеть.

Процесс установки под ключ:

1

Заявка и уточнение требований

Количество доменов, ящиков, требования ИБ.

2

SSH-доступ к серверу

Временный доступ инженеру, чистый Ubuntu/Debian.

3

Установка SPZGate

curl ... | sudo bash. 15–30 минут с загрузкой образов.

4

Настройка доменов и правил

Ящики, первичные правила фильтрации.

5

MX-запись и тестирование

Меняем MX, проверяем почту, настраиваем карантин.

6

Сдача системы и обучение

Показываем панель, подписываем акт выполненных работ.

SPZGate — шлюз на вашем сервере

On-Premise · Docker · Linux x86_64 / arm64 · полный контроль данных



Docker-based, 6 контейнеров

gmail · nginx · php · MySQL 8 · Redis · Memcached



Офлайн-установка ~625 МБ

Для закрытых сетей и госсектора. Без apt-get и docker pull



Автообновление с откатом

Создаёт бэкап, обновляет, откатывается при ошибке



Данные только у вас

SIEM-интеграция, REST API, полный контроль



SHA-256 верификация

Контрольная сумма к каждому пакету — проверьте до установки



Ubuntu/Debian

Ubuntu 22.04/24.04/26.04 LTS · Debian 11/12 · x86_64 и arm64

root@server:~

```
$ curl -fsSL spamorez.ru/spzgate/install.sh | sudo bash
```

✓ Проверка ОС: Ubuntu 26.04 LTS (amd64)

✓ Docker CE 26.1.4 установлен

✓ Порты 25, 80, 443 свободны

↓ Загрузка образов... (6 контейнеров)

✓ Все сервисы запущены (6/6)

✓ SPZGate 2.0 установлен!

Откройте <http://<IP>> для настройки

2 ядра

CPU

2 ГБ

RAM

20 ГБ

Диск

Ubuntu/Debian

ОС

SPZGate — офлайн-установка

Единый архив для полностью изолированных сетей



Один архив — всё внутри

~625 МБ: образы Docker, бинарники qmail, конфиги, скрипт установщика



Верификация SHA-256

Контрольная сумма публикуется рядом с архивом. Проверьте целостность до распаковки



Проверьте своими средствами ИБ

Антивирус, SAST, сканер уязвимостей — до установки в закрытой сети



Обновления тоже офлайн

Каждый релиз — такой же архив. Скачайте один раз, обновите без интернета



Для закрытых контуров

Госсектор, банки, ОПК, промышленные предприятия — где интернет ограничен по требованиям ИБ

root@server:~

```
$ ls -lh spzgate-2.0.1-offline-amd64.tar.gz
623M  spzgate-2.0.1-offline-amd64.tar.gz
$ sha256sum -c ...sha256
✓ spzgate-2.0.1-offline-amd64.tar.gz: OK
$ tar xzf spzgate-2.0.1-offline-amd64.tar.gz

$ sudo bash install-offline.sh

✓ Docker-образы загружены (без интернета)
✓ Все сервисы запущены (6/6)
✓ SPZGate установлен без интернета!
```

Три шага установки:

1

Перенесите архив на хост

USB, scp, или другой носитель. Проверьте SHA-256.

2

Распакуйте архив

```
tar -xzf spzgate-2.0.1-offline-amd64.tar.gz
```

3

Запустите установщик

```
sudo bash install-offline.sh — без интернета
```

Как это работает

Три этапа защиты каждого письма — автоматически

1

Мониторинг входящего трафика

- ✓ Письмо поступает на наш шлюз вместо вашего сервера
- ✓ Фиксируем IP, проверяем репутацию отправителя
- ✓ Анализируем заголовки и структуру сообщения
- ✓ RBL / SPF / DKIM / DMARC проверки

2

Обнаружение угроз

- ✓ Байесовские фильтры + нейросети
- ✓ 20 000+ спам-ловушек по всему миру
- ✓ Проверка вложений на вирусы
- ✓ Обнаружение фишинговых ссылок в теле

3

Блокировка или доставка

- ✓ Спам и вирусы → карантин
- ✓ Чистые письма доставляются без задержки
- ✓ Уведомление администратора при угрозе
- ✓ Полный лог в трекере — за 90 дней

SMTP вход



RBL / SPF
DKIM / DMARC



Байес +
ловушки



Антивирус
фишинг



Карантин /
Доставка

поток каждого письма · обработка < 1 сек

Управление фильтрацией

Все инструменты в одной веб-панели



Карантин писем

- ✓ Подозрительные письма не удаляются
- ✓ Просмотр полного содержимого
- ✓ Выпуск в inbox одним кликом
- ✓ Хранение до 30 дней



Белые и чёрные списки

- ✓ Всегда доставлять / всегда блокировать
- ✓ По домену, адресу или теме письма
- ✓ Индивидуально для каждого ящика
- ✓ Работает до всех остальных проверок



Правила обработки

- ✓ Условия AND / OR с вложенностью
- ✓ Regexp и wildcard
- ✓ Переадресация, тег, блокировка, отклонение
- ✓ Фильтр по вложениям и типу файла



Трекер доставки

- ✓ Поиск любого письма за секунды
- ✓ По отправителю, получателю, теме
- ✓ Причина фильтрации с деталями
- ✓ История 90 дней · Экспорт в CSV



Антивирус и антифишинг

Проверка всех вложений на вирусы · Обнаружение фишинговых ссылок в теле письма · Уведомление администратора при угрозе · Более 5 000 вирусов заблокировано в сутки

НОВОЕ

Link Shield: защита от фишинговых ссылок

Ссылки в письмах заменяются на подписанные и проверяются при каждом переходе



Подмена ссылок

- ✓ Каждый URL в письме заменяется на ссылку вашего домена
- ✓ Подпись HMAC-SHA256 — адрес нельзя подделать
- ✓ Домен и правила замены задаются в панели



Проверка при переходе

- ✓ URL проверяется при каждом клике
- ✓ Оценка степени опасности
- ✓ Опасные ссылки блокируются



Капча и предупреждение

- ✓ Предупреждение о переходе по внешней ссылке
- ✓ Капча на основе proof-of-work, без внешних сервисов
- ✓ Страница в веб-панели по адресу /secure/



Журнал переходов

- ✓ Логируется каждый переход
- ✓ Счётчики: получено, открыто, заблокировано
- ✓ Данные хранятся в Redis



Как это работает

Письмо → ссылки заменены при обработке → клик получателя → проверка и капча → переход на исходный адрес

НОВОЕ

Вкладка «Ссылки» в панели

Статистика по ссылкам и настройки Link Shield в одном месте



Топ ссылок

- ✓ Самые частые присланные ссылки
- ✓ Счётчики входящих и открытых
- ✓ Степень опасности каждой ссылки



Настройки

- ✓ Имя домена для подменных ссылок
- ✓ Правила замены
- ✓ Включение и отключение защиты



Границы защиты

- ✓ Проверяется адрес ссылки, а не содержимое страницы
- ✓ Песочницы для страниц нет
- ✓ Защита срабатывает в момент клика



Ошибка разбора письма

В трекер записывается, что письмо не удалось разобрать; в настройках выбирается действие: пропустить или отправить в карантин.

Роли, импорт и самообслуживание

Роли · Индивидуальные настройки · Импорт · Самообслуживание



Роли доступа
Администратор домена, пользователь ящика — каждый видит только своё.



Индивидуальный карантин
Каждый пользователь работает со своим карантином. Дайджест на почту.



Личные списки
Пользователь настраивает фильтры своего ящика без доступа к домену.



Импорт пользователей
Загрузка списка ящиков через CSV или API — тысячи записей за раз.



Дайджест писем
Регулярный отчёт на email — пользователь выпускает нужное сам.



Смена пароля
Пользователь меняет пароль от панели без обращения к администратору.

Матрица ролей:

Возможность	Админ	Польз.
Просмотр карантина домена	✓	—
Управление своим карантином	✓	✓
Белые/чёрные списки домена	✓	—
Личные белые/чёрные списки	✓	✓
Дайджест задержанных писем	✓	✓
Импорт/экспорт пользователей	✓	—
Журнал доставки всего домена	✓	—
Журнал своего ящика	✓	✓
Настройка правил домена	✓	—
Смена пароля	✓	✓

Управление через веб-панель или REST API · LDAP/AD-интеграция по запросу

Лимиты, DKIM и репутация

Лимиты · DKIM · Репутация · Защита от компрометации аккаунта



Лимиты отправки

Максимум писем в час/сутки на ящик или домен. Превышение — блокировка + уведомление.



DKIM-подпись

Автоматическая подпись исходящих — повышает доставляемость и защищает репутацию.



SPF и DMARC

Проверка исходящих на соответствие политикам домена до отправки.



Антивирус исходящих

Вложения также проверяются — чтобы ваш сервер не рассылал вирусы.



Детектор компрометации

Аномальный рост объёма отправки — автоблокировка ящика и алерт администратору.



Статистика отправки

Трекер исходящих: кто, сколько, куда, с каким результатом доставки.

Компрометация аккаунта — как это выглядит:

- 09:12 user@company.ru отправил 1 письмо
- 09:13 отправил 47 писем — аномалия!
- 09:13 ⚠ Лимит 50/час — ящик заблокирован
- 09:13 ✓ Уведомление → admin@company.ru
- 09:14 ✓ Поток остановлен. Репутация сохранена.

Лимит на ящик

50/час · 500/сутки

Лимит на домен

500/час · без огр.

DKIM

RSA-2048, fallback 1024

Антивирус исх.

ClamAV + Rspamd

Работает с любым почтовым сервером

Без изменения инфраструктуры



Microsoft Exchange

On-Premise и гибридные схемы



Office 365

Настройка за 10 минут



Яндекс Почта

Через MX-записи домена



Postfix / Exim

Любой Linux-сервер



Google Workspace

Маршрутизация через шлюз



Любой SMTP-сервер

Стандарт SMTP

Принцип подключения — смена MX-записи

Интернет
(входящая почта)



MX → Spamorez
(шлюз)



Фильтрация
< 1 сек



Ваш сервер
(чистая почта)

Ваш сервер не меняется. Очередь до 10 суток при недоступности сервера.

Надёжность и инфраструктура

Работает, даже когда ваш сервер недоступен

99,9%

гарантированный SLA

20 000

спам-ловушек

2 000+

доменов

5 000

вирусов/сутки

10 сут

очередь писем



Несколько датацентров

Москва · СПб · Новосибирск ·
Екатеринбург · Франкфурт.
Автобалансировка без потери писем



Очередь до 10 суток

Если ваш сервер недоступен —
письма ждут и доставляются
автоматически



Мониторинг 24/7

Инженеры следят за качеством
фильтрации непрерывно — в
выходные и праздники



Бэкап конфигурации

AES-256, ежедневно, хранение 30
дней. Для клиентов в ДЦ и On-
Premise

21

год на рынке

5 000+

компаний

3 млн

писем/сутки

99,9%

точность

Отказоустойчивый кластер узлов

Несколько шлюзов реплицируют данные друг другу в реальном времени — без единой точки отказа

1

Репликация в реальном времени

- Узлы обмениваются данными по собственному бинарному протоколу
- Без промежуточного HTTP и единой точки маршрутизации
- Каждая запись подтверждается перед следующей
- Работает поверх обычной сети между узлами

2

Автообнаружение кластера

- Одна пара узлов — и новый шлюз виден всему кластеру
- Не нужно вручную соединять каждый узел с каждым
- Новый узел получает полную историю данных при входе
- Проверка целостности данных при подключении

3

Работа при отказе узла

- Почта продолжает обрабатываться на других узлах
- Обновление одного узла не останавливает приём почты
- Очередь к отключённому узлу копится и досылается
- Полная история сохраняется на каждом узле

SMTP вход

→

Узел А принимает

→

Репликация на узел В, С

→

Применение записи

→

Единая история на всех узлах

↑ репликация каждой записи · подтверждение < 1 сек

SPZGate — продукт под вашим брендом

Whitelabel · Свой домен · Свой логотип · Партнёрская установка



Своё название везде в панели

Переменная окружения — без пересборки образа



Свой логотип и favicon

Подставляются автоматически при первом запуске



Свой домен для лицензирования

Без необходимости поднимать свой удостоверяющий центр



Свои языковые строки

Полная замена переводов, не только правки



Отдельный канал обновлений

Обновляется независимо, кастомизация сохраняется



Один архив — всё внутри

Лого, favicon, конфиги — в whitelabel.tar.gz

root@server:~

```
$ curl -fsSL https://<ваш-хост>/spzgate/clone.sh | sudo bash
```

✓ Собран whitelabel.tar.gz (лого, favicon, конфиги)

✓ Развёрнут базовый релиз SPZGate

✓ Whitelabel-контент установлен в custom/

↓ Сборка и запуск (6 контейнеров)

✓ Все сервисы запущены (6/6)

✓ SPZGate готов — под вашим брендом!

Откройте `http://<IP>` для настройки

Название

SERVICE_NAME

custom/

лого + конфиги

5 языков

из коробки

Что делает clone.sh: ① Заявка партнёра ② Собираем whitelabel.tar.gz ③ Базовый релиз SPZGate ④ Устанавливаем custom/ ⑤ Настраиваем cert-proxu ⑥ Запуск под вашим брендом

SPAMOREZ

Mail Security Platform

Ваша почта заполнена спамом? Мы это поправим.

 Облако SaaS

 SPZGate On-Premise

 Офлайн-установка

 5 датацентров

 Реестр РФ ПО

Начните сегодня. Первые 14 дней — бесплатно.

Настройка за 5 минут · Смена MX-записи · Без установки программ

spamorez.ru · sn@spamorez.net · ООО «Спаморез»

Exchange · Office 365 · Яндекс Почта · Postfix · Любой SMTP