?????????? KSMG ? KATA

????????

Kaspersky Secure Mail Gateway (KSMG) — защищает корпоративную почту от спама, фишинга, вредоносных вложений и целевых атак.
Kaspersky Anti Targeted Attack Platform (KATA) — обнаруживает и предотвращает целевые атаки, APT-угрозы и сложные инциденты в корпоративной инфраструктуре.

Интеграция этих решений позволяет:

- Передавать письма из KSMG на анализ в KATA.
- Получать вердикт от KATA и автоматически блокировать, помещать в карантин или помечать письма.
- Увеличить уровень защиты почтовой системы от сложных угроз.

???????????? ???????????

KSMG может быть настроен для работы с KATA в двух режимах:

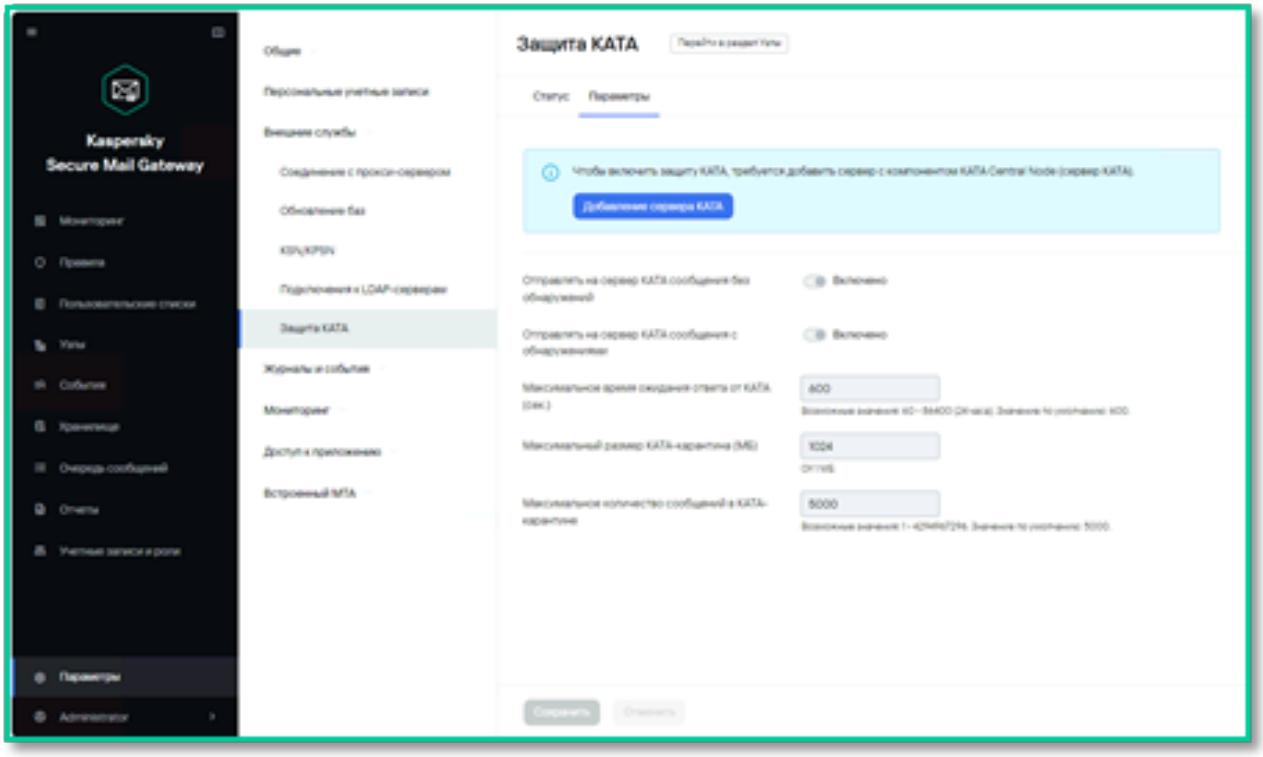
1. **Подключение к одному серверу KATA** — указывается IP/FQDN Central Node.
2. **Подключение к нескольким серверам с балансировкой** *(KATA 5.0+)* — автоматическое распределение нагрузки и переключение при отказе.

В этой статье разбираем **вариант с одним сервером**.

?????????? ?????????? ???????????

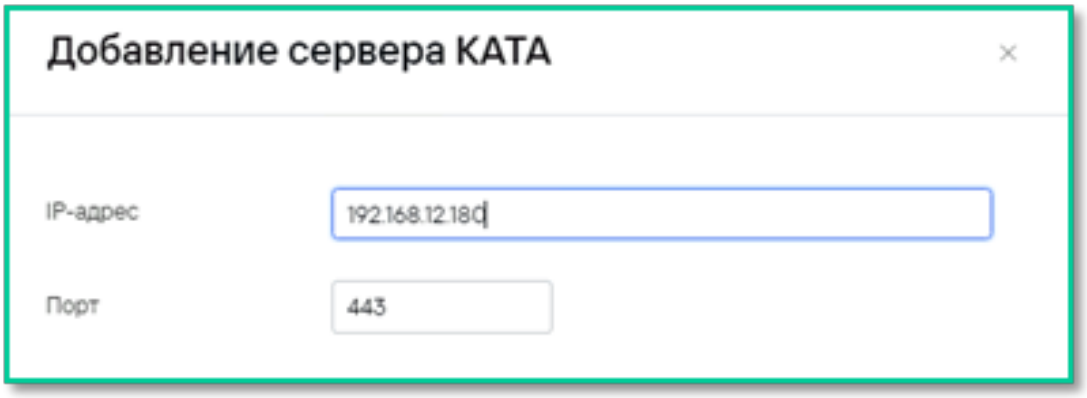
Шаг 1. Настройка KSMG

1. Войдите в веб-интерфейс KSMG.
2. Перейдите в: **Параметры → Внешние службы → Защита KATA**



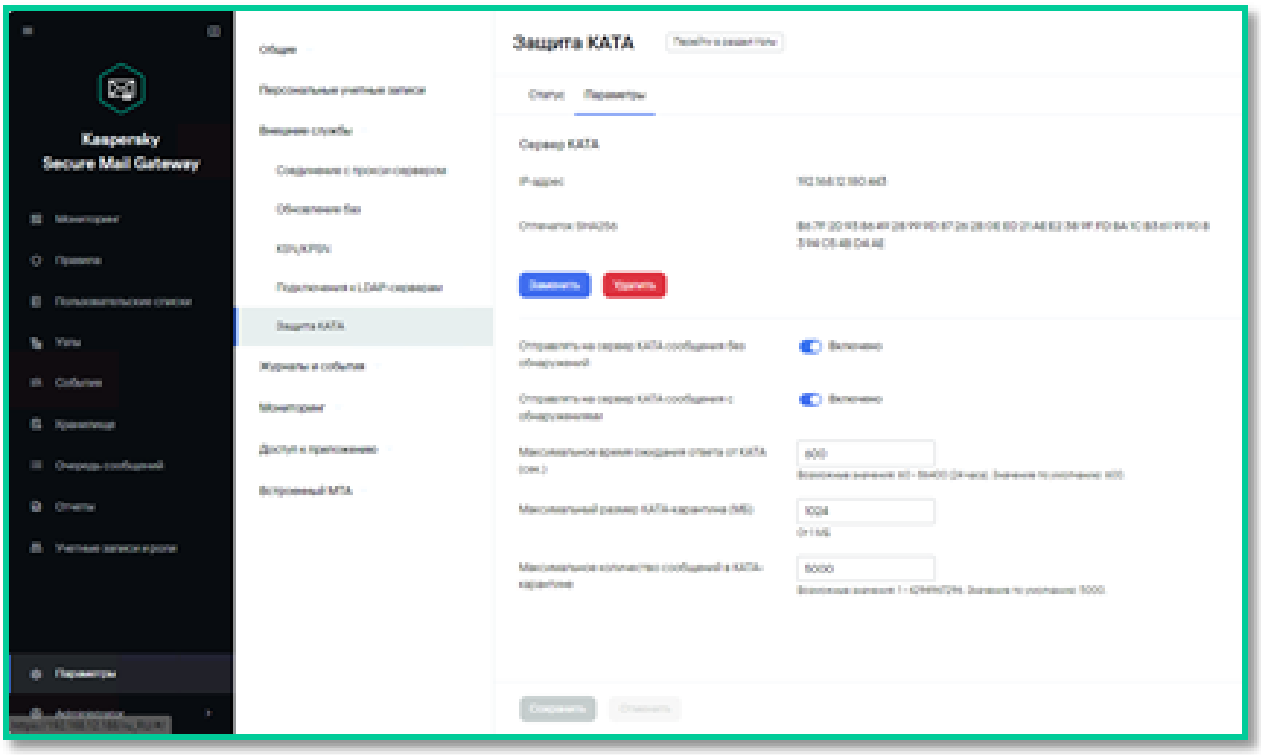
На скриншоте показан раздел, где настраивается подключение KATA.

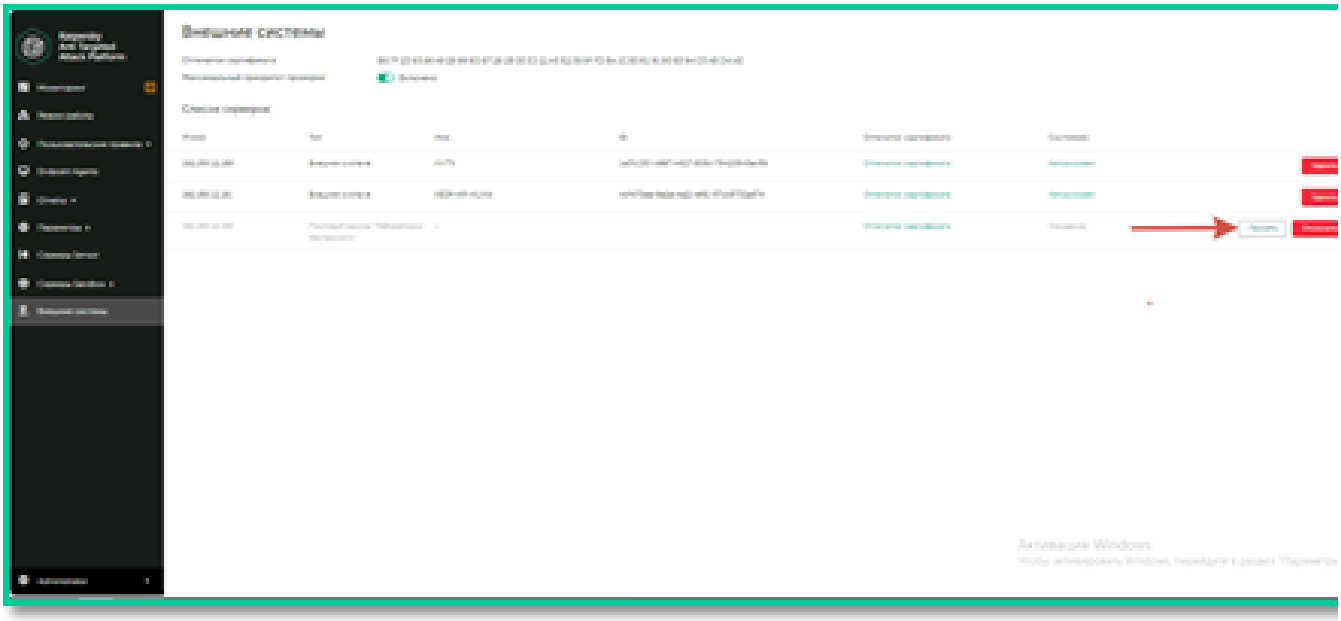
3. Нажмите **Добавить сервер KATA**.



В этом окне задаются IP/FQDN и порт подключения к KATA.

4. Введите:
   - **IP-адрес или FQDN** Central Node.
   - **Порт** (по умолчанию `443`).
5. Нажмите **Далее** — появится окно с сертификатом.





Проверьте отпечаток SHA256 и подтвердите.

6. Активируйте опции:
   - `Отправлять на сервер KATA сообщения без обнаружений` — для полной проверки.
   - `Отправлять на сервер KATA сообщения с обнаружениями` — для дополнительного анализа подозрительных писем.
7. Настройте лимиты:
   - **Время ожидания ответа**: `600 сек` (от 60 до 86400).
   - **Размер карантина**: `1024 МБ` (от 1 МБ).
   - **Максимум писем в карантине**: `5000` (от 1 до 4 294 967 296).
8. Сохраните изменения.

Шаг 2. Авторизация KSMG в KATA

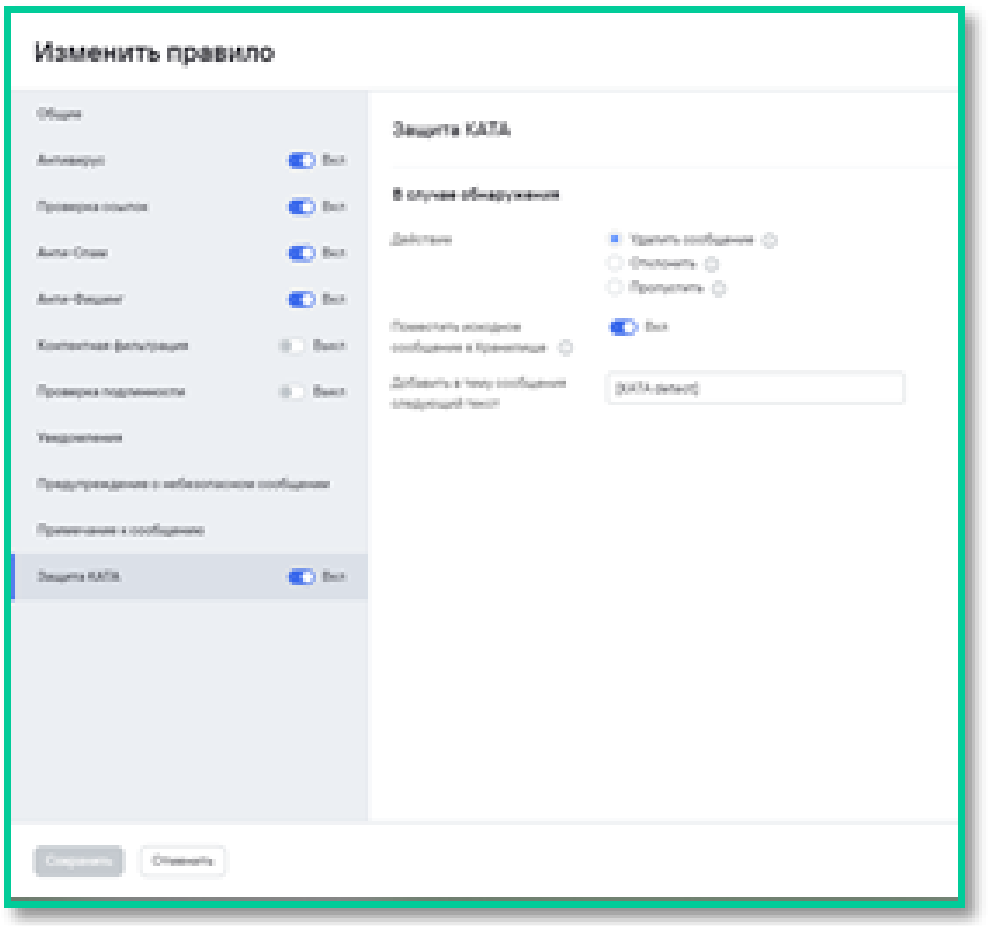
1. Войдите в веб-интерфейс **Central Node KATA**.
2. Перейдите в раздел **Внешние системы**.
3. Найдите KSMG и подтвердите запрос на авторизацию.

Внешние системы.png

После подтверждения статус изменится на «Авторизован».

Шаг 3. Настройка правил KSMG

1. Перейдите в раздел **Правила**.
2. Выберите нужное правило и нажмите **Изменить**.
3. Включите опцию **Защита KATA**.



Опция включает проверку всех писем по этому правилу в KATA.

4. Настройте действия: Удалить сообщение, Отклонить, Пропустить.
5. Сохраните правило.

???????? ??????????????????

1. Отправьте тестовое письмо (например, с EICAR-файлом).
2. Убедитесь, что:
   - Письмо отправилось на проверку в KATA.
   - В KATA появился вердикт.
   - KSMG выполнил заданное действие.

???????????

- Включайте **проверку всех писем** для максимальной защиты.
- Следите за заполнением карантина.
- При высокой нагрузке используйте **кластер KATA**.
- Периодически проверяйте журналы событий KSMG и KATA.
- Обновляйте версии ПО для получения актуальных алгоритмов анализа.

Revision #13
Created 13 August 2025 14:21:16 by Николай
Updated 6 February 2026 11:28:39 by Кирилл