?????????? ? ????????
???????? ??? ????????
????????? ?? ?????????
SMTP

Руководство по настройке KATA/NDR 7.1

> **Информация:** Приведенная на данной странице информация, является разработкой команды **pre-sales** и/или **AntiAPT Community** и **НЕ является** официальной рекомендацией вендора.

- **Версия решения:** 7.1
- **Тип инструкции:** Настройка источников данных SMTP

> **Важно!**
> Интеграция через SMTP позволяет **анализировать вложения из почтовых сообщений** в реальном времени с использованием трёх ключевых технологий:
> - **Anti-Malware Engine** — сигнатурный и эвристический анализ
> - **YARA-правила** — детектирование по шаблонам
> - **Sandbox** — динамический анализ поведения

Администратор настраивает почтовую систему (Microsoft Exchange) на отправку **скрытой копии (BCC)** всех сообщений на адрес в **служебном фиктивном домене** (например, `**sensor@kata.abc.corp**`). При этом **Central Node или Sensor** указывается в DNS как **почтовый сервер (MX)** для этого домена.

? Преимущества SMTP-интеграции:

- KATA получает письма **как почтовый сервер**, а не как клиент → **нет уведомлений о доставке/прочтении**

- Нет задержек, связанных с опросом (в отличие от POP3)
- Полный контроль над фильтрацией (внешние/внутренние письма, отправители и т.д.)

> ⚠ **Ограничения:**
> - Подходит **только для локальных (on-premises) почтовых систем**
> - **Не поддерживается в облачных службах** (Microsoft 365, Gmail и др.), где нельзя настроить MX для внутреннего домена и автоматическую пересылку BCC

1.1. Обязательные условия

Перед настройкой SMTP-интеграции убедитесь, что:

- ☐ Установлена и настроена **Central Node** или выделенный **Sensor**
- ☐ Активирована лицензия **KATA** или **KATA/NDR**
- ☐ Добавлен **дополнительный сетевой интерфейс** (кроме Management), находящийся в состоянии **«Не инициализирован»**
- ☐ Настроена сетевая связность между Exchange и KATA по **TCP-порту 25**
- ☐ Есть доступ к **Exchange Admin Center (EAC)** или **Exchange Management Shell** с правами администратора

---

1. Подготовка

1.1. Лицензии и функциональность

Лицензия	Требуется для
KATA	Анализ почтового трафика, проверка вложений по **Anti-Malware**, **YARA**, **Sandbox**
NDR	Не требуется для SMTP-интеграции
KATA/NDR	Полный функционал: периметр + внутренняя сеть

□□KATA

- Принимает копии писем по SMTP
- Анализирует вложения **тремя независимыми технологиями**
- Фиксирует угрозы в разделе **«Угрозы → События»**
- Поддерживает интеграцию с Exchange, Postfix, Cisco ESA и др. (при наличии управления маршрутизацией)

> ⚠**ВАЖНО:**
> Без лицензии **KATA** функционал анализа **недоступен**, даже если письма поступают на SMTP-точку.

> “ **Рекомендация:**
> Используйте служебный домен (`**katasmtp.corp**`) **только внутри сети** — не публикуйте его во внешнем DNS.

1.2. Сетевые требования

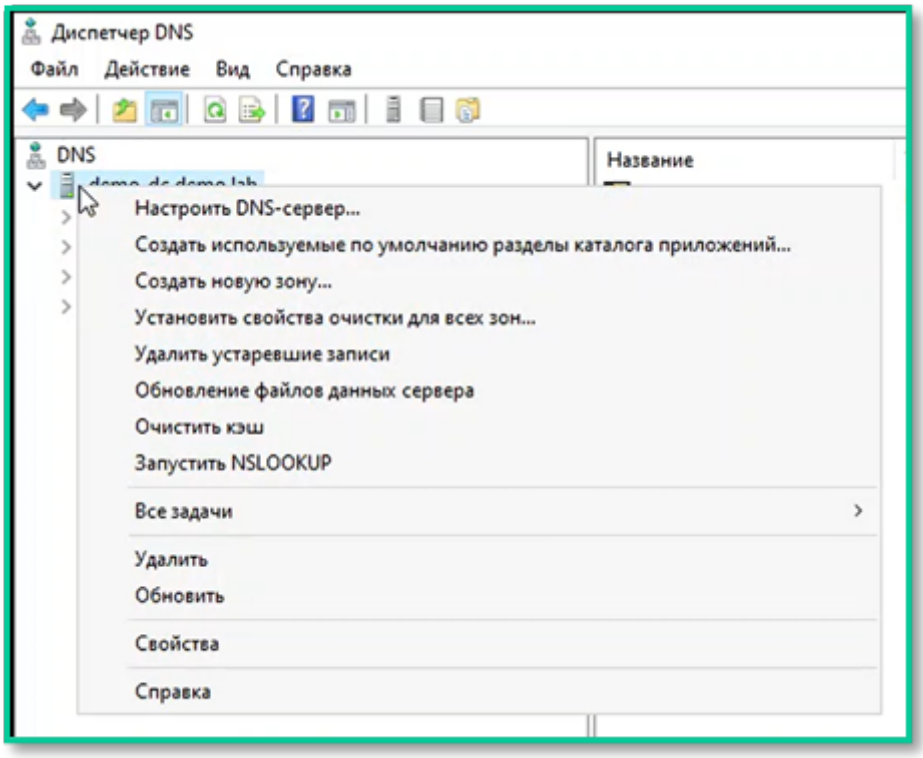
- Для приёма SMTP-трафика используется management-интерфейс.
- Exchange должен иметь возможность **напрямую подключаться** к KATA по **TCP-порту 25**.
- Внутренний DNS должен содержать **MX-запись** для служебного домена, указывающую на **IP KATA**.

> i**Примечание:**
> SMTP-интеграция **не требует зеркалирования трафика** — почтовый сервер **активно отправляет** копии писем на обработку.

1.3. Настройка DNS сервера

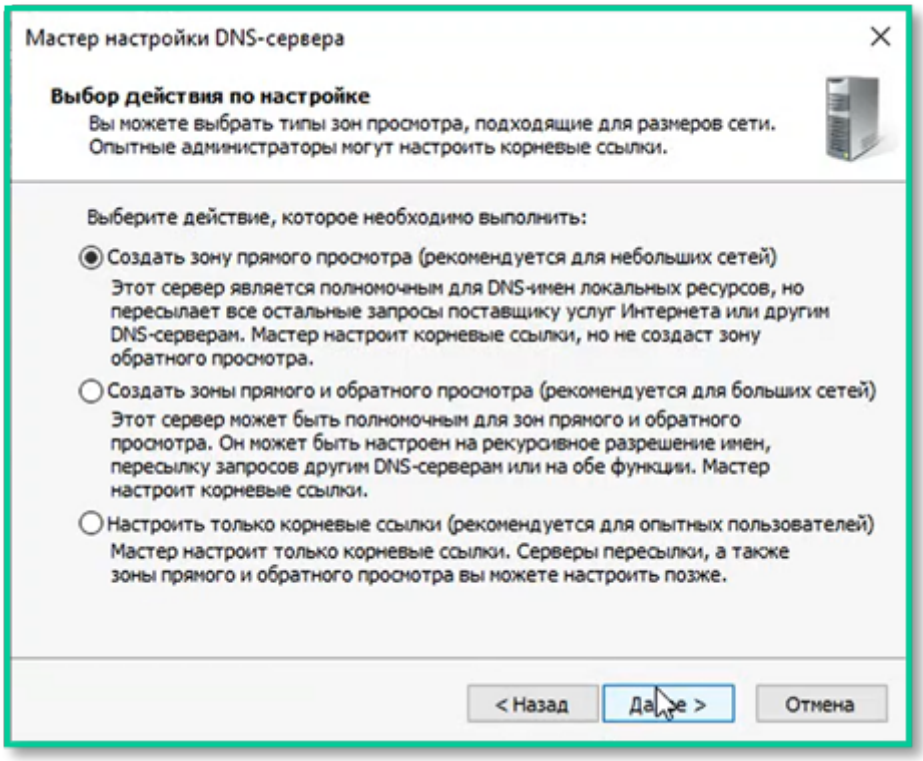
Чтобы создать дополнительную зону на DNS-сервере, выполните следующие шаги на внутреннем DNS-сервере:

1. Откройте настройки DNS-сервера. Щелкните правой кнопкой мыши по вашему серверу и выберите «Настроить DNS-сервер», чтобы запустить мастер настройки.



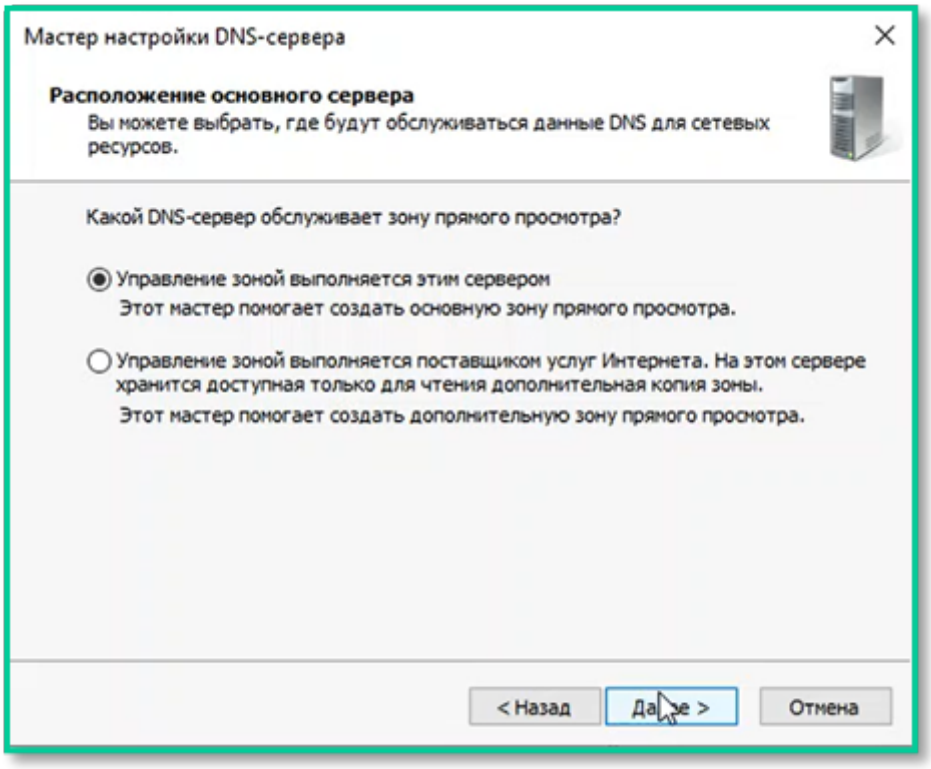
Скриншот 1: Поле примера вызова

2. Выберите "**Создать зону прямого просмотра**".



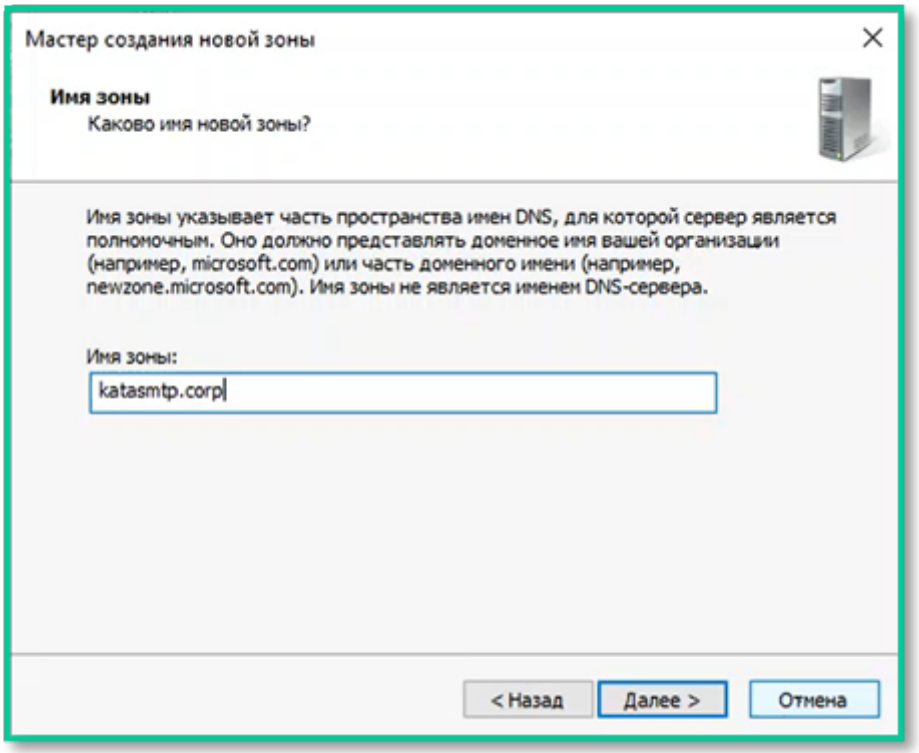
Скриншот 2: Поле примера вызова

3. Выберите какой DNS-сервер обслуживает данную зону:



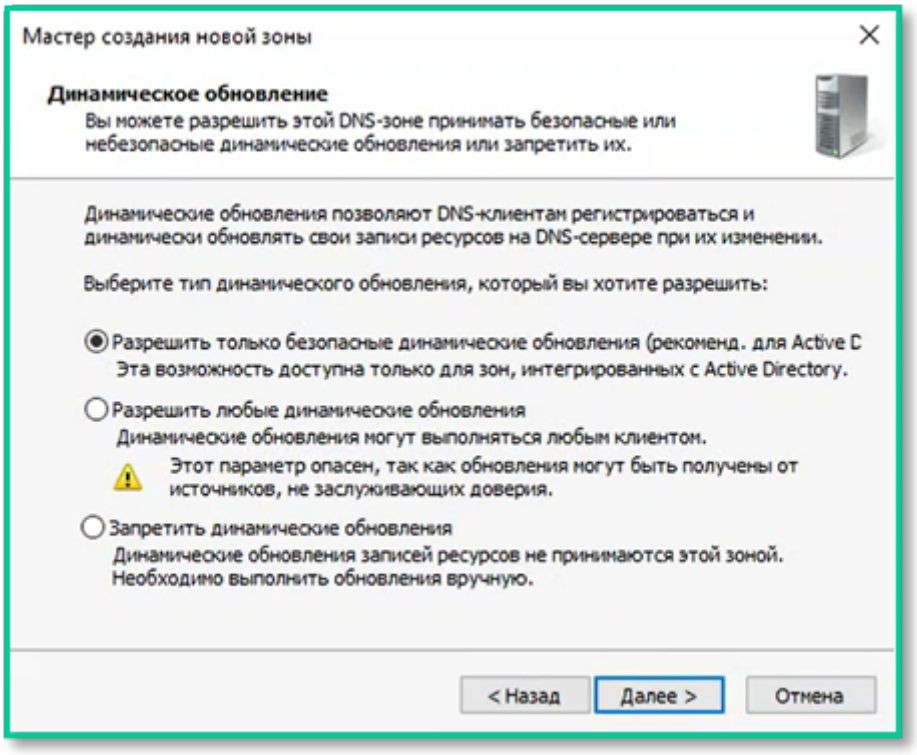
Скриншот 3: Поле примера вызова

4. Укажите имя новой зоны, например: '**katasmtp.corp**'.



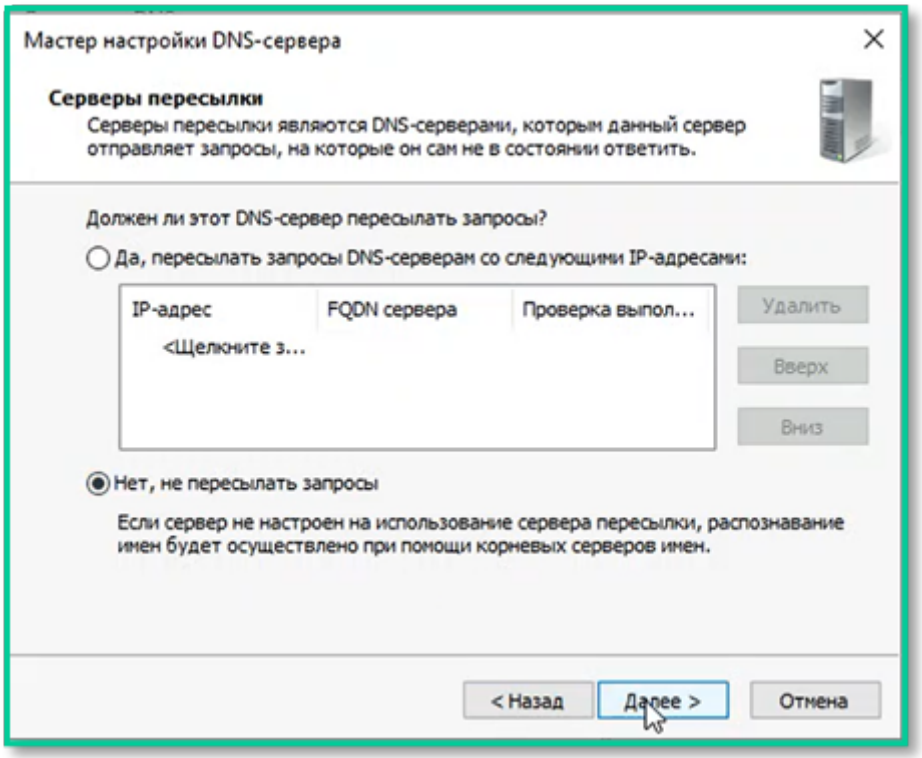
Скриншот 4: Поле примера вызова

5. Выбираем тип обновления.



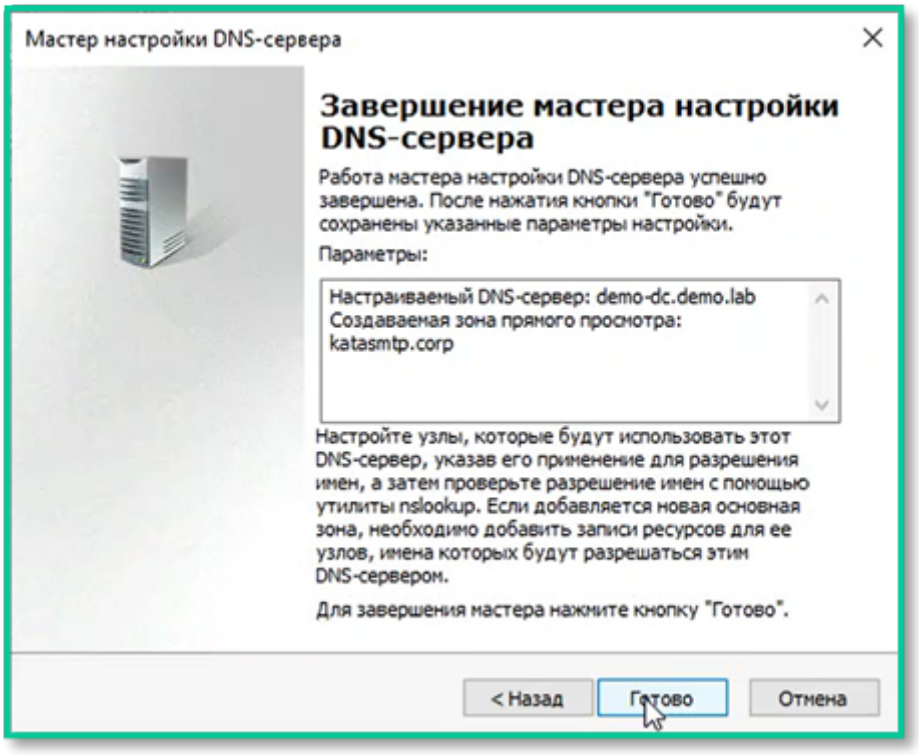
Скриншот 5: Поле примера вызова

6. Убираем сервер пересылки.



Скриншот 6: Поле примера вызова

7. Завершаем мастер настройки DNS-сервера.

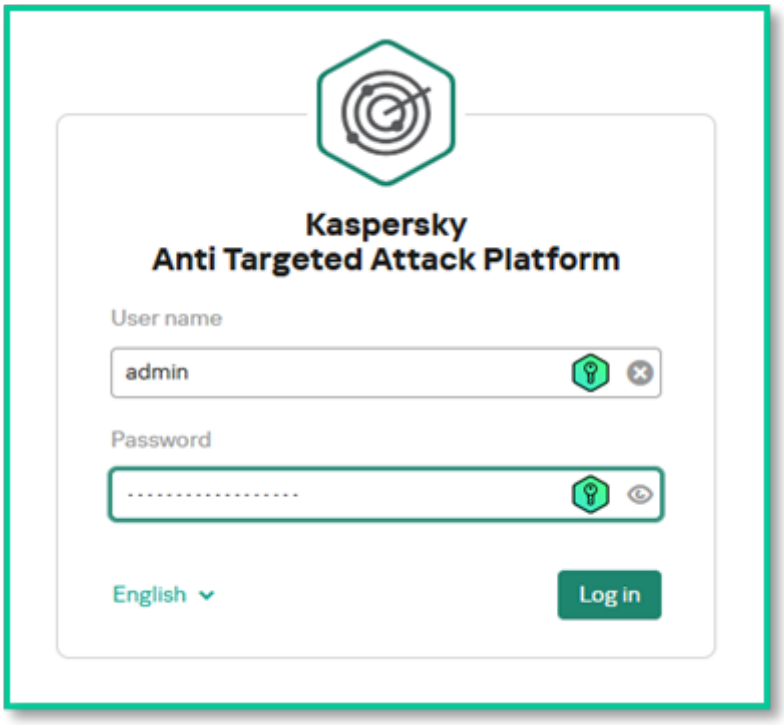


Скриншот 7: Поле примера вызова

2. Настройка на стороне KATA

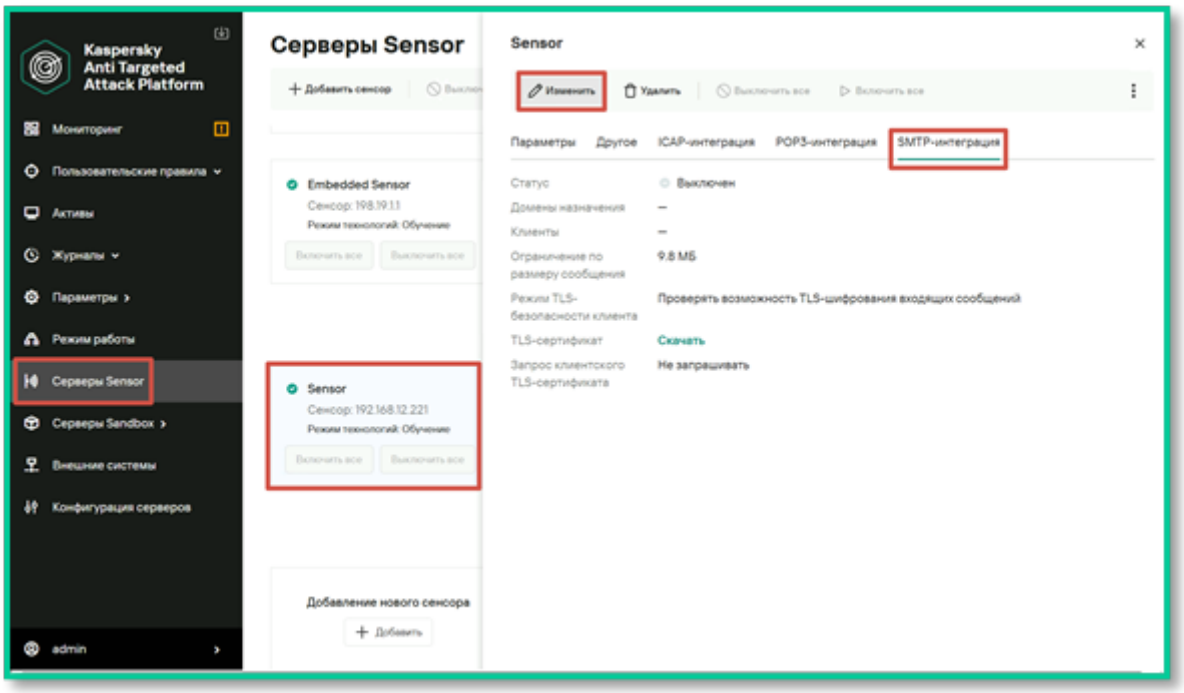
2.1. Включение SMTP-интеграции

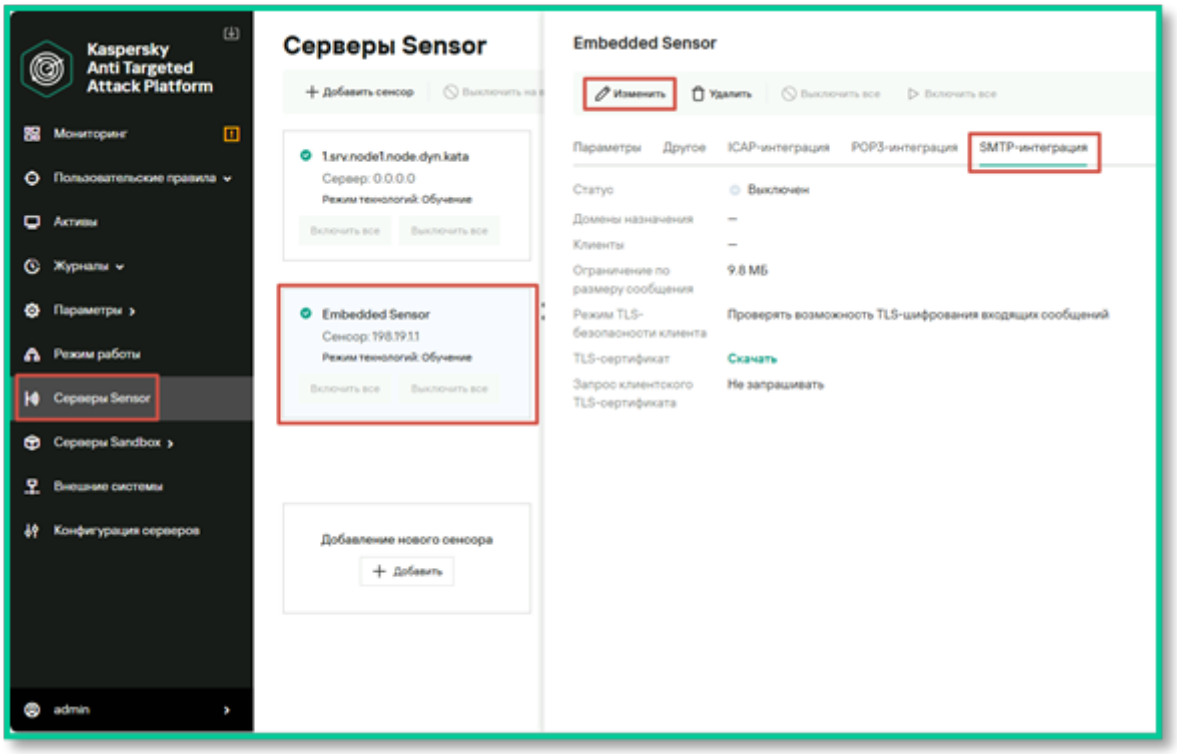
1. Войдите в веб-интерфейс Central Node под учётной записью `**admin**`.



Скриншот 8: Экран входа в KATA

2. Перейдите: **Серверы Sensor**.

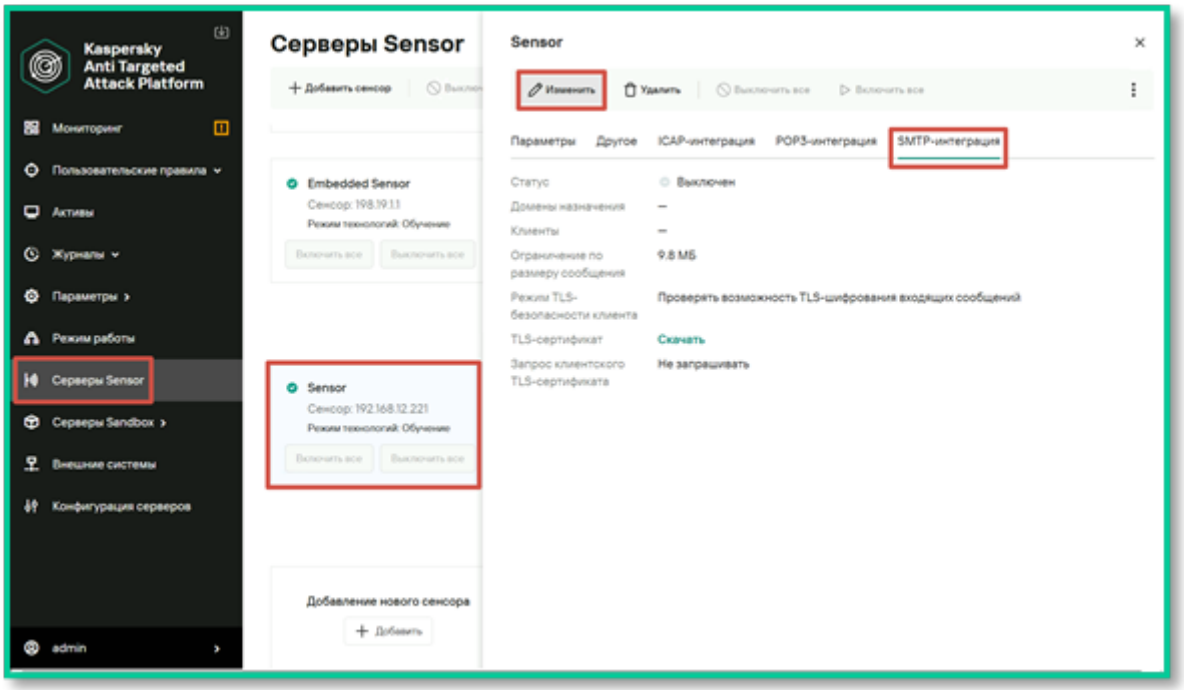




Скриншот 9: Список сенсоров (включая «**Embedded Sensor**»)

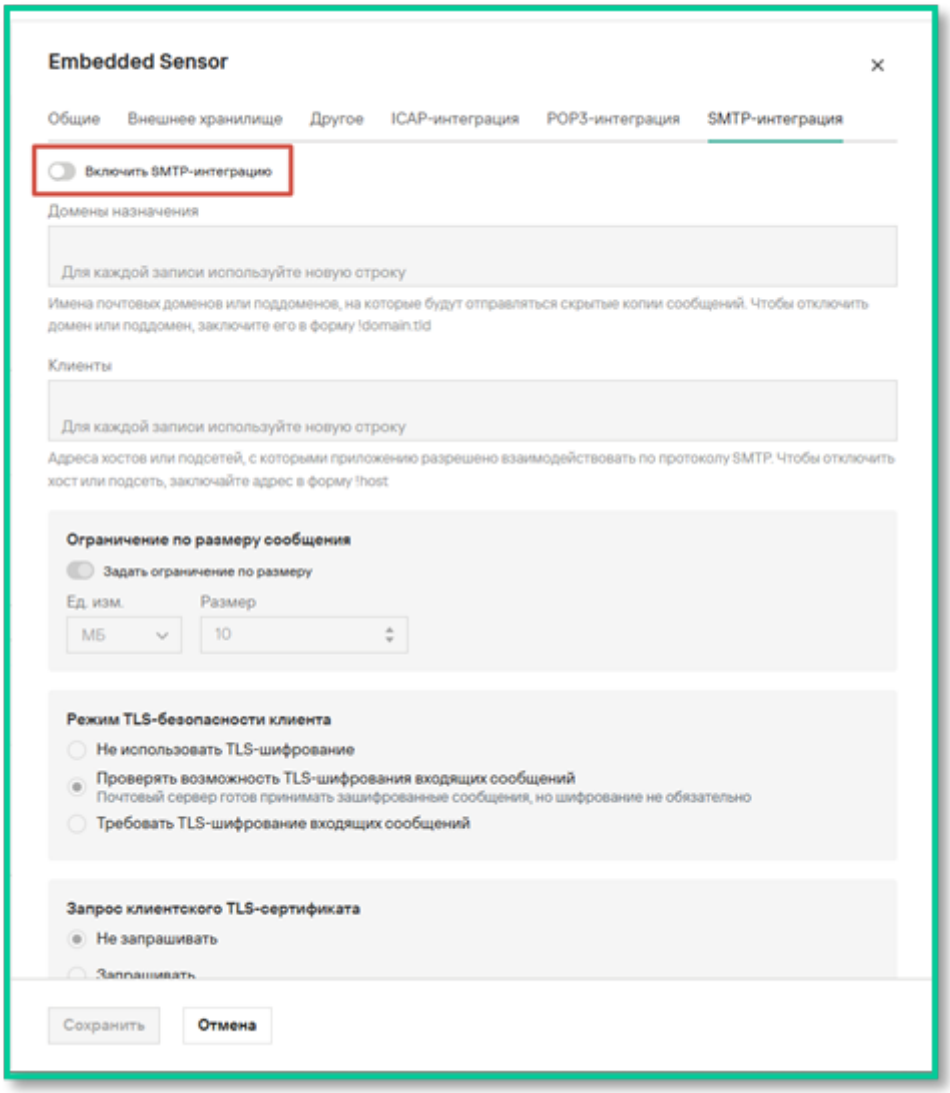
3. Нажмите **«Изменить»** напротив нужного Sensor (обычно — **Embedded Sensor**).

4. Перейдите на вкладку **«SMTP-интеграция»**.



Скриншот 10: Вкладка «SMTP-интеграция» с переключателем

5. Переведите параметр **«SMTP-интеграция»** в состояние **«Включено»**.



Скриншот 11: Вкладка «SMTP-интеграция»

2.2. Настройка доменов назначения

> ⚠**Обязательный шаг!**
> Без этого KATA **не примет письма**.

6. В том же разделе **«SMTP-интеграция»** найдите поле:

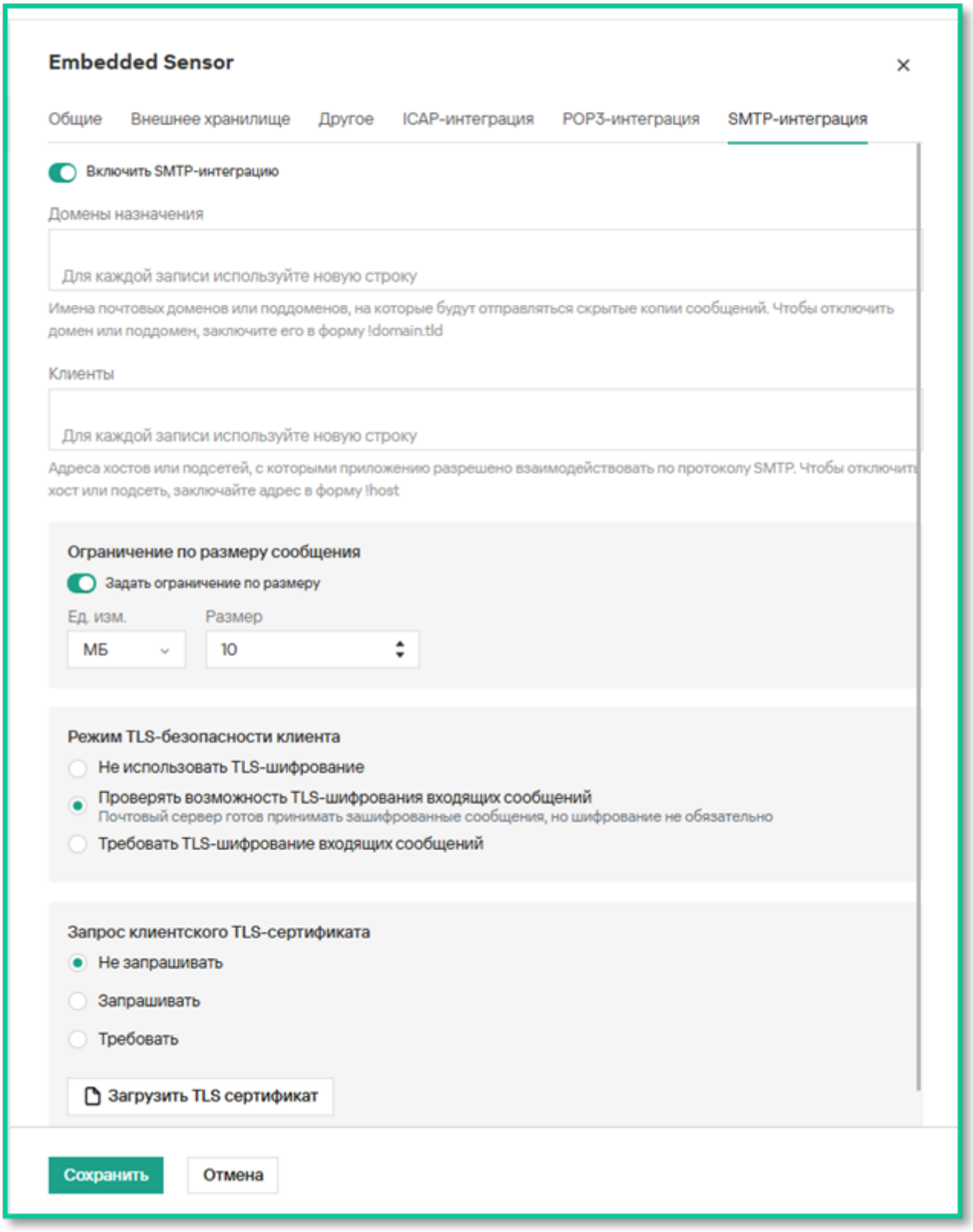
«Домены назначения»

7. Укажите служебный домен, например:

katasmtp.corp

> Можно указать несколько доменов — по одному на строку.

8. Нажмите **«Применить»**.



Скриншот 12: Поле «Домены назначения» с введённым `**kata.abc.corp**`

После этого KATA:

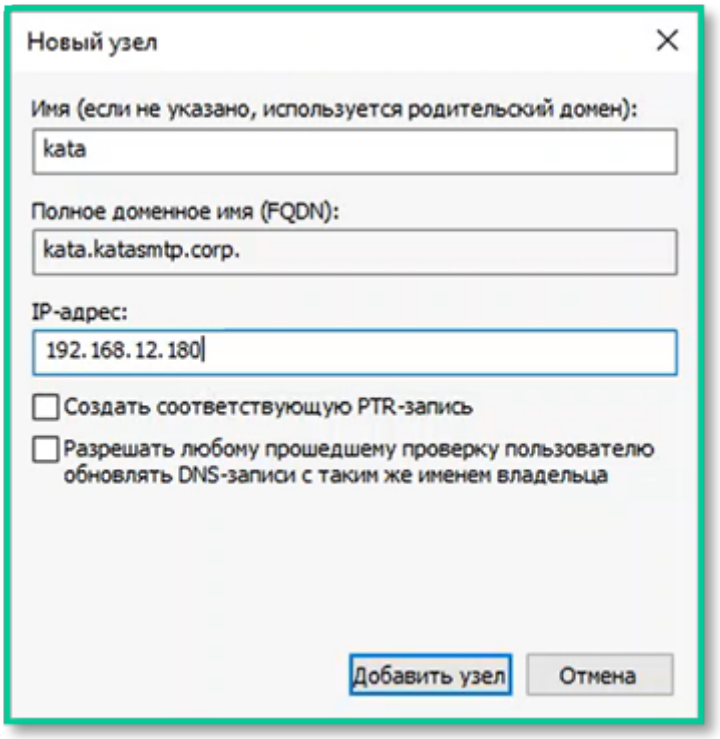
- Активирует встроенный SMTP-сервер на порту **25**
- Примет письма **только на указанные домены**
- Начнёт анализировать вложения по **Anti-Malware**, **YARA**, **Sandbox**

3. Настройка на стороне Microsoft Exchange

3.1. Регистрация A-записи в DNS

1. В ранее созданной дополнительной зоне внутреннего DNS-сервера создайте запись типа **A**.

- **Имя:** kata
- **Домен**: `kata.katasmtp.corp`
- **Целевой хост**: IP-адрес интерфейса KATA

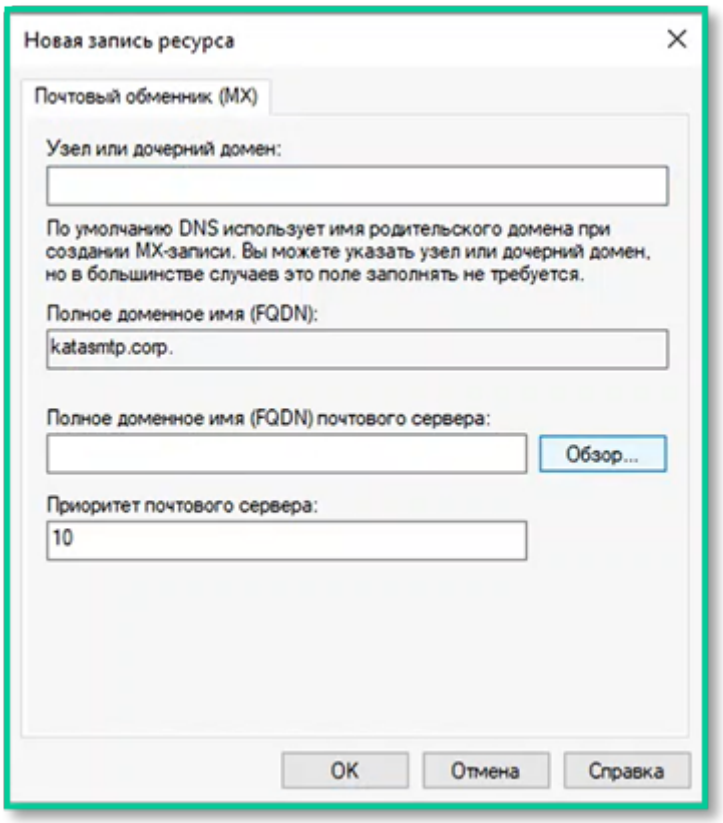


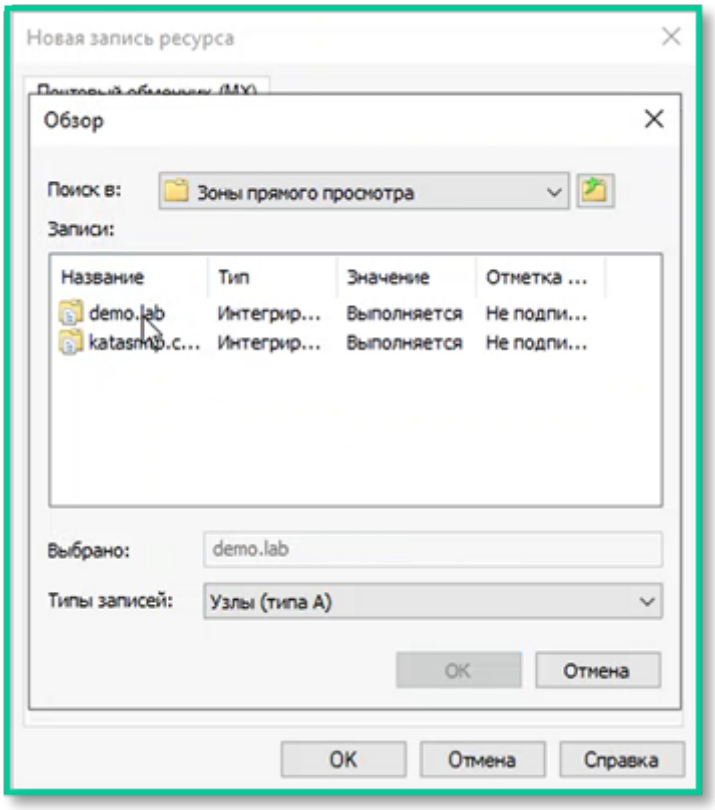
Скриншот 13: DNS-запись A

3.2. Регистрация MX-записи в DNS

1. Внутренний DNS-сервер: создайте запись типа **MX**

- **Домен**: `kata.abc.corp`
- **Приоритет**: `10`
- **Целевой хост**: IP-адрес интерфейса KATA





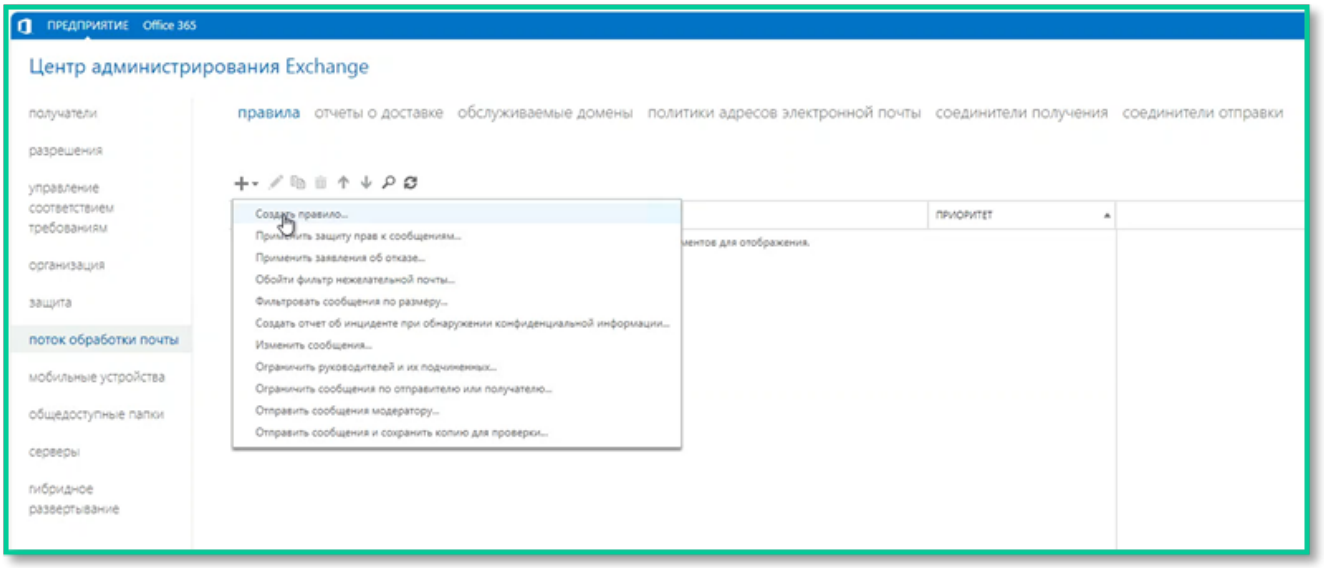
□□ **Скриншот 14:** DNS-запись **MX**

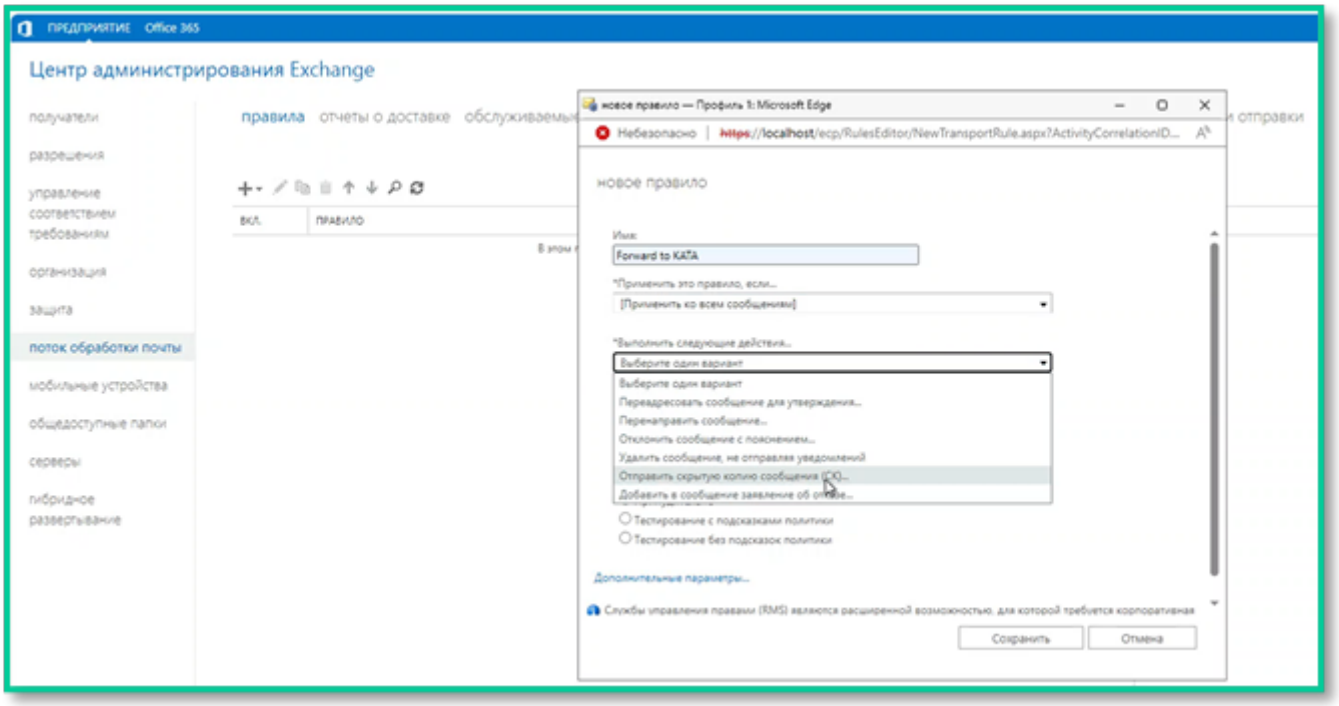
3.3. Создание правила BCC

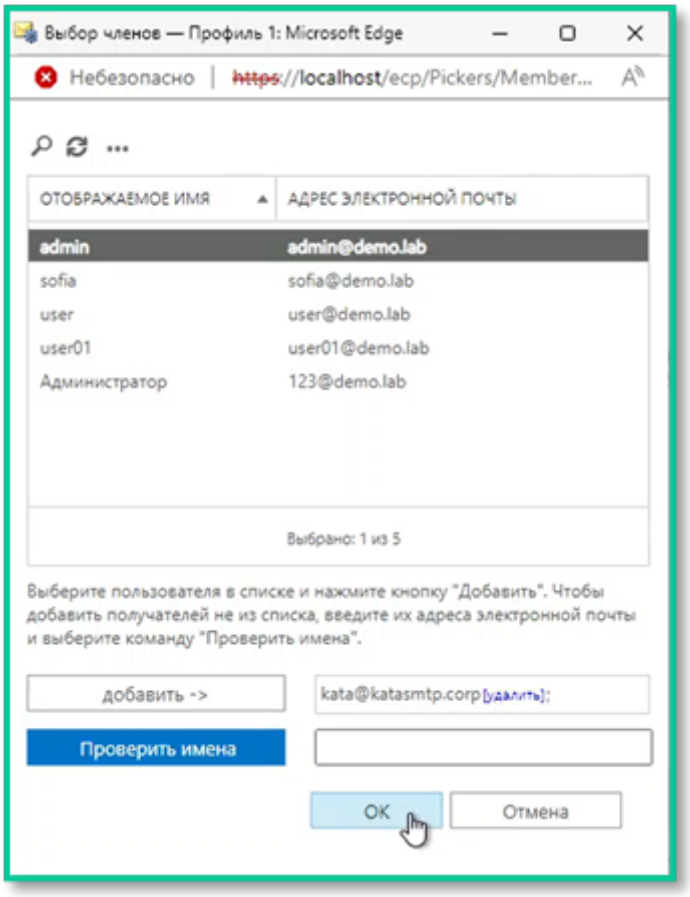
1. В **Exchange Admin Center → Mail flow → Rules →+ Create a new rule**

2. Укажите:

- **Имя:** `Send BCC to KATA`
- **Условие:** `The recipient is located...` → `Outside the organization`
- *(или `Any recipient` — по политике)*
- **Действие:** `Blind carbon copy (BCC) the message to...` → `sensor@kata.abc.corp`


ПРЕДПРИЯТИЕ Office 365
Центр администрирования Exchange
получатели
разрешения
управление соответствием требованиям
организация
защита
поток обработки почты
мобильные устройства
общедоступные папки
серверы
гибридное развертывание
правила
отчеты о доставке
обслуживаемые домены
политики адресов электронной почты
соединители получения
соединители отправки
Создать правило...
Применить защиту прав к сообщениям...
Применить заявления об отказе...
Обойти фильтр нежелательной почты...
Фильтровать сообщения по размеру...
Создать отчет об инциденте при обнаружении конфиденциальной информации...
Изменить сообщения...
Ограничить руководителей и их подчиненных...
Ограничить сообщения по отправителю или получателю...
Отправить сообщения модератору...
Отправить сообщения и сохранить копию для проверки...
ПРИОРИТЕТ


ПРЕДПРИЯТИЕ Office 365
Центр администрирования Exchange
получатели
разрешения
управление соответствием требованиям
организация
защита
поток обработки почты
мобильные устройства
общедоступные папки
серверы
гибридное развертывание
правила
ВКЛ.
ПРАВИЛО
новое правило — Профиль 1: Microsoft Edge
Небезопасно
https://localhost/ecp/RulesEditor/NewTransportRule.aspx?ActivityCorrelationID...
новое правило
Имя:
Forward to KATA
*Применить это правило, если...
[Применить ко всем сообщениям]
*Выполнить следующие действия...
Выберите один вариант
Выберите один вариант
Перенаправить сообщение...
Отклонить сообщение с пояснением...
Удалить сообщение, не отправляя уведомлений
Тестирование с подсказками политики
Тестирование без подсказок политики
Дополнительные параметры...
Службы управления правами (RMS) являются расширенной возможностью, для которой требуется корпоративная
Сохранить
Отмена



Скриншот 15: Правило BCC

3.3. Настройка исходящего коннектора

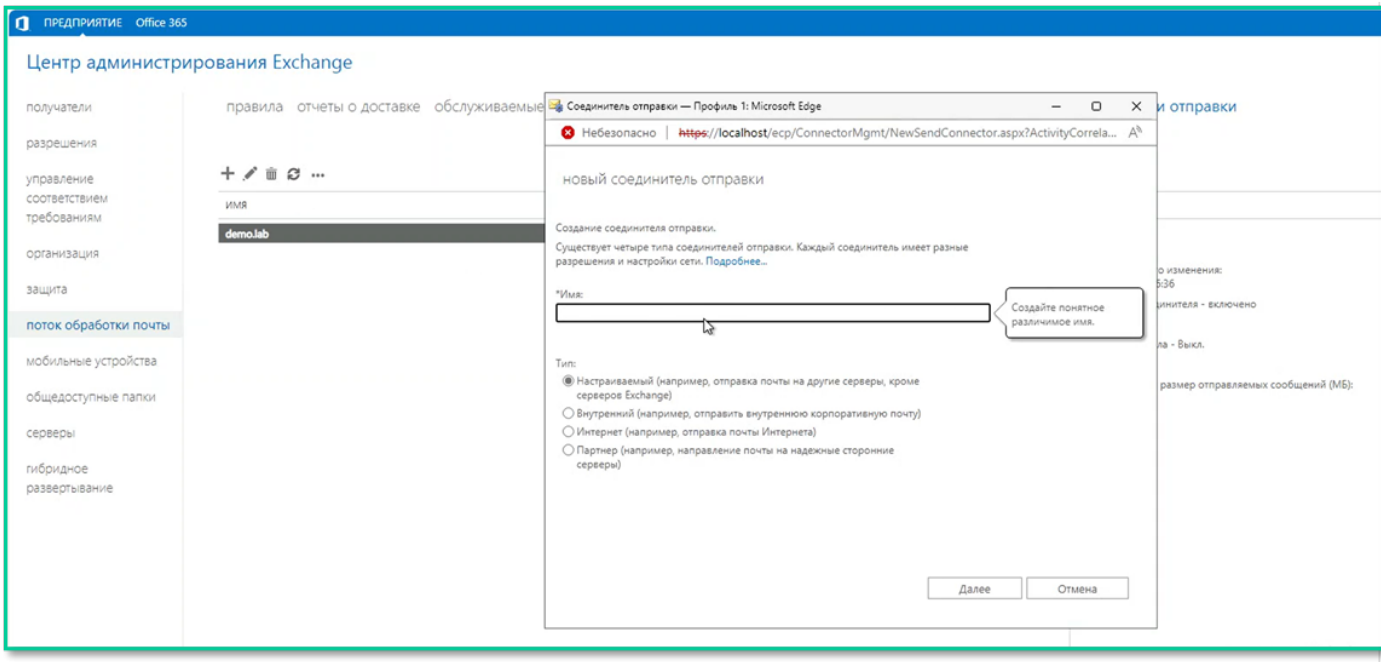
1. **Перейдите:** Mail flow → Send connectors → + Create

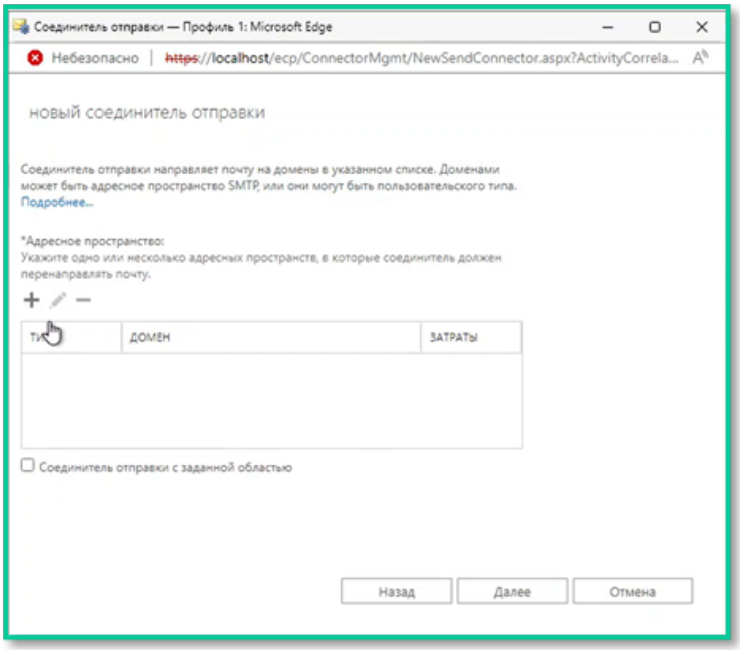
2. **Укажите:**

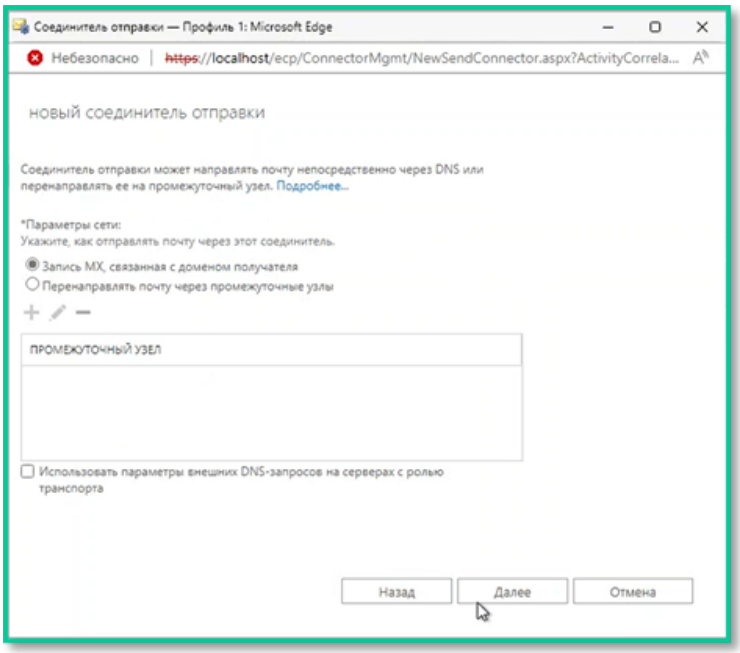
   - **Имя:** `KATA SMTP Connector`
   - **Тип:** Custom

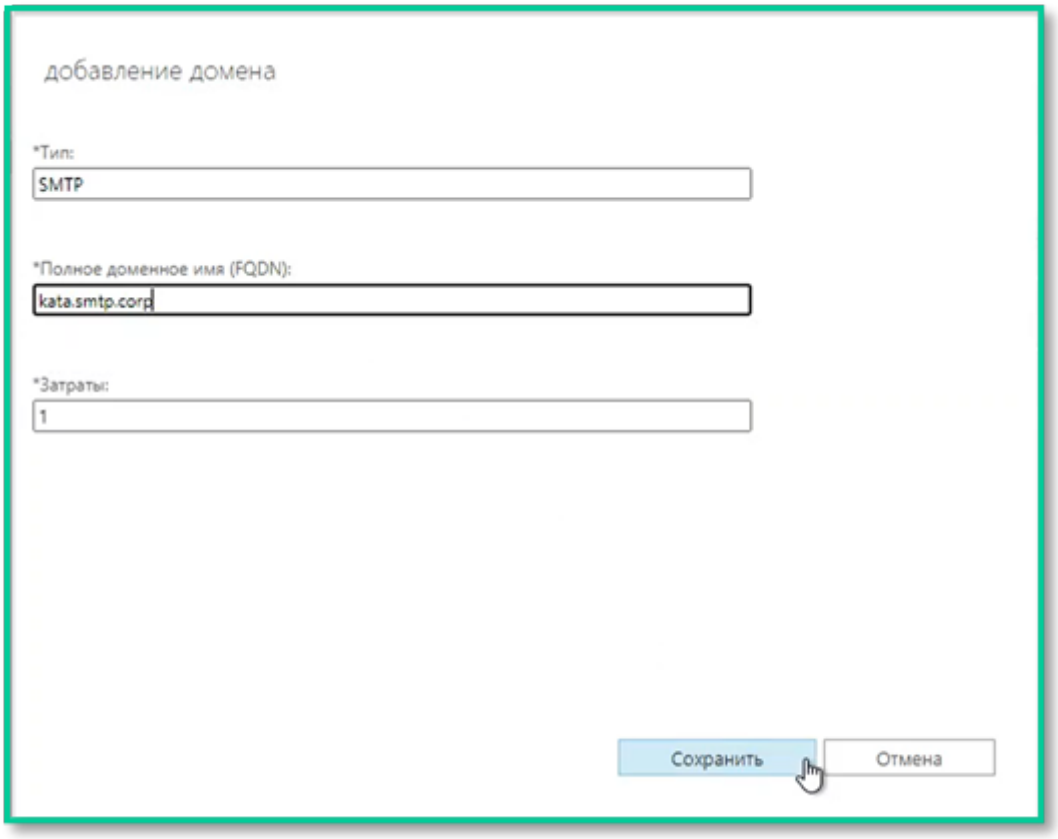
3. На шаге **Address space**:

   - Нажмите **+**
   - **Тип:** `SMTP`
   - **Домен:** `kata.abc.corp`
   - **Cost:** `1`


ПРЕДПРИЯТИЕ Office 365
Центр администрирования Exchange
получатели
разрешения
управление соответствием требованиям
организация
защита
поток обработки почты
мобильные устройства
общедоступные папки
серверы
гибридное развертывание
правила
отчеты о доставке
обслуживаемые
и отправки
имя
demo.lab
Соединитель отправки — Профиль 1: Microsoft Edge
Небезопасно | https://localhost/ecp/ConnectorMgmt/NewSendConnector.aspx?ActivityCorrela...
новый соединитель отправки
Создание соединителя отправки.
Существует четыре типа соединителей отправки. Каждый соединитель имеет разные разрешения и настройки сети. Подробнее...
*Имя:
Создайте понятное различимое имя.
Тип:
Настраиваемый (например, отправка почты на другие серверы, кроме серверов Exchange)
Внутренний (например, отправить внутреннюю корпоративную почту)
Интернет (например, отправка почты Интернета)
Партнер (например, направление почты на надежные сторонние серверы)
Далее
Отмена

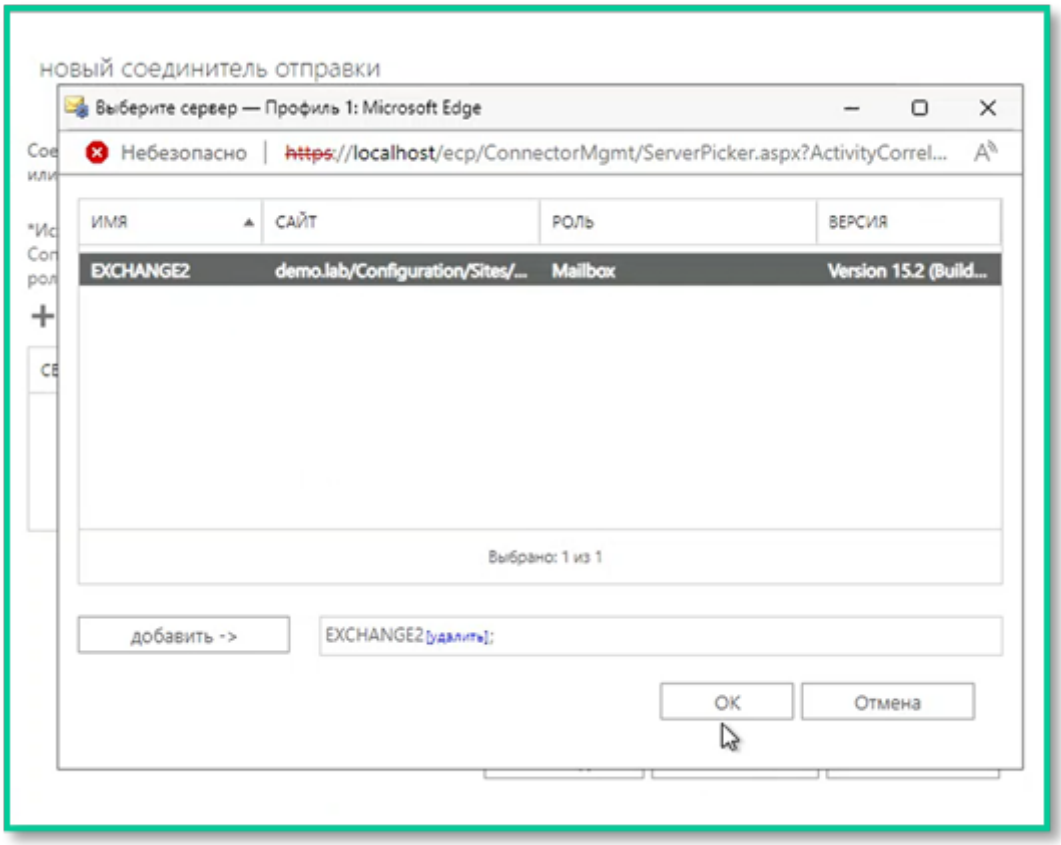

Соединитель отправки — Профиль 1: Microsoft Edge
Небезопасно | https://localhost/ecp/ConnectorMgmt/NewSendConnector.aspx?ActivityCorrela...
новый соединитель отправки
Соединитель отправки направляет почту на домены в указанном списке. Доменами может быть адресное пространство SMTP, или они могут быть пользовательского типа.
Подробнее...
*Адресное пространство:
Укажите одно или несколько адресных пространств, в которые соединитель должен перенаправлять почту.
ТИП
ДОМЕН
ЗАТРАТЫ
Соединитель отправки с заданной областью
Назад
Далее
Отмена


Соединитель отправки — Профиль 1: Microsoft Edge
Небезопасно | https://localhost/ecp/ConnectorMgmt/NewSendConnector.aspx?ActivityCorrela...
новый соединитель отправки
Соединитель отправки может направлять почту непосредственно через DNS или перенаправлять ее на промежуточный узел. Подробнее...
*Параметры сети:
Укажите, как отправлять почту через этот соединитель.
Запись MX, связанная с доменом получателя
Перенаправлять почту через промежуточные узлы
ПРОМЕЖУТОЧНЫЙ УЗЕЛ
Использовать параметры внешних DNS-запросов на серверах с ролью транспорта
Назад
Далее
Отмена



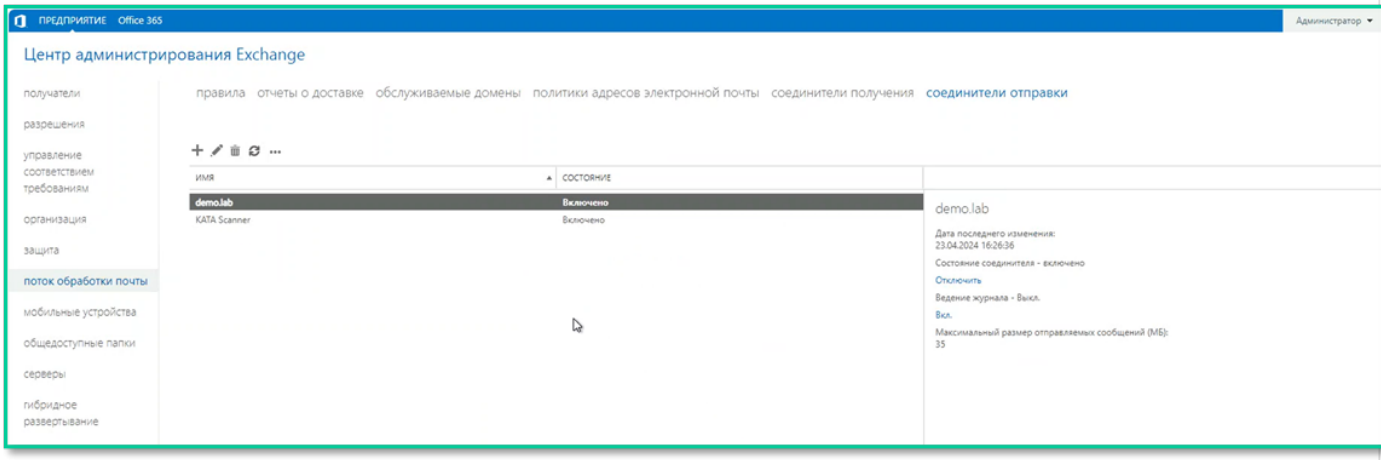
Скриншот 16: Address space

4. На шаге **Source server** выберите ваш Exchange Server



Скриншот 17: Выбор сервера

5. На всех остальных шагах оставьте **настройки по умолчанию**



Скриншот 18: Шаг с параметрами по умолчанию

4. Проверка работы

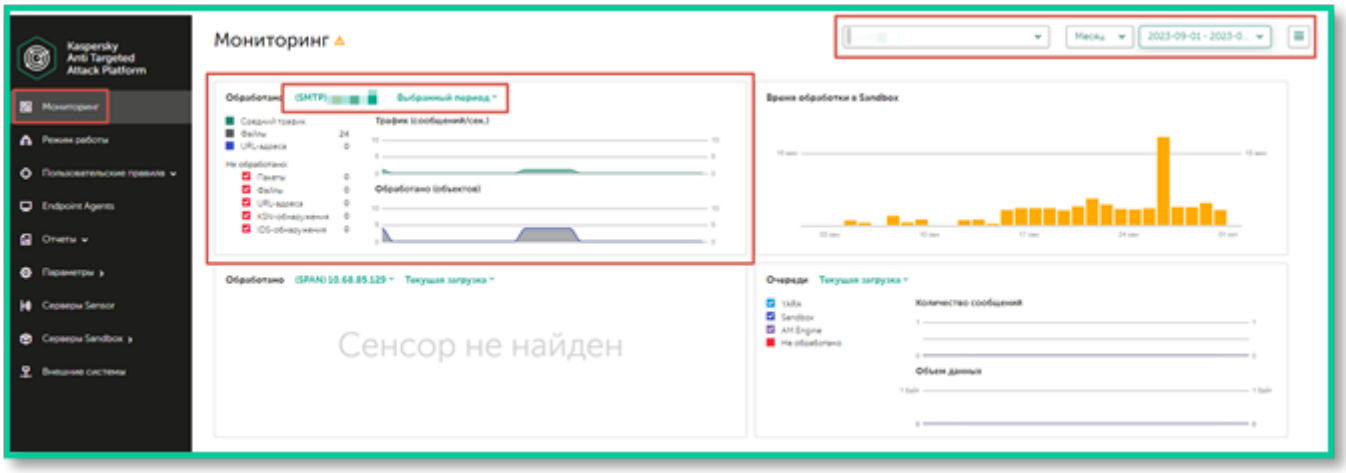
4.1. Проверка поступления писем

1. Перейдите: **Мониторинг → Обработано**

2. Выберите источник: **SMTP**

3. Укажите тип отображения:

- **Текущая загрузка**
- **Выбранный период** (настраивается в правом верхнем углу)



Скриншот 19: График нагрузки по SMTP-трафику

> Если письма поступают — вы увидите график.

4.2. Просмотр результатов анализа

1. Перейдите под учётной записью **«Офицер безопасности»**

2. Откройте: **Угрозы → События**

3. В колонке **«Технология детектирования»** вы увидите:

- **Anti-Malware**
- **YARA**
- **Sandbox**

> Объект может быть детектирован **одной или несколькими** технологиями.

Данные отображаются **только под ролью «Офицер безопасности»**.

Полезные ссылки

- Официальная документация KATA 7.1
- SMTP-интеграция
- Kaspersky Tech на YouTube
- Kaspersky на Rutube

? Настройка SMTP-интеграции с Microsoft Exchange завершена!

Теперь KATA:

- Принимает копии писем как почтовый сервер
- Анализирует вложения **тремя технологиями**: Anti-Malware, YARA, Sandbox
- Фиксирует угрозы в реальном времени
- Готов к расследованию инцидентов, связанных с почтовыми атаками

Revision #16
Created 18 November 2025 13:46:29 by Николай
Updated 6 February 2026 11:30:32 by Кирилл