Как настроить ГОСТ TLS шифрование

Инструкция для администраторов

© VK WorkSpace, 2026 г. Все права защищены

Портал с документацией: https://biz.mail.ru/docs/on-premises/

Оглавление

Термины и определения

ГОСТ TLS — реализация международного протокола TLS (Transport Layer Security), которая использует российские криптографические стандарты: ГОСТ Р 34.12-2015 (шифрование) и ГОСТ Р 34.10-2012 (электронные подписи), для обеспечения безопасного соединения.

AS (Автономная система) — группа IP-сетей и маршрутизаторов под единым управлением, имеющая свою политику маршрутизации и уникальный номер (ASN).

КриптоПро — средство криптографической защиты информации (СКЗИ).

PFX-контейнер — бинарный контейнер для хранения криптографических данных, в первую очередь для SSL/TLS-сертификатов и электронных подписей.

Дополнительная документация

Настройка ГОСТ TLS-шифрования на сервере Мессенджера и ВКС — в инструкции описано, как включить и выключить ГОСТ TLS-шифрование на сервере Мессенджера и ВКС.

Назначение документа

В инструкции описано, как включить и выключить ГОСТ TLS-шифрование на сервере Почты VK WorkSpace. ГОСТ Настройка TLS-шифрования обеспечивает поддержку российских криптографических стандартов для шифрования трафика между клиентскими приложениями Супераппа VK WorkSpace.

Предварительные действия

> ⚠ **Внимание**
>
> После настройки ГОС TLS-шифрования вы не сможете делать бэкапы через BMWCLIENT и пользоваться редактором «Мой офис».

- До настройки ГОСТ TLS-шифрования приобретите лицензию на право использования СКЗИ «КриптоПро CSP» версии 5.0 для одного TLS-сервера. Лицензия позволяет осуществлять подключение к серверу по зашифрованному протоколу. Лицензионный ключ понадобится вам на шаге 3.

- Настройка ГОСТ TLS-шифрования доступна начиная с версии Почты VK WorkSpace 25.4 и выше. Обновите инсталляцию на одну виртуальную машину по инструкции: Инструкция по установке обновлений Почты на одну машину. Если у вас распределенная инсталляция, то по инструкции: Инструкция по обновлению кластера Почты.
- Приобретите сертификат ГОСТ TLS у подходящего удостоверяющего центра, который покрывает поддомены Почты VK WorkSpace. Полный перечень доменов указан в веб-интерфейсе установщика или в документе по установке Почты. Рекомендуется выпустить wildcard-сертификаты по аналогии с инструкцией Как работать с Wildcard-сертификатами.

Если планируется или имеется интеграция с Мессенджером и ВКС, получите от администраторов Мессенджера и ВКС следующие данные:

1. Адрес стенда и AS (например: `100.70.80.91`, `64401`).
2. Адрес мастера k8s (например: `https://10.32.0.1:6442`).
3. Файл `kubeconf`.
4. Адрес ingress (например: `apigwv2-apigw.vkteams.svc.cluster.local`).
5. Домен инсталляции (например: `cluster.local`).
6. Адреса внутренней сети (например: `10.31.0.1/32`, `10.32.0.1/32`).

Шаг 1. Обновите клиентские приложения

Пропустите этот шаг, если у вас нет Мессенджера и ВКС или вы не используете его для работы с Почтой VK WorkSpace. Перейдите к шагу 2.

Начиная с версии 25.4 клиентские приложения при подключении к серверу могут использовать как стандартные алгоритмы шифрования (RSA, ECDHE и т. д.), так и ГОСТ-алгоритмы.

После настройки ГОСТ TLS-шифрования на сервере все клиентские приложения, не поддерживающие работу по ГОСТ TLS, перестанут работать. У пользователей будет отображаться предупреждение, что нет связи с сервером, даже если на устройстве есть интернет.

> **Примечание**
>
> Такое поведение так же может соответствовать не обновленному приложению или отсутствию на устройстве пользователя нужных библиотек.

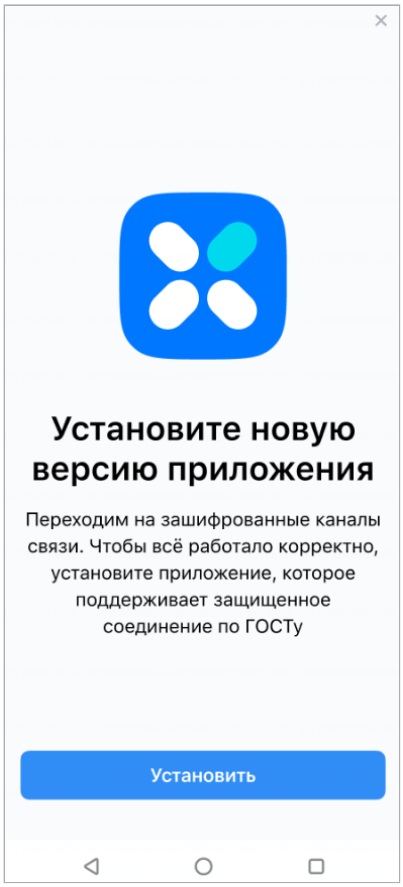
Чтобы клиентские приложения работали после настройки ГОСТ TLS-шифрования на сервере, выполните следующее:

1. На все компьютеры и ноутбуки, на которых пользователи будут пользоваться десктоп-версией клиентского приложения (Windows, macOS, Linux), установите библиотеки для шифрования. Скачать их можно по ссылке https://www.cryptopro.ru/downloads

> **Важно**
>
> Эксплуатация СКЗИ должна осуществляется в соответствии с правилами, изложенными в документации на изделие.

2. Обновите клиентские приложения Суперапп VK WorkSpace:
   - Десктоп-версии клиентского приложения обновите до версии 25.4 и выше.
   - Пользователям Android необходимо скачать приложение с RuStore. Клиентские приложения, скачанные с Google Play не содержат себе библиотеку шифрования ГОСТ TLS.
   - Пользователям с iOS необходимо скачать приложение с AltStore.
   - Для пользователей, которые будут пользоваться веб-версией, установите Яндекс Браузер — в него уже встроены необходимые сертификаты. Также можно использовать браузер Chromium-Gost.

   Чтобы ускорить переход пользователей на новую версию на Android и iOS, включите отображение на мобильных устройствах баннера с предложением скачать новую версию:



Данная функциональность доступна в версии Мессенджер и ВКС 25.4 и выше.

Для этого:

1. На сервере Мессенджера и ВКС перейдите в конфигурационный файл `/usr/local/nginx-im/html/myteam/myteam-config.json` и укажите следующие настройки (значения параметров даны для примера):

```
"gost_universal_popup": true,
"gost_universal_popup_header": “Установите новую версию приложения”,
"gost_universal_dialog_body": “Переходим на зашифрованные каналы связи. Чтобы всё работало
корректно, установите приложение, которое поддерживает защищенное соединение по ГОСТ”,
"gost_universal_dialog_button ": “Установить”,
"gost_universal_popup_ttl_minutes": 1440,
"gost_android_app_download_url": "https://app.com"
```

где:

- gost_universal_popup – если true, показываем пользователям баннер с предложением обновить приложение.
- gost_universal_popup_header — текст заголовка баннера.
- gost_universal_dialog_body – основной текст баннера.
- gost_universal_dialog_button — название кнопки для скачивания приложения.
- gost_universal_popup_ttl_minutes — время, через которое баннер будет показан снова.
- gost_android_app_download_url — ссылка для скачивания ГОСТ-сборки приложения. Ссылка должна вести в RuStore или AltStore в для скачивания клиентского приложения Суперапп VK WorkSpace с поддержкой ГОСТ TLS-шифрования.

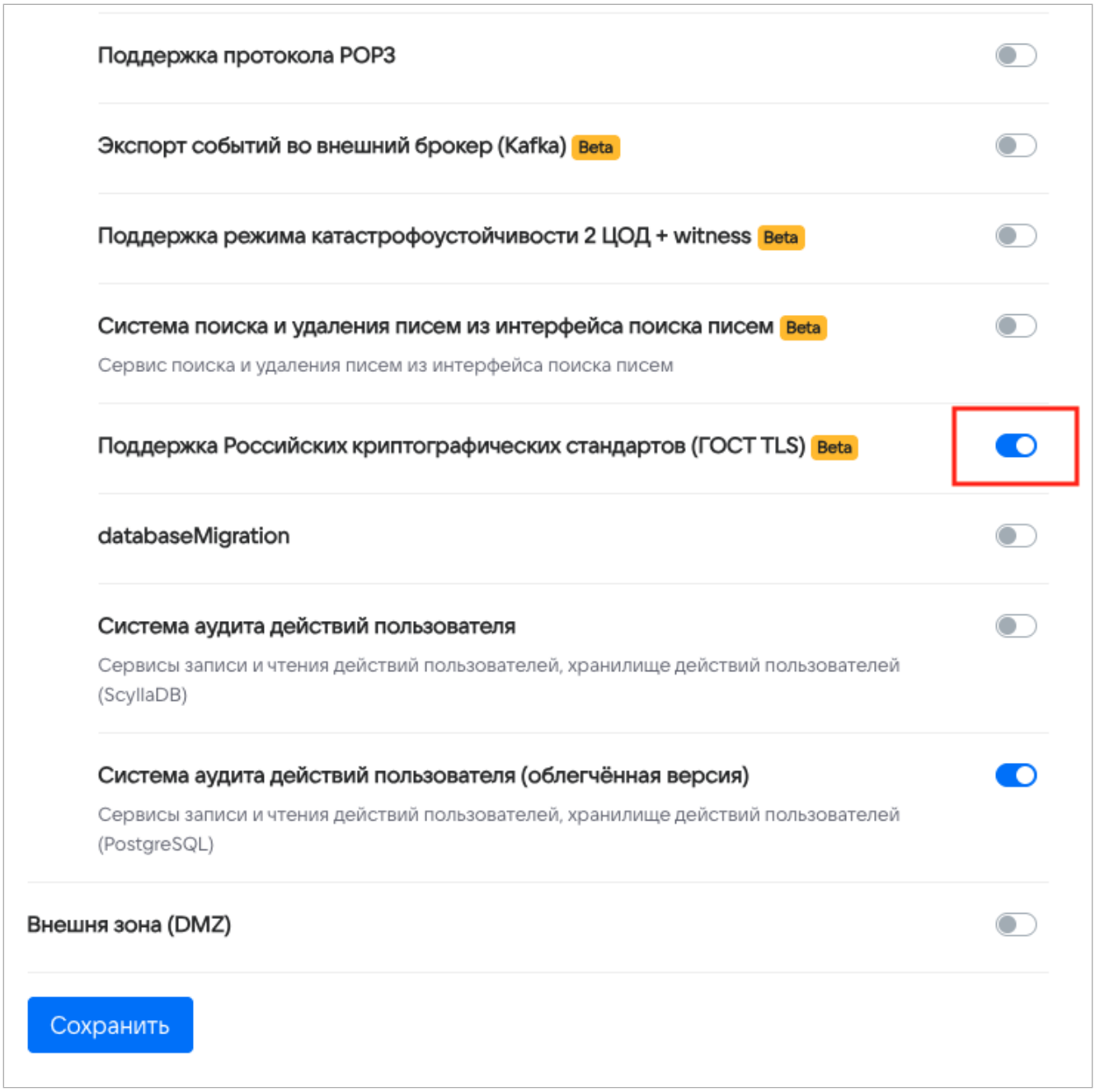
> **Примечание**
>
> Баннер отображается при старте приложения, если для параметра gost_universal_popup указано значение true и «(сейчас() - время_последнего_показа_в_минутах())» больше чем gost_universal_popup_ttl_minutes.

2. На сервере Мессенджера и ВКС перезапустите pod **myteam-admin**:

```
kubectl delete pods -n vkteams -l app=myteam-admin
```

Шаг 2. Включите продукт

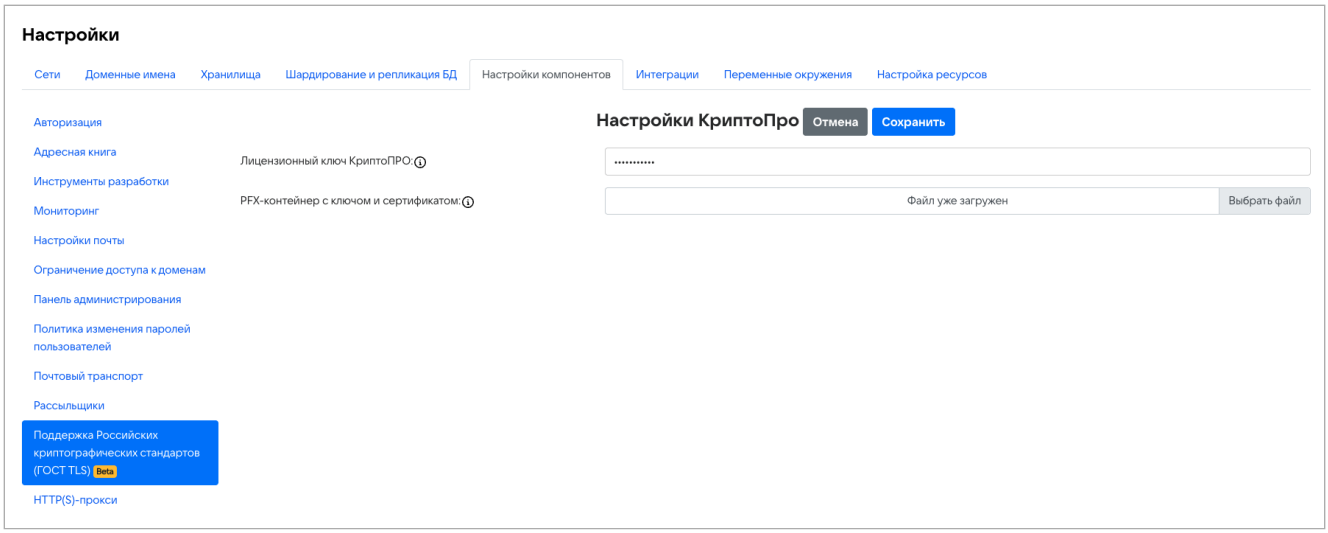
1. Откройте веб-интерфейс установщика Почты VK WorkSpace `http://server-adress:8888`.
2. Нажмите на кнопку  в правом верхнем углу, выберите пункт **Продукты**.
3. Включите компонент **Поддержка российских криптографических стандартов (ГОСТ TLS)**.



4. Нажмите кнопку **Сохранить** внизу страницы.

Шаг 3. Настройте ГОСТ TLS

1. Перейдите в раздел **Настройки** → **Настройки компонентов** → **Поддержка российских криптографических стандартов (ГОСТ TLS)**.
2. Добавьте **Лицензионный ключ КриптоПро**. Тип лицензии должен быть **TLS Server**.
3. Добавьте **PFX-контейнер с ключом и сертификатом**.



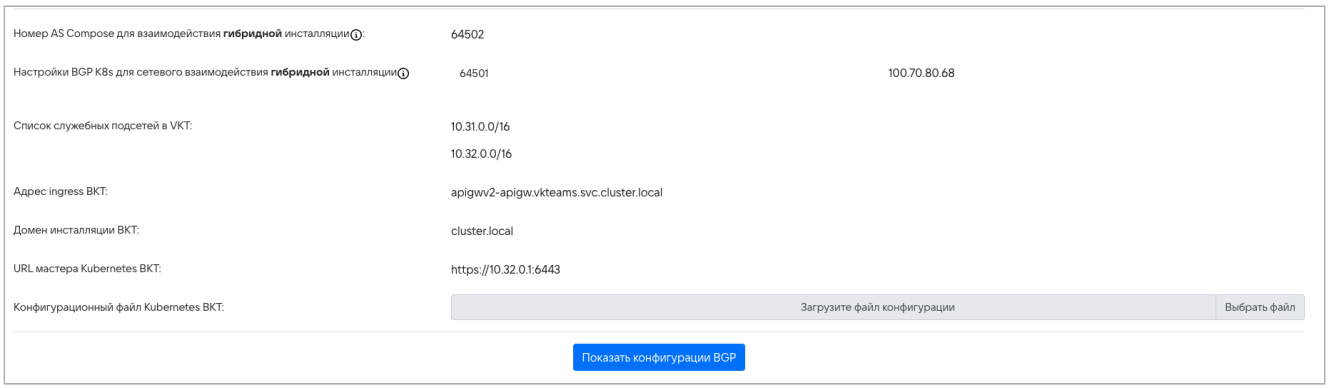
4. Нажмите кнопку **Сохранить**.

Шаг 4. Настройте интеграцию с Мессенджером и ВКС

Пропустите этот шаг, если у вас нет Мессенджера и ВКС или интеграция не настроена. Перейдите к шагу 5.

Настройка сетей

1. Перейдите в раздел **Настройки** → **Сети**. Внизу страницы вы увидите новые поля настроек.



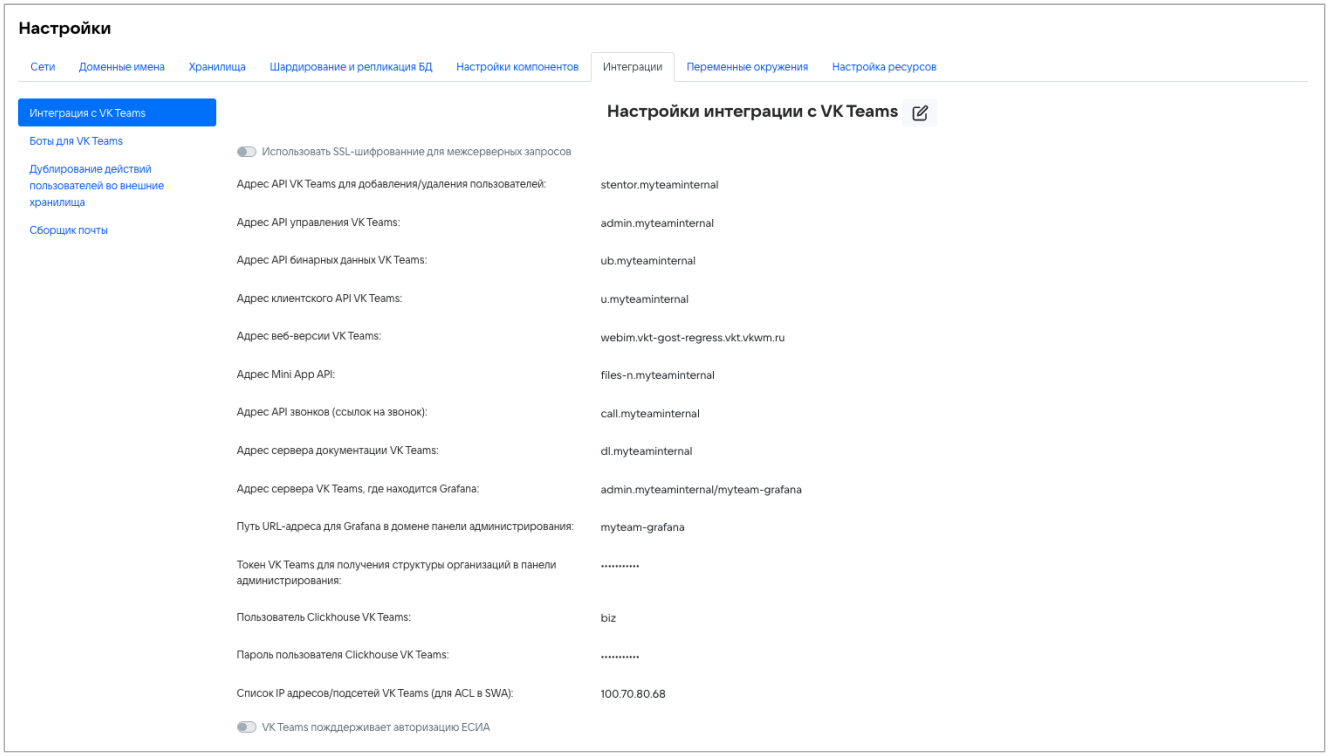
- **Номер AS Compose для взаимодействия гибридной инсталляции** — придумайте номер AS. Номер AS должен отличаться от номера AS в Мессенджере и ВКС.
- **Настройки BGP K8s для сетевого взаимодействия гибридной инсталляции** — введите IP и номер AS. Они указаны в пункте №1 Предварительных действий.
- **Список служебных подсетей в VKT** — укажите служебные подсети, которые вы получили от администраторов Мессенджера и ВКС (пункт №6 в Предварительных действиях). Это нужно для добавления адресов в ippool Calico.

- **Адрес ingress ВКТ** — укажите доменное имя, для получения доступа к доменам. Пункт №4 в Предварительных действиях.
- **Домен инсталляции ВКТ** — введите домен инсталляции. Пункт №5 в Предварительных действиях.
- **URL мастера Kubernetes ВКТ** — укажите URL мастера Kubernetes. Пункт №2 в Предварительных действиях.
- **Конфигурационный файл Kubernetes ВКТ** — загрузите файл kubeconf. Пункт №3 в Предварительных действиях.

2. Нажмите кнопку **Сохранить**.

Настройки в разделе Интеграция с VK Teams

1. Перейдите в раздел **Настройки → Интеграции → Интеграция с VK Teams**.



2. Отключите опцию **Использовать SSL-шифрованние для межсерверных запросов**, если она была включена.
3. Для всех доменов, кроме **Адрес веб-версии VK Teams** и **Путь URL-адреса для Grafana в домене панели администрирования**, замените корневой домен на `myteaminternal`.

   Пример: `stentor` + `myteaminternal`.

   Исключение — **Адрес сервера VK Teams, где находится Grafana**. Для него в конец надо добавить еще `/myteam-grafana`.
4. Нажмите кнопку **Сохранить**.

Настройки в разделе Боты для VK Teams

1. Перейдите в раздел **Боты для VK Teams**.
2. Замените содержание поля **Адрес bot-api VK Teams** на `api.myteaminternal`.
3. Нажмите кнопку **Сохранить**.

Шаг 5. Примените настройки

> **Внимание**
>
> Нельзя вносить изменения в контейнеры, которые будут созданы для работы ГОСТ-TLS. Например, мы не сможем поддерживать функциональность, если будет использована другая версия Nginx.

1. Перейдите к списку ролей, на главную страницу веб-интерфейса установщика.
2. Распределите контейнеры **pub-gost*** по машинам с типом **Фронт**.
3. Запустите автоустановку.
4. Дождитесь окончания установки.
5. Удалите контейнеры, подсвеченные для удаления.

Шаг 6. Проверьте работу интеграции

Проверка производится, когда интеграция настроена и в Почте VK WorkSpace и в Мессенджере и ВКС.

Для проверки перейдите в `/home/deployer/configs/coredns`.

Выполните следующие команды для проверки:

- Проверка создания ippool — `calicoctl get ippool`. Должны отобразиться адреса Мессенджера и ВКС и их подсети.
- Проверка установки BGP-соединения — `docker exec -it calico-node1 birdctl`, затем `show protocols all`. Должен появиться IP Мессенджера и ВКС с пометкой, что соединение установлено.
- Ping до адреса Мессенджера и ВКС — `ping <vk teams ip>`.

12 марта 2026 г.