

# Мессенджер и ВКС

**Инструкция по установке на одну виртуальную машину. Версия 26.1**

Назначение документа	5
Дополнительная документация	5
Архитектура проекта	6
Обязательные компоненты	6
Опциональные компоненты	7
Технические требования	8
Совместимость	9
Предварительные условия для установки	10
Установка Мессенджер и ВКС из графического интерфейса	11
Шаг 1. Предварительные условия для установки	11
Шаг 2. Проверка целостности полученных образов виртуальных машин	11
Шаг 3. Создание виртуальной машины	12
Шаг 4. Запуск образа виртуальной машины	12
Шаг 5. Подключение к виртуальной машине	12
Шаг 6. Генерация SSH-ключа для установщика	12
Шаг 7. IP-адрес	13
Шаг 8. Настройки DNS-зоны	13
Шаг 9. Выпуск SSL-сертификата	15
Шаг 10. Открыть доступы до внутренних ресурсов	15
Шаг 11. Запуск установщика	16
Шаг 12. Добавление сервера в установщик	16
Шаг 13. Настройки Мессенджер и ВКС	18
Домен пользователя	18
Список DNS-серверов	19
Список серверов точного времени (NTP)	19
Настройка SMTP-сервера	19
Настройка сервиса записи звонков	20
Настройка SSO-аутентификации	20
Установка разрешений для пользователей	20

Настройки SSL-сертификата	21
Протокол ACME (Let`s Encrypt) для SSL-сертификатов	22
Настройка окружения администратора	23
Настройка обратной связи	24
Настройка LDAP	26
Шаг 14. Проверка конфигурации	29
Шаг 15. Запуск установки	30
Шаг 16. Рестарт машины	31
Установка Мессенджер и ВКС из консоли	32
Шаг 1. Предварительные условия для установки	32
Шаг 2. Проверка целостности полученных образов виртуальных машин	32
Шаг 3. Создание виртуальной машины	32
Шаг 4. Запуск образа виртуальной машины	33
Шаг 5. Подключение к виртуальной машине	33
Шаг 6. Настройка сети	33
Шаг 7. IP-адрес	34
Шаг 8. Настройки DNS-зоны	34
Шаг 9. Выпуск SSL-сертификата	36
Шаг 10. Открыть доступы до внутренних ресурсов	36
Шаг 11. Настройка LDAP	37
Как получить Distinguished Name для bindDN и usersDN в Active Directory	38
Шаг 12. Подготовка конфигурационного файла инсталляции	39
Список серверов точного времени (NTP)	40
Список DNS-серверов	40
Настройка SMTP-сервера	41
Настройка SSO-аутентификации	41
Доменное имя сервера Мессенджер и ВКС	41
IP-адрес	42
Настройка сервиса записи звонков	42
Настройки SSL-сертификата	42
Протокол ACME (Let`s Encrypt) для SSL-сертификатов	43
Установка разрешений для пользователей	44

Настройка окружения администратора	45
Настройка обратной связи	47
Шаг 13. Проверка конфигурационного файла на ошибки	49
Шаг 14. Инициализация сервисов	49
Шаг 15. Запуск скрипта конфигурации	49
Шаг 16. Рестарт машины	49
Проверки после инсталляции	50
Повторный запуск конфигуратора	52
Внесение изменений в настройки инсталляции	52

# Назначение документа

---

В инструкции описана установка Мессенджер и ВКС на одну виртуальную машину.

В документе рассматриваются два способа установки системы:

1. [Установка из графического интерфейса](#)
2. [Установка из консоли](#)

Документ предназначен для использования администраторами организации.

## Дополнительная документация

---

[Инструкция по интеграции с контроллером домена по протоколу LDAP](#) — в документе описано управление параметрами синхронизации LDAP.

[Управление пользователями без контроллера домена](#) — в документе описано управление пользователями без контроллера домена.

[Инструкция по установке обновлений на одну виртуальную машину](#) — в документе прописано обновление системы, установленной на одну виртуальную машину.

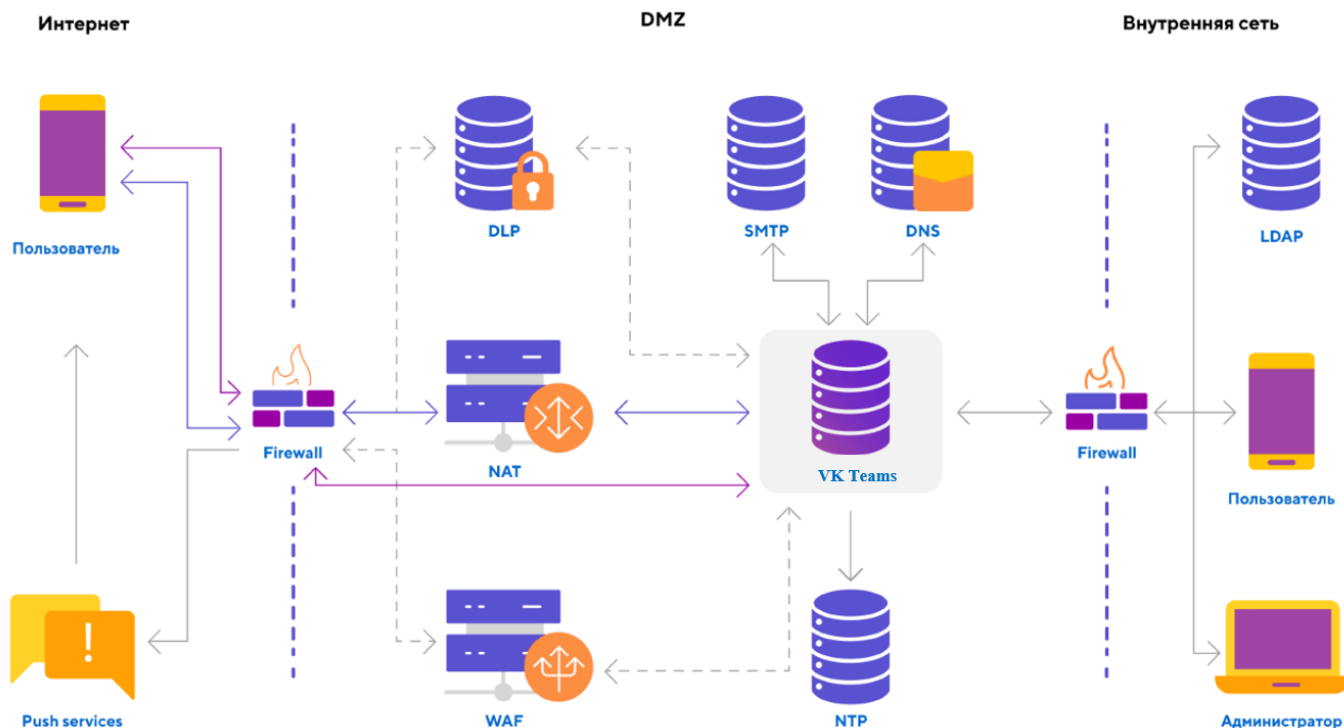
**Архитектура и описание системы** — в документе описана архитектура инсталляции на одну виртуальную машину, кластерной инсталляции, возможные интеграции со сторонними сервисами, а также технические данные и требования. Не является частью публичной документации, обратитесь к представителю VK Tech, чтобы ознакомиться с документом.

### Примечание

Ранее Мессенджер и ВКС назывался Myteam, что находит отражение некоторых в технических моментах (например, команды в консоли).

# Архитектура проекта

В данном разделе представлено краткое описание архитектуры проекта. Подробное описание архитектуры представлено в документе «Архитектура и описание системы» (не является частью публичной документации, обратитесь к представителю VK Tech, чтобы ознакомиться с документом).



Мессенджер и ВКС представляет собой одну виртуальную машину и может рассматриваться как один компонент сети.

Инсталляция не требует отдельных компонентов вне сегмента сети DMZ. Однако Мессенджер и ВКС активно взаимодействует с внешними и внутренними компонентами сети.

Как правило, сервер Мессенджер и ВКС устанавливается внутри DMZ и не имеет внешнего IP-адреса. Вместо этого весь необходимый трафик идет через NAT или WAF.

## Обязательные компоненты

### Сервер Мессенджер и ВКС

В сегменте сети DMZ.

### Сервер NTP

Используется для синхронизации времени, предоставляется заказчиком. Может быть использован как публичный, так и ваш собственный сервер. На схеме предполагается, что сервер находится в вашем сегменте DMZ.

## Сервер SMTP

Используется для отправки OTP-сообщений, предоставляется заказчиком. Может быть использован как публичный, так и ваш собственный сервер. На схеме предполагается, что сервер находится в вашем сегменте DMZ.

## Сервер DNS

Используется для преобразования имен в IP-адреса и обратно, предоставляется заказчиком. Может быть использован как публичный, так и ваш собственный сервер. На схеме предполагается, что сервер находится в вашем сегменте DMZ.

## Push-сервисы

Внешние сервисы Apple и Google для отправки push-сообщений на мобильные платформы. Расположены во внешнем периметре. Серверу Мессенджер и ВКС требуются исходящие соединения к этим сервисам и не требуются входящие соединения.

## Суперапп VK WorkSpace

Пользовательское приложение, установленное на одной из допустимых платформ. Сервер Мессенджер и ВКС должен иметь возможность принимать входящие сообщения от этого приложения, а также отправлять ответы. Основное взаимодействие осуществляется через протокол HTTPS (443/TCP). Для работы видео- и аудиозвонков необходимы протоколы STUN и TURN: входящие соединения на порты 3478/TCP и 3478/UDP, а также входящий и исходящий трафик UDP по портам 1024+ (RTP-трафик).

# Опциональные компоненты

## WAF (Web application firewall)

Осуществляет фильтрацию входящего HTTP-трафика, а также акселерацию SSL-трафика. Предоставляется заказчиком.

## DLP (Data Leak Prevention)

Система для предотвращения утечки данных. Предоставляется заказчиком.

## LDAP

Используется для получения списка пользователей в системе. Мессенджер и ВКС может обслуживать как пользователей, заведенных в LDAP заказчика, так и внутренних пользователей. Интеграция с LDAP не является обязательным условием, но очень удобна для тех, кто имеет внутренний LDAP, например MS Active Directory.

## Антивирус

Используется для проверки файлов на вирусы. Не является обязательным компонентом. Предоставляется заказчиком.

# Технические требования

Дистрибутив Мессенджер и ВКС поставляется в виде образа виртуальной машины сервера, а также набора приложений для мобильных устройств или компьютера.

**Минимальные требования к серверу** в зависимости от количества пользователей:

Количество пользователей	vCPU	RAM, GB	SSD, GB	S3, GB / год
<b>Тестовая установка</b>				
1 000	22	56	400: root 150 GB data 250 GB	-
<b>Продуктивная установка</b>				
От 1 до 2 000	22	56	400: root 150 GB data 250 GB	500

Минимальные требования к SSD-дискам:

Операций чтения, IOPS	Операций записи, IOPS	Максимальная задержка операции, мс
10 000	5 000	< 1

Если планируется настройка Федерации, добавьте на серверы каждой инсталляции дополнительные вычислительные ресурсы:

- 10% от имеющихся мощностей vCPU
- 1 ГБ SSD
- 2 ГБ RAM на каждую тысячу федеративных пользователей. Ожидаемый прирост RAM — около 1 ГБ в год в зависимости от количества сообщений федерации

Если количество пользователей более 1 500, требования к предоставляемым вычислительным ресурсам (виртуальным машинам) для продуктивной среды рассчитываются индивидуально для Заказчика.

Свяжитесь с представителями VK для помощи с расчетом сайзинга.

## vCPU

Обязательная поддержка Time Stamp Counter (TSC). Проверить наличие можно поиском флага `constant_tsc` в `/proc/cpuinfo`. Любой современный процессор поддерживает эту технологию, однако иногда этого регистра нет внутри виртуальной машины. В этом случае необходимо правильно настроить систему виртуализации.

Не допускайте переподписку. Суммарные vCPU на хосте не должны превышать количество физических ядер, выделенных всем виртуальным машинам. При этом не рекомендуется считать Hyper-Threading полноценными ядрами.

Не выделяйте одной виртуальной машине количество ядер больше, чем количество ядер на физическом соquete.

## **RAM**

Не назначайте суммарную vRAM выше физической RAM хоста.

## **Механизмы экономии памяти**

Не включайте механизмы ballooning и сжатия памяти.

## **swap**

Не используйте swap — как на гипервизоре, так и внутри виртуальных машин.

## **Резервирования ресурсов виртуальных машин**

Устанавливайте всю выделенную память и процессоры в резерв для виртуальных машин системы.

## **Хранилище**

Не используйте тонкие диски (диски типа Thin) — диски с отложенным выделением пространства на СХД.

## **Входящий трафик**

TCP — 10 Мбит/с; UDP — 10 Мбит/с.

# **Совместимость**

---

- ПО VMware версий 6.x — 7.x.
- Любые системы виртуализации, основанные на KVM, например OpenStack.
- VK Cloud Solutions.

Более подробно технические данные и требования представлены в документе «Архитектура и описание системы» (не является частью публичной документации, обратитесь к представителю VK Tech, чтобы ознакомиться с документом).

# Предварительные условия для установки

---

Перед установкой необходимо обеспечить:

## Роутинг исходящих соединений

Необходим для отправки push-сообщений (через сервисы Apple, Google) и для работы голосовых и видео-звонков.

## SMTP-сервер

Авторизация пользователей в Мессенджер и ВКС выполняется с помощью одноразовых кодов (OTP via email). Для доставки писем с одноразовыми кодами необходим SMTP-сервер, на котором разрешена отправка почтовых сообщений для данной виртуальной машины — без авторизации и блокировки антиспам-системой.

## NTP-серверы

Нужны для синхронизации времени. Возможно указание внешних серверов, если нет сложностей с прохождением сетевых фильтров.

## Исходящие соединения на стороне клиента

Разрешить подключение: 80/TCP, 443/TCP, 3478/TCP + UDP, UDP-порты выше 1024.

## LDAP

Сервис Мессенджер и ВКС может работать как обособленно, так и в связке с корпоративным LDAP-сервером.

Система предоставляет возможность указать настройки для соединения с LDAP-сервером (при его наличии) во время инсталляции или после ее завершения.

Информация по управлению параметрами синхронизации LDAP **после** инсталляции Мессенджер и ВКС представлена в документе [Инструкция по интеграции с контроллером домена по протоколу LDAP](#).

Если настройки для соединения с LDAP-сервером производятся **в момент** инсталляции, Вам необходимы:

- Доступ к LDAP-серверу.
- Настройки для соединения с LDAP-сервером: bind\_dn, user\_dn, url, password, CA-сертификат.
- Название группы пользователей, которым будет доступно окружение администратора, например, **myteam-admin**. Название группы будет использовано при настройке доступа к окружению администратора.

Возможна работа без LDAP, с добавлением пользователей вручную (подробнее см. [Управление пользователями без контроллера домена](#)).

# Установка Мессенджер и ВКС из графического интерфейса

Процесс установки условно делится на:

1. Действия в консоли — шаги 1-9.
2. Действия в графическом интерфейсе установщика — шаги 10-14.
3. Рестарт виртуальной машины в консоли — шаг 15.

Для установки Мессенджер и ВКС из графического интерфейса необходимо выполнить шаги, представленные ниже.

## Внимание

Все команды в консоли выполняются под пользователем root.

## Шаг 1. Предварительные условия для установки

Перед началом инсталляции убедитесь, что выполнены все предварительные условия (см. раздел [Предварительные условия для установки](#)).

## Шаг 2. Проверка целостности полученных образов виртуальных машин

Чтобы проверить целостность образов виртуальных машин, в директории со скачанными файлами выполните в командной строке:

### Linux

```
md5sum *
```

### Windows

```
CertUtil -hashfile myteam.ova MD5  
CertUtil -hashfile myteam.qcow2 MD5  
CertUtil -hashfile myteam-data.qcow2 MD5
```

### Mac

Далее сравните полученное значение с хеш-суммой, указанной в текстовом файле **md5.txt**, распространяемом с дистрибутивом.

## Шаг 3. Создание виртуальной машины

Создайте виртуальную машину на основе предоставленных образов.

При создании виртуальной машины с предоставленного образа (root), необходимо создать и подключить новый пустой раздел data для хранения данных, генерируемых при работе системы. При обновлении версии дистрибутива, раздел root будет пересоздаваться из нового образа, раздел data — переноситься с рабочего экземпляра.

## Шаг 4. Запуск образа виртуальной машины

Запустите образ виртуальной машины.

## Шаг 5. Подключение к виртуальной машине

Подключитесь к виртуальной машине по SSH.

Пользователь: **centos**

Пароль: **djhMRG1vO**

### **Внимание**

Чтобы получить пароль для пользователя root, обратитесь в службу технической поддержки.  
После подключения к виртуальной машине пароли для пользователей root и centos необходимо сменить.

**macOS или Linux:**

```
ssh centos@<VM IP address>
```

**Windows:** зависит от используемого SSH-клиента.

## Шаг 6. Генерация SSH-ключа для установщика

Для доступа установщика к серверу Мессенджер и ВКС необходимо сгенерировать ключ на сервере Мессенджер и ВКС:

```
ssh-keygen -f vkt_key
```

После этого публичную часть ключа необходимо добавить пользователю **centos** в список авторизованных ключей:

```
cat vkt_key.pub >> /home/centos/.ssh/authorized_keys
```

Приватная часть ключа (`vkt_key`) будет использоваться при запуске установщика.

## Шаг 7. IP-адрес

Перед началом инсталляции необходимо определить, будет ли доступен сервис в интернете.

Если сервис не будет доступен в интернете, то необходимо использовать внутренний IP-адрес разворачиваемой виртуальной машины.

Если сервис будет доступен в интернете, необходимо использовать внешний IPv4 адрес виртуальной машины. Адрес может быть поднят как внутри виртуальной машины, так и проброшен через NAT. Преобразование сетевых адресов (NAT) должно быть вида 1-в-1 (сеть в сеть), то есть с сохранением номера порта. Иначе видео и голосовые звонки могут не работать.

IP-адрес в дальнейшем будет использоваться при запуске установщика.

## Шаг 8. Настройки DNS-зоны

Заведите в DNS-зоне имена хостов, которые будут смотреть на внешний IPv4 адрес.

Список имен (CNAME либо A-записи на ваше усмотрение):

- `admin` — адрес API управления Мессенджер и ВКС (административного веб интерфейса).
- `akesadmin`
- `api` — API бота.
- `biz` — адрес сервера Мессенджер и ВКС, где находится сервис Grafana.
- `calendar` — API календаря. Работает только в интеграции с Почтой VK WorkSpace.
- `calendar-mobile` — API мобильного календаря. Работает только в интеграции с Почтой VK WorkSpace.
- `call` — URL для формирования ссылок на звонки.
- `di` — поддомен сервиса Keycloak для версий до 25.2.
- `dl` — портал загрузки дистрибутивов (система автоматического обновления клиентских приложений).
- `files-n` — оргструктура организаций.
- `kc` — поддомен сервиса Keycloak для версии 25.2 и выше.
- `notp`

- outlook-plugin — плагин MS Outlook для создания конференций.
- rapi
- s — обмен стикерпаками.
- stentor — адрес API Мессенджер и ВКС для добавления/удаления пользователей.
- u — адрес клиентского API Мессенджер и ВКС.
- ub — файловое API.
- webim — веб-версия Мессенджер и ВКС.

Например, для домена vkteams.example.com имя хоста будет выглядеть как u.vkteams.example.com.

### Вариант 1.

Если есть возможность создания записи Wildcard CNAME в DNS, то можно создать A-запись, указывающую на адрес сервера Мессенджер и ВКС, и запись Wildcard CNAME, указывающую на A-запись сервера Мессенджер и ВКС.

```
$ host -t axfr example.com | grep vkteams
vkteams.example.com.          3600    IN      A       172.27.59.10
*.vkteams.example.com.       3600    IN      CNAME   vkteams.example.com.
```

### Вариант 2.

Если нет возможности создания записи Wildcard CNAME в DNS, то можно создать A-запись, указывающую на адрес сервера Мессенджер и ВКС, и отдельные записи CNAME, которые будут разрешаться на созданную A-запись. Записи CNAME должны соответствовать перечню имен, представленному выше.

```
$ host -t axfr example.com | grep vkteams
vkteams.example.com.          3600    IN      A       172.27.59.10
admin.vkteams.example.com.    3600    IN      CNAME   vkteams.example.com.
akesadmin.vkteams.example.com. 3600    IN      CNAME   vkteams.example.com.
api.vkteams.example.com.      3600    IN      CNAME   vkteams.example.com.
biz.vkteams.example.com.      3600    IN      CNAME   vkteams.example.com.
calendar.vkteams.example.com. 3600    IN      CNAME   vkteams.example.com.
calendar-mobile.vkteams.example.com. 3600    IN      CNAME   vkteams.example.com.
call.vkteams.example.com.     3600    IN      CNAME   vkteams.example.com.
di.vkteams.example.com.       3600    IN      CNAME   vkteams.example.com. # только для
версий до 25.2
dl.vkteams.example.com.       3600    IN      CNAME   vkteams.example.com.
files-n.vkteams.example.com.   3600    IN      CNAME   vkteams.example.com.
kc.vkteams.example.com.       3600    IN      CNAME   vkteams.example.com. # только для
версии 25.2 и выше
notp.vkteams.example.com.     3600    IN      CNAME   vkteams.example.com.
outlook-plugin.vkteams.example.com. 3600    IN      CNAME   vkteams.example.com.
rapi.vkteams.example.com.     3600    IN      CNAME   vkteams.example.com.
s.vkteams.example.com.        3600    IN      CNAME   vkteams.example.com.
stentor.vkteams.example.com.   3600    IN      CNAME   vkteams.example.com.
u.vkteams.example.com.        3600    IN      CNAME   vkteams.example.com.
ub.vkteams.example.com.       3600    IN      CNAME   vkteams.example.com.
webim.vkteams.example.com.    3600    IN      CNAME   vkteams.example.com.
```

## **Внимание**

Не вносите изменения в **etc/resolv.conf**. Если изменения всё же необходимо внести, то первым должен быть указан хост 127.0.0.1.

## Шаг 9. Выпуск SSL-сертификата

В целях безопасности используется SSL-шифрование, для работы сервера необходимо выпустить SSL-сертификат.

Если вы используете сертификаты собственного центра сертификации, выпустите сертификат, который далее понадобится при настройке Мессенджер и ВКС (см. [Настройки SSL-сертификата](#)). Используйте Wildcard-сертификат, например \*.vkteams.EXAMPLE.com, или сертификат с указанием всех необходимых имен (см. раздел [Настройки DNS-зоны](#)).

Для SSL-сертификатов также можно использовать протокол ACME (поддерживается только провайдер Let`s Encrypt). В этом случае получение и продление сертификатов — автоматическое.

## Шаг 10. Открыть доступы до внутренних ресурсов

### **Входящие соединения на стороне сервера Мессенджер и ВКС:**

Открыть порты: 80/TCP, 443/TCP, 3478/TCP + UDP, UDP-порты выше 1024.

### **Исходящие соединения на стороне сервера Мессенджер и ВКС:**

#### **• Открыть доступ для серверов отправки уведомлений:**

необходимо обеспечить доступ к серверам Google и Apple для отправки и корректной работы push-уведомлений на мобильных платформах Android и iOS.

#### **Сервер Apple**

TCP 5223; 443; 2197

IP 17.0.0.0/8

[Статья на сайте apple.com](#)

#### **Сервер Google**

TCP 5228; 5229; 5230; 443

[Информация на ipinfo.io](#)

[Статья на сайте google.com](#)

Если в вашей организации используются механизмы ограничения доступа сетевого трафика, убедитесь, что открыт доступ к следующим доменам (по HTTPS, порт 443):

fcm.googleapis.com

www.googleapis.com

oauth2.googleapis.com

accounts.google.com

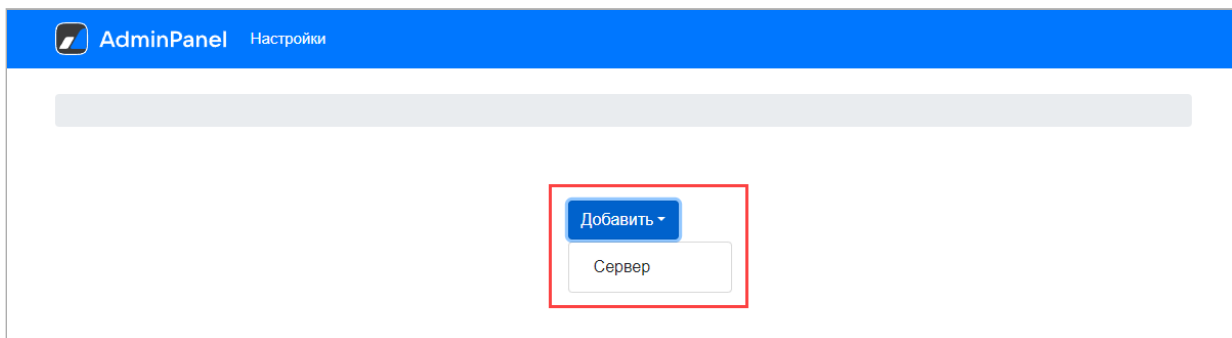
- Открыть доступ до всех внутренних ресурсов: LDAP, NTP, SMTP, DNS.

## Шаг 11. Запуск установщика

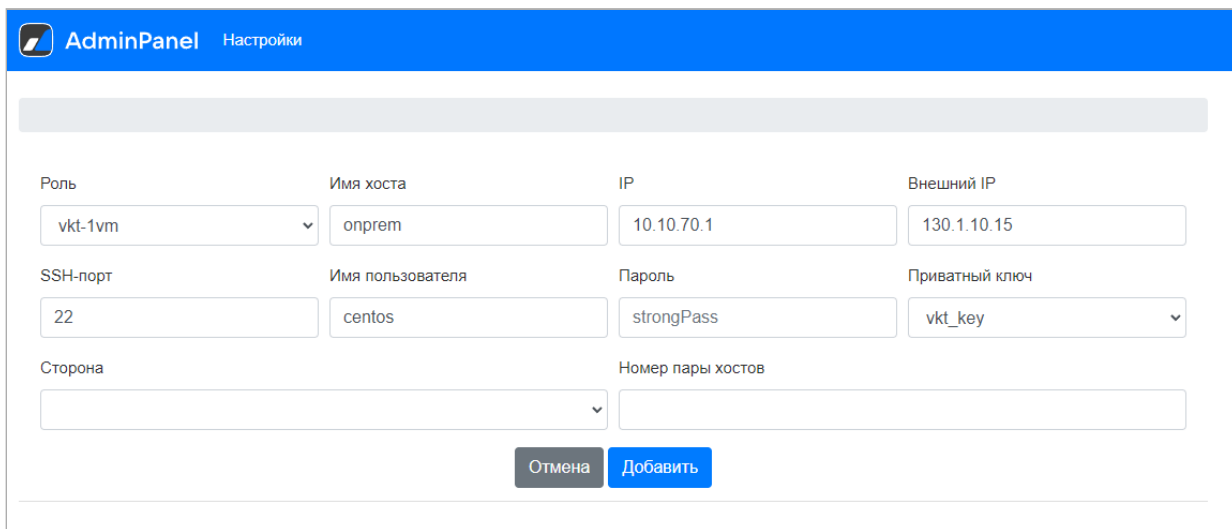
Распакуйте архив **vkt-web-deployer.tar.gz.zip** в отдельную директорию и запустите исполняемый файл. Далее перейдите по адресу <http://127.0.0.1:8888>.

## Шаг 12. Добавление сервера в установщик

На главной странице установщика нажмите кнопку **Добавить** → **Сервер**:



На отобразившейся форме добавления сервера заполните поля:

The image shows a screenshot of the server addition form in the AdminPanel. The form is titled 'AdminPanel' and 'Настройки'. It contains several input fields and dropdown menus. The fields are: 'Роль' (Role) with a dropdown menu showing 'vkt-1vm'; 'Имя хоста' (Hostname) with a text input field containing 'onprem'; 'IP' with a text input field containing '10.10.70.1'; 'Внешний IP' (External IP) with a text input field containing '130.1.10.15'; 'SSH-порт' (SSH port) with a text input field containing '22'; 'Имя пользователя' (Username) with a text input field containing 'centos'; 'Пароль' (Password) with a text input field containing 'strongPass'; 'Приватный ключ' (Private key) with a dropdown menu showing 'vkt\_key'; 'Сторона' (Side) with a dropdown menu; and 'Номер пары хостов' (Host pair number) with a text input field. At the bottom of the form, there are two buttons: 'Отмена' (Cancel) and 'Добавить' (Add).

- **Роль** — для установки standalone нужно выбрать **vkt-1vm**.
- **Имя хоста** — короткое имя сервера (без домена).
- **IP** — IP-адрес, по которому будет осуществляться доступ установщика к серверу Мессенджер и ВКС.
- **Внешний IP** — внешний или внутренний IP-адрес, присвоенный на шаге [IP-адрес](#). Может совпадать со значением в поле **IP**;
- **SSH-порт** — порт SSH-сервера (по умолчанию — 22).
- **Имя пользователя** — имя пользователя для соединения установщика по SSH (по умолчанию **centos**).

- **Пароль** — при использовании авторизации по паролю — **djhMRG1vO**. Поле не заполняется при использовании приватного ключа.
- **Сторона** — поле не используется при установке standalone.
- **Номер пары хостов** — поле не используется при установке standalone.
- **Приватный ключ** — ключ для доступа установщика к серверу Мессенджер и ВКС. Выберите в выпадающем списке поля + **Добавить новый ключ**. В отобразившейся форме заполните поля:

### Добавление приватного ключа

Имя ключа:

Приватный ключ: 

```
-----BEGIN RSA PRIVATE KEY-----  
  
  
  
  
  
  
  
  
  
-----END RSA PRIVATE KEY-----
```

Пароль ключа:

Использовать по умолчанию

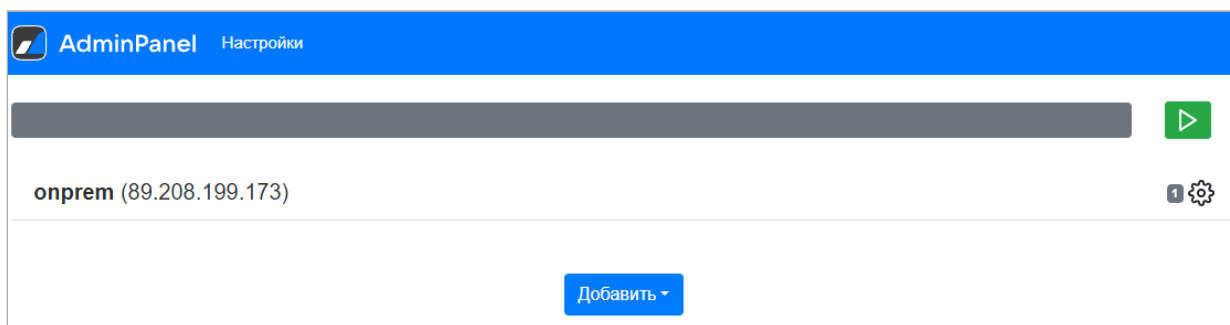
В поле **Приватный ключ** необходимо скопировать содержимое приватной части SSH-ключа, созданного на шаге выше (см. раздел [Генерация SSH-ключа для установщика](#)). Приватный ключ необходимо указать полностью, включая `-----BEGIN RSA PRIVATE KEY-----` и `-----END RSA PRIVATE KEY-----`.

В поле **Пароль ключа** указать пароль, созданный при генерации SSH-ключа (если пароль не был создан — поле не заполнять).

Нажмите на кнопку **Сохранить**.

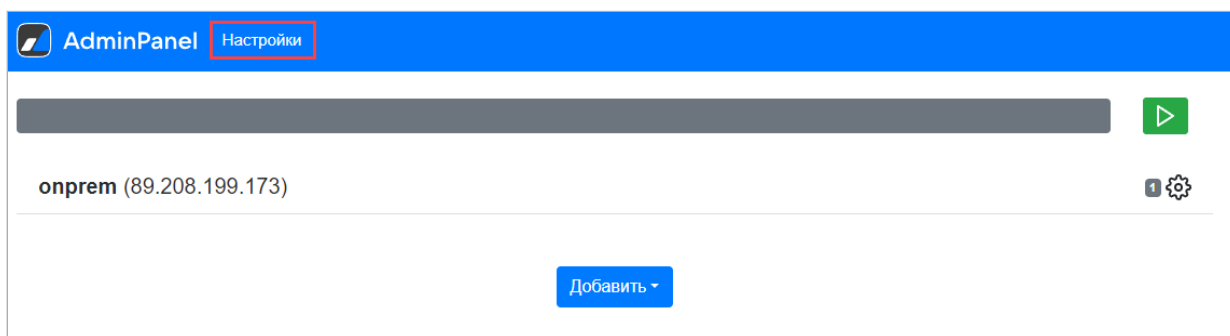
После заполнения полей на форме добавления сервера нажмите на кнопку **Добавить**.


Добавленный сервер отобразится в панели установщика:

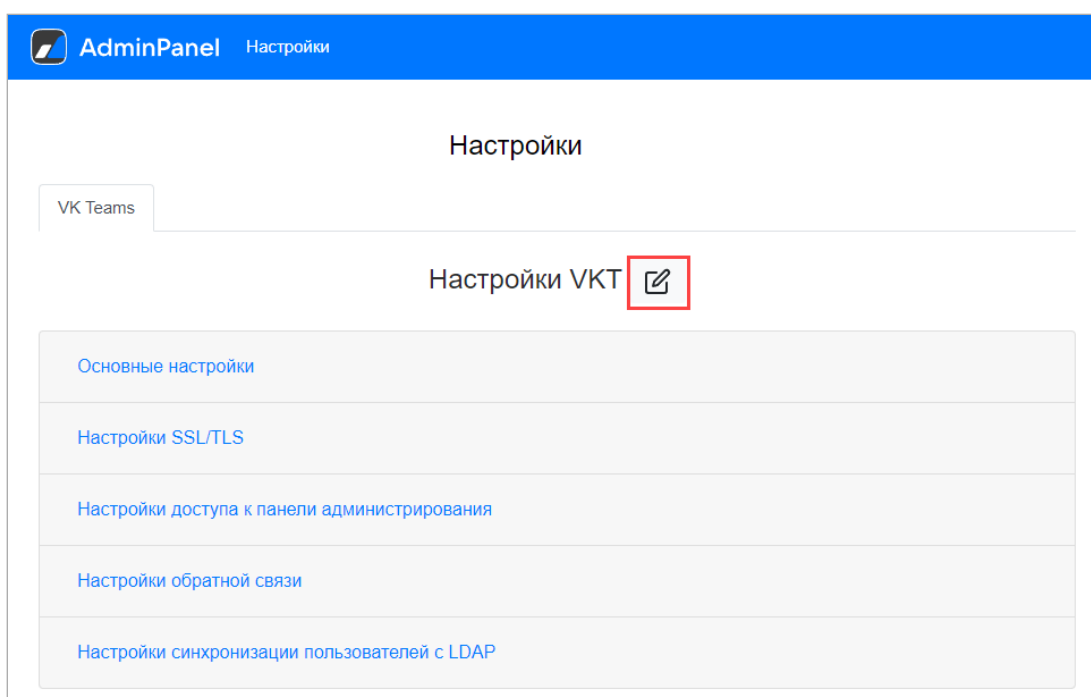


## Шаг 13. Настройки Мессенджер и ВКС

После добавления сервера перейдите в раздел **Настройки**:



На отобразившейся странице нажмите на пиктограмму  , чтобы перейти в режим редактирования:



Ниже приведено подробное описание каждого пункта конфигурации.

### Домен пользователя

Выберите раздел **Основные настройки**:

Настройки VKT Отмена Сохранить

**Основные настройки**

[Настройки SSL/TLS](#)

[Настройки доступа к панели администрирования](#)

[Настройки обратной связи](#)

[Настройки синхронизации пользователей с LDAP](#)

Для настройки сервера Мессенджер и ВКС укажите базовый домен. Например, vkteams.example.com означает, что клиентские приложения будут пытаться получить доступ к сайтам u.vkteams.example.com, ub.vkteams.example.com и т. д.

Внешний домен VK Teams:

## Список DNS-серверов

Укажите список DNS-серверов (IP-адреса серверов, которые будут использованы для разрешения имен).

Список DNS серверов:

8.8.8.8	—
8.8.4.4	—

[+ Добавить](#)

## Список серверов точного времени (NTP)

Укажите список NTP-серверов (IP-адреса или имена хостов):

Список NTP серверов:

0.pool.ntp.org	—
1.pool.ntp.org	—

[+ Добавить](#)

## Настройка SMTP-сервера

Чтобы настроить OTP via email, укажите:

- Имя или IP-адрес SMTP-сервера.
- Порт SMTP-сервера (как правило, не требует редактирования).

- Обратный адрес для сообщений с OTP-кодами (поле **From:** в письме). Рекомендуется использовать реально существующий адрес.

Адрес почтового сервера (SMTP relay):

Порт почтового сервера (SMTP relay port):

From: адрес для исходящих почтовых сообщений:

## Настройка сервиса записи звонков

Данный параметр контролирует сервис записи звонков. При его включении звонки будут записываться, готовая запись будет отправлена пользователю в личные сообщения с помощью бота.

На данный момент запись доступна только в esktop приложениях. По умолчанию запись включена.

Включить сервис записи звонков:

## Настройка SSO-аутентификации

Если в дальнейшем планируется настройка SSO-аутентификации по протоколу SAML, установите переключатель в активное положение:

Будет ли использоваться авторизация SAML в ADFS:

## Установка разрешений для пользователей

Чтобы разрешить пользователям изменять информацию о себе в профиле мессенджера, установите переключатели:

Разрешить изменение аватара пользователем:

Разрешить изменение Имени и Фамилии пользователем:

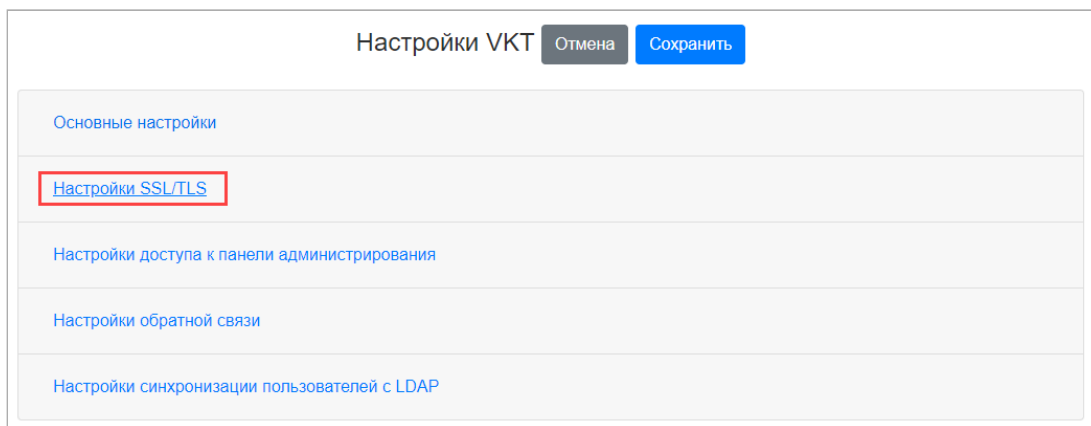
Разрешить смену раздела About me пользователем:

Чтобы разрешить удаление отправленного сообщения в личных чатах/группах без уведомления участников, установите переключатель:

Разрешить 'тихое удаление':

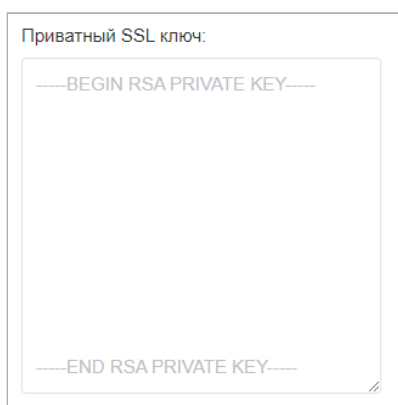
# Настройки SSL-сертификата

Чтобы указать сертификаты, перейдите в раздел **Настройки SSL/TLS**:



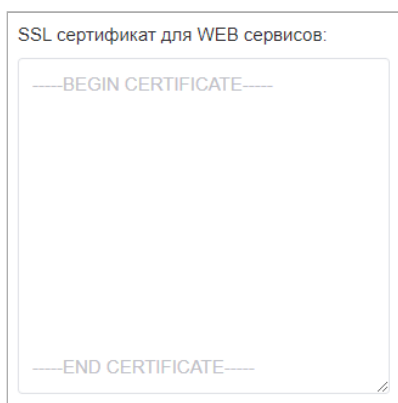
Укажите SSL-сертификат, выпущенный на шаге выше (см. [Выпуск SSL-сертификата](#)).

1. Приватный ключ для SSL-сертификата указывается в формате PEM и не должен быть защищен паролем:



Приватный ключ необходимо указать полностью, включая `-----BEGIN RSA PRIVATE KEY-----` и `-----END RSA PRIVATE KEY-----`.

2. SSL-сертификат сервера в формате PEM. Для корректной работы укажите всю цепочку сертификатов (full chain):



SSL-сертификаты необходимо указать полностью, включая `-----BEGIN RSA PRIVATE KEY-----` и `-----END RSA PRIVATE KEY-----`.

3. Укажите способ проверки SSL-сертификата:

Способ проверки SSL сертификата:

Способ проверки SSL-сертификата может принимать 3 вида значений: True, False, путь до файла **.ca\_bundle**:

- True — проверять сертификат с центрами сертификации (CA) встроенными в ОС (по умолчанию).
- False — не проверять SSL сертификат, например в случае использования самоподписанного сертификата.
- Путь до файла **.ca\_bundle** — использовать свой центр сертификации (CA) для проверки сертификата.

4. Если планируется добавлять самоподписанные сертификаты, установите соответствующий переключатель:

Использовать самоподписанные сертификаты:

## Протокол ACME (Let`s Encrypt) для SSL-сертификатов

1. Чтобы использовать протокол ACME, установите переключатель **Автоматическое получение и продление SSL-сертификатов через протокол ACME**:

Автоматическое получение и продление SSL сертификатов через протокол ACME:

### **Внимание**

Включение этой опции и использование этого функционала означает согласие с условиями использования сервиса Let`s Encrypt, с которыми можно ознакомиться по адресу <https://letsencrypt.org/repository/>.

Поля **SSL-сертификат для WEB сервисов** и **Приватный SSL-ключ** можно не заполнять, при включении сертификатов через ACME они игнорируются.

2. Чтобы отключить получение SSL-сертификата через ACME для внешнего домена Мессенджер и ВКС, установите переключатель в соответствующее положение:

Отключить получение SSL-сертификата через ACME для внешнего домена (например, получать для u.example.com, но не для example.com):

Данный переключатель необходимо установить, если в DNS нет записи, которая позволяет разрешить имя домена на внешний IP-адрес. Если переключатель неактивен, сертификат будет выпускаться.

3. Укажите почту, которая будет использоваться при обращении к Let's Encrypt (обязательный параметр, без корректной почты сертификаты выданы не будут). На эту почту будут поступать уведомления от сервиса Let's Encrypt:

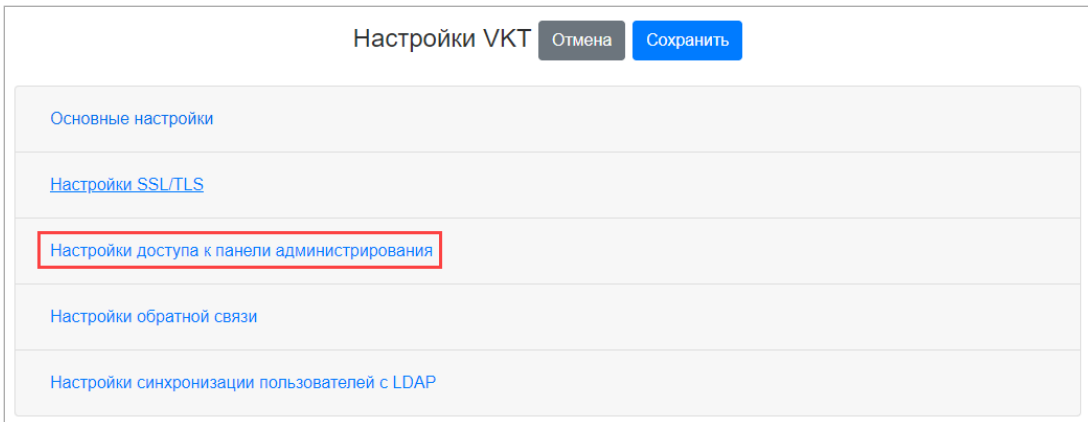
Почта, которая будет использоваться при обращении к Let's Encrypt:

#### **Примечание**

Сертификат продлевается автоматически каждые 3 месяца, поэтому 80й порт должен быть открыт — иначе сертификат не обновится.

## Настройка окружения администратора

Перейдите в раздел **Настройки доступа к панели администрирования**:

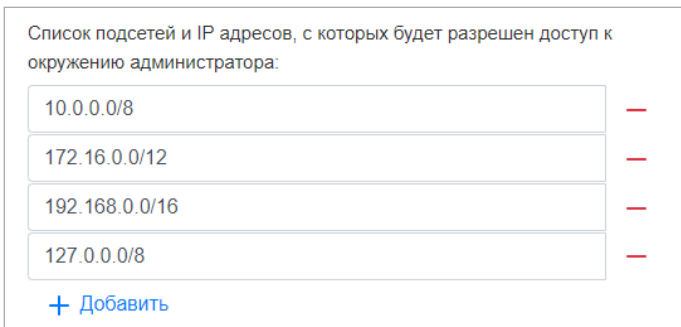


Настройки VKT Отмена Сохранить

- Основные настройки
- [Настройки SSL/TLS](#)
- Настройки доступа к панели администрирования**
- Настройки обратной связи
- Настройки синхронизации пользователей с LDAP

Интерфейс администратора доступен только с выбранных IP-адресов и только выбранным пользователям. Также предусмотрена настройка ограничения доступа к выбранным разделам окружения администратора (например, к выгрузке чатов).

По умолчанию окружение администратора доступно с IP-адресов частных сетей (10.0.0.0/8, 172.16.0.0/12 и 192.168.0.0/16):



Список подсетей и IP адресов, с которых будет разрешен доступ к окружению администратора:

10.0.0.0/8	—
172.16.0.0/12	—
192.168.0.0/16	—
127.0.0.0/8	—

[+ Добавить](#)

Доступ в окружение администратора настраивается через группы. Изначально перечень групп с доступом в окружение администратора пуст, потому окружение недоступно никому.

Если настройки для соединения с LDAP-сервером производятся **во время инсталляции**, укажите в поле **Список LDAP групп доступа к панели администрирования** заранее подготовленное наименование группы из LDAP, в которую будут входить пользователи с доступом в окружение администратора (см. раздел [LDAP](#) в предусловиях):

Список LDAP групп доступа к панели администрирования:

 —

[+](#) [Добавить](#)

Если инсталляция производится без связи с корпоративным LDAP-сервером, укажите в поле наименование группы из LDAP, в которую будут входить пользователи с доступом в окружение администратора (см. раздел [LDAP](#) в предусловиях). Информация по управлению параметрами синхронизации LDAP после инсталляции Мессенджер и ВКС представлена в документе [Инструкция по интеграции с контроллером домена по протоколу LDAP](#).

При отсутствии LDAP — укажите в поле наименование группы, которое будете использовать при создании пользователей в системе вручную после окончания процесса инсталляции (описание процесса представлено в документе [Управление пользователями без контроллера домена](#)).

Управление доступом по группам к компонентам панели администрирования осуществляется через следующие параметры:

Доступ к информации в панели администрирования:

Доступ к аналитике в панели администрирования:

Доступ к экспорту в панели администрирования:

Каждое поле может принимать следующие значения:

- deny — доступ запрещен для всех пользователей;
- allow — доступ разрешен для всех пользователей;
- любое другое значение — наименование группы, которой будет разрешен доступ к данному компоненту. Можно перечислить несколько групп через пробел.

## Настройка обратной связи

Перейдите в раздел **Настройка обратной связи**:

Настройки VKT Отмена Сохранить

- Основные настройки
- [Настройки SSL/TLS](#)
- [Настройки доступа к панели администрирования](#)
- [Настройки обратной связи](#)
- [Настройки синхронизации пользователей с LDAP](#)

По умолчанию все обращения пользователей поступают на адрес `myteamsupport@USER-DOMAIN`, через локальный SMTP-релей. Например, в случае домена **example.com** обращение поступит на адрес **myteamsupport@example.com**.

Обратный адрес для писем:

Адрес получателя:

 —  
[+ Добавить](#)

Тема письма:

Адрес SMTP сервера:

Порт SMTP сервера:

Имя пользователя для SMTP авторизации:

Пароль для SMTP авторизации:

Принудительно использовать TLS для SMTP сервера:

В полях **Обратный адрес для писем** и **Адрес получателя** в адреса, оканчивающиеся символом @, автоматически подставляется домен пользователя.

Параметр	Описание	Примеры
<b>Обратный адрес для писем</b>	Обратный адрес для письма, формируемого системой в адрес технической поддержки	<ul style="list-style-type: none"> <li>• test@ — обратный адрес будет test@user-domain</li> <li>• test@example.com — обратный адрес будет test@example.com, независимо от домена пользователя</li> </ul>

Параметр	Описание	Примеры
<b>Адрес получателя</b>	Адрес получателей. Получателей может быть несколько	<ul style="list-style-type: none"> <li>['test@'] — получателем письма будет test@user-domain</li> <li>['test@', 'example@example.com'] — получателями письма будут test@user-domain и example@example.com</li> </ul>
<b>Тема письма</b>	Тема отправляемого письма	

### Расширенные настройки сервиса:

Используйте расширенные настройки, если хотите отправлять обращения пользователей через отдельный SMTP-сервер с использованием авторизации.

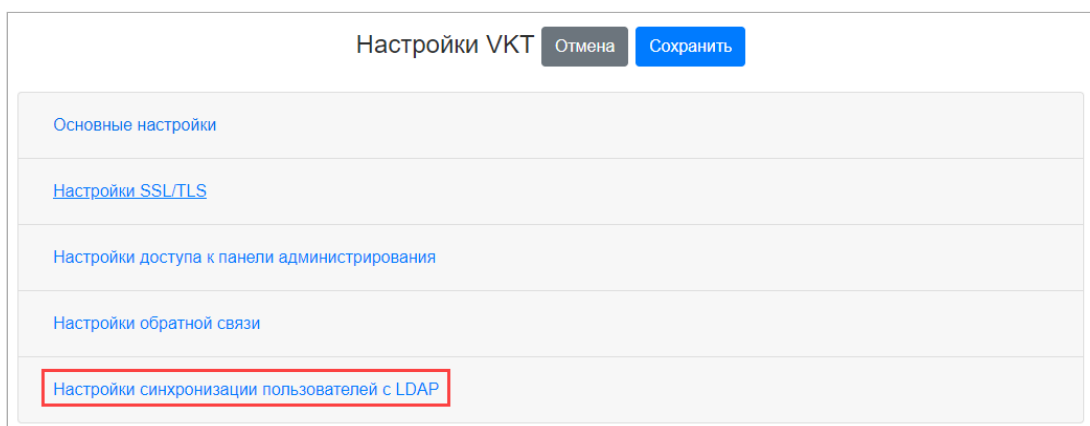
## Настройка LDAP

Пропустите этот шаг, если планируете подключить Панель администратора VK WorkSpace. Перейдите к шагу проверки конфигурации.

Система предоставляет возможность указать настройки для соединения с LDAP-сервером во время инсталляции или после ее завершения.

Если инсталляция производится без связи с корпоративным LDAP-сервером или LDAP-сервер отсутствует, пропустите данный шаг и [перейдите к проверке конфигурации](#). Описание процесса настройки интеграции с LDAP после инсталляции представлено в документе [Инструкция по интеграции с контроллером домена по протоколу LDAP](#).

Если настройки для соединения с LDAP-сервером производятся во время инсталляции, в установщике перейдите в раздел **Настройка синхронизации пользователей с LDAP**:



Рекомендуется предварительно проверить корректность заданных конфигурационных параметров LDAP с помощью утилиты **ldapsearch**:

```
//установка клиента для подключения к AD
yum install openldap-clients -y
```

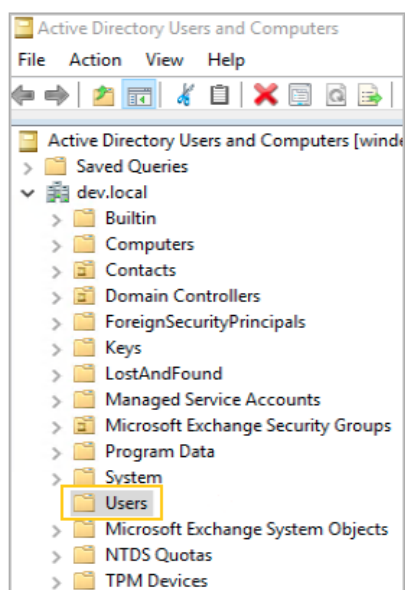


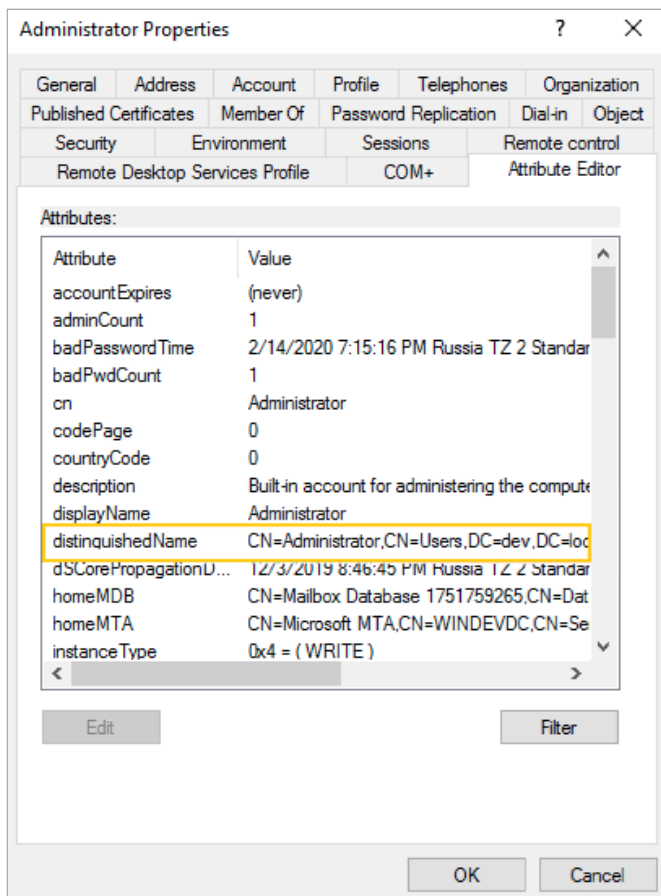
- **Частота полной синхронизации с LDAP-сервером, в секундах** — как часто осуществлять полную синхронизацию с LDAP-сервером, в секундах.
- **Частота частичной синхронизации с сервером, в секундах** — как часто осуществлять частичную синхронизацию с LDAP-сервером, в секундах (значение **-1** — отключить).
- **Максимальное количество пользователей, обновляемых одной транзакцией** — изменяйте в случае, если ваш LDAP-сервер отказывается отдавать пользователей с ошибкой о превышении размера транзакции.
- **Фильтр для получения пользователей** — позволяет получать не всех пользователей из указанного дерева. По умолчанию выборка пользователей не ограничена.

## Как получить Distinguished Name для bindDN и usersDN в Active Directory

1. В оснастке **Active Directory Users and Computers** выберите пользователя, под которым будет происходить подключение и поиск пользователей.
2. Выберите свойства и перейдите на вкладку **Attribute Editor** (если вкладки нет, выберите в меню **View**, затем **Advanced Features**).

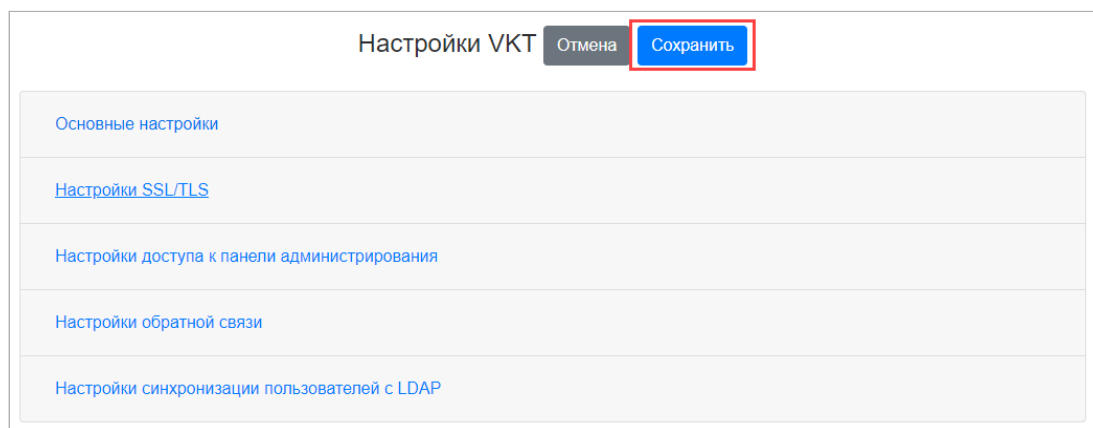
На вкладке будет отображено значение **distinguishedName**. Повторите операцию, чтобы получить **distinguishedName** для каталога, в котором будет выполняться поиск пользователей.





## Шаг 14. Проверка конфигурации

Чтобы сохранить указанные настройки, нажмите на кнопку **Сохранить**:




После сохранения настроек будет произведена их проверка. Если открыты не все нужные порты, либо нет интеграции с базовым набором сервисов (DNS, SMTP, NTP), отобразится уведомление о необходимости правок:



В случае обнаружения ошибок, их необходимо исправить.

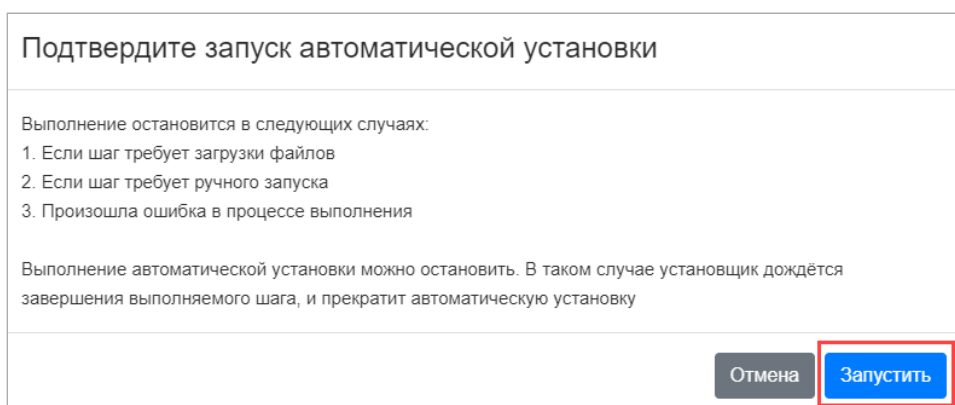
## Шаг 15. Запуск установки

После завершения настройки и проверки ошибок необходимо перейти на главную страницу и запустить

установку нажатием на кнопку  :

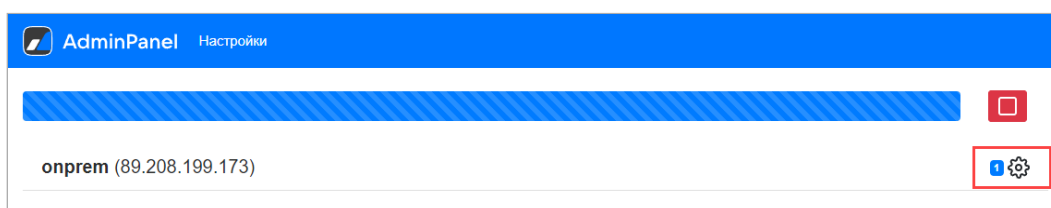


Подтвердите запуск автоматической установки, нажав на кнопку **Запустить**:



Для просмотра результата выполнения установки:

1. Нажмите на пиктограмму  :



2. Нажмите на ссылку **Результат выполнения**:

**AdminPanel** Настройки

Название машины	Имя хоста	IP	Внешний IP
vkt-1vm1	onprem	89.208.199.173	89.208.199.173
SSH-порт	Имя пользователя	Пароль	Приватный ключ
22	centos	*****	key
Сторона	Номер пары хостов		
	0		

### Выполните шаги по настройке машины

**vkt\_premsetup** inProgress  
Настроить VKT1VM

Результат выполнения

По окончании процесса инсталляции в строке состояния отображается сообщение **Установка завершена**:

**AdminPanel** Настройки

Установка завершена

onprem (89.208.199.173)

## Шаг 16. Рестарт машины

По окончании процесса установки выполните в консоли рестарт машины:

```
reboot
```

На этом установка Мессенджер и ВКС считается завершенной. [Перейдите к проверкам](#) инсталляции и основных функциональностей.

# Установка Мессенджер и ВКС из консоли

Для установки из консоли необходимо выполнить шаги, представленные ниже.

## Внимание

Все команды в консоли выполняются под пользователем root.

## Шаг 1. Предварительные условия для установки

Перед началом инсталляции убедитесь, что выполнены все предварительные условия (см. раздел [Предварительные условия для установки](#)).

## Шаг 2. Проверка целостности полученных образов виртуальных машин

Чтобы проверить целостность образов виртуальных машин, в директории со скачанными файлами выполните в командной строке:

### Linux

```
md5sum *
```

### Windows

```
CertUtil -hashfile myteam.ova MD5  
CertUtil -hashfile myteam.qcow2 MD5  
CertUtil -hashfile myteam-data.qcow2 MD5
```

### macOS

```
md5 *
```

Далее сравните полученное значение с хеш-суммой, указанной в текстовом файле **md5.txt**, распространяемом с дистрибутивом.

## Шаг 3. Создание виртуальной машины

Создайте виртуальную машину на основе предоставленных образов.

При создании виртуальной машины с предоставленного образа (root), необходимо создать и подключить новый пустой раздел data для хранения данных, генерируемых при работе системы. При обновлении версии дистрибутива, раздел root будет пересоздаваться из нового образа, раздел data — переноситься с рабочего экземпляра.

## Шаг 4. Запуск образа виртуальной машины

Запустите образ виртуальной машины.

## Шаг 5. Подключение к виртуальной машине

Подключитесь к виртуальной машине по SSH.

Пользователь: **centos**

Пароль: **djhMRG1vO**

### **Внимание**

Чтобы получить пароль для пользователя root, обратитесь в службу технической поддержки.  
После подключения к виртуальной машине пароли для пользователей root и centos необходимо сменить.

**macOS или Linux:**

```
ssh centos@<VM IP address>
```

**Windows:** зависит от используемого SSH-клиента.

## Шаг 6. Настройка сети

По умолчанию виртуальная машина получит сетевую конфигурацию по DHCP. Если необходимо заменить динамическую конфигурацию на статическую, воспользуйтесь инструкцией ниже.

Сконфигурировать сетевой интерфейс **eth0** или **ens160**:

1. В файле **/etc/sysconfig/network-scripts/ifcfg-ens160** указать необходимые параметры (адреса, маску и mac-адрес от конкретной инсталляции):

```
BOOTPROTO=none
DEFROUTE=yes
DEVICE=eth0
GATEWAY=85.192.35.254
HWADDR=fa:16:3e:a4:72:39
IPADDR=85.192.33.158 MTU=1500 NETMASK=255.255.252.0
```

```
ONBOOT=yes
STARTMODE=auto
TYPE=Ethernet
USERCTL=no
```

### Важно

HWADDR должен совпадать с тем, что отображается у виртуальной машины в веб-интерфейсе виртуализации.

2. Активировать сетевой интерфейс командой:

```
ifup ens160
```

## Шаг 7. IP-адрес

Перед началом инсталляции необходимо определить, будет ли доступен сервис в интернете.

Если сервис не будет доступен в интернете, то необходимо использовать внутренний IP-адрес разворачиваемой виртуальной машины.

Если сервис будет доступен в интернете, необходимо использовать внешний IPv4 адрес виртуальной машины. Адрес может быть поднят как внутри виртуальной машины, так и проброшен через NAT. Преобразование сетевых адресов (NAT) должно быть вида 1-в-1 (сеть в сеть), то есть с сохранением номера порта. Иначе видео и голосовые звонки могут не работать.

IP-адрес в дальнейшем будет использоваться для заполнения конфигурационного файла инсталляции.

## Шаг 8. Настройки DNS-зоны

Заведите в DNS-зоне имена хостов, которые будут смотреть на внешний IPv4 адрес.

Список имен (CNAME либо A-записи на ваше усмотрение):

- admin — адрес API управления Мессенджер и ВКС (административного веб интерфейса).
- akessadmin
- api — API бота.
- biz — адрес сервера Мессенджер и ВКС, где находится сервис Grafana.
- calendar — API календаря. Работает только в интеграции с Почтой VK WorkSpace.
- calendar-mobile — API мобильного календаря. Работает только в интеграции с Почтой VK WorkSpace.
- call — URL для формирования ссылок на звонки.
- di — поддомен сервиса Keycloak для версий до 25.2.

- dl — портал загрузки дистрибутивов (система автоматического обновления клиентских приложений).
- files-n — оргструктура организаций.
- kc — поддомен сервиса Keycloak для версии 25.2 и выше.
- notp
- outlook-plugin — плагин MS Outlook для создания конференций.
- rapi
- s — обмен стикерпаками.
- stentor — адрес API Мессенджер и ВКС для добавления/удаления пользователей.
- u — адрес клиентского API Мессенджер и ВКС.
- ub — файловое API.
- webim — веб-версия Мессенджер и ВКС.

Например, для домена vkteams.example.com имя хоста будет выглядеть как u.vkteams.example.com.

### Вариант 1.

Если есть возможность создания записи Wildcard CNAME в DNS, то можно создать A-запись, указывающую на адрес сервера Мессенджер и ВКС, и запись Wildcard CNAME, указывающую на A-запись сервера Мессенджер и ВКС.

```
$ host -t axfr example.com | grep vkteams
vkteams.example.com.      3600    IN      A       172.27.59.10
*.vkteams.example.com.   3600    IN      CNAME   vkteams.example.com.
```

### Вариант 2.

Если нет возможности создания записи Wildcard CNAME в DNS, то можно создать A-запись, указывающую на адрес сервера Мессенджер и ВКС, и отдельные записи CNAME, которые будут разрешаться на созданную A-запись. Записи CNAME должны соответствовать перечню имен, представленному выше.

```
$ host -t axfr example.com | grep vkteams
vkteams.example.com.      3600    IN      A       172.27.59.10
admin.vkteams.example.com. 3600    IN      CNAME   vkteams.example.com.
akesadmin.vkteams.example.com. 3600    IN      CNAME   vkteams.example.com.
api.vkteams.example.com.  3600    IN      CNAME   vkteams.example.com.
biz.vkteams.example.com.  3600    IN      CNAME   vkteams.example.com.
calendar.vkteams.example.com. 3600    IN      CNAME   vkteams.example.com.
calendar-mobile.vkteams.example.com. 3600    IN      CNAME   vkteams.example.com.
call.vkteams.example.com. 3600    IN      CNAME   vkteams.example.com.
di.vkteams.example.com.   3600    IN      CNAME   vkteams.example.com. # только для
версий до 25.2
dl.vkteams.example.com.   3600    IN      CNAME   vkteams.example.com.
files-n.vkteams.example.com. 3600    IN      CNAME   vkteams.example.com.
kc.vkteams.example.com.   3600    IN      CNAME   vkteams.example.com. # только для
версии 25.2 и выше
notp.vkteams.example.com. 3600    IN      CNAME   vkteams.example.com.
outlook-plugin.vkteams.example.com. 3600    IN      CNAME   vkteams.example.com.
rapi.vkteams.example.com. 3600    IN      CNAME   vkteams.example.com.
s.vkteams.example.com.    3600    IN      CNAME   vkteams.example.com.
stentor.vkteams.example.com. 3600    IN      CNAME   vkteams.example.com.
```

u.vkteams.example.com.	3600	IN	CNAME	vkteams.example.com.
ub.vkteams.example.com.	3600	IN	CNAME	vkteams.example.com.
webim.vkteams.example.com.	3600	IN	CNAME	vkteams.example.com.

### **Внимание**

Не вносите изменения в **etc/resolv.conf**. Если изменения всё же необходимо внести, то первым должен быть указан хост 127.0.0.1.

## Шаг 9. Выпуск SSL-сертификата

В целях безопасности используется SSL-шифрование, для работы сервера необходимо выпустить SSL-сертификат.

Если Вы используете сертификаты собственного центра сертификации, выпустите сертификат, который далее понадобится при настройке Мессенджер и ВКС (см. [Настройки SSL-сертификата](#)). Используйте Wildcard-сертификат, например \*.vkteams.EXAMPLE.com, или сертификат с указанием всех необходимых имен (см. раздел [Настройки DNS-зоны](#)).

Для SSL-сертификатов также можно использовать протокол ACME (поддерживается только провайдер Let`s Encrypt). В этом случае получение и продление сертификатов — автоматическое.

## Шаг 10. Открыть доступы до внутренних ресурсов

### **Входящие соединения на стороне сервера Мессенджер и ВКС:**

Открыть порты: 80/TCP, 443/TCP, 3478/TCP + UDP, UDP-порты выше 1024.

### **Исходящие соединения на стороне сервера Мессенджер и ВКС:**

- **Открыть доступ для серверов отправки уведомлений:**

необходимо обеспечить доступ к серверам Google и Apple для отправки и корректной работы push-уведомлений на мобильных платформах Android и iOS.

**Сервер Apple** TCP 5223;443;2197.

IP 17.0.0.0/8

[Статья на сайте apple.com](#)

**Сервер Google** TCP 5228;5229;5230;443

[Информация на ipinfo.io](#)

[Статья на сайте google.com](#)

Если в вашей организации используются механизмы ограничения доступа сетевого трафика, убедитесь, что открыт доступ к следующим доменам (по HTTPS, порт 443):

fcm.googleapis.com

www.googleapis.com

oauth2.googleapis.com  
accounts.google.com

- **Открыть доступ до всех внутренних ресурсов:** LDAP, NTP, SMTP, DNS.

## Шаг 11. Настройка LDAP

Пропустите этот шаг, если планируете подключить Панель администратора VK WorkSpace. Перейдите к шагу проверки конфигурации.

Система предоставляет возможность указать настройки для соединения с LDAP-сервером во время инсталляции или после ее завершения.

Если инсталляция производится без связи с корпоративным LDAP-сервером или LDAP-сервер отсутствует, пропустите данный шаг и [перейдите к подготовке конфигурационного файла инсталляции](#). Описание процесса настройки интеграции с LDAP после инсталляции представлено в документе [Инструкция по интеграции с контроллером домена по протоколу LDAP](#).

Ниже представлено описание процесса настройки интеграции с LDAP во время инсталляции Мессенджер и ВКС.

Для включения интеграции с LDAP необходимо скопировать в каталог `/usr/local/etc/premsetup/ldap`:

- Настройки ваших LDAP-серверов — файлы с расширением **\*.yaml**. Название файла может быть произвольным.
- Root CA сертификаты ваших LDAP-серверов в формате PEM — файлы с расширением **\*.pem**. Требуется только для подключения с использованием SSL (протокол `ldaps://`) и не требуется для подключения без SSL (протокол `ldap://`).

Далее выполните команды:

```
//установка клиента для подключения к AD
yum install openldap-clients -y

// проверка, что параметры подключения к AD валидны
ldapsearch -H <ldap_url> -w <ldap_password> -x -D
<ldap_bind_dn> -b <ldap_users_dn> mail=ldap-user-email@EXAMPLE.com
```

, где **mail=ldap-user-email@EXAMPLE.com** — почтовый ящик пользователя

Пример настройки LDAP-сервера в **\*.yaml**:

```
name: onpremise
config:
  connectionUrl: "ldaps://ad.ad.on-premise.ru:636"
  usersDn: "OU=ad,DC=ad,DC=onpremise,DC=ru"
  bindDn: "CN=VKTeams Syncer,CN=Users,DC=ad,DC=onpremise,DC=ru"
  bindCredential: "PASSWORD"
  searchScope: 1
  fullSyncPeriod: 600
  changedSyncPeriod: -1
```

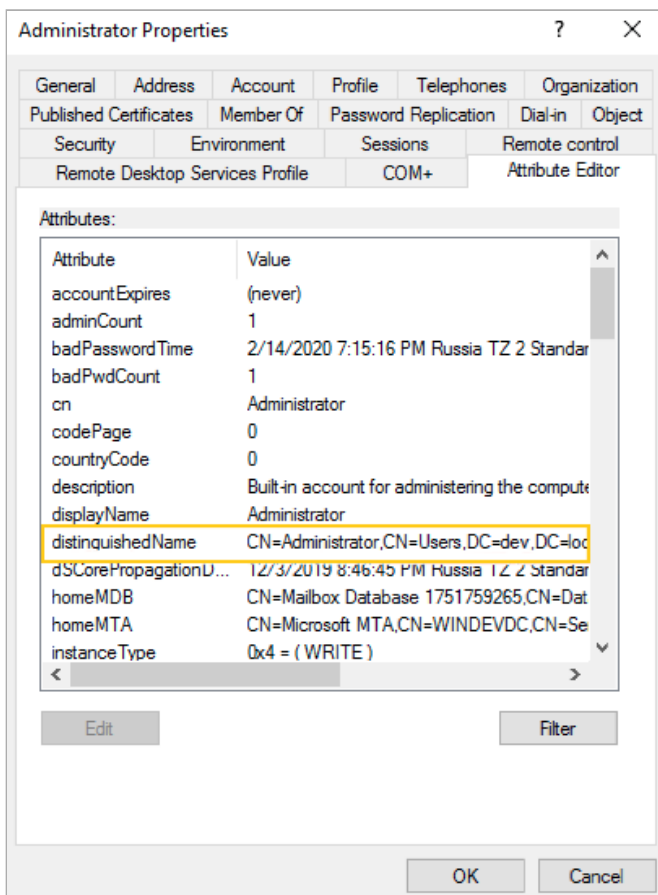
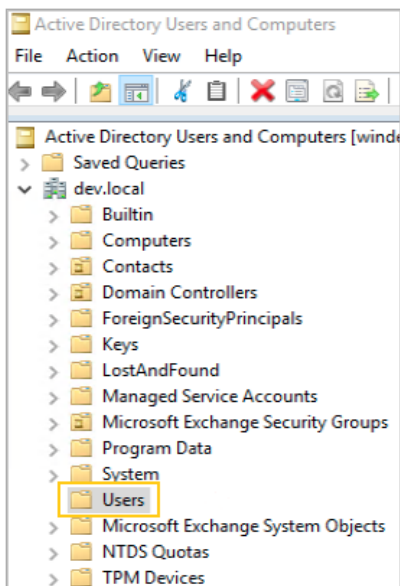
В случае если одно из полей не заполнено, то устанавливается значение по умолчанию для сервиса Keycloak. Основные доступные поля:

- **name** — имя LDAP-сервера. Данное имя уникально, может быть заведен только один сервер с определенным именем.
- **connectionUrl** — адрес подключения к LDAP-серверу.
- **usersDn** — указание на точку входа для поиска в LDAP.
- **bindDn** — пользователь, под которым осуществляется подключение к LDAP-серверу.
- **bindCredential** — пароль для подключения к LDAP-серверу.
- **searchScope** — использование рекурсивного поиска по дереву LDAP:
  - 1 — искать в одном уровне (по умолчанию).
  - 2 — искать по всем уровням.
- **fullSyncPeriod** — частота полной синхронизации с LDAP-сервером, в секундах.
- **changedSyncPeriod** — частота частичной синхронизации с LDAP-сервером, в секундах (значение **-1** — отключить).
- **batchSizeForSync** — максимальное количество пользователей, обновляемых одной транзакцией. Изменяйте в случае, если ваш LDAP-сервер отказывается отдавать пользователей с ошибкой о превышении размера транзакции.
- **customUserSearchFilter** — фильтр для получения пользователей. Позволяет получать не всех пользователей из указанного дерева. По умолчанию выборка пользователей не ограничена.

## Как получить Distinguished Name для bindDN и usersDN в Active Directory

1. В оснастке **Active Directory Users and Computers** выберите пользователя, под которым будет происходить подключение и поиск пользователей;
2. Выберите свойства и перейдите на вкладку **Attribute Editor** (если вкладки нет, выберите в меню **View**, затем **Advanced Features**).

На вкладке будет отображено значение **distinguishedName**. Повторите операцию, чтобы получить **distinguishedName** для каталога, в котором будет выполняться поиск пользователей.



## Шаг 12. Подготовка конфигурационного файла ИНСТАЛЛЯЦИИ

Настройки сервера Мессенджер и ВКС расположены в файле `/usr/local/etc/premsetup/defaults.yaml`.

Все настройки задокументированы внутри файла. Необходимо удалить дефолтные значения и указать параметры вашей инсталляции.

### **Примечание**

Изменения необходимо вносить под учетной записью root.

```
sudo su
vi /usr/local/etc/premsetup/defaults.yaml
```

Нажать клавишу клавиатуры **I** для перехода в режим вставки и указать параметры инсталляции. Ниже приведено более подробное описание каждого пункта конфигурации.

## Список серверов точного времени (NTP)

Укажите список NTP-серверов (IP-адреса или имена хостов) в виде массива имен или IP-адресов серверов точного времени.

**Тип** — Массив строк

**Пример:**

```
ntp: [ '0.pool.ntp.org', '1.pool.ntp.org' ]
```

или

```
ntp:
  - 0.pool.ntp.org
  - 1.pool.ntp.org
```

## Список DNS-серверов

Укажите список DNS-серверов (IP-адреса серверов, которые будут использованы для разрешения имен).

**Тип** — Массив строк

**Пример:**

```
dns: [ '8.8.8.8', '1.1.1.1' ]
```

или

```
dns:
  - '1.1.1.1'
  - '8.8.8.8'
```

## Настройка SMTP-сервера

Чтобы настроить OTP via email, укажите:

- Имя или IP-адрес SMTP-сервера:

**Тип** — Строка

**Пример:**

```
smtp_server: '127.0.0.1'
```

- Порт SMTP-сервера. Как правило, не требует редактирования:

**Тип** — Строка

**Пример:**

```
smtp_port: '25'
```

- Обратный адрес для сообщений с OTP-кодами (поле **«From:»** в письме). Рекомендуется использовать реально существующий адрес:

**Тип** — Строка

**Пример:**

```
smtp_from: 'otp@vkteams.EXAMPLE.com'
```

## Настройка SSO-аутентификации

Если в дальнейшем планируется настройка SSO-аутентификации по протоколу SAML, установите в секции **saml\_enabled**: значение **True**.

**Тип** — Булевый

**Пример:**

```
saml_enabled: True
```

## Доменное имя сервера Мессенджер и ВКС

Для настройки сервера Мессенджер и ВКС укажите базовый домен. Например, vkteams.example.com означает, что клиентские приложения будут пытаться получить доступ к сайтам u.vkteams.example.com, ub.vkteams.example.com и т. д.

**Тип** — Строка

Пример:

```
domain: 'vkteams.EXAMPLE.com'
```

## IP-адрес

Укажите внешний или внутренний IP-адрес, присвоенный на шаге [IP-адрес](#).

Внешний IP-адрес должен быть проброшен внутрь виртуальной машины. Без его указания будут некорректно работать голосовые и видео-шлюзы.

**Тип** — Строка

**Пример:**

```
ext_ip: '172.27.59.10'
```

## Настройка сервиса записи звонков

Данный параметр контролирует сервис записи звонков. При его включении звонки будут записываться, готовая запись будет отправлена пользователю в личные сообщения с помощью бота. На данный момент запись доступна только в desktop приложениях. По умолчанию запись включена.

**Тип** — Булевый

**Пример:**

```
call-recording-enabled: True
```

, где:

- флаг **True** — включает запись звонка;
- флаг **False** — выключает запись.

## Настройки SSL-сертификата

Укажите SSL-сертификат, выпущенный на шаге выше (см. [Выпуск SSL-сертификата](#)).

- **ssl\_key:"** — приватный ключ для SSL-сертификата. Указывается в формате PEM и не должен быть защищен паролем. Приватный ключ необходимо указать полностью, включая `-----BEGIN RSA PRIVATE KEY-----` и `-----END RSA PRIVATE KEY-----`;
- **ssl\_cert:"** — SSL-сертификат сервера в формате PEM. Для корректной работы укажите всю цепочку сертификатов (full chain). SSL-сертификаты необходимо указать полностью, включая `-----BEGIN RSA PRIVATE KEY-----` и `-----END RSA PRIVATE KEY-----`;
- **verify\_ssl** — способ проверки SSL-сертификата. Возможные значения: True, False, путь до файла .ca\_bundle:
  - True — проверять сертификат с центрами сертификации (CA), встроенными в ОС (по умолчанию).

- `False` — не проверять SSL-сертификат, например в случае использования самоподписанного сертификата.
- Путь до `.ca_bundle` — использовать свой центр сертификации для проверки сертификата.
- `self_signed_cert` — если планируется добавлять самоподписанные сертификаты, то необходимо добавить этот флаг со значением `True`. По умолчанию значение `False`, а флага нет в файле `defaults.yaml`. Флаг нужно добавить самостоятельно и только в случае использования самоподписанных сертификатов.

#### **Внимание**

Обязательно указание вертикальной черты | после переменной и четырех пробелов в начале строк (см. пример ниже).

**Тип** — Многострочные переменные

**Пример:**

```
ssl_key: |
  -----BEGIN PRIVATE KEY-----
  your private key could be here
  -----END PRIVATE KEY-----
ssl_cert: |
  -----BEGIN CERTIFICATE-----
  First certificate in chain
  -----END CERTIFICATE-----
  -----BEGIN CERTIFICATE-----
  Second certificate in chain
  -----END CERTIFICATE-----
```

## Протокол ACME (Let`s Encrypt) для SSL-сертификатов

Переменные `ssl_key` и `ssl_cert` можно не заполнять, при включении сертификатов через ACME они игнорируются.

Настройки для управления ACME:

- `ssl_acme_enabled` — установите `True`, чтобы использовать протокол ACME (`ssl_key` и `ssl_cert` игнорируются). По умолчанию установлено `False` (ACME не используется).
- `ssl_acme_email` (строка) — почта, используемая при обращении к Let`s Encrypt. На эту почту будут поступать уведомления от сервиса Let`s Encrypt. Обязательный параметр, без корректной почты сертификаты выданы не будут.
- `use_default_domain` — включает получение SSL-сертификата через ACME для домена, указанного в переменной `domain` файла `defaults.yaml`. Если в DNS нет записи, которая позволяет разрешить имя домена на внешний IP-адрес, этот параметр нужно выключить (`False`). По умолчанию сертификат будет выпускаться (`True`).

### **Внимание**

Включение этой опции и использование указанной функциональности означает согласие с условиями использования, с которыми можно ознакомиться по адресу <https://letsencrypt.org/repository/>

**Тип** — Булевый/строка

**Пример:**

```
// использовать сертификаты от Let's Encrypt:
ssl_key: ''
ssl_cert: ''
ssl_acme_enabled: true
ssl_acme_email: ssl@vkteams.EXAMPLE.com

// использовать ssl_key / ssl_cert (вариант по умолчанию):
ssl_acme_enabled: false
ssl_key: |
  -----BEGIN PRIVATE KEY-----
  your private key could be here
  -----END PRIVATE KEY-----
ssl_cert: |
  -----BEGIN CERTIFICATE-----
  First certificate in chain
  -----END CERTIFICATE-----
  -----BEGIN CERTIFICATE-----
  Second certificate in chain
  -----END CERTIFICATE-----
```

### **Примечание**

Сертификат продлевается автоматически каждые 3 месяца, поэтому 80-й порт должен быть открыт — иначе сертификат не обновится.

## Установка разрешений для пользователей

Чтобы разрешить пользователям изменять информацию о себе в профиле мессенджера, установите значение **True** в следующих секциях:

- Разрешить изменение аватара:

**Тип** — Булевый

**Пример:**

```
allow_self_avatar_change: True
```

- Разрешить изменение имени и фамилии:

**Тип** — Булевый

**Пример:**

```
allow_self_name_change: True
```

- Разрешить внесение изменений в раздел «О себе»:

**Тип** — Булевый

**Пример:**

```
allow_self_info_change: True
```

Чтобы разрешить удаление отправленного сообщения в личных чатах/группах без уведомления участников, установите значение **True** в секции **silent\_message\_delete**.

**Тип** — Булевый

**Пример:**

```
silent_message_delete: True
```

## Настройка окружения администратора

Интерфейс администратора доступен только с выбранных IP-адресов и только выбранным пользователям. Также предусмотрена настройка ограничения доступа к выбранным разделам окружения администратора (например, к выгрузке чатов).

По умолчанию окружение администратора доступно с IP-адресов частных сетей (10.0.0.0/8, 172.16.0.0/12 и 192.168.0.0/16).

Доступ в окружение администратора настраивается через группы.

Изначально перечень групп с доступом в окружение администратора пуст, потому окружение недоступно никому. Управление доступом по группам осуществляется через параметр **otp\_permission**, который управляет настройками OTP-авторизации для разных сценариев.

Если настройки для соединения с LDAP-сервером производятся **во время инсталляции** — для параметра **otp\_permission** необходимо указать заранее подготовленное наименование группы из LDAP, в которую будут входить пользователи с доступом в окружение администратора (см. раздел [LDAP](#) в условиях).

Если инсталляция производится без связи с корпоративным LDAP-сервером — укажите для параметра **otp\_permission** наименование группы из LDAP, в которую будут входить пользователи с доступом в окружение администратора (см. раздел [LDAP](#) в условиях). Информация по управлению параметрами синхронизации LDAP после инсталляции Мессенджер и ВКС представлена в документе [Инструкция по интеграции с контроллером домена по протоколу LDAP](#)».

При отсутствии LDAP — укажите для параметра **otp\_permission** наименование группы, которое будете использовать при создании пользователей в системе вручную после окончания процесса инсталляции (описание процесса представлено в документе [Управление пользователями без контроллера домена](#)).

**Тип** — Словарь строка → Массив строк

## Пример:

```
// окружение администратора доступно всем пользователям:
otr_permission: {}

// окружение администратора недоступно никому (значение по умолчанию):
otr_permission:
  myteam-admin: []

// окружение администратора доступно группе myteam-admin в LDAP (через distinguished name,
подробнее про получение distinguished name из AD см. в разделе "Как получить Distinguished
Name для bindDN и usersDN в Active Directory" выше):
otr_permission:
  myteam-admin:
    - 'CN=myteam-admin,OU=HQ,DC=dev,DC=local'

// окружение администратора доступно группе myteam-admin без LDAP:
otr_permission:
  myteam-admin:
    - 'myteam-admin'
```

Управление доступом по группам к выбранным компонентам осуществляется через параметры **myteam\_admin\_permissions** и **myteam\_admin\_default\_permissions**.

Перечень доступных компонентов:

- **Information** — информация о системе, документация.
- **Analytics** — информация о состоянии системы, графики и аналитика.
- **Export** — выгрузка участников групп.

Параметр **myteam\_admin\_default\_permissions** определяет правило доступа к компоненту по умолчанию, а параметр **myteam\_admin\_permissions** позволяет разграничить доступ на уровне групп в LDAP.

По умолчанию доступ к компонентам **Information** (раздел «Информация») и **Analytics** (раздел «Аналитика») имеют все пользователи с доступом к окружению администратора. К компоненту **Export** (раздел «Выгрузка») доступа нет ни у кого.

**Тип** — Массив строк

## Пример:

```
// компоненты Information и Analytics доступны всем, Export – никому (значение по умолчанию):
myteam_admin_default_permissions:
myteam_admin_permissions:

// компоненты Information и Analytics доступны всем, а Export – группе myteam-admin-export в
LDAP (через distinguished name, подробнее см. в разделе "Как получить Distinguished Name для
bindDN и usersDN в Active Directory" выше):
myteam_admin_default_permissions:
myteam_admin_permissions:
  Export:
    - 'CN=myteam-admin-export,OU=HQ,DC=dev,DC=local'

// компоненты Information и Export доступны всем, а Analytics – группе myteam-admin-analytics
без LDAP:
myteam_admin_default_permissions:
```

```
Export: allow
Analytics: deny
myteam_admin_permissions:
  Analytics:
    - 'myteam-admin-analytics'
```

Управление доступом на уровне IP осуществляется через параметр **myteam\_admin\_acl**. По умолчанию доступ предоставляется из подсетей rfc1918 (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) и 127.0.0.0/8.

**Тип** — Массив строк

#### Пример:

```
// окружение администратора недоступно ни с одного IP-адреса:
myteam_admin_acl: []

// окружение администратора доступно для подсетей rfc1918 и 127.0.0.0/8 (значение по умолчанию):
myteam_admin_acl:

// окружение администратора доступно с адреса 1.1.1.1 и 10.11.12.0/24:
myteam_admin_acl:
  - '1.1.1.1'
  - '10.11.12.0/24'
```

## Настройка обратной связи

По умолчанию все обращения пользователей поступают на адрес `myteamsupport@USER-DOMAIN`, через локальный SMTP-релей. Например, в случае домена **example.com** обращение поступит на адрес **myteamsupport@example.com**.

#### Базовые настройки сервиса:

В полях **from** и **rcpt\_to** в адреса, оканчивающиеся символом @, автоматически подставляется домен пользователя.

```
feedback_config:
  from: "myteamsupport@"
  rcpt_to: ["myteamsupport@"]
  subject: "Мессенджер и ВКС. Обратная связь"
```

Параметр	Тип	Описание	Примеры
<b>from</b>	Строка	Обратный адрес для письма, формируемого системой в адрес технической поддержки	<ul style="list-style-type: none"><li>• test@ — обратный адрес будет test@USER-DOMAIN</li><li>• test@example.com — обратный адрес будет test@example.com, независимо от домена пользователя</li></ul>
<b>rcpt_to</b>	Массив		<ul style="list-style-type: none"><li>• ['test@'] — получателем письма будет test@USER-DOMAIN</li></ul>

Параметр	Тип	Описание	Примеры
		Адрес получателей. Получателей может быть несколько	• [ 'test@', 'example@example.com' ] – получателями письма будут test@USER-DOMAIN и example@example.com
<b>subject</b>	Строка	Тема отправляемого письма	

### Расширенные настройки сервиса:

Используйте расширенные настройки, если хотите отправлять обращения пользователей через отдельный SMTP-сервер с использованием авторизации.

```
feedback_config:
  host: "localhost"
  port: 25
  username: ""
  password: ""
  use_tls: false
  from: "myteamsupport@" # myteamsupport@external_domain
  rcpt_to: ["myteamsupport@"] # myteamsupport@external_domain
  subject: "Myteam Feedback"
```

Параметр	Тип	Описание	Значение / настройка по умолчанию
<b>host</b>	Строка	Адрес SMTP-сервера	localhost
<b>port</b>	Int	Порт SMTP-сервера	25
<b>username</b>	Строка	Имя пользователя для авторизации на SMTP-сервере	без авторизации
<b>password</b>	Строка	Пароль для авторизации на SMTP-сервере	без авторизации
<b>use_tls</b>	Boolean	Форсировать использование TLS для SMTP-сервера	выключено

#### Примечание

По окончании заполнения конфигурационного файла инсталляции необходимо последовательно нажать **Esc :wq Enter** для сохранения внесенных изменений.

## Шаг 13. Проверка конфигурационного файла на ошибки

Чтобы проверить конфигурационный файл инсталляции `/usr/local/etc/premsetup/defaults.yaml` на ошибки, выполните команду:

```
im_deployer -t
```

Данная команда позволяет проверить, верно ли указаны настройки системы. Если открыты не все нужные порты, либо нет интеграции с базовым набором сервисов (DNS, SMTP, NTP), в консоли отобразится уведомление о необходимости правок.

## Шаг 14. Инициализация сервисов

После заполнения конфигурационного файла инсталляции необходимо произвести инициализацию сервисов Мессенджер и ВКС.

Для инициализации всех сервисов выполните команду:

```
im_deployer --init
```

## Шаг 15. Запуск скрипта конфигурации

Чтобы запустить скрипт конфигурации сервера Мессенджер и ВКС, выполните команду:

```
im_deployer --install
```

Если скрипт отработал без ошибок, в результатах выполнения отобразится список установленных модулей и сообщение в консоли `all is fine`.

## Шаг 16. Рестарт машины

Далее выполните рестарт виртуальной машины командой:

```
reboot
```

На этом установка Мессенджер и ВКС считается завершенной. [Перейдите к проверкам](#) инсталляции и основных функциональностей Мессенджер и ВКС.

# Проверки после инсталляции

По прошествии 15 минут после рестарта машины подключитесь к ней по SSH и выполните следующие проверки инсталляции:

## 1. Правильность версии релиза:

```
cat /etc/myteam-release
```

## 2. Состояние служб:

```
- systemctl status | grep '^ *State:'
```

Если в выводе есть статус «degraded», то список служб, которые завершились с ошибкой, можно посмотреть при помощи команды:

```
- systemctl --all --failed
```

## 3. Результаты выполнения скриптов внутреннего мониторинга системы:

```
mon.sh clean // очищаем логи  
mon.sh
```

Проанализируйте вывод команды в соответствии с [мониторингом параметров сервиса](#).

### Примечание

Отличие скрипта `mon.sh` от `/usr/share/check-mk-agent/local/local_check_exec.py` в том, что скрипт `mon.sh` отображает только ошибки, игнорируя успешно выполненные проверки.

## 4. Готовность сервисов Мессенджер и ВКС:

```
ic srvs
```

Все сервисы должны находиться в состоянии **alive**.

## 5. Состояние подов Kubernetes:

```
kubectl get pods -A
```

Все сервисы должны быть в состоянии Running.

## 6. Понаблюдайте за нагрузкой CPU и памяти при помощи утилиты k9s.

Также выполните проверки функциональностей Мессенджер и ВКС. Рекомендуется проводить тест при помощи разных типов клиентов, например веб и десктоп.

#### 1. Базовые функциональности:

- Возможность залогиниться в учетной записи.
- Отправить/получить текстовое сообщение с одного клиента на другой и обратно. Убедиться, что сообщения пришли.
- Удалить отправленные сообщения у себя и у всех. Убедиться, что сообщения успешно удаляются.
- Отправить/получить фото/видео/gif с одного клиента на другой и обратно. Проверить, что есть превью.
- Отправить/получить голосовое сообщение с одного клиента на другой и обратно. Убедиться, что запись полноценная и хорошего качества.
- Открыть витрину стикеров, открыть стикерпак. Убедиться, что все отображается корректно.
- Отправить/получить стикер с одного клиента на другой и обратно. Убедиться, что у стикера есть превью.
- Открыть собственный профиль и профиль другого пользователя.

#### 2. Группы:

- Создать группу/канал.
- Добавить пользователя в канал
- Отправить/получить несколько сообщений, которые содержат стикеры и файлы. Убедиться, что сообщения доходят до всех участников.
- Заблокировать/разблокировать участника.
- Закрепить сообщение.
- Удалить пользователя.
- Удалить группу/канал.

#### 3. Звонки:

- Позвонить пользователю. Добавить еще одного пользователя в звонок.
- Создать ссылку на звонок, перейти в звонок по ссылке.
- Проверить работу длительных звонков (около 5 минут).

#### 4. Статусы:

- Поставить/удалить статусы.

# Повторный запуск конфигуратора

---

Конфигуратор возможно запускать повторно в случае возникновения ошибок во время инсталляции или при обновлении дистрибутива.

Однако при повторном запуске нужно учитывать некоторые особенности — они определяются флагами, создаваемыми командой `im_deployer --install` при первом запуске:

- `/var/tmp/premsetup.run` — удалите этот флаг, после чего команду `im_deployer --install` можно запустить снова.
- `/mnt/data/premsetup/flags/premsetup.run` — при наличии этого флага команда `im_deployer --install` не будет изменять настройки LDAP, однако будет изменять остальные настройки. Это предотвращает поломку системы синхронизации пользователей, в случае если изменения вносились через веб-интерфейс.

## Внесение изменений в настройки инсталляции

---

Если необходимо внести изменения в конфигурацию:

1. Подключитесь к виртуальной машине ([шаг 5](#)).
2. Внесите необходимые изменения в настройки сети, LDAP, DNS, открытые доступы и/или конфигурационный файл инсталляции ([шаги 6-12](#)).
3. Выполните проверку конфигурации на ошибки и запустите скрипт конфигурации ([шаги 13, 15](#)).

### Примечание

Инициализацию сервисов Мессенджер и ВКС (шаг 14) производить не надо.

4. Перезагрузите виртуальную машину ([шаг 16](#)) и проверьте инсталляцию и основные функциональности Мессенджер и ВКС (см. [необходимые проверки](#)).

 Технический писатель: Белова Ирина

 25 марта 2026 г.