# Мессенджер и ВКС

## Настройка ГОСТ TLS-шифрования



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).

# Дополнительная документация

Настройка ГОСТ TLS-шифрования на сервере VK WorkSpace — в инструкции описано, как включить и выключить ГОСТ TLS-шифрование на сервере Почты VK WorkSpace.

# Назначение документа

В инструкции описано, как включить и выключить ГОСТ TLS-шифрование на сервере Мессенджер и ВКС. ГОСТ Настройка TLS-шифрования обеспечивает поддержку российских криптографических стандартов для шифрования трафика между Супераппами VK WorkSpace.

> **Важно**
>
> Не вносите изменения в настройки контейнеров для работы ГОС- TLS-шифрования. При внесении изменений шифрование может не работать.

# Предварительные условия

1. 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.
2. Приобретите сертификат ГОСТ TLS. Это можно сделать с помощью инструкций на сайте УЦ КриптоПро или по инструкции Национального удостоверяющего центра.

   Ниже представлен список поддерживаемых Issuer:

   - C=RU, O=The Ministry of Digital Development and Communications, CN=Russian Trusted Root CA
   - ОГРН=1037700085444, ИНН=007717107991, C=RU, S=Moscow, L=Moscow, O="LLC ""Crypto-Pro""", CN=CryptoPro GOST Root CA
   - C=RU, O=The Ministry of Digital Development and Communications, CN=Russian Trusted Root CA
   - CN=НУЦ России, O=Минцифры России, ИНН ЮЛ=7710474375, ОГРН=1047702026701, C=RU, L=г. Москва, S=77 г.Москва, STREET="Набережная Пресненская, дом 10, строение 2"
   - E=dit@digital.gov.ru, C=RU, S=77 Москва, L=г. Москва, STREET="Пресненская набережная, дом 10, строение 2", O=Минцифры России, ОГРН=1047702026701, ИНН ЮЛ=7710474375, CN=Минцифры России
   - E=dit@minsvyaz.ru, C=RU, S=77 Москва, L=г. Москва, STREET="улица Тверская, дом 7", O=Минкомсвязь России, ОГРН=1047702026701, ИНН=007710474375, CN=Минкомсвязь России

   Также при создании сертификата одним из этапов будет создание файла .cnf. Он потребуется для дальнейшего создания сертификата.

   В нем должно быть указано:

   - В значении **CN** — имя основного домена вашей инсталляции Мессенджера VK WorkSpace.
   - В значении **subjectAltName** — имена доменов и поддоменов инсталляции, например: {domain}, *.{domain}. Если планируется использование Мессенджера VK WorkSpace вместе с Почтой VK WorkSpace, добавьте также почтовые домены.

     Если для обеспечения безопасности требуется указать весь список поддоменов, добавьте следующие поддомены:

     - admin.{domain}
     - akesadmin.{domain}
     - api.{domain}
     - calendar-mobile.{domain}
     - calendar.{domain}
     - call.{domain}
     - dl.{domain}

- files-n.{domain}
- kc.{domain}
- notp.{domain}
- outlook-plugin.{domain}
- rapi.{domain}
- s.{domain}
- stentor.{domain}
- u.{domain}
- ub.{domain}
- webim.{domain}

- В значении **certificatePolicies** — СКЗИ класса КС1 — 1.2.643.2.25.1.14.2, 1.2.643.100.113.1.

3. Настройка ГОСТ TLS-шифрования доступна начиная с версии Мессенджер и ВКС 25.4 и выше. Обновите инсталляцию на одну виртуальную машину по инструкции https://biz.mail.ru/docs/on-premises/vk-teams/1vm-upgrade-guide/index.html. Если у вас распределенная инсталляция, обратитесь за помощью в техническую поддержку.
4. Убедитесь, что до настройки ГОСТ TLS-шифрования в конфигурационном файле **/usr/local/nginx-im/html/myteam/myteam-config.json** для параметра **gost-hosts-regexes** указан пустой список или параметр отсутствует.

   Если вы внесли изменения в файл, примените изменения:

   Для инсталляции на одну виртуальную машину выполните команду:

   ```
   HELMWAVE_USE_LOCAL_REPO_CACHE=true hwup -t godmod
   ```

   Для кластерной инсталляции:

   ```
   HELMWAVE_USE_LOCAL_REPO_CACHE=true HELMWAVE_ENV_NAME=cluster hwup -t godmod
   ```

   Перезапустите под в технологическое окно (может приводить к сбою в новых подключениях):

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

5. Если настроена интеграция с Почтой VK WorkSpace, получите от администратора Почты следующие данные для интеграции по сети:
   - IP-адрес интерфейса пира.
   - IP-адрес BGP-пира.
   - Номер AS пира.
   - Префиксы импортируемых сетей.
   - IP-адреса DNS VK WorkSpace.
6. Получите от представителей VK ссылки для скачивания клиентского приложения на iOS.

# Как включить ГОСТ TLS-шифрование

## Шаг 1. Настройте интеграцию с сервером VK WorkSpace

Пропустите этот шаг, если:

- у вас нет Почты VK WorkSpace
- есть Почта VK WorkSpace, но интеграция с Мессенджер и ВКС не настроена.

Чтобы настроить интеграцию:

1. Перейдите в конфигурационный файл **/etc/ctfact3.yaml** и укажите следующие настройки (значения параметров даны для примера):

```
service_configs:
  ws_integration_enabled: true
  ws_dns:
    - 172.5.5.5
    - 172.5.5.6
  bird_conf:
    local:
      as: 64501
    peers:
      - ip: 100.70.80.161
        as: 64502
      - ip: 100.70.80.162
        as: 64502
    import_prefix: 172.0.0.0/8
```

   где:

   - ws_integration_enabled — если true, включаем интеграцию сетей с VK WorkSpace.
   - ws_dns — массив IP-адресов DNS VK WorkSpace.
   - import_prefix — префиксы импортируемых сетей. По умолчанию — 172.0.0.0/8.
   - local — локальный пир, по умолчанию — 64501.
   - peers — массив удаленных пиров. У каждого пира можно указать: IP-адрес пира и as (номер автономной сети). У локального пира IP-адрес нужно указывать только, если Мессенджер развернут на одной виртуальной машине.

2. Чтобы применить изменения, выполните команду:

```
im_deployer --init-integration
```

# Шаг 2. Обновите клиентские приложения

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), скачайте и установите СКЗИ «КриптоПро CSP» версии 5.0R3 или выше. Скачать можно по ссылке https://www.cryptopro.ru/downloads

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

2. Обновите 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 DL-лендинга.
   - Для пользователей, которые будут пользоваться веб-версией, установите Яндекс Браузер — в него уже встроены необходимые сертификаты. Также можно использовать браузер Chromium-Gost.

#### DL-лендинг для дистрибуции клиентских приложений

Для дистрибуции клиентских приложений, поддерживающих ГОСТ-алгоритмы шифрования, используется специальный лендинг. Его можно включить после завершения настройки ГОСТ TLS-шифрования. Для этого перейдите в директорию /usr/local/bin и запустите скрипт apps_deploy.sh. После окончания работы скрипта клиентские приложения будут доступны по адресу dl.<ваш домен>.ru.

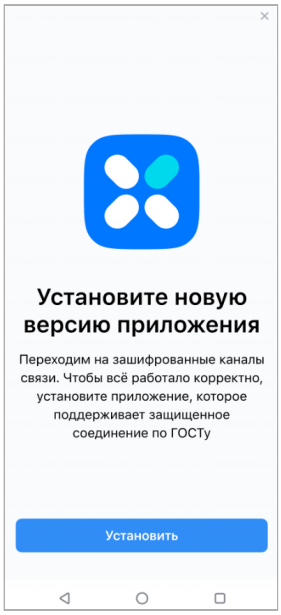
DL-лендинг поддерживает динамическую смену списка страниц в TestFlight. Таким образом DL предоставляет возможность оставлять только актуальные ссылки на TestFlight.

Как поменять ссылки на лендинге на iOS приложение:

1. Открыть или создать файл dl-config.json в корневой директории GOST-DL: /srv/myteam-onpremise-www-gost/htdocs.
2. В dl-config.json, в переменную-массив ios-build-links добавить ссылки на скачивание iOS приложения (например через TestFlight). Ссылки получите у представителей VK.
3. На DL будут отображены все ссылки из массива списком. Если массив пустой, секция iOS в DL будет содержать стандартную ссылку на приложение в магазине приложений.

**Если надо ускорить обновление приложений пользователями**

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 25.4 и выше.

Для этого:

1. В конфигурационном файле **/usr/local/nginx-im/html/myteam/myteam-config.json** 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 Супераппа 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. Для инсталляции на одну виртуальную машину выполните команду:

```
HELMWAVE_USE_LOCAL_REPO_CACHE=true hwup -t godmod
```

Для кластерной инсталляции:

```
HELMWAVE_USE_LOCAL_REPO_CACHE=true HELMWAVE_ENV_NAME=cluster hwup -t godmod
```

3. Перезапустите под в технологическое окно (может приводить к сбою в новых подключениях):

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

# Шаг 3. Настройте ГОСТ TLS-шифрование на сервере Мессенджер и ВКС

1. Перейдите в конфигурационный файл **/etc/ctfact3.yaml**, добавьте и заполните поля:

```
service_configs:
  gost_enabled: true
  gost_license:
  gost_certificate:
  gost_cert_password:
```

где:

- gost_enabled — если true, включаем ГОСТ TLS-шифрование на сервере.
- gost_license —лицензионный ключ КриптоПро.
- gost_certificate — сертификат ГОСТ TLS. Сертификат должен быть в формате PKCS#12 (.pfx), закодированный в Base64.
- gost_cert_password — пароль от сертификата ГОСТ TLS (при наличии).

2. Примените изменения.

Для инсталляции на одну виртуальную машину выполните команды:

```
im_deployer --init-gost
HELMWAVE_USE_LOCAL_REPO_CACHE=true hwup -t nginx-gost
```

Для кластерной инсталляции:

```
im_deployer --helmwave --update --hw-once --hw-project nginx-gost
```

# Шаг 4. Включите использование ГОСТ TLS-шифрования на клиентских приложениях

1. В конфигурационном файле **/usr/local/nginx-im/html/myteam/myteam-config.json** укажите для параметра **gost-hosts-regexes** список доменов, для которых будет использоваться ГОСТ TLS-шифрование.

   Домены указываются в виде регулярных выражений. Если домен соответствует хотя бы одному регулярному выражению в списке **gost-hosts-regexes**, то будет использоваться ГОСТ TLS-шифрование. Во всех остальных случаях будут использоваться стандартные алгоритмы.

   Если поле **gost-hosts-regexes** отсутствует в **/usr/local/nginx-im/html/myteam/myteam-config.json**, или значением является пустой список, то ГОСТ TLS-шифрование использоваться не будет.

   Примеры:

   Клиент будет использовать только стандартные алгоритмы шифрования:

   ```
   "gost-hosts-regexes": []
   ```

   Клиент будет использовать только ГОСТ TLS-шифрование — при запросах к vkt.mycompany.ru и запросах к любым другим ресурсам в интернете:

   ```
   "gost-hosts-regexes": [".*"]
   ```

   ГОСТ TLS-шифрование будет использоваться в запросах к доменам u.vkt.mycompany.ru и ub.vkt.mycompany.ru:

   ```
   "gost-hosts-regexes": ["u.vkt.mycompany.ru", "ub.vkt.mycompany.ru"].
   ```

   или

   ```
   "gost-hosts-regexes": ["(u|ub).vkt.mycompany.ru"]
   ```

   ГОСТ TLS-шифрование будет использоваться в запросах к vkt.mycompany.ru и ко всем его поддоменам (включаем шифрование на уровне инсталляции):

   ```
   "gost-hosts-regexes": [".*vkt.mycompany.ru$"].
   ```

ГОСТ TLS-шифрование будет использоваться в запросах к vkt.mycompany.ru и его поддоменам, кроме bot.vkt.mycompany.ru (и его поддоменов):

```
"gost-hosts-regexes": ["(?!.*bot).*vkt.mycompany.ru"].
```

> **Примечание**
>
> Можно обойтись одним регулярным выражением для любого списка доменов, но рекомендуется разбивать список на разные элементы для лучшей читаемости и удобства изменения.

2. После внесения изменений в **/usr/local/nginx-im/html/myteam/myteam-config.json** для инсталляции на одну виртуальную машину выполните команду:

   ```
   HELMWAVE_USE_LOCAL_REPO_CACHE=true hwup -t godmod
   ```

   Для кластерной инсталляции:

   ```
   HELMWAVE_USE_LOCAL_REPO_CACHE=true HELMWAVE_ENV_NAME=cluster hwup -t godmod
   ```

3. Перезапустите под в технологическое окно (может приводить к сбою в новых подключениях):

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

# Как проверить, что ГОСТ TLS-шифрование работает

В декстоп-версии клиентского приложения в разделе сервисов рядом с кнопкой настроек отображается иконка с надписью «Защищенное соединение по ГОСТ».

В мобильных версиях приложения вверху экрана отображается надпись «Защищенное соединение по ГОСТ».

В логах клиентских приложений есть строки «start vkgostproxy with gost hosts: ["u.vkt.mycompany.ru", "ub.vkt.mycompany.ru"]» и «gost support is enabled» (в пределах 5-10 строк друг от друга).

# Как выключить ГОСТ TLS-шифрование

## Шаг 1. Выключите ГОСТ TLS-шифрование на сервере Мессенджер и ВКС

1. В конфигурационном файле **/etc/ctfact3.yaml** установите для параметра **gost_enabled** значение false.

   Примените изменения:

   ```
   im_deployer --init-integration
   ```

   2. В конфигурационном файле **/usr/local/etc/k8s/helmwave/store/gost.yml** установите для параметра **gost_enabled** значение false.

   Примените изменения:

   Для инсталляции на одну виртуальную машину выполните команду:

   ```
   HELMWAVE_USE_LOCAL_REPO_CACHE=true hwup -t istio-ingress -t apigw
   ```

   Для кластерной инсталляции:

   ```
   HELMWAVE_ENV_NAME=cluster HELMWAVE_USE_LOCAL_REPO_CACHE=true hwup -t istio-ingress -t apigw
   ```

2. В конфигурационном файле **/usr/local/etc/k8s/helmwave/projects.yml** добавьте в список отключенных проектов **nginx-gost**:

   ```
   envs:
     all:
       projects:
         disabled:
           contactz:
           pacman:
           vipper:
           nginx-gost:
   ```

   Примените изменения:

   ```
   helm uninstall nginx-gost -n vkteams
   ```

3. Для инсталляции на одну виртуальную машину выполните команду:

   ```
   HELMWAVE_USE_LOCAL_REPO_CACHE=true hwup -t istio-ingress
   ```

   Для кластерной инсталляции:

   ```
   im_deployer --helmwave --update --hw-once --hw-project istio-ingress
   ```

## Шаг 2. Выключите ГОСТ TLS-шифрование на сервере VK WorkSpace

Пропустите этот шаг, если у вас нет Почты VK WorkSpace.

Если у вас есть Почта, выключите ГОСТ TLS-шифрование на сервере VK WorkSpace по инструкции... <ссылка на Почтовую>

## Шаг 3. Выключите использование ГОСТ TLS-шифрования на клиентских приложениях

1. В конфигурационном файле **/usr/local/nginx-im/html/myteam/myteam-config.json** укажите для параметра **gost-hosts-regexes** пустой список:

   ```
   "gost-hosts-regexes": []
   ```

2. Для инсталляции на одну виртуальную машину выполните команду:

   ```
   HELMWAVE_USE_LOCAL_REPO_CACHE=true hwup -t godmod
   ```

   Для кластерной инсталляции:

   ```
   HELMWAVE_USE_LOCAL_REPO_CACHE=true HELMWAVE_ENV_NAME=cluster hwup -t godmod
   ```

3. Перезапустите под в технологическое окно (может приводить к сбою в новых подключениях):

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

Технический писатель: Белова Ирина

16 марта 2026 г.