

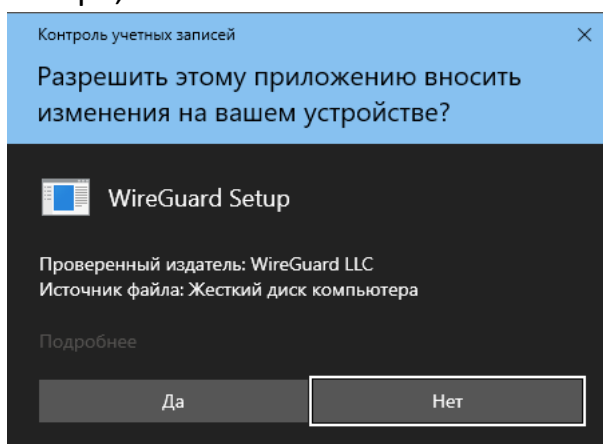
# Инструкция по установке и использованию VPN WireGuard для доступа к административному разделу сайта АТиСО за пределами территории академии

Если у Вас нет статического IP-адреса или вы не знаете, что это такое, проследуйте инструкции. **Если у Вас есть статический IP-адрес, сообщите его и название своей учётной записи на сайте на почту [xan@xan.dev](mailto:xan@xan.dev). В этом случае данная инструкция вам не потребуется.**

Для удобства установки и настройки выдаётся два компонента: QR-код и файл конфигурации. Первый используется для настройки на мобильных устройствах, второй – на настольных компьютерах. После установки не изменяйте существующие настройки!

## Windows

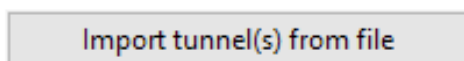
Скачать установщик по ссылке <https://download.wireguard.com/windows-client/wireguard-amd64-0.1.0.msi>, и нажать «да» при вопросе о внесении изменений на компьютере, если таковой возникнет:



Программа будет установлена автоматически.

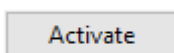
Запустить программу WireGuard, например, из главного меню.

Нажать кнопку

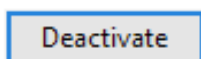


и выбрать предоставленный файл с конфигурацией.

Для включения нажать кнопку



, для выключения нажать кнопку



, либо завершить работу приложения.

## Mac OS

Установите приложение из AppStore. Это можно сделать, пройдя по ссылке <https://itunes.apple.com/us/app/wireguard/id1451685025?ls=1&mt=12> и нажав кнопку

[View in Mac App Store ↗](#)

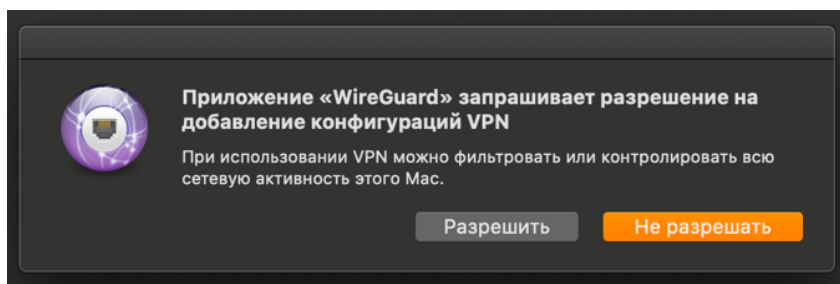
, если приложение AppStore не открылось автоматически.

В приложении AppStore нажать на кнопку Скачать. После установки открыть приложение WireGuard.

Import tunnel(s) from file

Нажать на кнопку , выбрать предоставленный файл с конфигурацией.

В случае появления окна, как представлено ниже, разрешить добавление VPN.



Для включения WireGuard нажать кнопку **Activate**, для выключения — **Deactivate**, которая будет находиться на том же месте.


## Linux/BSD


Пожалуйста, следуйте инструкциям на странице <https://www.wireguard.com/install/> в зависимости от используемого дистрибутива. В случае необходимости обращайтесь за поддержкой на почту [xan@xan.dev](mailto:xan@xan.dev).

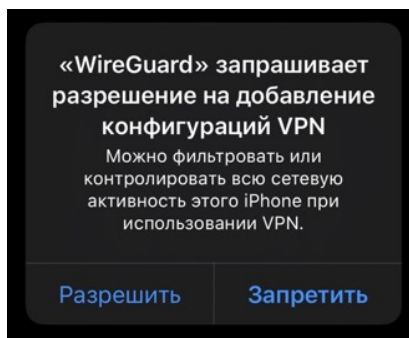
## iPhone или iPad

Скачайте приложение WireGuard из AppStore, открыв на мобильном устройстве ссылку:

<https://itunes.apple.com/us/app/wireguard/id1441195209?ls=1&mt=8>



Откройте установленное приложение и нажмите кнопку , а из появившегося меню — «Create from QR code». Разрешите приложению доступ к камере для того, чтобы иметь возможность сканировать QR-код. Откройте предоставленную картинку с QR-кодом и наведите на неё камеру телефона, разрешите добавление VPN



— настройки будут установлены автоматически.


Для включения WireGuard нажмите на переключатель напротив установленного в приложении WireGuard профиля, для выключения — нажмите ещё раз.

## Телефоны и планшеты на базе Android

Установите приложение WireGuard из PlayStore, открыв на мобильном устройстве ссылку:

<https://play.google.com/store/apps/details?id=com.wireguard.android>

После открытия приложения нажмите на кнопку «», а в появившемся

меню выберите пункт  SCAN FROM QR CODE . Разрешите приложению доступ к камере для сканирования QR-кода. Откройте на компьютере предоставленную картинку с QR-кодом и наведите на неё камеру мобильного устройства.

Введите любое название для добавленной конфигурации, после чего нажмите на кнопку CREATE TUNNEL:

Import Tunnel from QR Code

Tunnel Name

[CANCEL](#) [CREATE TUNNEL](#)

Для включения WireGuard нажмите на переключатель напротив установленного в приложении WireGuard профиля, для выключения — нажмите ещё раз.

## Конфиденциальность и технические детали

WireGuard – это VPN-туннель нового типа с простой настройкой, в связи с чем был выбран именно этот вариант. Использование VPN связано с необходимостью подключения к административной части сайта академии с заранее определённого статического IP-адреса. Представленная конфигурация VPN предусматривает маршрутизацию в туннель только одного конкретного IP-адреса, по которому расположен сайт академии — 195.208.1.108, а также всего исходящего DNS-трафика (на порт UDP/53) в период подключения к сети. Попытка расширения диапазона разрешённых для маршрутизации через туннель адресов в клиенте WireGuard приведёт только к блокировке остального трафика, так как все остальные запросы фильтруются. На сервере, к которому производится подключение, не осуществляется сбор никакой информации о подключении (включая DNS-запросы на порт UDP/53) в случае, если файл конфигурации не подвергался изменению получившим его пользователем. По всем вопросам просьба обращаться на почту [xan@xan.dev](mailto:xan@xan.dev).