

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО  
ОБРАЗОВАНИЯ РФ Федеральное государственное  
бюджетное образовательное учреждение высшего  
образования  
«Московский Авиационный Институт»  
(Национальный Исследовательский Университет)

Институт: №8 «Компьютерные науки и  
прикладная математика» Кафедра: 806  
«Вычислительная математика и  
программирование»

Курсовая работа  
по курсу «Фундаментальная информатика»  
I семестр  
ЗАДАНИЕ:  
ВПН Приложение на Андроид

Группа	М8О-109Б-22
Студент	Юсуфов Р.Г.
Преподаватель	Сысоев М. А.
Оценка	
Дата	8 января 2023 г.

Москва, 2023

## Содержание

1. В первую очередь, что такое VPN?

2. В чём проблема VPN?
3. Создание собственного VPN
4. Заключение.

#### **В первую очередь, что такое VPN?**

**VPN** (Virtual Private Network) - или **виртуальная частная сеть**, — это безопасное зашифрованное подключение пользователя к сети, с которым он может обходить локальные ограничения и сохранять конфиденциальность.

**Почему виртуальная?** значит, что на ее работу не влияет то, по каким и скольким каналам связи она проложена. Потому что физическая сеть (группа компьютеров или устройств, соединенных общими каналами связи) не принадлежит пользователю виртуальной.

**Почему частная сеть?** Это значит, что в ней может находиться ограниченный круг лиц. VPN маркирует всех ее участников и передаваемую ими информацию. Данные защищаются от третьих лиц путем шифрования. VPN отвечает за то, чтобы данные оставались конфиденциальными — не пускает посторонних пользователей, проверяет источник трафика и следит, чтобы передаваемые данные не утекали за пределы сети в открытом виде.

#### **В чём проблема VPN?**

На самом деле, VPN используется не только для обхода ограничений и санкций в интернете, как уже можно понять. С интернетом дела идут куда сложнее. Конечно же, данные не уходят третьим лицам только в лучшем случае. В самом худшем, смогут украсть пароли от социальных сетей, да и всё, что человек делал в сети будет у злоумышленников. Но сначала у “поставщика” услуги, а потом у провайдера. Вот и суть VPN в том, что провайдер не сможет узнать, чей это запрос, а в крайнем случае, не узнает и то, что вы выходили в сеть. Это, кстати, и отделяет конфиденциальность от анонимность.

#### **Проблема VPN приложений.**

Если с провайдером всё понятно и в случае чего он остаётся “с носом”, то как обезопасить свои данные от третьих лиц? На просторах интернета множество VPN приложений разной степени глючности, но всех их объединяет одно - вы не знаете, чей этот сервер и собирает ли он о вас данные. Если хостинг находится в России, то обязательно из-за пакета Яровой. А что касается других стран, об этом попозже. Что действительно важно, это как обезопасить себя и свои данные от третьих лиц. Ответ лишь один - заплатить. Почти во всех приложениях есть бесплатный тариф и платный. Отличаются они скоростью, наличием рекламы, объёмом трафика и прочее. Конечно же, в платном доступе можно ожидать всего хорошего, а в бесплатном - всего плохого и худшего.

Казалось бы, плати и живи. Да, но опять же, вы не знаете ничего о хостере. Даже о таких гигантах, как ProtonVPN, что уж говорить про мелкие конторы, коих развелось на просторах Play Market.

#### **Создание собственного VPN**

### а) План, выбор хостинга, протоколы и ОС

Но как же можно себя обезопасить на 100%? Как и было сказано выше, заплатить. Только купить не тарифный план, а настоящий виртуальный сервер. И поднять свой VPN. Займёт это от силы 30 минут, не считая времени ожидания регистрации виртуального сервера. Я покупал сервер в Нидерландах у FirstByte. Да, хостер российский и это навевает тревогу. Не могу не согласиться, но, к сожалению, с недавних пор ни один заграничный сайт не может принимать оплату с российских банковских карт. Конечно же можно купить тот же нидерландский сервер у заграничного поставщика за криптовалюту, но сейчас не особо хочется заморачиваться с этим. В общем, с выбором поставщика услуг туговато.

Вот мы купили сервер. Теперь на нём нужно развернуть VPN. Как это сделать, на просторах интернета множество инструкций, но инструкцию напишу. Хочу лишь отметить, что виртуальный сервер на операционной системе Linux Ubuntu 20 (я понимаю, что какой-нибудь Debian или Centos подошёл бы лучше) с протоколом IKEv2/IPSec. К слову о последнем: Безопасность подключения зависит от **VPN-протокола**, то есть набора инструкций, определяющего, каким именно образом два устройства могут обмениваться данными. Принципы работы VPN-протоколов различаются. Как правило, они выполняют две базовые функции: **авторизация (проверка подлинности)** и шифрование. Авторизация позволяет гарантировать, что ваше устройство обменивается данными с надёжным VPN-сервером, а шифрование данных не позволяет посторонним получить доступ к вашему трафику.

Разные протоколы используют разные стандарты шифрования и методы проверки подлинности, из-за чего возникает разница в скорости и безопасности подключений для пользователей VPN. Кроме того, VPN-протоколы используют разные правила обработки потенциальных ошибок, что влияет на стабильность и надёжность подключений.

Существует много протоколов, например L2TP, PPTP, Wireguard, OpenVPN, IKEv2 и так далее. Один из самых лучших - Wireguard. Я использовал IKEv2 только лишь потому, что L2TP устарел и (выявлено на практике) имеет плохую стабильность соединения на андроид. Это можно поправить утилитой Xauth, что было и сделано, но как оказалось, мой телефон (в отличие от телефона моей матери) не поддерживает тип соединения L2TP/Xauth PSK. Именно это и заставило меня переписать VPN сервер на IKEv2. На самом деле, это является недостатком моего VPN приложения, так как с двумя и более протоколами оно работает некорректно.

### б) Инструкция

На почту присылается вот такое письмо:

## Активация Виртуального сервера

Здравствуйте, Билли Бобер!

Настоящим письмом уведомляем, что на ваше имя был зарегистрирован Виртуальный Сервер. Предлагаем распечатать данное сообщение для удобства использования в дальнейшем.

### Информация о сервере

- Тарифный план: KVM-SSD-START-AMS
- Дата открытия: 2023-01-05
- Доменное имя: tonytony.chopper
- IP-адрес сервера: [REDACTED]
- Пользователь: [REDACTED]
- Пароль: [REDACTED]

Необходимо подключиться к нашей виртуальной машине. Я использую Britvise SSH Client. Вводим в соответствующие поля наши данные и заходим в терминал. Я сразу проверил наличие docker (не было). Докер надо установить (ссылка на инструкцию - <https://www.digitalocean.com/community/tutorials/how-to-install-and-use-docker-on-ubuntu-20-04-ru>)

```
root@185.94.165.17:22 - Bitvise xterm - root@tonytony: ~
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.4.0-136-generic x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

root@tonytony:~# docker
Could not find command-not-found database. Run 'sudo apt update' to populate it.
Б docker: command not found
root@tonytony:~# docker
Could not find command-not-found database. Run 'sudo apt update' to populate it.
docker: command not found
root@tonytony:~#
```

После установки Докера, пишем следующее

```
docker run \

--name ipsec-vpn-server \

--restart=always \

-v ikev2-vpn-data:/etc/ipsec.d \

-v /lib/modules:/lib/modules:ro \
```

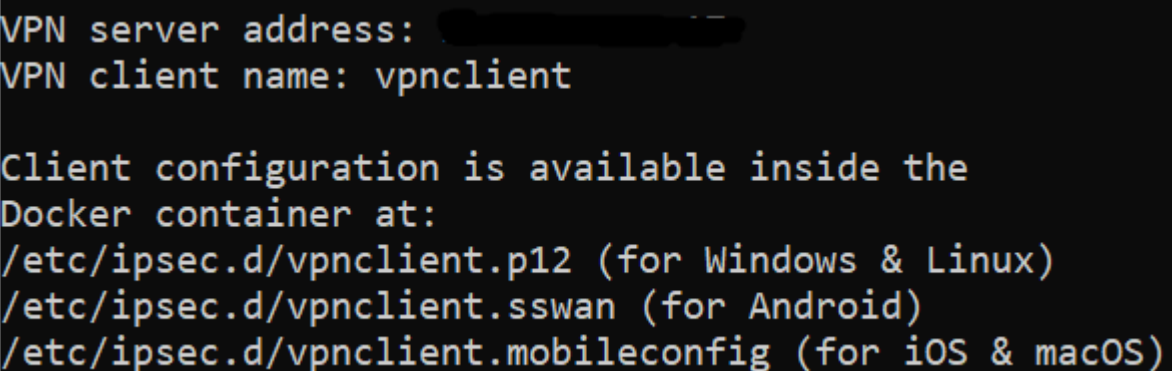
```
-p 500:500/udp \  
-p 4500:4500/udp \  
-d --privileged \  
hwds12/ipsec-vpn-server
```

Она автоматически настроит VPN сервер и протоколы.

Далее проверим процесс работы сервера командой “docker ps”

Теперь нужны сертификаты для андроида (в моём случае), вводим команду

docker logs ipsec-vpn-server которая выведет эту информацию



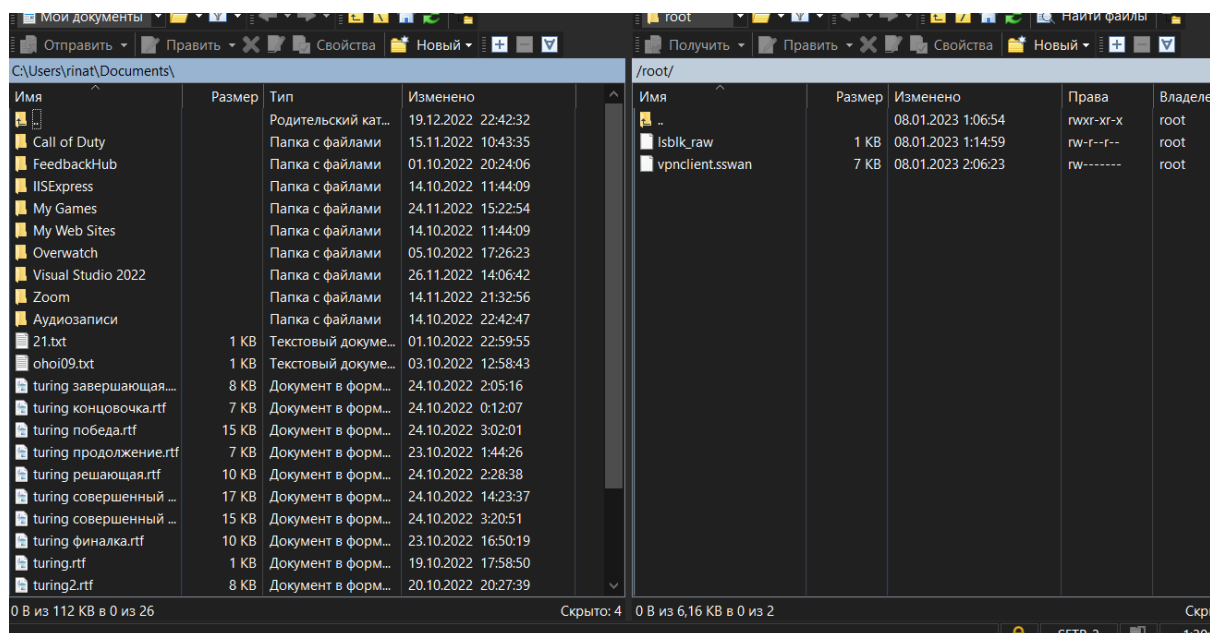
```
VPN server address: [REDACTED]  
VPN client name: vpnclient  
  
Client configuration is available inside the  
Docker container at:  
/etc/ipsec.d/vpnclient.p12 (for Windows & Linux)  
/etc/ipsec.d/vpnclient.sswan (for Android)  
/etc/ipsec.d/vpnclient.mobileconfig (for iOS & macOS)
```

Адрес был замазан. Чуть выше (уже не на скриншоте) можно увидеть пароли и PSK ключ.

Теперь для скачивания нужного сертификата прописываем следующее:

```
docker cp ipsec-vpn-server:/etc/ipsec.d/vpnclient.sswan .
```

Далее нужно скачать из сервера на ПК этот файл. Я использовал WinSCP.



Файл `vpncclient.sswan`. Это для андроида. Но у меня андроид 11+ версии, поэтому я скачиваю файл с расширением `.p12`.

Далее нужно открыть этот сертификат, задать имя соединения, а в настройках VPN выбрать типа соединения IKEv2/IPSec RSA. Вводим значения, сертификат пользователя выбираем наш, сертификат ЦС - аналогично. Сертификат сервера - получено с сервера. Сохраняем. Теперь в нашем распоряжении имеется собственный VPN сервер.

## Заключение

Возможности VPN велики, особенно когда речь заходит об обходе запретов. Так как никто не может быть до конца уверенным в то, что данные не уходят третьим лицам, то разумно предположить, что рациональнее потратить полчаса на создание собственного VPN.