МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский Томский государственный университет»

**Институт прикладной математики и компьютерных наук  
Кафедра прикладной информатики**

РЕФЕРАТ

по дисциплине «основы информационной безопасности»

на тему:

«Виртуальные частные сети (VPN)»

Работу выполнила:  
студент 1 курса 932102 гр.  
Селуянов Данила Дмитриевич

Проверил преподаватель:   
Тренькаев Вадим Николаевич

**Содержание**

Титульный лист 1

Основные понятия и предназначение VPN 2

Применение на практике базовых возможностей 3

Список литературы 8

**Основные понятия и предназначение VPN**

VPN (англ. Virtual Private Network - виртуальная частная сеть) – логическая сеть, создаваемая поверх другой сети, например Internet. Несмотря на то, что коммуникации осуществляются по публичным сетям с использованием небезопасных протоколов, за счёт шифрования создаются закрытые каналы обмена информацией.

Виртуальная частная сеть позволяет защищать свои каналы связи, зашифровывая данные и передавая из по открытым сетям. VPN позволяет скрыть все свои действия в интернете, ибо никто не узнает что было получено и отправлено, т. к. настоящий источник подключения не виден.

Реализация виртуальной частной сети на практике выглядит следующим образом. В локальной вычислительной сети офиса фирмы устанавливается сервер VPN. Удаленный пользователь c использованием клиентского ПО VPN инициирует процедуру соединения с сервером. Происходит аутентификация пользователя – первый шаг установления VPN-соединения. После подтверждения аутентификации наступает вторая фаза – между клиентом и сервером выполняется согласование безопасности соединения. После этого организуется VPN-соединение, обеспечивающее обмен информацией между клиентом и сервером в форме, когда каждый пакет с данными проходит через процедуры шифрования/дешифрования и проверки целостности - аутентификации данных.

Основные составляющие и протоколы VPN сетей

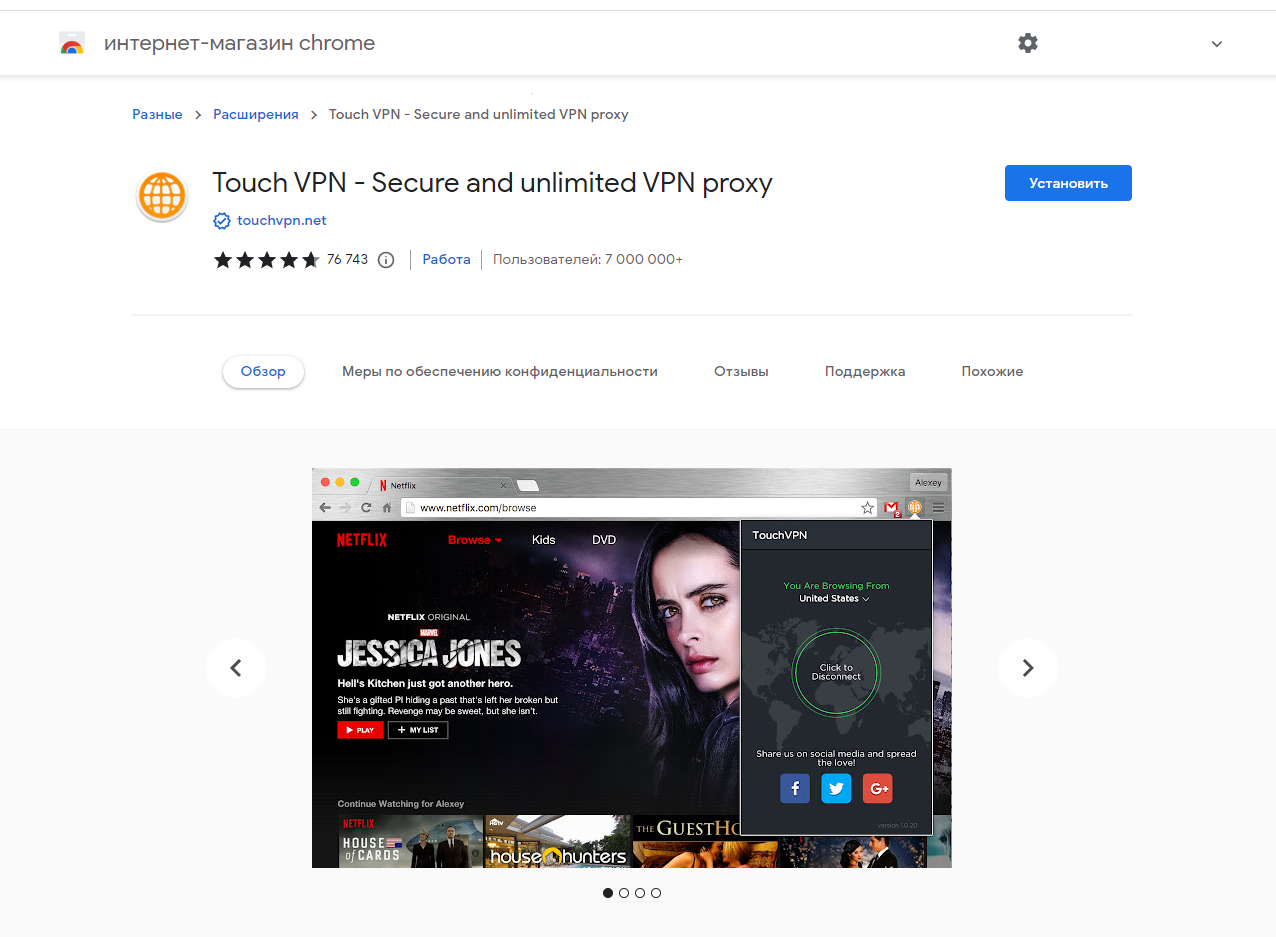
* Туннелирование – передача данных между двумя точками таким образом, что для источника и приемника данных вся сетевая инфраструктура, лежащая между ними, остается скрытой.
* Шифрование – данные шифруются благодаря современным методам криптографической защиты информации
* Аутентификация – доступ к содержанию зашифрованных данных осуществляется с помощью двух факторов. Первый фактор называется «я имею» и состоит в том, что пользователь обладает конкретным криптографическим ключевым носителем (токеном) или смарт-картой. Эти ключи используются для установки сеанса связи между клиентом и сервером VPN, а также для защиты передаваемых данных. Доступ к памяти, где хранятся ключи, защищён с помощью PIN-кода, знание которого и является вторым фактором аутентификации («я знаю»).

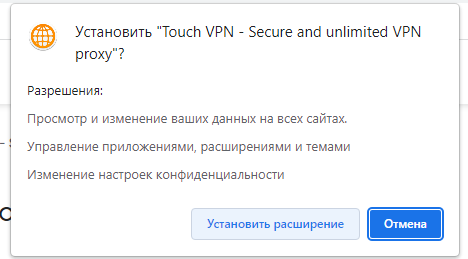
**Применение на практике базовых возможностей**

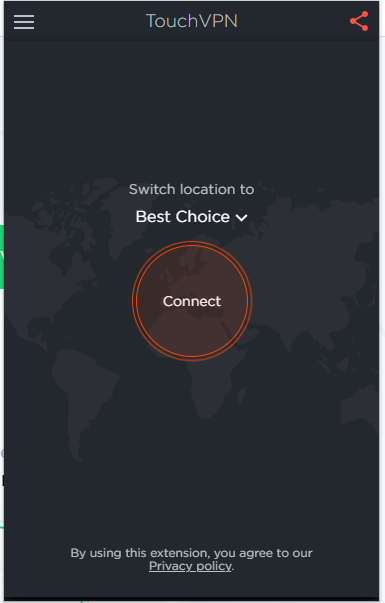
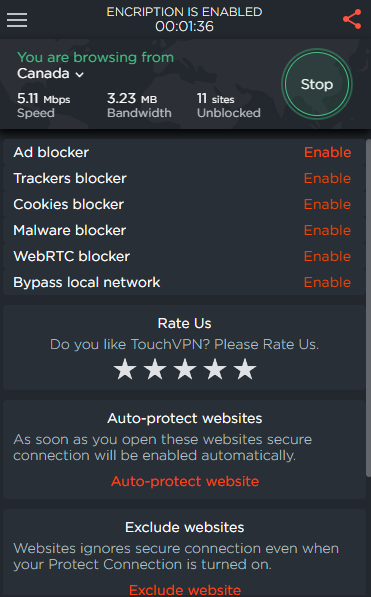
Из вышесказанного можно понять, что VPN широко распространён среди крупных компаний для передачи информации и избежание ее утечки, но что же насчет обычных пользователей интернета? Любой среднестатистический пользователь может легко и быстро скачать специальное ПО и воспользоваться им без особых сложностей. Можно найти множества предложений на рынке сервисов, которые предлагаю услуги по подключению к VPN, однако, если вам требуется надежное соединение и высокая скорость, то стоит обратиться к платным вариантам.

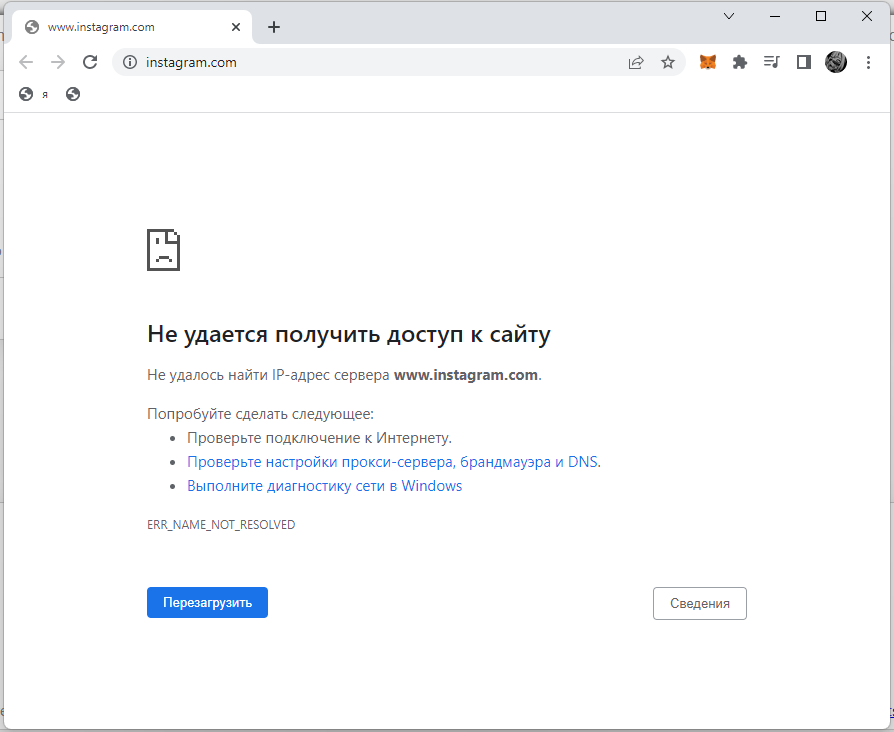
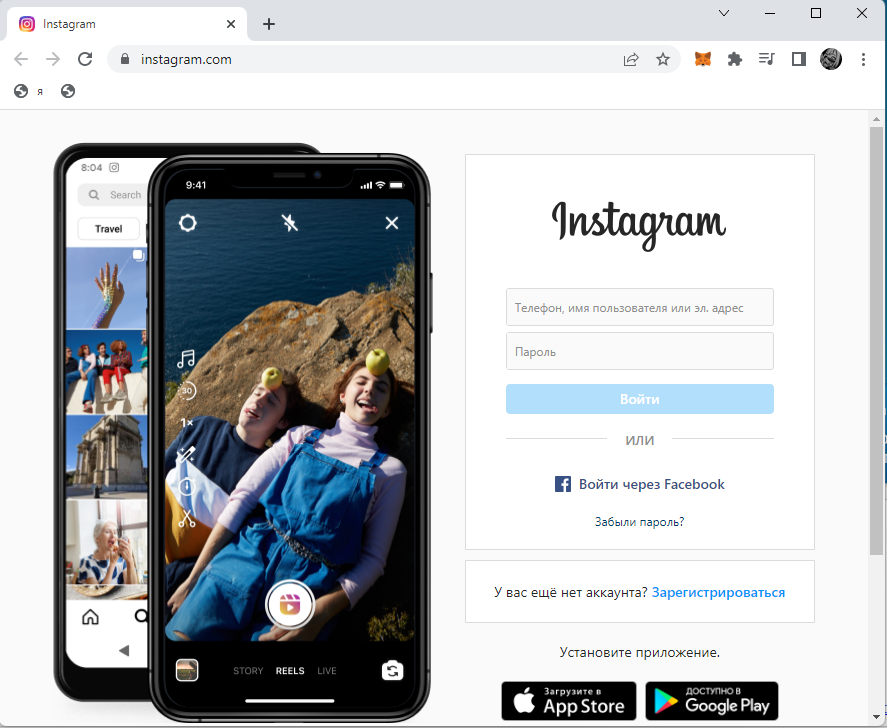
В рамках данной работы мы разберем установку, настройку и подключение VPN сервиса “Touch VPN”

**  
Сайт сервиса**

Установить ПО для подключения можно с официального сайта, или же из магазина расширений для браузера (в рамках теста будет использоваться браузера Google Chrome)  
  
**Страница ПО в магазине расширений**

Установка производится в пару кликов мышки  
  
**Установка ПО**

После установки прямо в браузере открывается интерфейс приложения, в котором можно за один клик подключиться к серверу  
   
**Интерфейс до подключения к сети и после**

Для проверки сервиса подключимся к сайту Instagram'а, который в данный момент заблокирован на территории РФ  
  
  
**Попытки подключения к сайту** [**https://www.instagram.com**](https://www.instagram.com) **без использования и с использованием VPN**

**Список литературы**

<http://vmk.ugatu.ac.ru/book/vpn.pdf> - большое количество теории о работе Виртуальный Частных Сетей  
<https://trends.rbc.ru/trends/industry/604f0a309a79477d332569e3> - теория для чайников  
<https://www.anti-malware.ru/analytics/Technology_Analysis/VPN-and-multi-factor-authentication> - теория про двухфакторную аутентификацию  
<https://touchvpn.net> – сервис VPN для теста  
<https://www.anti-malware.ru/analytics/Technology_Analysis/VPN-and-multi-factor-authentication> - страница сервиса в магазине расширений браузера  
<https://ipleak.net> – проверка ip адреса  
<https://www.instagram.com> – сайт для проверки работоспособности сервиса