УДК 004.056

ОЦЕНКА ЭФФЕКТИВНОСТИ VPN В ОБХОДЕ ЦЕНЗУРЫ И ГЕОГРАФИЧЕСКИХ ОГРАНИЧЕНИЙ

Веселова А.А., студент гр. 21-К-КБ1, 4 курс,
Волынко А.С., студент гр. 21-К-КБ1, 4 курс,
Таран Е.А., ассистент кафедры,
Научный руководитель: Шарай В.А., к.т.н., доцент
Кубанский государственный технологический университет
г. Краснодар

В современном мире во время активной цифровой глобализации доступ к информации становится все более важным, но цензура и географические ограничения препятствуют свободному доступу в интернет. Ограничение доступа к информации приводит к нарушению свободы слова, сдерживанию экономического роста и инноваций, торможению научного прогресса, дезинформации людей и многому другому. Одним из основных инструментов для обхода цензуры и географических ограничений рассматривается VPN (Virtual Private Network, виртуальная частная сеть). VPN – это безопасная частная сеть, которая позволяет пользователям беспрепятственно просматривать интернет-ресурсы, не беспокоясь о конфиденциальности в сети, краже данных или цензуре.

Основные функции виртуальной частной сети представлены на рисунке 1.

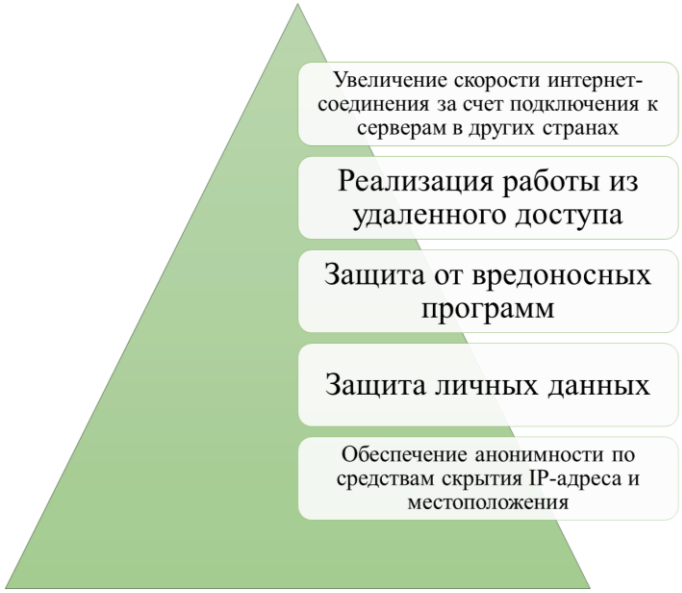

Рисунок 1. – Основные функции VPN

Для оценки эффективности важно правильное понимание работы инструмента. VPN по своей сути работает следующим образом:

1. Изменение IP-адреса и маскировка реального местоположения: VPN заменяет реальный IP-адрес на IP-адрес сервера. Таким образом становится не-

возможно перехватить трафик. А также это позволяет обходить географические ограничения.

2. Шифрование трафика: VPN шифрует весь интернет-трафик между устройством и VPN-сервером, что делает нечитаемыми данные для пытающихся перехватить трафик.

3. Обход блокировок DNS (Domain Name System): использование альтернативных DNS-серверов, что позволяет обойти блокировки DNS, которые могут применяться для цензуры или ограничения доступа к определенным сайтам.

4. Различные протоколы VPN, которые выбираются в зависимости от цели использования, а также от потребностей в скорости, безопасности, простоте настройки и совместимости с устройствами.

Для использования VPN как инструмента обхода блокировок необходимо понимать, какой бывает уровень цензуры, для этого разделим варианты блокировок по уровням сложности:

1. Простые блокировки: к ним отнесем блокировку по IP-адресу, блокировку по DNS и блокировку по URL:

1.1. Блокировка по IP-адресу: самый простой метод. Блокируются определенные IP-адреса, принадлежащие нежелательным веб-сайтам. Эффективность такого вида блокировки низкая, так как для обхода используется VPN, прокси или Tor (The Onion Router).

1.2. Блокировка по DNS: серверы, предоставляемые интернет-провайдером, подменяют IP-адрес заблокированного сайта на несуществующий или на страницу с предупреждением. Также является простым для преодоления видом блокировки, если есть возможность использования альтернативных DNS-серверов.

1.3. Блокировка по URL: блокировка к определенным URL-адресам, содержащим ключевые слова или фразы. Для скрытия URL используется HTTPS (зашифрованное соединение).

2. Блокировки средней сложности: блокировка по портам и блокировка по ключевым словам в незашифрованном трафике (HTTP):

2.1. Блокировка по портам: блокируются определенные порты, используемые для определенных сервисов. Для обхода необходимо использовать другие порты.

2.2. Блокировка по ключевым словам в незашифрованном трафике (HTTP) строится на основе анализа HTTP-запросов на наличие определенных ключевых фраз или слов. Вариантом обхода является использование HTTPS.

3. Продвинутые методы цензуры: DPI (Deep Packet Inspection, глубокий анализ пакетов), анализ поведения трафика, блокировка VPN-серверов, криптоанализ, деанонимизация пользователей Tor:

3.1. DPI – это технология, позволяющая анализировать содержимое пакетов данных, проходящих через сеть. Способен идентифицировать приложения, протоколы, обнаруживать ключевые слова, фразы и другие характеристики. Для обхода этого вида блокировки используются: обфускация трафика

(маскировка трафика VPN, Tor, или других запрещенных сервисов, чтобы он выглядел как обычный трафик HTTPS), Stealth VPN (VPN-серверы, использующие техники обфускации), Shadowsocks/SSR (прокси-серверы, разработанные специально для обхода цензуры, часто использующие обфускацию) [1].

3.2. Анализ проведения трафика заключается в анализе паттернов трафика, связанных с использованием VPN, даже если трафик зашифрован и обфусцирован. Очень сложный обход данной блокировки, так как требуются сложные механизмы маскировки и изменения паттернов трафика.

3.3. Блокировка VPN-серверов, которая основывается на автоматическом обнаружении и блокировке IP-адресов, связанных с VPN-серверами. Обход блокировки связан с использованием VPN-провайдеров.

3.4. Криптоанализ: попытки взлома шифрования, используемого VPN или других сервисов. Для обхода необходимо использование надежных алгоритмов шифрования и регулярное обновление протоколов шифрования.

3.5. Деанонимизация пользователей Tor – атаки, направленные на раскрытие личности пользователей Tor. Для обхода используется: использование Tor Browser с повышенными настройками безопасности и дополнительных средств защиты конфиденциальности [2].

На эффективность работы VPN сервисов влияют такие факторы как: размер серверной сети, скорость соединения, функции обфускации и другие. Основные характеристики VPN-сервисов представлены ниже:

1. Использование протоколов: различные протоколы обеспечивают различные уровни безопасности и скорости и надежности.

2. Количество и расположение серверов. Чем больше серверов расположено в разных странах, тем больше возможности сервиса в вопросе обхода географических и цензурных ограничений, а также меньше вероятность перегрузки серверов.

3. Пропускная способность, которая при ее ограничении может привести к снижению скорости и нестабильному соединению.

4. Обфускация трафика: функция, маскирующая трафик, делая его похожим на обычный HTTPS-трафик, что делает данную функцию эффективной в обходе цензуры.

Каждая из характеристик является важным фактором при использовании VPN для обхода блокировок, так как именно эти факторы позволяют обходить различные уровни цензуры. Однозначно можно определить, что любой VPN является эффективным инструментом для обхода простых блокировок и достаточно эффективными при работе с некоторыми блокировками, которые мы отнесли к категории блокировок средней сложности. Однако при работе с продвинутыми методами цензуры VPN является малоэффективным.

Преимуществами VPN-сервисов при их использовании для обхода цензуры и географических ограничений являются:

– повышенная конфиденциальность и анонимность;

– безопасность данных за счет шифрования трафика;

– защита от DDoS-атак за счет скрытия IP-адреса;

– возможность изменения местоположения при помощи выбора сервера из другой страны.

Недостатками VPN-сервисов при их использовании для обхода цензуры и географических ограничений являются:

– активная блокировка различных VPN-сервисов цензорами;

– разница в эффективности разных сервисов;

– риски безопасности и конфиденциальности;

– необходимость использования альтернативных решений при сложных блокировках;

– возможная нестабильность работы.

Оценка эффективности использования VPN при преодолении цензурных ограничений – это процесс, который зависит во многом от целей пользователя. При рассмотрении различных цензурных ограничений в статье были выделены различные способы их преодоления, что говорит о том, что в тех или иных случаях эффективны разные методы. То есть некоторые VPN могут быть более эффективны для обхода простых методов цензуры, но менее эффективными для обхода более сложных методов. Важно выбрать VPN который гарантирует надежное шифрование, обфускацию трафика и ротацию IP-адресов, а также не мало важно, чтобы была учтена текущая ситуация и происходила быстрая адаптация к новым методам цензуры.

Важно помнить, что абсолютной гарантии обхода цензуры не существует, VPN является лишь одним из инструментов для обхода цензурных и географических ограничений [3].

Список литературы:

1. Коробейников А.Г. Анализ методов обфускации / А.Г. Коробейников, И.М. Кутузов, П.Ю. Колесников // NB: Кибернетика и программирование. – 2012. – № 1. – С. 31-37.

2. Фурер О.В. Луковая маршрутизация в браузере «тор» / О.В. Фурер, Д.О. Якупов // Международный журнал информационных технологий и энергоэффективности. – 2024. – Т. 9, № 3(41). – С. 16-21.

3. Шабаев М.Б. Как работает VPN и обзор лучших VPN провайдеров / М.Б. Шабаев, М.М. Матыгов // Тенденции развития науки и образования. – 2020. – № 68-1. – С. 140-142.