УДК 004

ВАЖНОСТЬ ИСПОЛЬЗОВАНИЯ VPN ДЛЯ ЗАЩИТЫ ДАННЫХ В СОВРЕМЕННОМ МИРЕ

Евсеева Е.В., студент группы ИК-22-3, 2 курс
Научный руководитель: Жижома А.И., преподаватель кафедры ПИМ
Северо-Кавказский социальный институт
г. Ставрополь

В современном мире большое количество людей активно используют Интернет для мгновенной передачи данных в режиме реального времени, возможности обмена информацией в различных форматах, получения удаленного доступа к данным предприятий, компаний и производств. Также Интернет является способом массового общения людей, объединенных различными интересами посредством социальных сетей, электронных почт, форумов, блогов, чатов и так далее.

Чем чаще люди пользуются Интернетом, тем больше вероятность угрозы их данным. Для обеспечения безопасности данных представляются несколько различных методов, например, шифрование. Им занимаются виртуальные сети – VPN. Приватная сеть представляет надежную защиту и конфиденциальность при передаче информации.

VPN (Virtual Private Network) – это виртуальная частная сеть, которая позволяет установить зашифрованное подключение между внешними серверами.

Когда пользователь подключается к Интернету, его устройству присваивается IP-адрес. Операторы связи используют этот IP-адрес для отслеживания действий пользователя в Интернете, таких как посещенные веб-сайты и приобретенные товары. Далее они анализируют эту информацию, анонимизируют ее и продают рекламным агентствам и другим лицам, а также существует возможность несанкционированного доступа при использовании общедоступных сетей.

При использовании VPN провайдер используемой сети никогда не видит применяемые интернет-ресурсы или отправляемые вами запросы – все, что он видит, это IP-адрес VPN-сервера, с которым вы обмениваетесь зашифрованным трафиком.

VPN-сервер не предоставляется возможность увидеть местоположение, веб-сайт и другие сервисы на внешних серверах, а только IP-адрес VPN-сервера, который может распознать и запомнить действия по заполнению форм или ввода поисковых запросов.

VPN-сервера могут создавать, как частные лица для собственных целей (для чего им необходимо арендовать компьютер или облачную виртуальную машину за рубежом), так и организации для подключения своих сотрудников.

Однако для этого требуются определенные возможности, поэтому многие используют частные VPN-провайдеры, которые могут подключаться к их собственным сетям.

Изначально VPN-сервисы использовались в корпоративных целях. Например, их развертывают крупные компании для подключения удаленных сотрудников, офисов или целых филиалов к корпоративной сети и предоставления доступа к внутренним ресурсам. Защищенный доступ при удалённом подключении возможен через VPN или прокси-сервер. Некоторые компании требуют использование VPN-сервисов, чтобы предотвратить перехват злоумышленниками информации компании.

В настоящее время эта технология широко используется для обхода ограничений и блокировки ресурсов, доступ к которым невозможен на территории той или иной страны. При применении с устройства, находящегося в другой стране, VPN помогает обойти блокировку. Когда пользователь подключается к VPN-сервису, запрос на доступ к заблокированному ресурсу отправляется на удаленный VPN-сервер за пределами страны по зашифрованному соединению.

Рекомендуется использовать VPN при подключении к интернету через публичный Wi-Fi, так как это может повлечь угрозу защиты данных на устройстве. В публичном Wi-Fi существует угроза подключения злоумышленников к устройству находящимся в этой сети, что и пользователь, которые могут перехватить трафик и украсть пароли, номера банковских карт и внедрить вредоносное ПО.

Различия между сервисами заключаются в размере серверной сети (количество и страна VPN-серверов, которые можно подключить), максимальной скорости соединения, используемом протоколе шифрования, ограничениях на трафик и количестве устройств, которые могут подключаться к сети одновременно.

Однако сервисы VPN предоставляют расширенные услуги, требующие дополнительной оплаты, а также общедоступный вариант бесплатного использования.

Бесплатные VPN-сервисы предоставляют доступ к виртуальной частной сети без необходимости платить за нее. Например, WARP's 1.1.1.1. или TurboVPN. Несмотря на недостатки, они имеют и плюсы, например, простота использования. Но при отправление личной информации – паролей или данных банковских карт, через бесплатный VPN все же не рекомендуется.

Платные VPN-сервисы обычно предлагают более высокий уровень безопасности и скорости. Так же сервис с дополнительными услугами может предоставить подключение нескольких устройств в защищенную сеть одновременно и блокировку трекеров. Антивирусная защита устройства включенная в данный тип сервиса включает в себя защиту от вредоносных сайтов, рекламы и слежения.

VPN-сервисы выполняют роль защитников при возникновении кибератак. Кибератака – это злонамеренное действие против компьютерной си-

стемы, сети, устройства или данных с целью нанесения ущерба, получения несанкционированного доступа или кражи информации. В кибератаках используются различные методы и приемы, включая вирусы, троянские кони, фишинг и DDoS-атаки.

Задачи кибератак различны: финансовая выгода, шпионаж, нарушение работы системы и уклонение от слежения. Они могут быть направлены как на отдельных пользователей, так и на крупные организации, правительства и критически важные объекты инфраструктуры.

Кибератаки сегодня очень распространены и угрожают безопасности наших данных. Однако использование VPN может значительно снизить риск от этих атак. Защита от них с помощью VPN обеспечивается за счет шифрования данных, что предотвращает доступ к ним. Таким образом, VPN сохраняет вашу информацию в безопасности, даже если вы подключаетесь к не доверенной сети.

Преимущества VPN включают в себя:

– маскировка вашего IP-адреса, позволяющая скрыть или изменить ваше местоположение от посещаемых сайтов;

– защита ваших данных путем шифрования веб-трафика при использовании небезопасного Wi-Fi;

– предотвращение контроля интернет-провайдеров и других третьих лиц за вашей интернет-активностью.

Но в тоже время, VPN не являются универсальным решением всех проблем конфиденциальности и безопасности в Интернете. Можно выделить несколько недостатков при использовании VPN:

– не обеспечивают полной анонимности (например, если вы вошли в свой личный аккаунт во время веб-серфинга, то использование VPN не будет проблемой, но компании могут отслеживать вашу активность и связывать ее с IP-адресом VPN-сервера);

– повышенная безопасность VPN требует оплаты сервиса;

– общедоступные VPN могут разглашать личную информацию, в том числе раскрывать ваш реальный IP-адрес и DNS-запросы;

– использование VPN в большинстве случаев снижает скорость интернета;

– использование VPN на мобильном устройстве увеличивает трафик;

– некоторые онлайн-сервисы пытаются помешать своим клиентам использовать VPN.

С 2019 года VPN-провайдеров обязали подключать список заблокированных сайтов к Федеральной государственной информационной системе Роскомнадзора, но абсолютное большинство провайдеров проигнорировали это требование.

В 2021 году Роскомнадзор начал блокировать VPN-сервисы, сначала VyprVPN и Opera VPN, а затем еще шесть сервисов. В ведомстве пояснили,

что использование VPN-сервисов приводит к постоянному доступу к запрещенной информации и создает условия для противоправной деятельности.

Для обеспечения безопасности и анонимности в Интернете, помимо VPN используются и прокси-серверы.

Прокси-сервер – это компьютер, выполняющий роль посредника между пользователем и целевым сервером. Компании используют прокси для обеспечения безопасности, повышения производительности сети, доступа к «удаленным» ресурсам. Частные лица применяют прокси для анонимизации трафика или обхода ограничений доступа.

VPN создают зашифрованный туннель между устройством пользователя и удаленным VPN-сервером, отправляя трафик в Интернет. Это позволяет скрыть IP-адрес пользователя и защитить его данные от подслушивания и взлома.

Прокси-серверы также используются для скрытия IP-адреса пользователя, но не создают зашифрованный туннель. Вместо этого они просто перенаправляют трафик через сервер и могут использоваться для фильтрации трафика и ускорения доступа к ресурсам.

Таким образом, VPN обеспечивают более высокий уровень безопасности и анонимности, но могут снижать скорость Интернет-соединения. Прокси-серверы обеспечивают более высокую скорость, но меньшую безопасность и анонимность.

В заключение следует отметить, что безопасность и конфиденциальность данных должны быть главным приоритетом в современном мире. Одним из способов достижения этой цели является использование VPN, однако для полной защищённости своих данных и устройства необходима комплексная защита. Данное средство помогает обеспечивать безопасность данных, защиту от кибератак и возможность обходить географические ограничения VPNs.

При выборе провайдера стоит обратить внимание на скорость соединения, количество доступных серверов и уровень безопасности. Чтобы защитить свои данные и оставаться в безопасности в онлайн-мире, не стоит пренебрегать мерами предосторожности.

Список литературы:

1. Виртуальные частные сети (VPN). – URL: https://cloud.yandex.ru/ru/docs/glossary/vpn

2. Скобелев, В. Что такое VPN, как он работает и что делать в случае его блокировки. – URL: https://www.forbes.ru/tekhnologii/459279-cto-takoe-vpn-i-kak-on-rabotaet

3. VPN – что это, как работает, какой сервис использовать. – URL: https://vc.ru/services/380238-vpn-chto-eto-kak-rabotaet-kakoy-servis-ispolzovat#anchor3