Нижлукченко И.Д. VPN: как это работает и почему это важно для вашей приватности. объяснение принципов работы виртуальных частных сетей и их роли в обеспечении конфиденциальности данных // Международный журнал информационных технологий и энергоэффективности.– 2024. –Т. 9 № 6(44) с. 70–74

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.7

VPN: КАК ЭТО РАБОТАЕТ И ПОЧЕМУ ЭТО ВАЖНО ДЛЯ ВАШЕЙ ПРИВАТНОСТИ. ОБЪЯСНЕНИЕ ПРИНЦИПОВ РАБОТЫ ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЕЙ И ИХ РОЛИ В ОБЕСПЕЧЕНИИ КОНФИДЕНЦИАЛЬНОСТИ ДАННЫХ

Нижлукченко И.Д.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: nizhluchenk@gmail.com

В эпоху, когда цифровая безопасность и конфиденциальность данных стали важнейшими аспектами нашего онлайн-присутствия, использование виртуальных частных сетей (VPN) выходит на передний план как эффективное средство защиты. Настоящая статья представляет собой всесторонний анализ принципов работы VPN, подчеркивая их критическую роль в обеспечении анонимности и безопасности пользовательских данных в интернете. Мы исследуем, как зашифрованный канал, создаваемый VPN, защищает информацию от внешних угроз, включая злоумышленников и наблюдение со стороны интернет-провайдеров. Освещается важность изменения IP-адреса пользователя на адрес сервера VPN для обеспечения анонимности и обхода географических ограничений.

Ключевые слова: Виртуальные частные сети, VPN, цифровая безопасность, конфиденциальность данных, шифрование, анонимность в интернете, защита персональных данных, политика конфиденциальности VPN, протоколы шифрования, выбор VPN-провайдера, обход географических ограничений, безопасное подключение, интернет-приватность, безопасность Wi-Fi, кибербезопасность, защита от слежки, сохранение анонимности.

VPN: HOW IT WORKS AND WHY IT'S IMPORTANT FOR YOUR PRIVACY. EXPLANATION OF THE PRINCIPLES OF VIRTUAL PRIVATE NETWORKS AND THEIR ROLE IN ENSURING DATA PRIVACY

Nizhlukchenko I.D.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: nizhluchenk@gmail.com

In an era when digital security and data privacy have become the most important aspects of our online presence, the use of virtual private networks (VPNs) is coming to the fore as an effective means of protection. This article provides a comprehensive analysis of the principles of VPN operation, emphasizing their critical role in ensuring the anonymity and security of user data on the Internet. We are investigating how the encrypted channel created by a VPN protects information from external threats, including intruders and surveillance by Internet service providers. The importance of changing the user's IP address to the address of the VPN server to ensure anonymity and circumvent geographical restrictions is highlighted.

Keywords: Virtual private networks, VPN, digital security, data privacy, encryption, anonymity on the Internet, personal data protection, VPN privacy policy, encryption protocols, choosing a VPN provider, circumventing geographical

restrictions, secure connection, Internet privacy, Wi-Fi security, cybersecurity, protection from surveillance, preservation anonymity.

VPN создает зашифрованный туннель между вашим устройством и сервером VPN, через который проходит весь ваш интернет-трафик. Это означает, что вся информация, отправляемая и получаемая через VPN, зашифрована и скрыта от любых внешних наблюдателей, включая вашего интернет-провайдера (ISP), правительственные органы и злоумышленников.

Ключевым элементом технологии VPN является использование протоколов шифрования, таких как OpenVPN, IKEv2/IPSec и WireGuard. Эти протоколы обеспечивают высокий уровень безопасности данных, передаваемых через интернет, благодаря сложным алгоритмам шифрования.

Кроме того, VPN позволяет пользователям скрыть свой истинный IP-адрес, заменив его IP-адресом сервера VPN. Это не только повышает анонимность в сети, но и позволяет обойти географические ограничения, предоставляя доступ к контенту, который может быть заблокирован в их стране.

Принцип работы виртуальных частных сетей (VPN) укоренен в создании безопасного и зашифрованного канала между устройством пользователя и интернетом. Этот процесс начинается, когда пользователь подключается к VPN-серверу, выбранному из списка доступных географических локаций. После установления соединения между устройством пользователя и VPN-сервером, все интернет-трафик пользователя начинает перенаправляться через этот сервер.

Суть работы VPN заключается в том, что перед отправкой данных из устройства пользователя в интернет, эти данные зашифровываются. Зашифрование обеспечивается благодаря использованию сложных алгоритмов, которые преобразуют передаваемую информацию в форму, недоступную для чтения любым сторонним наблюдателям без соответствующего ключа для расшифровки. Таким образом, даже если данные перехватываются в процессе передачи, они остаются защищенными и конфиденциальными.

После того как данные достигают VPN-сервера, они расшифровываются и отправляются в интернет от имени сервера. Это означает, что внешние наблюдатели, такие как интернет-провайдеры или веб-сайты, видят IP-адрес VPN-сервера, а не истинный IP-адрес пользователя. Такой подход не только способствует анонимности пользователя в сети, но и позволяет обходить географические ограничения контента, поскольку пользователь может казаться подключенным к интернету из любой точки мира, где расположен VPN-сервер.

Данный механизм работы VPN обеспечивает критический уровень безопасности и приватности в современном цифровом мире, где угрозы персональным данным и конфиденциальности постоянно растут. Путем зашифровки данных и скрытия истинного IP-адреса пользователя, VPN помогает защитить личную информацию от несанкционированного доступа, снижает риск кибератак и способствует сохранению конфиденциальности в сети.

Использование VPN важно по нескольким причинам. Во-первых, оно защищает вашу онлайн-активность от внешнего наблюдения, что критически важно в условиях современного цифрового мира, где данные пользователя часто собираются и анализируются без его согласия. Во-вторых, VPN обеспечивает защиту данных при использовании публичных Wi-Fi сетей, которые часто являются уязвимыми для атак злоумышленников.

Важность использования виртуальных частных сетей (VPN) для защиты приватности в современном мире трудно переоценить, учитывая масштабы и разнообразие угроз в интернете. Приватность в интернете не просто о защите личных данных от посторонних глаз; это также вопрос сохранения контроля над информацией, которую мы делимся в сети, и предотвращения ее использования без нашего согласия.[3] В этом контексте VPN выступает как мощный инструмент, обеспечивающий защиту и анонимность пользователям.

Во-первых, зашифрованный канал, создаваемый VPN, обеспечивает безопасность данных пользователя во время их передачи в интернет. Это особенно важно при использовании незащищенных сетей Wi-Fi, таких как общественные точки доступа в кафе или аэропортах, где риск перехвата данных злоумышленниками особенно высок. Благодаря VPN пользователи могут быть уверены, что их персональная информация, включая пароли, финансовые данные и личные сообщения, защищена от подобных атак.

Во-вторых, изменение IP-адреса пользователя на адрес сервера VPN помогает сохранить анонимность в интернете. Это не только усложняет задачу для сайтов и рекламодателей, пытающихся отслеживать онлайн-активность и создавать детализированные профили пользователей для таргетирования рекламы, но и предоставляет возможность обхода цензуры и доступа к информации без ограничений, которые могут быть наложены правительствами или интернет-провайдерами.

Кроме того, в условиях постоянно растущего объема сбора данных и наблюдения со стороны государственных органов и частных компаний, использование VPN становится важным инструментом для защиты права на частную жизнь.[4] Оно позволяет пользователям в некоторой степени восстановить контроль над своей личной информацией, сократить количество собираемых о них данных и снизить вероятность их неправомерного использования.

Таким образом, в контексте непрерывно расширяющегося цифрового пространства, где личная информация становится все более уязвимой, VPN выступает не просто как средство для улучшения сетевой безопасности, но и как фундаментальный элемент в стремлении к сохранению приватности в интернете. Он предоставляет пользователям возможность защитить свои данные и сохранить анонимность, что является ключевым аспектом в обеспечении свободы и конфиденциальности в цифровую эпоху.

Выбор надежного VPN-провайдера является критически важным аспектом в обеспечении онлайн-безопасности и приватности. В мире, где цифровая безопасность играет все более значительную роль, качество и надежность VPN-сервиса напрямую влияют на степень защиты, которую пользователь получает при его использовании.[5] Надежный VPN-провайдер обеспечивает не только высокий уровень шифрования и безопасности данных, но и строгую политику конфиденциальности, гарантирующую, что пользовательские данные не собираются, не хранятся и не передаются третьим лицам без согласия пользователя.

Одним из ключевых аспектов надежности VPN-сервиса является использование передовых технологий шифрования. Это обеспечивает, что даже в случае перехвата данных злоумышленниками, они останутся недоступными для чтения без соответствующего ключа расшифровки. Но технологии шифрования — это лишь один из элементов. Важно также обратить внимание на протоколы безопасности, которые использует провайдер, поскольку они определяют уровень защиты и скорость соединения.

Другой критически важный аспект — политика конфиденциальности провайдера. Надежные VPN-сервисы придерживаются политики «без журналов», что означает отсутствие сохранения записей о действиях пользователя в интернете. Это предотвращает возможность доступа к пользовательским данным даже при получении официального запроса от правоохранительных органов, тем самым обеспечивая анонимность пользователя.

Кроме того, репутация и прозрачность деятельности VPN-провайдера играют значительную роль в выборе надежного сервиса. Провайдеры, которые открыто делятся информацией о своих операционных процедурах, политиках безопасности и конфиденциальности, а также регулярно проходят независимые аудиты безопасности, заслуживают большего доверия. Отзывы пользователей и экспертные обзоры также могут служить хорошим ориентиром при выборе сервиса, так как они отражают реальный опыт использования.

В заключение, выбор надежного VPN-провайдера не только увеличивает эффективность защиты пользовательских данных в интернете, но и обеспечивает спокойствие пользователя, зная, что его приватность находится в надежных руках.[1] Учитывая широкий спектр предложений на рынке VPN-сервисов, важно провести тщательный анализ и выбрать провайдера, который соответствует высоким стандартам безопасности, приватности и пользовательского опыта.

Роль виртуальных частных сетей (VPN) в современном цифровом пространстве не может быть недооценена. Как мощный инструмент для обеспечения анонимности и безопасности в интернете, VPN предоставляет пользователям необходимые средства для защиты их персональных данных от внешних угроз. Через создание зашифрованного туннеля и скрытие IP-адреса, VPN способствует сохранению конфиденциальности и предотвращению несанкционированного доступа к информации.

Однако выбор надежного VPN-провайдера является ключевым аспектом, определяющим эффективность защиты. Пользователям следует уделять внимание таким факторам, как политика конфиденциальности, качество шифрования, репутация и отзывы о сервисе.[2] Важно помнить, что VPN является лишь одним из элементов комплексной стратегии кибербезопасности, и его использование должно дополняться другими методами защиты, включая соблюдение мер безопасности при онлайн-активности и использование надежных антивирусных программ.

В контексте постоянно растущих угроз в интернете, VPN остается незаменимым инструментом для тех, кто стремится к максимальной защите своей приватности и безопасности данных. Внедрение и активное использование VPN становится важным шагом на пути к обеспечению цифровой свободы и защиты в глобальной сети, подчеркивая важность информационной безопасности в нашей повседневной жизни.

Список литературы

1. Гельфанд А. М. и др. Разработка модели распространения самомодифицирующегося кода в защищаемой информационной системе//Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2018. – №. 8. – С. 91-97.

2. Красов А. В. и др. Способы коммутации пакетов в сетях CISCO//Материалы Всероссийской научно-практической конференции" Национальная безопасность России: актуальные аспекты" ГНИИ" Нацразвитие". Июль 2018. – 2018. – С. 31-35.
3. Штеренберг С. И., Москальчук А. И., Красов А. В. Разработка сценариев безопасности для создания уязвимых виртуальных машин и изучения методов тестирования на проникновения–Информационные технологии и телекоммуникации, 2021 //Т. – 2021. – Т. 9. –С. 1-2
4. Катасонов А. И., Штеренберг С. И., Цветков А. Ю. Оценка стойкости механизма, реализующего Мандатную сущностно-ролевую модель разграничения прав доступа в операционных системах семейства gnu linux//Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2020. – №. 2. – С. 50-56.
5. Бударный Г. С. и др. Разновидности нарушений безопасности и типовые атаки на операционную систему//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). – 2022. – С. 406-411

References

1. Gelfand A.M. et al. Development of a model for the distribution of self-modifying code in a protected information system //Modern science: actual problems of theory and practice. Series: Natural and Technical Sciences. – 2018. – No. 8. – pp. 91-97.
2. Krasov A.V. et al. Packet switching methods in CISCO networks //Materials of the All-Russian scientific and practical conference "National Security of Russia: current aspects of the "GNII" National Development". July 2018. – 2018. – pp. 31-35.
3. Shterenberg S. I., Moskalchuk A. I., Krasov A.V. Development of security scenarios for creating vulnerable virtual machines and studying penetration testing methods–Information technologies and Telecommunications, 2021 //Vol. – 2021. – vol. 9. –pp. 1-2
4. Katasonov A. I., Shterenberg S. I., Tsvetkov A. Yu. Assessment of the stability of the mechanism implementing... The mandatory essential role model of access rights differentiation in gnu linux operating systems //Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and Technical Sciences. – 2020. – No. 2. – pp. 50-56.
5. Budarny G. S. et al. Types of security breaches and typical attacks on the operating system //Actual problems of infotelecommunications in science and education (APINO 2022). – 2022. – pp. 406-411.