Молодёжный вестник НФ БГТУ. 2022. Том 02. № 04 (08)
https://rio-nb-bstu.science

ИНФОРМАТИКА. КРАТКИЕ СООБЩЕНИЯ

doi: 10.51639/2713-0576_2022_2_4_77
УДК 004.7:004.056.5
ГРНТИ 50.41.23
ВАК 05.13.11

Виртуальные частные сети и кибербезопасность

[*] Новичихина А. А., Морковкин Е. А., Замулин И. С.

Хакасский государственный университет им. Н. Ф. Катанова (ХГУ им. Н. Ф. Катанова), 655017, Россия, Республика Хакасия, г. Абакан, ул. Ленина 92/1

e-mail: [*] belka15math@mail.ru, morkowka12@mail.ru, zamulin_is@khsu.ru

Использование виртуальной частной сети (VPN) считается более безопасным способом просмотра страниц в Интернете. Однако, далеко не всегда этот ресурс может гарантировать безопасность своим пользователям. Использование бесплатного инструментария VPN может быть сопряжено с распространением рекламы посредством сети, разглашением и продажей персональных данных пользователей третьим лицам. Кроме того, может снижаться скорость передачи данных по сети, а также ограничиваться объём и время работы с ресурсами.

Ключевые слова: виртуальные частные сети (VPN), конфиденциальность данных, инструменты отслеживания, кибератаки, кибербезопасность.

Использование виртуальной частной сети (VPN) считается более безопасным способом просмотра страниц в Интернете. VPN позволяет пользователям защищать свою конфиденциальность в Интернете и предотвращать отслеживание активности интернет-провайдером. Однако, и VPN далеко не всегда может гарантировать полную безопасность [1]. Рассмотрим особенности, а также возможности и ограничения частной сети. VPN – это набор технологий, позволяющих создать логическую сеть поверх физической. Он используется для защиты трафика от перехвата злоумышленниками и обеспечения безопасности действий в Интернете [1]. Существует два широко используемых метода управления трафиком в программном обеспечении VPN: реализация на основе политик и реализация на основе маршрутов. Маршруты являются наиболее распространёнными методами туннелирования. В типичной конфигурации программное обеспечение VPN на клиентском устройстве изменяет таблицу маршрутизации для отправки всего трафика на интерфейс туннелирования, указав ему более конкретный маршрут, чем шлюз по умолчанию. Весь трафик, принимаемый туннельным интерфейсом, шифруется и инкапсулируется программным обеспечением VPN, а затем направляется по общедоступному интерфейсу на VPN-сервер, где он подключается к общедоступному IP-адресу VPN-сервера и отправляется конечному получателю пакета через Интернет. VPN на основе политик не использует дополнительный интерфейс в качестве конечной точки виртуального соединения. Вместо этого для определения трафика VPN и шифрования любого трафика, соответствующего политике, используются правила брандмауэра [2].

Цель VPN состоит в том, чтобы помешать кому-либо на пути между VPN-клиентом и VPN-сервером видеть содержимое трафика пользователя. Обычно предполагается, что эта часть туннеля защищена. Даже если злоумышленник может видеть пакеты, отправленные с VPN-сервера на конечный сервер (например, веб-сервер), он не сможет определить VPN-клиента только путём анализа пакетов. Злоумышленник может выполнять традиционные атаки по пути между VPN-сервером и Интернет-сервером, особенно когда трафик, генерируемый приложением, дополнительно не шифруется стандартами SSL/TLS. Зашифрованный туннель

между VPN-клиентом и VPN-сервером предназначен для предотвращения этих атак [1]. Также VPN-сервис скрывает информацию о просмотре и затрудняет сбор или мониторинг онлайн-активности пользователя злоумышленниками. Тем не менее, использование VPN не всегда полностью защищает данные и скрывает активность пользователя в Интернете. Рассмотрим основные ограничения виртуальной сети.

1. Инструменты VPN и безопасность пользователей. Отдельные инструменты VPN могут содержать вредоносные программы, которые, в свою очередь, могут использоваться киберпреступниками для кражи данных пользователей, получения несанкционированного доступа к устройству пользователя, осуществления кибератаки. Отчёт об исследовании ICSI Networking and Security Group показал, что 38 % из 283 изученных приложений Android VPN содержали некоторую форму присутствия вредоносных программ [2]. Поэтому приложение VPN не всегда может быть безопасным при использовании его бесплатных инструментов.
2. Инструменты VPN и онлайн-активность. Безопасный VPN предназначен для защиты активности пользователей во время просмотра Интернета, но некоторые частные сети могут отслеживать онлайн-активность пользователей. То же исследование ICSI показало, что 72 % VPN-сервисов проанализировали встроенные сторонние инструменты отслеживания в своём программном обеспечении. Их наличие позволяет средствами инструментария VPN собирать информацию о пользователях для различных целей [2].
3. Сервисы VPN и использование данных. VPN хорошо подходят для защиты данных или скрытия местоположения пользователя при просмотре видео-контента из потоковой службы, которая недоступна в регионе. В то же время, VPN обычно ограничивает объём данных, которые пользователи могут получить с помощью данного инструмента. Это касается как ограничения объёма данных, которые они могут использовать в месяц, так и ограничения времени, в течение которого VPN доступен за сеанс просмотра, а также контетных ограничений (разблокировка только определённых веб-сайтов). Поэтому инструменты VPN могут не подойти пользователям, которые хотят защитить свои данные или замаскировать своё местоположение в течение значительного периода времени.
4. VPN и скорость Интернета пользователей. Сервисы VPN могут снижать скорость Интернета по сравнению с прямым подключением.
5. Инструменты VPN и реклама. Виртуальные частные сети используют рекламу для получения дохода. Опасность состоит в том, что посредством рекламы могут распространяться вредоносные программы. Наличие рекламы в VPN-сервисе также может стать проблемой конфиденциальности, поскольку через провайдера могут происходить утечки информации об онлайн-активности пользователей. Платные VPN включают в себя инструменты блокировки рекламы, а также такие функции, как защита от вредоносных программ и неограниченная пропускная способность. Эти функции повышают безопасность пользователей виртуальных частных сетей [2].

Один из популярных сервисов VPN Hotspot Shield собирал данные своих пользователей и перехватывал трафик, несмотря на утверждения разработчиков о «полной анонимности». Сервис собирал cookies и предоставлял другим организациям в коммерческих целях. В июле 2020 года эксперты по цифровой безопасности обнаружили в открытом доступе 1,2 терабайта логов сервисов UFO VPN, Fast VPN, Free VPN, Super VPN, Flash VPN, Secure VPN и Rabbit VPN. В базе данных содержались незашифрованные пароли, IP-адреса устройств, данные о моделях смартфонов и идентификаторы устройств пользователей [3]. В 2021 году среди выявленных утечек данных через частные сети можно выделить две наиболее крупномасштабные. В открытом доступе оказалась база с данными около 21 миллиона пользователей таких сервисов, как Gecko VPN, Super VPN и Chat VPN. Среди них – сведения о мобильных устройствах, адреса электронных почт, пароли и информация о совершённых пользователями платежах [4]. В ноябре 2021 года в даркнете выставили на продажу базу данных 45,5 миллионов пользователей сервисов FreeVPN.org и DashVPN.io. В ней была собрана информация с 2017 по 2021 год. Она включала адреса электронных почт пользователей, зашифрованные пароли, даты регистрации,

обновления профиля и последнего входа [5]. Такой набор информации даёт мошенникам возможность взламывать ресурсы, где пользователи регистрировались с теми же данными, а также шантажировать клиентов VPN-сервисов посещаемыми ими запрещёнными сайтами.
Таким образом, виртуальная частная сеть действительно может помочь в обеспечении безопасности данных, конфиденциальности, однако эта защита определённым образом ограничена. VPN использует достаточно надёжные алгоритмы шифрования, но включение VPN-клиента на компьютере не гарантирует 100 %-ной защиты конфиденциальной информации. VPN открывает доступ к некоторым заблокированным ресурсам, поэтому многие готовы мириться с более низкой скоростью и возможными задержками программы. Необходимо тщательно подходить к выбору самого VPN-сервиса, особенно если склоняться к использованию бесплатного инструментария. Есть ряд примеров, когда различные сервисы без подписки похищали персональные данные или допускали их утечку.

Конфликт интересов

Авторы статьи заявляют, что у них нет конфликта интересов по материалам данной статьи с третьими лицами на момент подачи статьи в редакцию журнала, и им ничего не известно о возможных конфликтах интересов в настоящем со стороны третьих лиц.

Список литературы

1. Толли У. Дж., Куджат Б., Хан М. Таха, Валлина-Родригес Н., Крэндалл Дж., Атаки вслепую в пути и приложения для VPN / 30-й симпозиум по безопасности USENIX 21, 3129-3146 с. (2021).
2. Безопасность VPN: насколько безопасна виртуальная сеть? [Электронный ресурс] / Fortinet: [сайт]. – URL: https://www.fortinet.com/ru/resources/cyberglossary/are-vpns-safe (дата обращения: 21.03.2022).
3. Шон Николс. Семь VPN-провайдеров «no log» обвиняются в утечке пользовательских логов в Интернете [Электронный ресурс] / The Register: [сайт]. – URL: https://www.theregister.com/2020/07/17/ufo_vpn_database/ (дата обращения: 02.04.2022).
4. Один из крупнейших VPN-сервисов Android взломан? Данные 21 миллиона пользователей из 3 Android VPN выставлены на продажу онлайн [Электронный ресурс] / Cybernews: [сайт]. – URL: https://cybernews.com/security/one-of-the-biggest-android-vpns-hacked-data-of-21-million-users-from-3-android-vpns-put-for-sale-online/ (дата обращения: 02.04.2022).
5. Исакова Т. Электронный след вывел в сеть [Электронный ресурс] / «Коммерсантъ»: [сайт]. – URL: https://www.kommersant.ru/doc/5062713 (дата обращения: 21.03.2022).

Virtual private networks and cybersecurity

* Novichikhina A. A., Morkovkin E. A., Zamulin I. S.

Katanov Khakass State University (N. F. Katanov KHSU)
655017, Russia, Republic of Khakassia, Abakan, Lenin Street, 92/1

Using a virtual private network (VPN) is considered a safer way to browse the Internet. However, this resource cannot always guarantee the safety of its users. The use of free VPN tools may involve the spread of spam through the network, disclosure and sale of users' personal data to third parties. In addition, the speed of data transmission over the network may decrease, as well as the volume and time of working with resources may be limited.

Key words: virtual private networks (VPN), data privacy, tracking tools, cyber attacks, cybersecurity.