4. **Делёз, Ж.** Анти-Эдип: Капитализм и шизофрения: пер. с франц. и послесл. Д. Кралечкина; науч. ред. В. Кузнецов / Ж. Делёз, Ф. Гваттари. – Екатеринбург: У-Фактория, 2007. – 672 с.

5. **Кара-Мурза, С. Г.** Постиндустриализм. Опыт критического анализа / С. Г. Кара-Мурза, С. С. Сулакшин, В. И. Якунин. – Москва: Litres, 2017. – 2165 с.

6. **Уэбстер, Ф.** Теории информационного общества: пер. с англ. / Ф. Уэбстер. – Москва: АСПЕКТ ПРЕСС, 2004. – 467 с.

УДК 1:2:004.056

В. Д. Зюзин

ОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ VPN-СЕРВИСОВ

Аннотация. Описываются опасности, которые могут возникать при использовании различных VPN-сервисов и технологии VPN в целом. Во-первых, пользователи ставят под удар утечку собственных данных, а во-вторых, могут поддаться искушению с точки зрения Православной церкви.

Ключевые слова: VPN, сервис, использование, ресурс, Российская Федерация, цель, технология, трафик, безопасность.

VPN (или виртуальные частные сети) – это технология безопасного зашифрованного подключения пользователей к сети с целью обхода локальных ограничений методом замены изначального IP-адреса на IP-адрес VPN-сервера. Но все же у данной технологии есть свои недостатки, что противоречит слову «безопасность». Со сложившейся мировой ситуацией и ее последствиями в виде санкций по отношению к Российской Федерации со стороны стран НАТО и США российские граждане были вынуждены пользоваться различными VPN-сервисами для допуска к некоторым зарубежным сервисам и ресурсам.

В мобильных магазинах Google Play, Apple Store и др. существует множество VPN-сервисов, которые предоставляются платно или бесплатно. Платные VPN-сервисы являются более защищенными, но все равно стоит понимать, что, пользуясь любыми VPN-сервисами, пользовательское устройство доверяет ему на таком же уровне, как доверяет интернет-провайдеру, поэтому данный сервис может отслеживать всю пользовательскую активность и весь трафик, который может использовать в своих целях. Бесплатные VPN-сервисы считаются очень небезопасными в силу того, что именно они и могут использовать пользовательскую информацию в своих целях в виде ее дальнейшей продажи на различных ресурсах, ведь целью любых сервисов является зарабатывание денежных средств. Платные VPN-сервисы зарабатывают их в виде платных подписок с пользователей за их использование, а бесплатные не все обходятся монетизацией рекламы и поэтому, чтобы заработать больше денег, они и ставят под удар пользовательскую безопасность и конфиденциальность. Поэтому лучше поль-

зоваться частным VPN-сервером, где меньше вероятность подобных угроз безопасности.

Но существует три типа ресурсов, к которым российские граждане хотят получить доступ:

1) ресурсы, которые официально прекратили деятельность на территории Российской Федерации в виде санкций из-за мировой ситуации (например, Netflix и Megogo);

2) ресурсы, которые официально запрещены Правительством Российской Федерации из-за нарушения законодательства (например, Meta);

3) ресурсы, которые официально запрещены за пределами Российской Федерации (например, ГосУслуги).

Для посещения первого типа ресурсов власти Российской Федерации не накладывают каких-то ограничений.

На второй тип распространяется закон о связи, средств обхода блокировки незаконного контента, поэтому Роскомнадзор принимает меры по ограничению VPN-сервисов [1].

Третий тип необходим в случае, если гражданин Российской Федерации на момент посещения ресурса находится за пределами государства. При таком раскладе рекомендуется использовать свой собственный VPN-сервер у себя дома, поскольку он даст 100-процентную безопасность при использовании данной технологии.

Стоит также добавить, что при использовании обычного интернет-соединения весь трафик видит только провайдер, который передает его Правительству Российской Федерации, а при использовании зарубежных VPN-сервисов трафик провайдер уже не видит, поскольку между пользователем и VPN-сервером создается зашифрованный туннель, но трафик полностью доступен данному VPN-серверу, который находится в юрисдикции другого государства, и, таким образом, трафик российских граждан доступен для правительств других стран, которые могут использовать его в своих целях. В связи с этим настоятельно рекомендуется использовать (включать) VPN-сервис только для конкретных ресурсов, а не пользоваться им постоянно, а в случае с ПК установить расширение VPN или использовать браузер Tor, в котором нет функции VPN-туннелирования, но есть встроенный прокси, который автоматически заменяет IP-адрес.

Также не стоит забывать, что цель VPN – это защита пользовательской конфиденциальности и создание анонимности от провайдера и третьих лиц, которые хотят просмотреть этот трафик, а также обход локальных ограничений. Поэтому даже при использовании VPN-сервиса также есть риск, что в систему пользователя может пробраться различное вредоносное ПО, следовательно, чтобы обезопасить себя, необходимо использовать VPN в тандеме с комплексным антивирусным решением, что даст большую защиту.

С точки зрения Православной церкви создатели VPN не несут какой-либо религиозной ответственности за то, что данная технология может быть использована с плохими намерениями, поскольку изначально она была создана с целью безопасности. Поэтому каждый человек несет собственную ответственность за ее использование, например просмотр порносайтов, пропаганду убийства, экстремизм, пользование пиратскими продуктами и т. д. С такой же стороны можно посмотреть и на обычный кухонный нож, который был создан с целью обработки продуктов, но некоторые применяют его с иными целями.

Стоит сделать вывод, что использование технологии VPN влечет за собой некоторые последствия. В-первую очередь, это собственная небезопасность, поэтому при использовании какого-либо VPN-сервиса стоит читать политику использования, а также понимать, что с точки зрения Православной церкви данная технология может быть инструментом искушения для применения ее в иных целях.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. **Приставка, Е.** В России массово блокируют ВПН. Что это значит и к чему готовиться [Электронный ресурс] / Е. Приставка // Хайтек. – Режим доступа: hightech.fm/2022/06/07/russia-vpn-new. – Дата доступа: 20.05.2022.

2. Общественник рассказал об опасностях VPN-сервисов [Электронный ресурс] // Лента.ру. 09.06.2022. – Режим доступа: lenta.ru/news/2022/06/09/vpn/. – Дата доступа 24.06.2022.

3. Уверены ли вы в том, что можете доверять своему VPN? [Электронный ресурс] // Хабр. – Режим доступа: habr.com/ru/post/443112/. – Дата доступа: 30.05.2022.

4. **Никифорова, А.** Опасность бесплатных VPN. Почему их нельзя скачивать и как защитить себя? [Электронный ресурс] / А. Никифорова // Хайтек. – Режим доступа: hightech.fm/2020/12/11/free-vpn-privacy. – Дата доступа: 03.06.2022.

5. **Бабкин, Н.** VPN – это грех? [Электронный ресурс] / Н. Бабкин // Яндекс.дзен. – Режим доступа: zen.yandex.ru/media/id/5bcf6261fc5ebc00ada412f5/vpn-eto-greh-622372e270765a7bf426e95f. – Дата доступа: 08.06.2022.

УДК 1 (091)

Н. Н. Павлюченков

ФИЛОСОФИЯ ВСЕЕДИНСТВА, ХРИСТИАНСКОЕ МИРОПОНИМАНИЕ И ПРОБЛЕМЫ СОВРЕМЕННОГО ГЛОБАЛИЗМА

Аннотация. Рассматривается дискуссионная проблема соотношения философии всеединства В. С. Соловьева и традиционного христианского мировоззрения в вопросах восприятия и оценки современного движения к глобальному объединению всего человечества. Делается главный вывод о необходимости особого внимания к главной ценности христианства, с которой В. Соловьев в конце своей жизни привел в согласие свою эсхатологию.
Ключевые слова: философия, всеединство, христианство, глобализм, человечество.