АРПП
Отечественный софт

Почтовый адрес: 125009,
Москва, ул. Тверская д.7, а/я 43

21 апреля 2026 г. № АИ-2046/04-26

Председателю Правительства
Российской Федерации

М.В. МИШУСТИНУ

Руководителю Администрации
Президента Российской Федерации

А.Э. ВАЙНО

Уважаемый Михаил Владимирович!
Уважаемый Антон Эдуардович!

Ассоциация разработчиков программных продуктов (АРПП) «Отечественный софт» хочет выразить позицию по поводу ограничения использования протоколов VPN и VPN-сервисов в России.

Министерство цифрового развития, коммуникаций и связи РФ с 1 апреля ввело ограничения по использованию VPN для российских граждан и бизнеса. Распоряжением Министерства с 15 апреля интернет-платформам и провайдерам предписано вычислять пользователей, которые используют VPN для обхода ограничений и ограничивать им доступ к платформам. Это сделано простым распоряжением Министерства, без принятия постановления или нормативно-правового акта, а также без обсуждения с общественностью и подведомственной ИТ-отраслью.

Изначально государством провозглашалось оправданное и обоснованное желание увеличить контроль и влияние на происходящее в информационном пространстве России. Но в качестве технического решения для реализации данной задачи была выбрана полная блокировка нежелательных цифровых платформ, таких как Фейсбук, Твиттер, Инстаграм, а также замедление Ютуба и Телеграма. Это было связано с изобилием враждебного контента на этих платформах, с невозможностью блокировать отдельные страницы и видео этих платформ, а также с отказом их владельцев сотрудничать с российским регулятором и выполнять законы РФ.

По мере увеличения числа блокируемых интернет-ресурсов снижалась надёжность этих блокировок, а также быстро росло число пользователей, использующих сервисы VPN для обхода блокировки. Сервисы обхода эволюционировали, стали простыми в использовании и широко распространились.

Следующим решением Министерства в ходе эскалации борьбы стала блокировка самих сервисов обхода. Однако, с введением блокировок сервисов и протоколов VPN, нарушилась работоспособность Интернета в России, так как блокировки не учли технологические и социальные реалии того, как устроен Интернет

и его российский сегмент. А именно:

1. Не существует никакого гарантированного способа отличить VPN от «обычного» шифрованного интернет-трафика.
2. Не существует технической возможности отличить «законные» корпоративные VPN от VPN, предназначенных для обхода блокировок.
3. Любой пользователь или компания сейчас может подключить или создать собственный VPN-сервер. Политика блокировок сделала технологию VPN широко известной, доступной миллионам неквалифицированных пользователей.
4. Блокировки подстегнут противников РФ (в частности, США) ускорить разработки изощренных технологий для обхода блокировок, а также маскировать трафик различных приложений под VPN-трафик, чтобы вызывать ложные срабатывания средств блокировки (ТСПУ).
5. Поскольку надёжно различить «легитимный» и «антиблокировочный» VPN-трафик нельзя, то блокировки VPN уже вызывают и будут всё чаще вызывать в будущем ложные срабатывания, что означает аварии и **приведение российского сегмента Интернета в нерабочее состояние**.
6. При этом блокировки VPN не решают проблему блокировок запрещённых ресурсов, поскольку помимо VPN существуют другие способы обхода блокировок (прокси, особые настройки оборудования и прочее).

Более подробно объяснения причин технической невозможности эффективных блокировок описаны в Приложении № 1.

Действия Минцифры России по борьбе с обходом блокировок привели к тому, что в РФ с начала апреля наблюдаются системные проблемы в работе Интернета (см. Приложение № 2).

Кроме того, попытки блокировок VPN вызывают **серьёзные проблемы в работе у российских разработчиков** программного обеспечения, а именно:

1. Проблемы с доступом к open-source библиотекам, находящимся на зарубежных ресурсах. Программисты используют VPN для работы с открытым исходным кодом в западных репозиториях, чтобы не показывать свой российский IP-адрес. 99% современного программного обеспечения использует открытый исходный код, подавляющая часть которого размещена в странах, недружественных к РФ. Без этого сейчас невозможно разрабатывать ПО, а блокировка VPN затрудняет этот доступ, мешая импортозамещению.
2. Системы DPI, как любые системы распознавания, неизбежно создают ложные срабатывания и блокируют не то, что было задано. Так, 14 апреля на несколько часов оказался заблокирован один из крупнейших репозиториев Линукса – Debian, а до этого оказался заблокирован репозиторий Rust. Такие сбои ведут к простоям в работе отечественных разработчиков.
3. Многие отечественные ИТ-компании используют труд зарубежных разработчиков, работающих из-за границы. Ограничения в работе VPN сделали работу с ними затруднительной.

Почтовый адрес: 125009,
Москва, ул. Тверская д.7, а/я 43

4. Компании, занимающиеся экспортом своих программных продуктов, столкнулись с серьёзными проблемами с коммуникацией со своими зарубежными партнёрами, поскольку она традиционно ведётся либо по запрещённым мессенджерам, либо через VPN.

К сказанному надо добавить ещё одно соображение. Отечественные разработчики последние 30 лет учили **иностранные языки программирования**, ИТ-продукты и инструменты. Большинство используемых в программировании терминов, информации по разработке, программных библиотек – на английском, что делает программистов зависимыми от мирового ИТ-сообщества. Они не чувствуют себя привязанными к своей стране и могут легко найти работу в любой точке мира. Ухудшение политической атмосферы и условий работы может их подтолкнуть к таким шагам. Мобилизация на СВО осенью 2022 года уже привела к оттоку десятков тысяч ценных разработчиков за рубеж; часть которых с трудом удалось вернуть обратно.

Ограничения доступа вызывают у разработчиков отторжение и азарт обойти эти ограничения. В настоящее время на сотнях программистских форумов в России идут обсуждения того, как обойти трудности с доступом к привычным платформам, к нужным репозиториям и сервисам. Программисты **относятся к блокировкам, как к технической проблеме, и ищут технические же способы эту проблему решить**.

А это значит, что **блокировки вызывают активное технологическое противодействие низового сообщества программистов и айтишников**, общее число которых в России достигает 1,2 миллиона человек, суммарные компетенции которых значительно превосходят всё, что можно организовать и использовать в государственных ведомствах.

Эту игру государственный орган и его технические специалисты выиграть не могут, даже если эскалировать конфликт, придумывая дальнейшие ужесточающие это противостояние меры и кары частным лицам и компаниям.

В частности, насколько нам известно, дальнейшая эскалация блокировок обсуждается в формате «белых списков» VPN для использования компаниями. Это также будет неэффективная мера: если даже компаниям удастся навязать «белые списки», то низовые разработчики будут использовать другие, более изощрённые способы обхода блокировок, а не предписанные начальством (в частности, чтобы их не блокировали западные сервисы и библиотеки, которым такой «белый список» сразу станет известен). А кроме того, вынуждать ИТ-компании ходить за рубеж через фиксированный набор белых сервисов означает помогать в реализации зарубежных антироссийских санкций.

И последнее важное соображение: проблема блокировок средств доступа перестала быть чисто технической проблемой (которой она и изначально не являлась), и стала заметной политической проблемой, вызывая огромное недовольство властью как в ИТ-сообществе, так и в широких слоях населения, что непосредственно видно по рейтингам и соцопросам.

Почтовый адрес: 125009,
Москва, ул. Тверская д.7, а/я 43

Что делать?

1. Политику блокировок, а также технические методы блокировок (как блокировать – необходимо признать неудачными и пересмотреть.
2. Это нужно сделать публично, объявив о пересмотре политики блокировки, параллельно ослабив блокировки, чтобы население этот эффект могло заметить в своей повседневной деятельности.
3. Нужно создать совместный орган для выработки взвешенной политики блокировок – вместе с профессиональными специалистами ИТ-сообщества. ИТ-сообщество умеет бороться с негативными явлениями Интернета (вирусы, атаки, мошенники, фишинг, спам) достаточно эффективно, и эти компетенции можно и нужно использовать.
4. Ассоциация разработчиков программных продуктов «Отечественный софт» готова выделить своих лучших технических специалистов из разных компаний в такой согласительный орган, пока проблема не вышла на очередной уровень эскалации, и в ИТ-среде не начались увольнения и очередная волна отъезда за границу. Мы готовы продумать и предложить взвешенные меры по суверенизации информационного пространства РФ без разрушения инфраструктуры Рунета.

Приложения:

1. Почему технически невозможно полностью заблокировать VPN?
2. Сбои Интернета с начала апреля 2026 года.

С уважением,

Председатель Правления
АРПП «Отечественный софт» Н.И. Касперская

Почтовый адрес: 125009,
Москва, ул. Тверская д.7, а/я 43

Приложение № 1

Почему технически невозможно эффективно заблокировать VPN?

Термин VPN (сокращение от Virtual Private Network) переводится, как «виртуальная частная сеть». Это средство построения виртуального шифрованного канала между произвольными компьютерами, подключенными к Интернет.

Исходно технологии VPN были задуманы и использовались, как средство построения частных сетей географически распределенных организаций, то есть для организации защищенной контролируемой связи между подразделениями и филиалами в разных городах или странах, и для доступа сотрудников в корпоративную сеть не из офиса.

«Классические» VPN работали по специальным протоколам (IPSec, OpenVPN, Wireguard и т.д.), которые легко мог определить транзитный провайдер. Однако по мере развития блокировок в мире (в частности, блокировки некоторых open-source репозиториев в 2022-2023 гг. для программистов из России) значительная часть VPN, помимо своей основной функции, стала маскировать свой трафик под «обычный» интернет-трафик, чтобы его нельзя было выявить. Назовём такие средства «VPN нового типа». Они обычно существуют в одном из двух видов:

А) сервис, который можно купить за небольшие деньги. Таких сервисов сотни, их периодически сотнями блокируют, но их постоянно обновляют и вновь выкладывают в сеть;

Б) виртуальный сервер, на котором запускают сервер VPN или прокси. Раньше это было доступно только специалистам, но сейчас процедура сильно упростилась и доступна любому, кто знаком с основами администрирования Linux.

Одновременно с развитием средств обхода блокировок сильно изменился сам Интернет-трафик. Если на заре Интернета использовалось множество разных протоколов[1], то сейчас основной протокол – шифрованный HTTP (обозначается, как HTTPS). Работа по HTTPS означает, что между клиентом и сервером устанавливается шифрованное соединение по протоколу TLS (Transport Layer Security), или туннель. Внутри этого туннеля трафик передается по обычному протоколу HTTP. **Шифрованный туннель HTTPS функционально не отличается от VPN**.

Блокировки в Интернете осуществляются с использованием Технических Средства Противодействия Угрозам (ТСПУ) и используют системы анализа пакетов Deep Packet Inspection (DPI). ТСПУ могут определить трафик VPN несколькими прямыми способами, а именно:

А) IP-адреса получателя сервера VPN, если адреса известны и стабильны, что сейчас почти не встречается;

[1] HTTP для обычного веб-серфинга, SMTP/POP3/IMAP4 для почты, FTP для передачи файлов, NNTP для сервиса новостей, IRC/Talk для онлайн-чата, SIP/STP/RDP для голосового трафика и т.д.

Б) особенности установления первичного VPN-соединения. Из-за шифрования протоколов этот метод сейчас работает крайне редко;

В) особенности реализации VPN-протокола, которые приводят к появлению повторяющихся шаблонов в пакетах данных (например, одна из реализаций протокола MTProto мессенджера Телеграм приводила к демаскировке трафика Телеграма).

Кроме прямых способов, DPI может накапливать долгосрочную (от минуты до десятков минут) статистику в отношении определенных сессий, на основании выявленных долговременных закономерностей – распределение размеров пакетов, соотношение входящего и исходящего трафика, характер трафика во времени – и делать предположение, что это – возможно, трафик VPN, и далее блокировать трафик между данными IP-адресами. Проблема с этим подходом следующая:

А) Эти признаки косвенные, ненадёжные и чреваты ложными срабатываниями;

Б) Эти признаки короткоживущие, так как нельзя выявленный IP-адрес признать адресом VPN дольше, чем максимум на 1-2 часа, поскольку в современном Интернете IP-адрес конкретного устройства или сервиса в подавляющем большинстве случаев динамический, часто меняется либо на самом конечном устройстве, либо на промежуточной сети.

В) Эти признаки легко подделать так, чтобы они выглядели как «легитимный» трафик.

Г) Несложно также создать поток трафика, который с точки зрения DPI был бы очень похож на трафик VPN, чтобы намеренно заставить DPI сработать. Это создаёт возможность для перегружающей атаки на ТСПУ (DoS-атаки), которая может привести к блокировке отдельных адресов или целых сетей провайдеров.

Д) Напротив, если трафик каких-то популярных VPN специально сделать похожим на адреса и/или трафик крупных банков, то ТСПУ заблокирует и их тоже, что приведёт к параличу банковской системы.

Е) Также ложные срабатывания ТСПУ могут происходить из-за использования корпоративных VPN, антивирусного ПО, средств виртуализации и контейнеризации, а также технологии NAT (позволяет преобразовывать внутренние IP-адреса локальных устройств в один или несколько внешних адресов).

Но даже, если удастся оперативно выявлять и блокировать «маскирующиеся VPN», то это не решит проблему использования запрещённых ресурсов, так как существуют другие способы обхода блокировок. А именно:

- Прокси – промежуточный сервер, пропускающий через себя трафик конкретного приложения. Отследить использование каждого прокси очень сложно.
- Особые настройки клиентского оборудования, например, фрагментация пакетов (разбиение одного пакета на несколько) на этапе установления шифрованного соединения, затрудняющая или делающая невозможным глубокий анализ пакетов трафика.

Сказанное означает, что «полностью» и эффективно осуществить блокировку VPN в масштабах страны – невозможно, а также технически и политически вредно.

Почтовый адрес: 125009,
Москва, ул. Тверская д.7, а/я 43

Приложение № 2

Сбои Интернета в России с начала апреля 2026 года

Сообщения о сбоях доступа в Интернет идут практические сплошным потоком, почти каждый день. Возможно, часть из них вызвана не блокированием VPN, а блокировками мобильного трафика в борьбе с БПЛА, однако широкая публика уже не отличает одно от другого.

Дата	Сообщения в СМИ
01.04.2026	Скорость Интернета значительно упала, порою до десятков килобит. Масштабные сбои в работе онлайн-сервисов случились друг за другом 20 и 30 марта. Не успели мы все перевести дух и вот опять... Даже неизвестно кого винить, многие склоняются к тому, что это была мощная DDoS-атака. Роскомнадзор уже под конец дня заявил, что крупные операторы связи сегодня меняли оборудование, с чем и связаны перебои в работе интернета
02.04.2026	Жалобы на отключение мобильного интернета поступают из десятков российских регионов. Абоненты МТС, «МегаФона», «Билайна», Т2, Yota и других операторов сообщают, что по причине падения скорости загрузки и нестабильного соединения не могут полноценно пользоваться онлайн-услугами, навигатором, каршерингом, поисковыми системами, а также мессенджерами и QR-кодами
03.04.2026	3 апреля мобильный интернет перестал работать в десятках регионов России. Проблемы затронули всех операторов «большой четверки», а следом «легли» банковские приложения, маркетплейсы и мессенджеры. Жители Москвы, Санкт-Петербурга и других городов остались без связи, платежей и доступа к привычным сайтам
04.04.2026	4 апреля мобильный интернет не работает в Москве, Свердловской области и других регионах России. С проблемами столкнулись абоненты операторов Т2, МТС, Yota, «Билайн» и «МегаФон»
06.04.2026	Вечером 6 апреля пользователи по всей стране сообщили о масштабном сбое в работе Рунета. По данным мониторинговых сервисов, проблемы затронули множество сервисов, включая: • игровые платформы (Steam, «Мир танков», Valorant, League of Legends); • банковские сервисы (Сбербанк, Альфа-банк, ВТБ, др.); • «Госуслуги»; • социальные сети и мессенджеры; • сервисы мобильных операторов; • стриминговые платформы («Кинопоиск», «Иви», Rutube).

07.04.2026	Пользователи сообщают о масштабном сбое в Рунете. Проблемы затронули десятки сервисов — в том числе Discord и Steam, также наблюдаются неполадки в работе «Ростелекома»
09.04.2026	Сегодня, 9 апреля, мобильный интернет не работает в Москве, Санкт-Петербурге и других регионах России. С проблемами столкнулись абоненты операторов Т2, МТС, Yota, «Билайн» и «МегаФон»
11.04.2026	11 апреля, жители многих российских городов вновь столкнулись с перебоями в работе мобильного интернета. Проблемы затронули всех крупных операторов: МТС, «Билайн», «МегаФон», Т2 и Yota
13.04.2026	Наибольшее количество сообщений о сбоях в работе мобильного интернета 13 апреля поступило от жителей Москвы. Также жалобы зафиксированы из Санкт-Петербурга, Татарстана, Чувашии, Марий Эл, Кузбасса, Алтайского, Красноярского и Краснодарского краев, Волгоградской, Новосибирской, Нижегородской, Свердловской, Московской, Омской, Ростовской, Самарской, Смоленской и Курганской областей
14.04.2026	14 апреля, наблюдаются сбои в работе мобильного интернета в Москве, Забайкальском крае и других регионах России
15.04.2026	15 апреля, мобильный интернет не работает в Москве, Ростовской области и других регионах России. С проблемами столкнулись абоненты операторов Т2, МТС, Yota, «Билайн» и «МегаФон»
17.04.2026	17 апреля, мобильный интернет не работает в Москве, Ханты-Мансийском автономном округе и других регионах России. С проблемами столкнулись абоненты операторов Т2, МТС, Yota, «Билайн» и «МегаФон»