

VPN в России: адаптация пользователей к цензуре



Исследование посвящено адаптации пользователей к интернет-цензуре и пользовательскому опыту в ходе применения VPN: как выбирают VPN, с какими трудностями сталкиваются при его использовании, как относятся к политике блокировок в России в целом и, в частности, к собственной кибербезопасности.

Исследование основано на 3 фокус-группах (2, состоящие из рядовых пользователей, 1 из гражданских активистов), экспертном интервью с главой поддержки Amnezia VPN и включенном наблюдении. Выборка из 16 человек включает информантов, сбалансированных по возрастным когортам 18–24, 25–34, 35–45, 46+ из Москвы, Московской области, Екатеринбурга и Ростова-на-Дону.

Контекст

Россия демонстрирует стремительный темп снижения уровня интернет-свободы последние 15 лет¹ и окончательно стала одной из передовых стран в отношении интернет-цензуры, уподобившись Ирану и КНР. Это комплекс мер, состоящий из:

- Правовых запретов на осуществление рекламы средств обхода блокировок, поиска запрещенных материалов, а также признания использования VPN отягчающим обстоятельством при совершении правонарушения, мер по деанонимизации пользователей
- Замедления сервисов без официального запрета (или с ним), блокировки по IP-адресам и подсетям, по протоколу (распознавание и пресечение использования VPN), удаления доменов из Национальной системы доменных имен, введения «белых списков» и полного отключения мобильной связи

Цензура стала повсеместной и затрагивает каждого, находящегося в России, поскольку под удар попали наиболее популярные сервисы. Таким образом, государство провоцирует gateway effect² – освоение средств обхода, которые непреднамеренно расширяют доступ и к иному заблокированному контенту.

● Блокировки платформ

○ Правовые меры

● **Март 2022**

Instagram и Facebook

○ **Март 2024**

Запрет популяризации средств обхода блокировок

● **Июль 2024**

Замедление YouTube

● **Август 2024**

Signal

● **Октябрь 2024**

Discord

● **Декабрь 2024**

Viber

● **Август 2025**

Блокировка звонков в WhatsApp и Telegram

○ **Сентябрь 2025**

Запрет рекламы VPN, VPN как отягчающее, штраф за поиск экстремистских материалов

● **Октябрь 2025**

Частичные ограничения WhatsApp и Telegram

● **Февраль 2026**

YouTube и WhatsApp удалены из НСДИ; официальное замедление Telegram

¹ Vesteinsson, K., & Baker, G. (2025). Freedom on the net 2025: An uncertain future for the global internet. Freedom House. <https://freedomhouse.org/report/freedom-net/2025/uncertain-future-global-internet>

² Hobbs, W. R., & Roberts, M. E. (2018). How sudden censorship can increase access to information. American Political Science Review, 112(3), 621–636.

При этом государство все чаще переступает границу между избирательными блокировками сервисов (пусть и самых востребованных) и полным отключением мобильной связи. В некоторых регионах последнее стало новой нормой, в частности в близких к Украине, но шатдауны уже происходили и в таких городах, как Москва и Санкт-Петербург. Блокировки и отключения интернета создают бытовое неудобство, тем самым вызывая раздражение и недовольство широких слоев населения.

Адаптация к этим процессам происходит по трем сценариям: подчинение (отказ от использования запрещенных сервисов в пользу «Мах», ВК, Яндекс.Дзен и других), избегание (поиск альтернатив, не связанных с продвигаемыми государством сервисами, демонстративный пример – рост аудитории американского мессенджера Iмо менее чем с миллиона пользователей до 8 миллионов в 2025 году³) и сопротивление (предмет нашего интереса, использование средств обхода блокировок). Повсеместный поиск обхода блокировок не только приводит к активному скачиванию VPN сервисов, но и создает новые формы кооперации и сообществ, имеющие целью противодействие цензуре, даже если их мотив носит потребительский, а не политический характер.

³ Американский мессенджер Iмо стал пятым по популярности в России. (2026, 4 февраля). Forbes.ru.
<https://www.forbes.ru/tekhnologii/554754-amerikanskij-messendzer-imo-stal-patym-po-populyarnosti-v-rossii>

Использование ВПН

На материалах фокус-групп был составлен путь пользователя (user journey), включающий в себя поиск и выбор сервиса для обхода блокировок, непосредственно опыт его применения и сопряженные трудности, а также условия, при которых пользователи готовы отказаться от использования ВПН.

Этап	Описание
Триггер	Осознание потребности привязано к конкретному событию блокировки. Преимущественно триггеры сопряжены с блокировками Instagram и YouTube, WhatsApp и Telegram. Цензурные меры стимулируют скачивание VPN, что подтверждается также словами представителя службы поддержки Amnezia VPN.
Бесплатный вход	Первые бесплатные VPN берутся из верхних строк выдачи App Store/Google Play, из рекламы блогеров. Нередко происходит накопление взаимозаменяемых бесплатных приложений, чтобы переключаться между разными вариантами в зависимости от того, работают ли они.
Переход на платные сервисы	Наращение усталости от издержек, сопряженных с использованием бесплатных приложений (реклама, нестабильность, автоматическое выключение VPN в процессе использования), выталкивает в платный сегмент. Выбор конкретного сервиса осуществляется преимущественно через личные рекомендации, также в выборке в меньшей степени представлен выбор на основе рекомендаций блогеров, профильных организаций (например, «Первый отдел», но это относится преимущественно к активистам), а также, в последнюю очередь, отзывов в App Store/Google Play. То есть ситуация прямо противоположна выбору бесплатного сервиса.

**Использование
и сопряженные
проблемы**

Главная переживаемая проблема – не блокировка, а распад сосуществования VPN и локальных сервисов: регулярное включение и выключение сервиса из-за противодействия со стороны лояльных государству структур повседневного пользования (банки, маркетплейсы, такси и иные). Региональная специфика («белые списки», отключение мобильной связи) во многих случаях непреодолима (обход «белых списков» пока не стал широко распространен и воспринимается как положительная отличительная черта отдельных сервисов). Нередко в фокус-группах упоминалось, что в случае, когда что-то не работает, информанты затрудняются определить, связано ли это с блокировкой со стороны России, со стороны сервиса, с неполадками VPN или проблемами со связью в целом.

**Удержание /
смена**

Первоочередные факторы удержания пользователей – это стабильность соединения и качество работы поддержки. Оплата VPN для многих стала считаться частью необходимых расходов домохозяйств наравне с оплатой интернета. В рамках фокус-групп удовлетворительным называют разброс цен от 100 до 800 рублей в месяц. Значимый фактор удержания – атрибуция сбоя: информанты, объясняющие неполадки действиями цензора, а не недостатками сервиса, не меняли VPN даже при регулярных обрывах соединения, поскольку исходили из убеждения, что сервис решит проблему (в этом отношении большую роль играет работа службы поддержки). Отдельно удерживает инерция. Возможность подключать несколько устройств превращает подписку в коллективную инфраструктуру и повышает издержки от смены сервиса.

Уходят в четырех случаях: поддержка не справилась с проблемой или иначе проявила себя неудовлетворительно (задержки ответов, игнорирование, применение бота вместо человека); продолжительная нестабильность соединения без объяснения причин; сервис исчез сам (заблокирован, удален

из магазина приложений, закрылся); несовместимость сервиса с устаревшей техникой.

Ретрансляция

Люди, уже использующие VPN, нередко становятся узлами раздачи: советуют сервис, делятся ключами, подключают близких к своей подписке, устанавливают и настраивают тем, кто не справится сам (преимущественно старшим родственникам).

Предельная форма ретрансляции в выборке – потребительский кооператив, который один из информантов построил вокруг собственного сервера: каждый новый вступительный взнос продлевает аренду сервера, а близких можно подключать без взносов. Само приглашение в кооператив распространяется только среди личных знакомых.

Отказ от VPN

Во всех фокус-группах возможность отказа от использования VPN неприемлема со слов информантов. Они выделяют только два сценария, при которых могут отказаться от обхода блокировок: резкое ужесточение законодательства (уголовные сроки за VPN) или отмена блокировок как таковых.

Впрочем, следует отметить, что для информантов старшего возраста техническая сложность может стать причиной недобровольного отказа от использования VPN. Также упоминаются кейсы перехода на незаблокированные ресурсы в связи с утомлением от проблем с доступом и необходимостью быть на связи (например, по работе).

Отношение к блокировкам и кибербезопасности

Вторым фокусом интереса исследования стало отношение к блокировкам, а также восприятие VPN в контексте личной кибербезопасности. Соответствующий блок вопросов был направлен на уточнение осведомленности в отношении кибербезопасности, используемых средств защиты, восприятия угроз.

В первую очередь следует отметить, что блокировки повсеместно воспринимаются негативно – они вызывают раздражение, усталость и ощущение деградации цифровой среды. Никто из информантов не высказывался о них в положительном ключе. Официальный государственный дискурс относительно защиты детей, экстремизма или суверенитета не воспроизводился ни в критике, ни в попытке объяснения причин блокировок. В этом отношении успехов пропаганды в рамках исследования не наблюдается, что позволяет предположить, что ей не верят.

Некоторые информанты в целом затрудняются дать для себя какое-то объяснение подобной политике, отмечая ее тщетность со ссылками на исторический опыт (приводя сравнение с сухим законом и запретом аборт). Те, кто дает объяснение, относятся к блокировкам как к государственному протекционизму для поддержки отечественных платформ, средству осуществления слежки и контроля за действиями граждан в цифровой среде. Информанты усматривают за этой политикой исключительно интересы государства, вступающие в конфликт с их собственными интересами, заключающимися в свободном доступе к информации и сохранении приватности в интернете.

Тем показательнее, что VPN почти не наделяется защитной функцией. Информанты видят в нем в первую очередь средство доступа к привычным сервисам (а двое из информантов даже рассматривают VPN как дополнительный источник угрозы, опасаясь кражи своих данных). В отношении кибербезопасности большинство пользователей декларируют безразличие. Половина из информантов-активистов, напротив, выражает обоснованную заинтересованность в кибербезопасности. Рядовые пользователи говорят о том, что им «нечего скрывать» и «как бы ни защищался, все в конечном итоге доступно», но при этом, если спрашивать про используемые меры безопасности, они вспоминают двухфакторную аутентификацию, антидетект-браузеры, шифрование на диске и иные технические

средства для защиты своих данных (вплоть до запуска «Маха» на виртуальной машине, когда им нужно воспользоваться).

Таким образом, рефлексия информантов не совпадает с исполняемыми ими практиками, базовые меры безопасности многими применяются.

Осведомленность в сфере кибербезопасности преимущественно коррелирует с осведомленностью в сфере IT. Важно отметить, что скорее само слово «кибербезопасность» для информантов звучит как нечто специфическое, нежели повседневное, в связи с чем, вероятно, и образуется разрыв между рефлексией и практикой. Отсутствие знаний не препятствует использованию программного обеспечения, направленного на обеспечение безопасности пользователя.

Срез	Активисты	Рядовые пользователи	Всего
Декларируется безразличие к кибербезопасности	3 из 6 информантов	7 из 10 информантов	10 из 16 информантов
Технические средства (ПО)	4 из 6 информантов	5 из 10 информантов	9 из 16 информантов
Меры предосторожности	5 из 6 информантов	8 из 10 информантов	13 из 16 информантов

Отдельно следует отметить меры предосторожности, которые вспоминают информанты, когда говорят о своей безопасности. В качестве основных источников угроз в этом контексте упоминались государство и мошенничество. Меры предосторожности, связанные с мошенничеством, направлены преимущественно на защиту от фишинга и в этом смысле тоже входят в сферу кибербезопасности, но

не представляют для нас существенного интереса в контексте исследования. В отношении государства опасения, например, толкают пользователей к избеганию установки навязываемого мессенджера «Мах» (при декларируемой позиции «мне нечего скрывать» в том числе) или российских приложений в целом. Отношение к «Маху» выглядит как отношение к общению по мобильной связи – это небезопасно, российский пользователь воспринимает риск прослушки как неизбежный (политические темы – это «не телефонный разговор»). Различие лишь в том, что «Мах» собирает куда больше информации, чем могло бы быть сказано по телефону.

Опасения перед государством при этом редко соотносятся с какими-то правовыми нормами, информанты не склонны вспоминать о них. Это в меньшей степени относится к активистам, лучше знакомым с законодательством. Представляет интерес тот факт, что один из информантов, который объяснил установку VPN именно опасением перед законом, упомянул закон, который никогда не принимали, но его обсуждение бурно велось в соцсетях (а именно новости о возможном списании платы за зарубежный трафик). В то же время, согласно данным поддержки Amnezia, широко распространено заблуждение, что оплата VPN может быть преступлением.

Это демонстрирует, что имеет место своеобразная «запуганность» пользователей, которые не следят за законодательством и могут иметь ложное представление о существующих законах.

Заключение

До массовых блокировок VPN был инструментом профессиональной среды, бытовой технологией его сделала цензура. Каждая волна освоения VPN начинается с блокировки того или иного популярного сервиса, чья аудитория не видит альтернатив в русскоязычном сегменте интернета (как в случае с YouTube, количество и качество контента которого несопоставимы с RuTube или VK Видео) или не желает ими пользоваться (как в случае с «Мах», установку которого многие избегают или купируют риски, используя для него отдельный телефон).

Качества самих VPN сервисов отвечают за удержание пользователей, но ничто так не способствует их скачиванию, как действия государства. В то же время по материалам фокус-групп мы можем утверждать, что подавить инструменты обхода у российской власти не получается (единичные случаи отказа от средств обхода блокировок зафиксированы, но их слишком мало) и ухудшение работы того или иного сервиса ведет не к отказу от VPN как такового, а только к перераспределению пользователей между сервисами. Формируется замкнутый круг: блокировка популярного сервиса создает массовое бытовое неудобство, неудобство конвертируется в установку средств обхода, рост обхода провоцирует новый виток ужесточения, а он, в свою очередь, рекрутирует следующую волну.

Добиваясь контроля над потреблением информации, государство само расширяет аудиторию инструментов противодействия цензуре. При этом люди не ищут пути обхода в индивидуальном порядке, они формируют множество маленьких и больших сетей взаимопомощи: начиная от раздачи ключей родным и близким, заканчивая созданием целых кооперативов на десятки человек.

В равной степени затрагивая лоялистов, оппозиционеров и аполитичных граждан, блокировки становятся необычным источником солидарности, поскольку выступают общей проблемой на бытовом уровне и формируют рутинную практику неподчинения.

Таким образом, политика блокировок если не контрпродуктивна, то как минимум имеет крайне неоднозначные результаты. С одной стороны, отток доли пользователей неизбежен при блокировке сервиса. С другой, массовое освоение средств обхода ради одного сервиса, отсутствие которого подтолкнуло пользователя к установке VPN, открывает доступ ко всему массиву

заблокированных ресурсов и затрудняет осуществление цензуры. То есть решение частной проблемы имеет как следствие преодоление имеющихся ограничений в целом.

Страхи пользователей при этом направлены мимо действительных рисков: со слов эксперта, самое стойкое заблуждение состоит в том, что платить за VPN незаконно, тогда как о настоящих правовых новшествах осени 2025 года (ответственности за умышленный поиск экстремистских материалов и признании VPN отягчающим обстоятельством) в фокус-группах вспоминают редко. Между тем перенос наказуемости с распространения запрещенной информации на ее потребление возвращает VPN к первоначальному назначению, то есть к сокрытию сетевой активности от провайдера и государства, однако пользователи этого сдвига не замечают (по крайней мере пока).

Несмотря на то, что среди информантов господствует убеждение, что блокировки бесполезны, это представляется верным только до определенного предела. Фильтрация, то есть ограничение доступа к конкретным сервисам, не является пределом возможностей государства. Существует следующая ступень эскалации – инфраструктурное ограничение связи: «белые списки» и полное отключение мобильного интернета. В некоторых регионах, включая Ростов-на-Дону, подобные ограничения стали частью повседневности, но пока не затрагивали домашний интернет.

«Белые списки» преодолимы, но технически это более затруднительно и сильно зависит от используемых для обхода промежуточных разрешенных серверов, блокировка которых со слов эксперта маловероятна, но все же возможна. Полному отключению связи на бытовом потребительском уровне противопоставить нечего. Пусть технологии mesh-сетей, использующих Bluetooth и локальный Wi-Fi, становятся более известны и способны противодействовать отключению связи, их применение упирается в проблему масштабирования (поскольку охват сети напрямую зависит от плотности активных пользователей). Впрочем, как показывает исследование практики шатдаунов в Индии, подобные ограничения связи, если применяются в ходе протестов, делают их более непредсказуемыми и насильственными⁴. Это не слишком актуально сейчас,

⁴ Rydzak, Jan, Of Blackouts and Bandhs: The Strategy and Structure of Disconnected Protest in India (February 7, 2019). Available at SSRN: <https://ssrn.com/abstract=3330413>

поскольку не происходит крупных протестов, но важно для понимания перспектив развития ситуации в России и оценки возможных последствий применения более жестких ограничений, чем фильтрация.

Прогнозирование

1. Сплошной протокольный анализ превышает мощности ТСПУ, а удержание пользователей держится на атрибуции сбоев цензору. На уровне фильтрации обход подавить не удастся: возможности цензора и способность сервисов адаптироваться будут держать колеблющийся пат, при котором пользователи перетекают между сервисами, а не отказываются от обхода блокировок, и переломить это может лишь переход к режиму «работают только разрешенные ресурсы» (белые списки, отключение связи). Следующий рубеж блокировок – домашний интернет, которого ограничения пока не касались. Следует ожидать, что домашний интернет будет не фильтроваться, а полностью отключаться при необходимости. Испытательным полигоном, вероятно, снова станут южные приграничные регионы.
2. У государства почти нет рычага против ушедших иностранных платформ, поэтому ответом на удаления из App Store сервисов экосистемы VK и мессенджера «Мам», вероятно, станет давление на пользователей внутри России. На сегодня использование VPN само по себе не наказуемо, но после сентябрьских выборов есть основания ожидать дальнейшего ужесточения законодательства вокруг VPN и его криминализации. Слухов достаточно, чтобы некоторые пользователи уже переоценивали свои риски (пример информанта, верившего в закон, который не принимался). Показательное уголовное или административное дело может выступать фактором запугивания для пользователей, что станет значительным вкладом в цензуру⁵.
3. Эффективным средством противодействия использованию VPN становится не борьба с ним, а создание помех для пользователей с VPN в основных

⁵ Roberts, M. E. (2018). Censored: Distraction and diversion inside China's Great Firewall. Princeton University Press.

бытовых сервисах, обрывающих соединение при использовании VPN (таких как доставка еды, такси, маркетплейсы). Эти меры дополнительно подкрепляются навязыванием инфраструктуры VK и мессенджера «Мах» (иностранные мессенджеры запрещены госорганам, банкам и маркетплейсам по 41-ФЗ, подключение аккаунта «Мах» к «Госуслугам» навязывается даже без установленного «Мах», а также этот мессенджер входит в число обязательно предустановленных приложений на телефоны, продающиеся в России). Есть основания ожидать роста количества пользователей, которые вынуждены будут мигрировать на отечественные платформы. В то же время значительная прослойка общества продолжит сопротивление интернет-цензуре – применение средств обхода и заблокированных сервисов может приобрести более политизированный характер. Так, при стабильных 36% пользующихся VPN (при этом есть предположение, что число занижено в связи с опасением респондентов опроса отвечать честно) осведомленность о средствах обхода заметно выше среди не одобряющих президента (51%) и не поддерживающих военные действия в Украине (55%)^{6,7}, и уход конформистов на отечественные платформы будет только усиливать эту селекцию.

4. По мере того как бесплатные массовые приложения перестают быть эффективны, обход может далее становиться в большей мере коллективной практикой, нежели индивидуальной. Каскадная раздача VPN (родственникам и друзьям) и кооперативы реализуют один из ключевых ресурсов устойчивости к цензуре: широкую личную социальную сеть. Осведомленность они конвертируют в коллективное сопротивление ограничениям. Фрагментированная, малообъемная, впускающая только знакомых инфраструктура вдобавок труднее подавляется, чем массовые сервисы.

⁶ Левада-Центр. (2026, 14 апреля). Пользование интернетом и социальными сетями в марте 2026 года [Пресс-выпуск]. <https://www.levada.ru/2026/04/14/internet-i-sotsseti-v-marte-2026-goda/>

⁷ Левада-Центр. (2026, 31 марта). Проблемы с мобильным интернетом и блокировка иностранных мессенджеров (март 2026) [Пресс-выпуск]. <https://www.levada.ru/2026/03/31/problems-s-mobilnym-internetom-i-blokirovka-inostrannyh-messendzhеров-mart-2026/>

5. Возможными факторами риска выступают статьи 13.29.2 КоАП⁸ и 274.5 УК⁹. 13.29.2 – антифрод-норма с исключением для передачи доступа с согласия в целях правомерного пользования, под которую сегодня раздача ключей не попадает. Пока обход блокировок остается законным, но исключение в рамках статьи держится на слове «правомерно». В случае с 274.5 УК деятельность кооператива, занимающегося подобным, может быть признана преступной, а его участники привлечены к ответственности по п.2 этой же статьи. Послевыборное ужесточение законодательства вокруг VPN может превратить раздачу ключей в административное или уголовное правонарушение.

⁸ Передача информации, необходимой для регистрации и (или) авторизации пользователя информационно-телекоммуникационной сети "Интернет" для получения доступа к функциональным возможностям информационного ресурса.

⁹ Организация деятельности по передаче информации, необходимой для регистрации и (или) авторизации пользователя сети "Интернет" для получения доступа к функциональным возможностям информационного ресурса, иным лицам, если эти деяния совершены из корыстной заинтересованности либо в целях совершения иного преступления.