Обмен файлами и Коммуникация при отключении интернета

Этот раздел является частью курса, посвященного Документированию при отключении интернета.

Последний пересмотр: 31 января 2020 г.

Продолжающееся отключение интернета и репрессии в Кашмире (а это была самая длительная блокировка интернета, когда-либо примененная в условиях демократии) катастрофически сказались на жизни людей в регионе. Более того, в декабре 2019 года в соответствии с политикой компании WhatsApp начал аннулировать аккаунты кашмирцев из-за 120-дневного бездействия пользователей.

На момент написания этой статьи в январе 2020 года Верховный суд Индии постановил, что блокировка интернета на неопределенный срок в Кашмире является незаконной и трактуется как злоупотребление властью. Ограниченный широкополосный и мобильный интернет был восстановлен в некоторых областях, но только для разрешенных сайтов из «белого списка».

Отключение интернета предпринимается для того, чтобы люди не могли обмениваться информацией и общаться (а также чтобы подтолкнуть людей использовать менее безопасные формы связи, такие как мобильный телефон и SMS, которые властям легче контролировать и перехватывать). При полном отключении интернета не всегда есть эффективные обходные пути. Например, в самые строгие периоды отключения интернета в Кашмире для передачи сообщений своим близким люди прибегали к рукописным заметкам и курьерам.

У нас нет гарантированных способов обойти все блокировки, но в ходе бесед с активистами и коллегами мы узнали некоторые методы и подходы для автономного обмена материалами и общения, которые могут быть вам полезны в зависимости от обстоятельств. Обратите внимание, что некоторые из этих опций подразумевают подключение к интернету для первоначальной настройки (например, для скачивания приложений и т.д.).

Обменивайтесь файлами напрямую через Bluetooth, Wi-Fi Direct или NFC

Вам не нужен интернет, чтобы подключить свой телефон к другому устройству, находящемуся поблизости, через Bluetooth, Wifi Direct или Near Field Communication (NFC) (иногда на более старых устройствах эта функция называется Android Beam). Bluetooth и Wifi Direct - это беспроводные технологии, которые могут «связать» два устройства без участия роутера или точки доступа. WiFi Direct обеспечивает более широкий радиус и более быструю передачу данных, чем Bluetooth, но потребляет гораздо больше энергии. Между тем, NFC работает в более коротком радиусе (~ 4 см) и с более низкой скоростью

передачи, чем Bluetooth или WiFi Direct, но подключается быстрее и потребляет меньше энергии, поэтому такой вариант может быть полезен для быстрой передачи небольших объемов данных, когда оба устройства находятся у вас в руках.

Скорее всего, в ваш телефон встроены функции Bluetooth, WiFi Direct и NFC, которые отображаются в меню "поделиться". Кроме того, эти технологии интегрированы в приложения с функцией обмена файлами, такие как Files By Google.

Важно: помимо преимущества в видео простоты подключения, эти сервисы имеют и недостаток - они небезопасны. Маяки / сканеры Bluetooth и Wi-Fi могут использоваться для отслеживания вашего местоположения или "прощупывания" вашего устройства на предмет информации. Злоумышленники могут попытаться подключиться к вашему устройству, отправить вам нежелательные файлы или даже получить контроль над вашим устройством, если оно уязвимо. **Для большей безопасности отключайте эти сервисы, когда не пользуетесь ими, и включайте только находясь в безопасных местах, ограничьте разрешения приложений только тем, что вам действительно нужно, и применяйте стандартные практики безопасности телефона, такие как установка обновлений и использование надежных паролей.**

Обменивайтесь файлами с помощью беспроводных накопителей или через беспроводную локальную сеть (WLAN).

Беспроводной жесткий диск или флэшка могут использоваться для одновременного обмена файлами между командой или несколькими людьми. Жёсткий диск с Wi-Fi обычно сопровождается инструкциями и / или приложением для подключения к телефону, и достаточно прост в использовании. Не забудьте для безопасности установить на диске пароль.

Если у вас нет беспроводного накопителя, вы также можете обмениваться файлами с помощью обычного USB-накопителя, подключив его к беспроводному роутеру. Например, дорожный роутер с USB-портом относительно недорог и очень портативен. Пользователи могут подключаться к USB-накопителю через локальную сеть (интернет для этого не требуется). Чтобы иметь доступ с вашего телефона к файлам на подключенном USB-накопителе, вам потребуется приложение для управления файлами, способное подключаться к сетевому хранилищу, например Solid Explorer. IP-адрес вашего роутера обычно можно найти в расширенных настройках Wi-Fi вашего телефона.

Между тем, еще одним решением является PirateBox - независимый проект, предоставляющий бесплатное лицензированное программное обеспечение. Пользователи этого сервиса могут обмениваться файлами аналогичным образом, но Piratebox позволяет это делать анонимно, а также предлагает дополнительные функции чата и мессенджера. Для настройки работы Piratebox необходимо скачать, установить и настроить несколько программ. Инструкции есть на сайте Piratebox.

Общайтесь с коллегами в специализированных чатах

Два новых приложения для обмена сообщениями с коллегами, о которых мы узнали от активистов, - это Briar и Bridgefy. Мы еще не пробовали эти приложения, но мы знаем людей, которые тестируют их.

Briar - это приложение для обмена сообщениями со сквозным шифрованием и открытым исходным кодом, которое не использует центральный сервер, а вместо этого синхронизирует сообщения между устройствами пользователей (так что контент сохраняется на устройстве каждого пользователя). Оно способно синхронизироваться даже без интернета, через Bluetooth или Wi-Fi (при наличии интернета приложение синхронизирует устройства с помощью сети Tor). В Briar также есть закрытые группы, общедоступные форумы и блоги. При использовании в автономном режиме ваш радиус охвата ограничен диапазоном Bluetooth или Wi-Fi (максимум ~100 метров).

Bridgefy - это приложение для обмена сообщениями со сквозным шифрованием (за исключением случаев использования функции «трансляции»), которое для отправки сообщений использует Bluetooth. В отличие от Briar, сообщения могут пересылаться на бóльшие расстояния, перемещаясь по сотовой сети других пользователей Bridgefy (но только предполагаемый получатель сможет прочитать сообщение). У Bridgefy, в отличие от Briar, нет закрытых групп, форумов и блогов, но есть режим Трансляции, с помощью которого вы можете отправить сообщение сразу до 7 пользователей Bridgefy в пределах досягаемости, которые при этом не обязательно должны быть в ваших контактах (сообщения типа "трансляция" в силу необходимости не шифруются).

Общайтесь через зашифрованные SMS

Текстовые SMS-сообщения отправляются по сотовым сетям и не привязаны к интернету, поэтому могут работать даже в периоды отключения интернета. Однако SMS считаются очень небезопасным средством коммуникации. В отличие от приложений, использующих интернет, таких как WhatsApp или Signal, SMS не шифруется сквозным шифрованием. Это означает, что текстовые сообщения (и их метаданные) могут быть прочитаны правительствами и операторами мобильной связи или перехвачены хакерами. SMS также можно «сфабриковать»; это значит, что отправитель может манипулировать своей контактной информацией и выдавать себя за другого пользователя.

Если вам нужно использовать SMS, Silence - это приложение, которое обеспечивает сквозное шифрование SMS-сообщений. Это приложение с открытым исходным кодом использует протокол шифрования Signal. Хотя мы сами не пробовали работать с ним, мы слышали отзывы других пользователей. Это приложение должны установить и отправитель, и получатель, после чего они обмениваются друг с другом ключами. Поскольку SMS-сообщения обязательно проходят через серверы вашей телекоммуникационной компании, даже при использовании Silence

телекоммуникационной компании будет известно, что вы отправляете зашифрованное сообщение, и доступны метаданные о вашем сообщении.

Частичное отключение: обход заблокированных сайтов

«Отключение интернета» зачастую означает не полное отключение интернета, а скорее блокирование доступа к определенным сайтам или платформам социальных сетей. Правительства через интернет-провайдеров (ISP) могут блокировать сайты на основе IP-адреса, контента или по DNS-запросам. Не уверены, заблокирован ли сайт? Такие организации, как Open Observatory of Network Interference и Netblocks, отслеживают и измеряют сбои в работе интернета и цензуру по всему миру.

К счастью, пока у вас есть доступ в интернет, есть несколько способов попробовать обойти частичные блокировки. Как и в случае с шифрованием, имейте в виду, что обход заблокированных сайтов может быть уголовно наказуем в вашей стране.

VPN

Один из способов обойти блокировку по IP и контенту - использовать виртуальную частную сеть или VPN, например ProtonVPN или TunnelBear. Когда вы подключаетесь через VPN, ваш интернет-трафик зашифровывается и маршрутизируется через VPN-сервер в другой локации, например, в другой стране, таким образом истинный адресат информации и содержимое вашего трафика скрываются от интернет-провайдера.

Имейте в виду, что некоторые правительства запрещают использование VPN или пытаются обнаружить и блокировать VPN-соединения. Также важно использовать надежный VPN-сервис, желательно такой, который не хранит данные или журналы посещений, иначе сервис сможет видеть вашу активность в интернете. Вы должны знать, в какой стране базируется VPN-сервис, и какие юридические процедуры могут к нему применяться в зависимости от юрисдикции. Также учтите, что VPN, одобренные правительством, могут фактически допускать слежку и проверку ваших данных.

DNS-серверы

Серверы DNS («система доменных имен») работают путем преобразования доменных имен или URL-адресов, которые пользователь вводит в браузер, в числовые IP-адреса, которые интернет использует для идентификации веб-страниц. Интернет-провайдер может изменить подконтрольные ему DNS-серверы, чтобы блокировать определенные запросы или выдавать неверную страницу, сообщающую, что сайт не существует. В 2014 году во время выборов в Турции с помощью этой техники премьер-министр Турции Реджеп Тайип Эрдоган пытался заблокировать Twitter. Запрет был быстро пресечен активистами, которые делились пошаговыми советами по использованию VPN и смене DNS-серверов.

Вы можете изменить DNS-сервер по умолчанию в настройках сети или Wi-Fi на вашем телефоне. Чтобы обойти блокировки на основе DNS, вместо DNS-сервера по умолчанию вы можете использовать альтернативные DNS-серверы, такие как Google Public DNS или CloudFlare. У Cloudflare также есть приложение под названием 1.1.1.1, которое позволяет пользователям переключаться на DNS-сервер Cloudflare в приложении с простым интерфейсом.

Это всего лишь два способа обойти наиболее распространенные методы блокировки. Для получения более подробной информации ознакомьтесь с полезными руководствами от Internet Society, Access Now, Security-in-a-Box и EFF.