Материал может показаться нудным и не требующим внимания. Но поверьте, мы живем в информационном мире, где, нравится вам это или нет, все записывается в нули и единицы.

Эпоха, когда в VK можно было строить безопасные чатики, давно прошла. Если хотите иметь доступ к информации, безопасно общаться, передавать материал, публиковаться — всему этому необходимо уделить время. Без этого просто НИКАК.

Нельзя поставить несколько программ и избавиться от цензуры или слежки. Так же, как нельзя начать разбираться в машине, если пару раз залезть под капот. Или научиться готовить еду, несколько раз сварив макароны.

Будьте терпеливы, почитайте, поищите видео. Вложения обязательно окупятся. В вашей безопасности никто, кроме вас, не заинтересован. Учитесь пользоваться поиском!

Борьба со свободным интернетом вышла на новый уровень. Роскомнадзор прежде не представлял собой сколько-нибудь значимой структуры, способной зацензурировать доступ.

Но прошли годы, списки заблокированных ресурсов расширились до огромных масштабов. Блокируется сеть Tor. Недоступны ведущие мировые социальные сети, список которых будет расширяться. Людей регулярно задерживают за разжигание, публикацию материалов, высказывание своего мнения. Продолжать можно бесконечно.

В материале будут предложены списки ПО и решения для обхода цензуры. Не все из них идеально подойдут каждому либо будут удобны для использования.

Также нет гарантии, что ваши данные не передадут по запросу властей. Репрессии носят рандомный характер, вашему другу/подруге может годами не прилетать никаких последствий, а вам за комментарий влетит штраф или арест. Законодательство меняется, как и актуальная информация.

Также не забываем, что скачивание необходимого софта может быть отслеживаемо. У автора нет информации на данный счет. Повсеместное использование VPN затруднило слежку за пользователями. Но нет гарантий, что «надежный швейцарский сервис» не отошлет ваши логи в ФСБ.

Почему так? Потому что если спецслужбы не будут обмениваться информацией, то, используя сервис враждебной страны, вы сможете развить бурную деятельность в своей, при этом не получив срок. Помогая российским силовикам, зарубежные службы могут рассчитывать на помощь, если им понадобятся данные о пользователях сервисов под юрисдикцией РФ.

Смартфон имеет более низкую степень безопасности, чем ПК. Его конструировали так, чтобы пользователь всегда имел доступ к связи (поэтому он так и называется). То есть вышки сотовой связи должны максимально быстро вас идентифицировать.

Его отключение также не может давать гарантий безопасности. Лучше вытаскивать аккумулятор, но это уже в более старых моделях. (Кстати, безопасность кнопочных телефонов тоже не доказана.)

Технические специалисты в курсе, как все устроено. Именно поэтому данная статья не будет иметь для них ценности. Они могут прочитать исходный код, иногда внести в него правки, подать жалобы.

Обычный пользователь этого сделать не может, поэтому для него нет разницы между свободным, открытым, и закрытым программным обеспечением. Тем не менее автор рекомендует

использовать по минимуму проприетарное, закрытое ПО.

Почему закрытое ПО — на примере **Microsoft** или **MacOS** — плохо? Хотя бы из-за недавней цензуры, когда маркеты начали блокировать установку приложений. Пользователь имеет право на свободу, а его у него ее отняли из-за санкционных ограничений.

Также подвергаются блокировке уже купленные программы (как и иные продукты интеллектуальной собтвенности: фильмы, книги, музыка — особая сердечная боль автора), где-то возникают проблемы с установкой обновлений безопасности. Даже с оплатой проблемы из-за блокировок денежных переводов. Криптовалютные биржи и ресурсы точно так же вводят «цензуру».

Что же использовать?

Браузеры/WEB-серфинг

Для ПК:

Librewolf -- уже настроенный браузер

Brave — вокруг него есть спорные моменты

GNU IceCat — свободный форк Firefox

Про Tor Browser думаю писать лишний раз не нужно.

Компромиссный вариант — обычный Firefox

Для Android:

Firefox Focus

Bromite

DuckDuckGO

Уточню, что приложения для Андроида есть в популярных маркетплейсах. Например https://f-droid.org/ Оставлять ссылку на них нет смысла, пользуйтесь поиском.

Для использования Tor (он пренаправляет трафик по цепочке серверов, шифруя его на каждом этапе): **Tor Browser, Orbot, inviZible Pro** — все приложения доступны в F-droid

Расширения для браузеров (как следует из названия, эти программы расширяют возможности браузера)

Privacy Badger — блокировка трекеров

uBlock Origin — блокировка рекламы

Decentraleyes — защищает вас от слежки, осуществляемой с помощью «бесплатной»

централизованной доставки контента

Cookie AutoDelete — удаление cookie после закрытия браузера

NoScrypt — защита от JavaScrypt

Их очень большое количество, и рассмотреть все не получится. Автор выбрал самые практичные.

Программы для создания надежного пароля

Для ПК:

KeepassXC

LessPass

Для Android:

KeepassDX

Почтовые сервисы (замена небезопасным в разной степени майл.ру, яндексу и гуглу)

Riseup

Disroot

systemli.org

Компромиссные варианты: Сервисы, которые были замечены в сливах

Tutanota

ProtonMail

Шифрование сообщений

Самый старый вариант для почты — дополнение **Enigmail** для почтовой программы Thunderbird

Для WEB-почты — **https://mailvelope.com/ru/**

Можно общаться с помощью ключей шифрования в любой сети или мессенджере. Например, с помощью **GnuPG** или gpg4usb Достаточно понять механизм работы и немного потренироваться.

Мессенджеры / Instant messaging

Важно помнить, что их политика часто может меняться. Также регулярно возникают новые либо дорабатываются старые мессенджеры.

Delta Chat — одно из наиболее цензуроустойчивых решений. Работает на ПК и Смартфонах.

Element — один из клиентов для децентрализованной платформы matrix.org , для которой есть и другие альтернативные клиенты. Подходит для Android.

Ricochet — наиболее радикальный клиент, основанный на p2p (прямая связь между вами и собеседником без посредничества сервера) через сеть Tor. Только для ПК.

Jabber/XMPP — старый-добрый протокол. Выбирайте клиент с поддержкой omemo. Это более надёжное и дружелюбное шифрование.

Briar — наиболее радикальное решение для переписки с телефона. Только для Android.

Компромиссные варианты:

Signal – требует телефон. Не был замечен в громких скандалах и сливах людей на момент написания статьи.

Status – еще сырой клиент (также на момент написания статьи). не требует телефон

Session — заявлено полное шифрование, не просит телефон, есть сообщество пользователей, но еще случаются баги, нет оценок от экспертов.

Wickr -- проприетарный клиент. Но могу порекомендовать, ибо не замечен в сливах, и не требует телефон. Достаточно стабилен

Для видеосвязи можно использовать:

Jitsi. прямо в web — https://meet.jit.si

Jami

Linephone

Можно также использовать браузер с Tor и развернуть известную программу там, но результат может быть сильно тормозным.

Плохой вариант:

Telegram, Viber, WhatsApp.

Мессенджер Телеграм стал уже национальным и сложно поверить, что столь «безопасная система» может быть у каждого человека. Поэтому в моих рекомендациях будет не использовать его для важной переписки. Даже поставлю под сомнение end-to-end (секретный). Не забывайте регулярно чистить кэш и локальную базу данных.

Единственное, что можно посоветовать, это клиент с двойным-дном от Киберпартизан:

Android: https://github.com/wrwrabbit/Partisan-Telegram-Android

ПК: https://github.com/wrwrabbit/tdesktop

Его смысл в том, что если ввести ложный пароль, то выйдете из аккаунта. И потеряется вся переписка. Полиция может заставить вас принят СМС, поэтому лучше, чтобы сим-карта физически находилась не в смартфоне, а где-то далеко. Хорошо иметь друга с сим-картой за рубежом либо виртуальный номер. В случае чего его просто не смогут включить.
Конечно же, помните про двухфакторную аутентификацию и 2 код-пароля.

Так же рекомендую ознакомиться: https://youtu.be/gxKWYs8KcUM

Шифрование данных:

Распространенным вариантом будет:

Veracrypt — создание криптоконтейнеров. Аналогичный вариант https://remontka.pro/veracrypt/ — подойдет для Linux.

В качестве альтернативы на ПК можно использовать

LUKS https://cryptopunks.org/article/awesome+truecrypt+alternative+for+linux/. В большинстве Linux-диструбитивов он уже установлен «из коробки». Но с помощью него также можно делать контейнеры .

Picocrypt

Обязательно шифруйте основной раздел жесткого диска при работе с Linux или Windows.

На смартфоне хорошим выходом будет: **EDS Lite** — создает криптоконтейнер.

Для передачи данных идеален вариант с Onionshare

Если в целом, то есть достаточно много удобных способов передачи файлов: отправить криптоконтейнер Veracrypt и пароль отдельным способом; зашифровать с помощью ключа GPG; создать архив с паролем (вариант чуть хуже, но многие юзают).

Для ПК

Bleachbit

Для Андроида подойдёт: **Shreddit , iShredder**

Не забывайте анонимизировать метаданные:

ExifCleaner

ExifEraser

Поисковые системы

Здесь не вижу смысла быть откровенным сектантом. Иногда оправданно использовать сервисы Google и других популярных систем, следящих за вами, если в рекомендованных выдается посредственный результат (такое бывает).

Меньше охотятся за вашими данными:

DuckDuckGO – https://duckduckgo.com/

StartPage – https://www.startpage.com/

MetaGer – https://metager.org/

SearX – https://searx.space/

Безопасные ОС

Традиционная ремарка о том, что система может быть более-менее безопасна, только если пользователь понимает, что делает. Либо если она отключена от сети интернет.

Tails – старенькая и проверенная live система.

Whonix – более продвинутая система, которая требовательнее к железу. С недавних пор тоже имеет live.

Parrot OS – новинка, можете потестировать.

Kodachi — спорная вещь. На мой взгляд, чрезмерно перегружена лишним софтом. Редко обновляется и толком не тестировалась. Но, может, со временем станет актуальна.

Немного про Kali Linux. Это система для тестирования уязвимостей. Она по умолчанию не предназначена для работы в качестве основной ОС. Да, продвинутый пользователь сможет все в ней настроить, но для обычного человека будет заблуждением считать, что данная ОС его обезопасит.

Как уже писал ранее, с выбором ОС подсказать не смогу — выбирайте по вкусу. Однако автор против сектантского подхода, когда пользователь не может поставить то, что ему хочется. Часто авторы либо почему-то решают, что все поддерживаемое в ОС должно быть только свободным (ограничивая тем самым свободу других), либо создают совершенно неюзабильное приложение и систему, при этом утверждая, что так и должно быть, для всех.

VPN

Не советую с помощью VPN заниматься какой-то подрывной деятельностью. Особенно если вы не сами его поднимали либо не доверяете хостеру. Во всех остальных случаях лучше выбрать тот, который можно как-то анонимно оплатить (значит, он уже нацелен на приватность). И находиться он должен вдали от юрисдикции вашей страны. Нужно ознакомиться.

VPN сгодится для обхода блокировок и поможет не схватить вирусов при серфинге в сети. Можно использовать в цепочке с Tor или другими прокси, но здесь тоже есть нюансы + прилично режется скорость.

Bitmask

ProtonVPN

RiseupVPN

Вы их, скорее всего, и так знаете. Советую обратить внимание на протоколы **Shadowsocks** (обходит пока все цензурные протоколы защиты), и конечно **Wireguard.**

Криптовалюта и кошельки

Несколько лет назад автор бы подсказал куда точнее. Но ситуация стремительно меняется, да и многие платформы стали себя вести откровенно неэтично, выдавая баны за географиечское положение. Поэтому мой совет: избегать чрезмерно крупных и централизованных площадок.

Electrum

Samourai

Monero GUI

Одноразовые сообщения и записки

Пользуйтесь с осторожностью. Не совсем ясно как всё это шифруется на стороне сервера, и кто имеет доступ к информации:

Privnote.com Или http://privnote7kxukf5un2ugvpxm2r7sr6j7477iquxeuuq2ctatuzyycdyd.onion/

Secserv.me

Итог

Наверное это все, что хотел подсказать. По-хорошему, еще достаточно много нюансов безопасности. Например, желательно использовать роутер со свободной прошивкой (можно прямо с него раздавать Tor-трафик).Или запустить весь траффик через сеть Top

Можно использовать программу pfSense, с помощью которой можно настроить целый домашний сервер вместе с роутером. Либо воспользоваться Raspbery Pi и туда установить все необходимое.

Было бы правильно установить на домашний ПК свободный Bios и скрипт usbdeath.

(Будьте с последним осторожны, можно «закирпичить устройство». Используйте только для предотвращения физического изъятия.)

Смартфон, в идеале, лучше использовать только для бытовых целей. Как-то серьезно его обезопасить без перепрошивки системы довольно сложно. Неплохо работает удаление всех данных при удаленном доступе (работает в iphone, не знаю, как с Android)

Использование популярных соцсетей в каких-то моментах оправдано. Если нужно дать клич о сборе средств либо помощи. Либо еще как-то связаться с нужным человеком/организацией.

Безопаснее всего использовать полноценную программу, а не web. Но далеко не всегда это практично. Особенно, когда не нужно оставлять следов на ПК/Смартфоне в виде лишних приложений и сервисов. Почистить браузер куда проще.

Сам автор советует использовать несколько методов связи с человеком, в случае если один заблокируется. Идеальный вариант: почта и какой-нибудь мессенджер.

Можно использовать сети, изначально настроенные на децентрализацию и уважение приватности: **Freenet, GNUnet, i2p, Diaspora**. Как вариант — **we.riseup.net**. Они не очень популярны, медленны, и у большинства не вызовут интереса.

Какие варианты для работы подойдут обычному человеку? Уже упомянутые мною ОС обеспечивающие приватность Tails/Whonix. Может быть полезно развернуть сеть виртуальных машин, в которой наиболее чувствительные вещи, будут работать изолированно друг от друга

(например браузер, криптокошельки, мессенджеры). Еще можно пользоваться снимками и после работы, восстонавливать виртуальную систему к исходному варианту.

Если есть причины предполагать, что к вам придут, лучше увезите подальше/уничтожьте ваши цифровые устройства. Только это станет гарантией, что ничего не найдут. Если у вас новый ПК, или смартфон, и вы с него не производили сомнительных дел, то никакой угрозы не будет.

Фраза «Не говори ничего лишнего в интернете», конечно, хороша — всячески поддерживаю, — но люди живые: опасная фраза может легко соскочить с языка или клавиатуры. Непроизвольно. И вы ничего с этим сделать не сможете. Так же, как не сможете быть уверенным в собеседнике и том, что он использует надежные средства коммуникации.

Многие авторы высказывают откровенно маразматические идеи, вроде отказа от смартфона и телефона вовсе. Платить только наличными и не тратить средства онлайн. Ничего не заказывать и не пользоваться никакими онлайн-средствами.

Не поддерживаю такой подход. Да и далеко вы с ним не уйдете. Жизнь затворника может быть оправдана только личными причинами, либо преследованием от государственных органов. Во всем остальном не имеет смысла

P.S. Также стали появляться ситуации, когда многие товарищи, пренебрегают безопасностью. Особенно это касается уже уехавших. Ведь им ничего не угрожает — значит, можно писать в небезопасные сети и мессенджеры вещи, способные дискредитировать других. Советую этого не делать. Вы подставляете других, пользуясь географическим положением.

О людях, которым «нечего терять», которые «никому не нужны» либо они уже под следствием и считают необходимым подставлять остальных, устраивая переписку в подцензурных сетях... автор умолчит. Ибо всячески осуждает такой подход. Не делайте так.