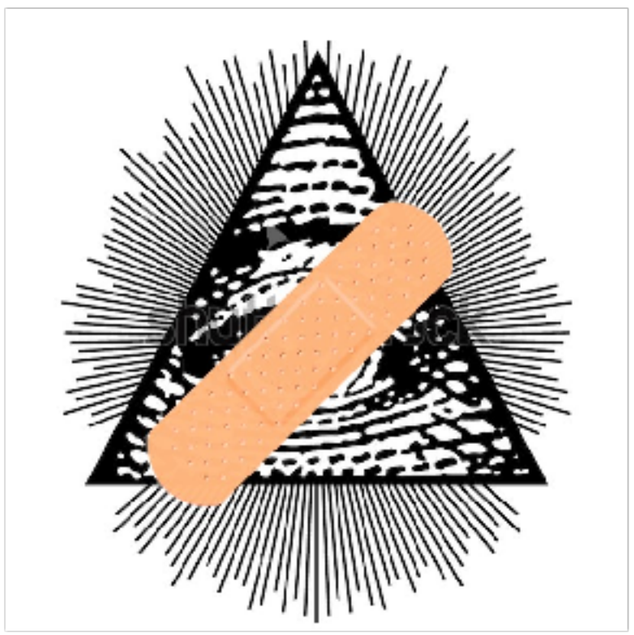
Конфиденциальность связи и защита информации.



«Существенным условием возникновения тоталитарной модели является современная технология. Эта черта тоталитаризма особенно заметно проявляется в области вооружений и массовой коммуникации, она тесно сопряжена также с осуществлением [государственного] террора, требующего новейших средств наблюдения за людьми и их перемещениями» Фридрих К., Збигнев Бжезинский «Тоталитарная диктатура и автократия»

«Руководство по производству полетов — книга написанная кровью»

Вероятно человеческий вид Homo sapiens появился, когда наши биологические предки приобрели способность к речи. Существование человека разумного неразрывно связано с обменом информации с другими индивидами. После возникновения речи следующим ключевым шагов в развитии цивилизации стало изобретение письменности, затем изобретение печатного станка, а затем изобретение компьютера и сети Интернет. Это демонстрирует тесную связь между речью, мышлением и практикой. Следовательно, контроль тоталитарной власти над словом, это контроль над мышлением. Как видим, формула «об этом не только говорить нельзя, об этом даже нельзя думать» появилась не на пустом месте. В путинской России в 2022 согласно закону слишком многое уже нельзя произносить «в группе лиц». Тоталитарная цензура представляет собой тоталитарную практику, преобразующую мышление в тоталитарное. Следовательно, мы не можем себе позволить заткнуть себе рот. Отсюда следует требование защиты информации.

«В действиях сопротивления имеются важные аспекты, требующие секретности. Редактирование, печатание и распространение подпольных публикаций, использование нелегального радиовещания внутри страны и сбор разведданных об операциях диктатуры являются специальными действиями ограниченного масштаба, требующими высокой степени секретности.» Джин Шарп, «От диктатуры к демократии».

Организованная борьба невозможна без средств конфиденциальной связи. Этой точки зрения придерживаются, не только злостные сторонники теорий заговора, но и такой борец с диктатурами, как Джин Шарп. Неслучайно всевидящее Око является важным органом тоталитаризма, ведь тот, кто владеет информацией, как известно, владеет миром. Отказались вы бы сами иметь полную информацию о распределении ролей и всех переговорах вашего противника?

Те, кто не ценят приватность и доказывают, что она не важна, не нужна, всячески стремятся пренебрегать средствами приватности, утверждают, что спецслужбы все равно все видят, те, кто произносят ключевую фразу «мне нечего скрывать» сами, как правило, являются латентными или открытыми сторонниками тоталитаризма и врагами свободы. Как я отмечал в первой главе, тоталитаризм через тоталитарную практику деформирует сознание, и переводит всевидящее око из области объективного в область иллюзии, которая сопровождает человека уже всюду и выполняет надзор гораздо эффективнее, чем реальная слежка спецслужб. Самоцензура худший вид цензуры. Терминальная стадия: «О таком не только говорить, о таком даже думать нельзя». Отметим, что на сегодняшний момент наука и техника не достигли такого уровня развития, чтобы читать ваши мысли в голове. Мысли в вашей голове скрыты от Всевидящего Ока, если конечно вы сами их не раскроете. Это краеугольный камень антитоталитаризма. Как было отмечено, сидром скрепоносца имеет несколько стадий слома человека. После иллюзии вездесущности надзора на следующем этапе этой болезни возникает тайная симпатия к всевидящему оку. Затем уже в стадии сформированного синдрома скрепоносца в его голове укореняется идея, что тотальный надзор жизненно необходим обществу. Во многом именно такие «нечего-скрыватели» и являются виновниками небывалого ранее в истории тотального наблюдения за людьми с помощью аппаратного и программного обеспечения в XXI веке, потому что это происходит с их молчаливого согласия.

Но так ли добро Всевидящее око? Грамотный следователь, получив, поскольку вы активный политический противник власти, доступ к вашим телефонным звонками и переписке, прежде всего изучает обстоятельства вашей жизни (вообще следует насторожиться когда, кто-то внезапно начинает выяснять обстоятельства вашей жизни, например спрашивать где или с кем вы живете, где и когда находитесь). Затем зная, например, что у вас недавно была авария водоснабжения, он может прийти с обыском, представившись соседом, которого вы заливаете водой, и вы откроете дверь. Или зная, что вы цените свой автомобиль сообщить, что ваш автомобиль повредили, для того, чтобы вы открыли дверь. Зная, что в вашем доме живут мигранты, просьба открыть дверь может быть озвучена под предлогом проверки на проживание мигрантов. И так далее. Зная что вы не переносите табачный дым, вас могут поместить в пресс-камеру с курящим подсадным сокамерником, запугивающим вас многими годами тюрьмы. Можно смело утверждать, что ваша приватная информация о том, что именно для вас крайне неприятно, что именно для вас дорого, или кто именно для вас дорог, полученная из ваших прослушанных телефонных разговоров и прочтенной переписки будет использована следователем, находящемся на службе у преступного политического режима, для оказания на вас давления с целью получения необходимых ему

признательных показаний, получения показаний на другого человека, возможно невиновного, с целью вашей вербовки в осведомители, или просто с целью, чтобы вы прекратили свою политическую деятельность. Если вы активный противник власти в России, то следственные действия в отношении вас не будут иметь никакого отношения к законности, справедливости и «порядочности», которые вы представляли, когда говорили, что «порядочным людям нечего скрывать». Вышеперечисленные примеры демонстрируют, что противники приватности, которые утверждают, что «им нечего скрывать», не обладая специальными знаниями в области психологии о механизмах психологической защиты против сильных стимуляций, которые заставляют человека действовать иррационально против собственных интересов, недооценивают насколько их приватные данные, полученные государством, могут быть использованы против их интересов совсем не в благих целях. Но сторонник тоталитаризма из-за любви к Всевидящему оку скорее всего попытается закрыть на это глаза, используя психологический защитный механизм диссоциации или отрицательной галлюцинации — невидения реально существующих вещей.

Тоталитарный надзор также является одной из духовных скреп. Многие вполне неплохие люди выдумывают себе воображаемого всевидящего надзирателя, чтобы вести себя этически и вполне правильным образом. Назовем для простоты это «идеей бога». Понятно, что под этим можно понимать и несколько богов, духов, народные суеверия или просто принятые жизненные правила, которых стоит придерживаться, чтобы не попадать в неприятности, и чтобы не ломать каждый раз голову над выбором. Например правило, что чужая вещь не принесет добра, и беря чужое надо отдать хотя бы копейку взамен. Эта методика столь стара, столь широко распространена и столь глубоко укоренена в человеческой психике с детства, что имеет исторически позитивную окраску, и как, правило, одобряется в обществе. Тоталитарный государственный надзор тоже декларирует своей целью борьбу со злом и направление поведения людей «в правильное русло» для упрощения и якобы улучшения жизни людей. Как мы видим, тоталитарный государственный надзор имеет ряд общих признаков с идеей бога. В результате тоталитарной практики, вознаграждающей либо наказывающей людей за их действия сообразно целям тоталитаризма, а также в результате тоталитарной пропаганды, идея надзора бога смешивается с идеей тоталитарного надзора государства. В результате у таких людей идея бога-надзирателя, заставлявшая ранее вести их этично и правильно, искажается, а идея тоталитарного надзора заимствует позитивную окраску от идеи надзора бога. Это очередной пример двоемыслия (или диалектической логики), подменяющей и разрушающей понятия путем насильственной тоталитарной практики. Здесь задействуется и характерный механизм защиты духовных скреп: нападки на тоталитарный надзор государства преподносятся как нападки на идею бога, проявление нигилизма, и склонение к вседозволенности. Такой защитой религиозной духовной скрепы много занимался идеолог русского тоталитаризма Федор Достоевский в своем романе «Бесы». Дистиллированное из Достоевского высказывание «Если Бога нет, всё дозволено» вызывает экзистенциальный ужас у скрепоносца. Менее понятно скрепоносцу высказывание Ницще «Бог мёртв; из-за сострадания своего к людям умер Бог», но тоже вызывает неодобрение, конечно как проявление загнивания Запада. Здесь мы находим и

характерный репрессивный механизм тоталитаризма «исключение подтверждает правило», с интузиазмом привлекающий по идеологическим уголовным статьям разного рода настоящих вандалов и хулиганов, чтобы доказать правоту этих идеологических уголовных статей, а затем уже привлекать по этой идеологической статье своих политических противников и создавать представление о борцах с тоталитаризмом как о преступниках.

Разительно от тоталитарной отличается в массе своей позиция людей на Западе, традиционно состоящая в том, что государство и полиция представляют огромную опасность для людей, и поэтому требуют ограничений. Например, власти ряда американских городов — Портленда, Сан-Франциско, Окленда, Сомервилля уже приняли решение полностью запретить использование технологии машинного распознавания лиц. Решения об этом приняли городские советы или местные жители на референдумах. Сотрудники американских вузов требуют запретить камеры с распознаванием лиц в кампусах.

Цитата: «*Депутаты Европарламента восстали против цифровой диктатуры и слежки за гражданами. Сразу три фракции — «Обновляя Европу», «Зеленые» и Прогрессивный альянс социалистов и демократов — поддержали запрет на использование систем распознавания лиц и прочие инструменты искусственного интеллекта в общественных местах. Эти либеральные и левоцентристские партии предлагают принять свод правил (его рабочее название — «Закон об искусственном интеллекте»), в которых будет четко прописано, где можно размещать камеры слежения, а где нельзя. Эти правила будут обязательными для всех членов ЕС.* ».

Такая позиция совершенно чужда для россиян, которые в массе своей все еще считают, что чем сильнее государственная власть и чем неограниченнее власть вождя, тем лучше, видя в государстве патерналиста и единственный способ удовлетворения собственной агрессии и нереализованных амбиций. Нелишне будет напомнить, что первейшая (в том числе исторически) функция демократических институтов состоит в противостоянии неограниченной власти. Отсутствие запроса у россиян на ограничение государственной власти является пожалуй основной причиной неприживаемости либеральной демократии в России. При этом и в странах Запада продолжается сражение с тоталитаризмом, на протяжении тысячелетий находящим питательную среду в глубоких слоях человеческой психики, прежде всего в страхе и агрессии. Отсутствие у россиян понимания тоталитаризма, отсутствие неприятия к нему, из-за переноса агрессии на другие объекты, и непонимание роли демократических институтов для противостояния тоталитаризму, вновь и вновь приводит российских мыслителей к «гениальному» как они считают открытию, что либеральная демократия тоже является тоталитарной системой. Это «открытие» в лучших традициях «диалектической логики» или двоемыслия, как известно не видящего различия между незнанием и силой, свободой и рабством. Тем не менее, никто не может гарантировать, что спецслужбы и непосредственное руководство других государств, имеющие на самом деле, как и любая исполнительная власть и как любые силовики, мало отношения к демократическим институтам, имея доступ к каналам связи российской оппозиции, может предать

российскую оппозицию по отношению к российской власти, преследуя собственные цели и собственное понимание о том, как должна меняться власть в России. Надеясь, что это не произойдет, все равно лучше использовать сквозное шифрование для защиты от лишних глаз.

Хорошей новостью для сторонников приватности является то, что в 1976 году американскими криптографами Уитфилдом Диффи и Мартином Хеллманом был изобретен алгоритм асимметричного шифрования, или как его называют, криптосистема с открытым ключом, который позволяет осуществлять защищенную связь между отправителем и получателем, даже если канал связи полностью прослушивается. Этот алгоритм широко используется сейчас в сети Интернет, например в https и прочих защищенных протоколах. Иначе без защиты банковских транзакций и данных аккаунтов в интернет магазинах и прочих электронных аккаунтов всемирная экономика в том развитом виде, в котором мы ее сейчас наблюдаем не смогла бы существовать.

Плохой новостью является то, что интернет корпорации, спецслужбы, а также производители программного обеспечения и цифрового оборудования вовсе не заинтересованы в вашей приватности, а заинтересованы в совсем противоположной задаче — сборе и анализе данных о вас для собственного коммерческого развития и для поддержания стабильности общественно-политической системы. Это происходит во многом потому, что нет общественного запроса на приватность. Ваши данные собираются, обрабатываются, а затем на их основе вам показывается реклама, а корпорациями, банками и правительствами государств принимаются решения. Для облегчения машинной обработки ваших данных, и только для облегчения обработки, а не ради вашей приватности, используются так называемые метаданные, о которых мы поговорим чуть ниже.

Система социального рейтинга в тоталитарном Китае, идет дальше и распространяет решения на все сферы жизни граждан. Например, обнаружив, что гражданин выражает антиправительственные взгляды и участвует в политических демонстрациях, система может лишить его возможности передвижения, заблокировав продажу билетов, отказать в праве занимать административные должности или в праве получения высшего образования. Или заблокировать аккаунты в социальных сетях, как совсем недавно летом 2022 произошло у российских активистов, выступавших против войны с Украиной.

Цитата [о системе социального рейтинга в Китае]: «*При действительном или мнимом нарушении порядка система снижает репутацию. Это может происходить, если, скажем, гражданин часами играет в онлайн-игры, курит в неположенном месте, выгуливает собаку без поводка, нарушает правила дорожного движения, задерживает уплату налогов, покупает много алкоголя или даже пишет исключительно прописными буквами (а значит, он ненадежен и недисциплинирован). Низкий рейтинг ограничивает права гражданина: ему снижают скорость подключения к интернету, не позволяют*

брать вещи в аренду, он не может устроиться на высокооплачиваемую работу или поселиться в отеле.»

Именно из-за того, что Китай является тоталитарной страной, российский фашизм, начав конфликт с Западом на почве требований сменяемости власти и соблюдения Всеобщей декларации прав человека, не совместимых с жизнью российского фашизма, попытался завести дружественные отношения именно с тоталитарным Китаем, поскольку считал его идеологически близким, следовательно не способным нанести российскому фашизму вред, сравнимый с экспансией западных демократических ценностей.

Спецслужбы во всем мире стремятся осуществлять слежку, как минимум в интересах контрразведки и для того, чтобы киберпреступники, террористы и политические «экстремисты» не разрушали сложившуюся общественно-политическую систему.

Цитата: «*По словам Павла Дурова, за неделю, когда разработчики Telegrat находились в США, агенты ФБР дважды пытались подкупить их чтобы создать «черный ход» в Telegrat. Дуров посетовал, что создать по-настоящему независимое приложение с криптографией в США практически невозможно*».

Цитата: «*Илон Маск заявил, что может сделать свой смартфон, если Google и Apple уберут Twitter из магазинов приложений iPhone и Android. Илон Маск заявил, что Apple пригрозила удалить Twitter из своего магазина приложений App Store* »

Цитата: «*Еврокомиссия грозит заблокировать Twitter, если Илон Маск вернет доступ ранее забаненным пользователям, — Financial Times. Еще одно требование — отказ от "агрессивного" продвижения дезинформации и необходимости провести "масштабный независимый аудит" платформы к 2023 году. Несоблюдение этих требований в Брюсселе пообещали расценивать как нарушение законодательства Евросоюза в сфере цифровых услуг.*»

Эта цитаты представляет собой одни из многих доводов в пользу того, что все Интернет корпорации сотрудничают с правительствами государств в вопросах слежки и цензуры.

Незаинтересованность производителей цифровой техники в вашей анонимности, можно продемострировать на примере технологии, которая называется «Желтые точки» (Machine Identification Code). «Это метки, ставящиеся многими цветными лазерными принтерами на каждую печатаемую страницу. Точки едва видны невооруженным глазом и содержат в себе информацию о серийном номере принтера, а также дате и времени печати. Они обычно наносятся краской жёлтого цвета, благодаря чему малозаметны на белой бумаге. Введение данной меры, согласно комментариям производителей, являлось частью сотрудничества с правительством, конкурирующими производителями и консорциумом банков, направленного на борьбу с фальшивомонетничеством. Эта отслеживаемость неизвестна многим пользователям. Использование технологии «жёлтых точек» помогло быстро выявить источник утечки засекреченных данных АНБ

в 2017 году, которым оказалась сотрудница подрядной организации Риалити Виннер, пересылавшая новостному сайту The Intercept печатные копии секретных материалов, что привело к ее аресту и осуждению.»

Манифест

Я утверждаю, что российская оппозиция на сегодняшний момент не имеет средств конфиденциальной и анонимной связи. Я утверждаю что российская оппозиция в принципе не добьется какого либо успеха, пока не получит и не освоит средства конфиденциальной связи.

Множество российских оппозиционеров, теоретиков и активистов, смутно решили для себя, что могут заниматься борьбой с путинским фашистски государством — групповым обсуждением, созданием ассоциаций, политической организацией, информированием и просвещением в мессенджере Telegram, потому что в Telegram якобы нет цензуры, и потому, что там они якобы свободны от воздействия тоталитарной практики российского фашистского государства, вообразив еще, что Telegram и был создан именно для этого. Однако Telegram, как мы рассмотрим ниже, как минимум концептуально против анонимности от российского государства, следовательно ведение общественных дискуссий (один из институтов демократии, который безусловно необходим для борьбы с тоталитаризмом), создание свободных ассоциаций, политическая организация и просвещение в широком диапазоне тем и методов (вполне достаточно если в рамках Всемирной декларации прав Человека) в Telegram просто невозможны, поскольку они происходят под присмотром «заботливого» Всевидящего Ока и приводят к репрессиям. Очевидно Telegram это только концептуальный пример мессенджера с неявным видом цензуры. На его месте мог быть другой мессенджер, но это ставит перед нами следующие фундаментальные вопросы: о какой свободе от российской тоталитарной практики идет речь, в частности о какой свободе от цензуры, о какой возможности общественного обсуждения, если за вполне определенные публичные высказывания в мессенджере вас могут посадить в тюрьму и это концептуальная задумка этого мессенджера? Разве это не другая разновидность цензуры со стороны российского государства? Можем ли мы хоть чего-то достичь, находясь под воздействием российской тоталитарной практики? Можем ли мы чего то достичь, не нарушая законы тоталитаризма? Разве не должны мы избавиться от надзора Всевидящего Ока? Ответ на эти вопросы демонстрируется опытом — в России нет ни

свободных публичных политических дискуссий ни независимой организованной оппозиции.

На сегодняшний момент существуют непопулярные но достаточно надежные средства конфиденциальной связи. Это Open Source Jabber мессенджеры со сквозным шифрованием (вышеупомянутое асимметричное шифрование непосредственно между отправителем и получателем), использующие сервера за пределами России, с использованием для подключения VPN и TOR. На мой взгляд, важнейшей задачей является популяризация использования таких мессенджеров и приватности в целом. Этого пока не делается, и вся Россия продолжает обсуждать свои дела в мессенджере Telegram.

«Безопасный» мессенджер Telegram

По моему мнению, ни что не причиняет большего вреда российской оппозиции, чем так называемый «безопасный месседжер»Telegram, количество уголовных дел по которому скоро превысит число уголовных дел по материалам из печально известной социальной сети Вконтакте, полностью прозрачной для российских силовиков.

Цитата: *«Выяснялось, что Telegram сотрудничает с властями Германии, хотя ранее заявлялось, что Telegram не передает государствам данные. Оказалось, что мессенджер Telegram в отдельных случаях передавал информацию о немецких пользователях Федеральному агентству по уголовным делам Германии, хотя утверждает, что не сотрудничает с правительствами. Министерство внутренних дел Германии в начале февраля 2022 провело прямые переговоры с Telegram для налаживания сотрудничества с немецкими правоохранителями и блокирования запретного контента. На встречах присутствовал основатель мессенджера Павел Дуров и еще три представителя компании. Дуров якобы заявил немецкой стороне, что считает рынок Германии важным и воспринимает требования немецких властей серьезно. Впоследствии Telegram и власти Германии создали прямой закрытый канал взаимодействия, через который мессенджер и предоставляет необходимые данные немецким правоохранителям, отмечает Spiegel.»*

Цитата: *«В США рассекретили документ от ноября 2020 года о том, какой доступ к каким мессенджерам имеет ФБР. Telegram: содержания сообщений не предоставляет, информацию по решению суда не выдает. В документе есть ссылка на политику Telegram, что он может выдать IP-адрес и номер телефона по расследованиям подтвержденных случаев терроризма».*

Цитата: «*Администраторы Telegram не предоставляли российским властям ключей шифрования к своим ресурсам, однако сотрудничают по конкретным запросам в рамках борьбы с экстремизмом и терроризмом, сообщил "Интерфаксу" источник в российских властных структурах*».

Здесь надо отметить, что российские силовики легко возбуждают уголовные дела о терроризме против своих политических оппонентов, называя терроризмом даже те случаи, которые терроризмом не являются, пользуясь тем, что российское общество не обращает на это внимания, ввиду юридической безграмотности. А статья уголовного кодекса РФ (ст. 205.2 УК РФ) об - «оправдании терроризма» вообще представляет собой пример юридического произвола. Все это показывает, что сотрудничество мессенджеров с ФСБ РФ даже по вопросам связанным с терроризмом исходя из принципов свободы неправильно.

Я могу предположить следующую картину: доступ к данным пользователей Telegram имеет очень ограниченный круг российских силовиков федерального уровня, но не региональные силовики. Об этом говорит то, что соответствующие уголовные дела возникают редко и в исключительных случаях, в связи с оппозиционной деятельностью именного всероссийского уровня и критической для политической системы. Такой подход позволяет властям не допускать коррупции связанной с продажей персональных данных Telegram на региональном уровне и поддерживать иллюзию безопасности Telegram для большинства пользователей. Очень удобно было бы подсадить всю страну на якобы «безопасный мессенджер» Telegram, чтобы, имея доступ к важнейшим планам оппозиции (и не только оппозиции), полностью контролировать ситуацию. Это не совсем конспирологическая теория, поскольку она соответствует критерию фальсифицируемости, поскольку желающие могут попытаться ее опровергнуть на собственной шкуре.

Но это излишне на мой взгляд, поскольку достаточно обратить внимание на то, как привязывает Telegram аккаунт пользователя к номеру телефона, на то, насколько его настройки по умолчанию противоречат принципам приватности и свободы, на то как он позволяет находить пользователя по номеру телефона. Здесь я имею ввиду один из базовых принципов свободы, который закреплен во Всемирной декларации прав человека как Свобода ассоциаций: «*Каждый человек имеет право на свободу мирных собраний и ассоциаций. Никто не может быть принуждаем вступать в какую-либо ассоциацию*». Это означает право не общаться с теми людьми, с которыми мы не хотим общаться. Отсюда вытекает право на анонимность. Но Telegram сообщает, что вы завели аккаунт всем, кто имеет ваш номер телефона в адресной книге мобильного телефона, в том числе и политической полиции. Вот он каков «свободный» мессенджер! Все это говорит о том, что Павел Дуров просто обманул когда заявил, что разработчики Telegram ставят в приоритет безопасность пользователей. Потому что как минимум, Telegram ставит в приоритет наращивание числа пользователей Telegram, за счет использования адресной книги мобильного телефона, но ни как не безопасность. Ведь очевидно одной из мотиваций для человека завести аккаунт в Telegram является то, что все его контакты из адресной книги мобильного телефона уже завели или заведут в будущем (о чем Telegram сообщит) свои аккаунты в Telegram, и он с ними свяжется, просто найдя их в Telegram по номеру мобильного телефона. Но это вовсе не похоже на свободу ассоциаций и безопасность. Заявление о безопасности Telegram очевидно было только PR акцией.

Только в 2019, после того как протестующие в Гонконге были деанонимированны из-за использования Telegram и были репрессированы китайским государством, Павел Дуров был вынужден добавить опцию скрыть номер телефона. Дело в том, что любой, кому был известен ваш номер телефона, а политической полиции очевидно известны номера телефонов политических активистов, мог видеть, что аккаунт в Telegram принадлежит именно вам. Полиция использует программу, которая представляет собой виртуальный мобильный телефон, в адресную книгу которого внесены телефоны всех граждан страны. Это не так сложно сделать. В результате Telegram сообщал этой программе, какому телефону телефона соответствовал интересующий их аккаунт. Если этот аккаунт призывал к митингам и акциям неповиновения, следовал арест или уголовное дело.

Если вы задумали ради своей безопасности сменить номер телефона, привязанный к аккаунту или никнейм в Telegram, то обратите внимание, что у каждого аккаунта в Telegram есть уникальный номер ID, привязанный к аккаунту раз и навсегда. Но официальный клиент Telegram волею судьбы не отображает ID пользователей, хотя некоторые неофициальные клиенты, например Kotatogram, установленный в кабинете политической полиции, отображают ID каждого аккаунта рядом с остальными данным аккаунта. Отсюда следует вывод, что вообще не имеет смысл ради анонимности использовать Telegram аккаунт, хоть однажды привязанный к номеру телефона, зарегистрированному на ваш паспорт. Регистрируйте Telegram аккаунт на левый телефонный номер с самого начала. Но вот только Telegram совсем не рад этому. Волею судьбы в начале 2021 года Telegram технически заблокировал возможность регистрации новых аккаунтов с Desktop а разрешил только с мобильного телефона. Отметим, что привязка аккаунта мессенджера к номеру телефона это одно из законодательных требований к любому мессенджеру со стороны правительства России. Совпадение?

Одни только настройки по скрытию номера телефона в Telegram говорят о многом. На моих глазах один неглупый человек на протяжении нескольких месяцев трижды пытался в настройках Telegram скрыть свой номер телефона, и вроде бы по началу это удавалось. Но в итоге его снова оказалось возможно найти по номеру телефона! Если есть понятие интуитивно-понятного интерфейса, то существуют также антиинтуитивно-понятные интерфейсы, специально созданные для затруднения действий людей в определенном направлении или обмана (классический пример это договор, в котором ключевая часть специально написана мелким шрифтом, или административные барьеры). Действительно, зачем облегчать скрытие номера телефона, если в приоритете наращивание пользователей за счет использования адресной книги мобильного телефона. Также остается загадкой, для удобства кого в групповых чатах существует возможность скачивания любым пользователем всей истории переписки чата, включенная по умолчанию. Также автор сталкивался с тем, что Telegram выпускал обновления с нововведениями, которые неожиданно ставили под угрозу анонимность пользователя.

Волею судьбы секретные чаты в Telegram, использующие сквозное шифрование, т.е. вышеупомянутую криптосистему с открытым ключом, существуют только в версии для мобильного телефона, а в Desktop версии их нет. Мобильный телефон сам по себе

представляет идеальное устройство для слежки за вами, и им вообще лучше не пользоваться. Совпадение? Секретные чаты в Telegram, в отличии от многих других мессенджеров со сквозными шифрованием, возможны только между двумя пользователями и следовательно не могут иметь существенного значение для общественно-политической организации. Групповые чаты, также как и обычная личная переписка, составляют безмерно большую часть информации в Telegram, чем «секретные чаты». При этом история сообщений групповых чатов и обычной личной переписки хранится на серверах Telegram. Для передачи данных при этом используется транспортное шифрование, т.е. шифрование между пользователем и сервером Telegram. Серверная часть программного кода Telegram закрыта, и нам доподлинно не известно, зашифрованной ли хранится ваша переписка на серверах Telegram, и кто к ней имеет доступ. Во всяком случае уверенно можно утверждать, что ключ шифрования от этих данных известен не только отправителю и получателю сообщений, но и Павлу Дурову, некогда разбрасывавшему пятитысячные банкноты с балкона. А серверы Telegram представляют собой лакомый кусок для подкупа и внедрения агентуры кремля среди их администраторов. Таким образом, секретные чаты в Telegram больше похожи на маркетинговый ход, чтобы только заявить, что в Telegram они есть, что Telegram поддерживает сквозное шифрование, и следовательно он не хуже остальных мессенджеров. Вы же слышали, что для безопасности следует использовать мессенджеры со сквозным шифрованием?

Перед глазами автора этой книги за несколько лет прошло множество уголовных дел об экстремизме, массовых беспорядках, и прочих расшатывающих политическую систему затеях, основанных на материалах из Telegram. Люди читали материалы своего уголовного дела и обнаруживали, что как будто полицейский стоял у них за спиной, когда они переписывались в Telegram. В материалах другого уголовного дела короткая справка о том, что Telegram аккаунт принадлежит такому то гражданину...

Резюмируя: принимая во внимание, что спецслужбы государств контролируют мессенджеры, имеющие юридическое лицо и физическую инфраструктуру, как минимум по вопросам разведки, терроризма и киберпреступности, а также принимая во внимание информацию о сотрудничестве Telegram с властями Германии, а также о сотрудничестве Telegram с ФБР и ФСБ РФ, а также учитывая репутацию Telegram, который презентовал себя как мессенджер, ставящий во главу угла безопасность пользователей, а затем достоверно обманувший пользователей, а также учитывая мнение пользователей Даркнета и специалистов в области информационной безопасности о Telegram, автор этой книги считает использование Telegram неприемлемым для конфиденциальной связи и крайне опасным.

Сотовые телефоны

Люди которые подозревают, что Бил Гейтс хочет чипировать человечество, а также видевшие как в фильме «Матрица» из живота главного героя вытаскивают электронного жука для слежки, наверное ужаснуться, но человечество уже давно чипировано, причем добровольно. Каждый из вас добровольно носит с собой устройство, привязанное к вашему паспорту и googe-аккаунту, которое в режиме online отслеживает ваше местонахождение, записывает ваше местонахождение за годы вашего перемещения, способно производить тайную аудио запись, непрерывно передает данные в глобальную сеть Интернет, хранит ваши фото, историю ваших поисковых запросов и вашу переписку в мессенджерах. Зачем? Потому что очень удобно. Как и пользоваться мессенджером Telegram. Отметим, что это устройство не так просто обесточить, поскольку крышка отсека аккумулятора зачастую крепится на нестандартные винты или приклеена.

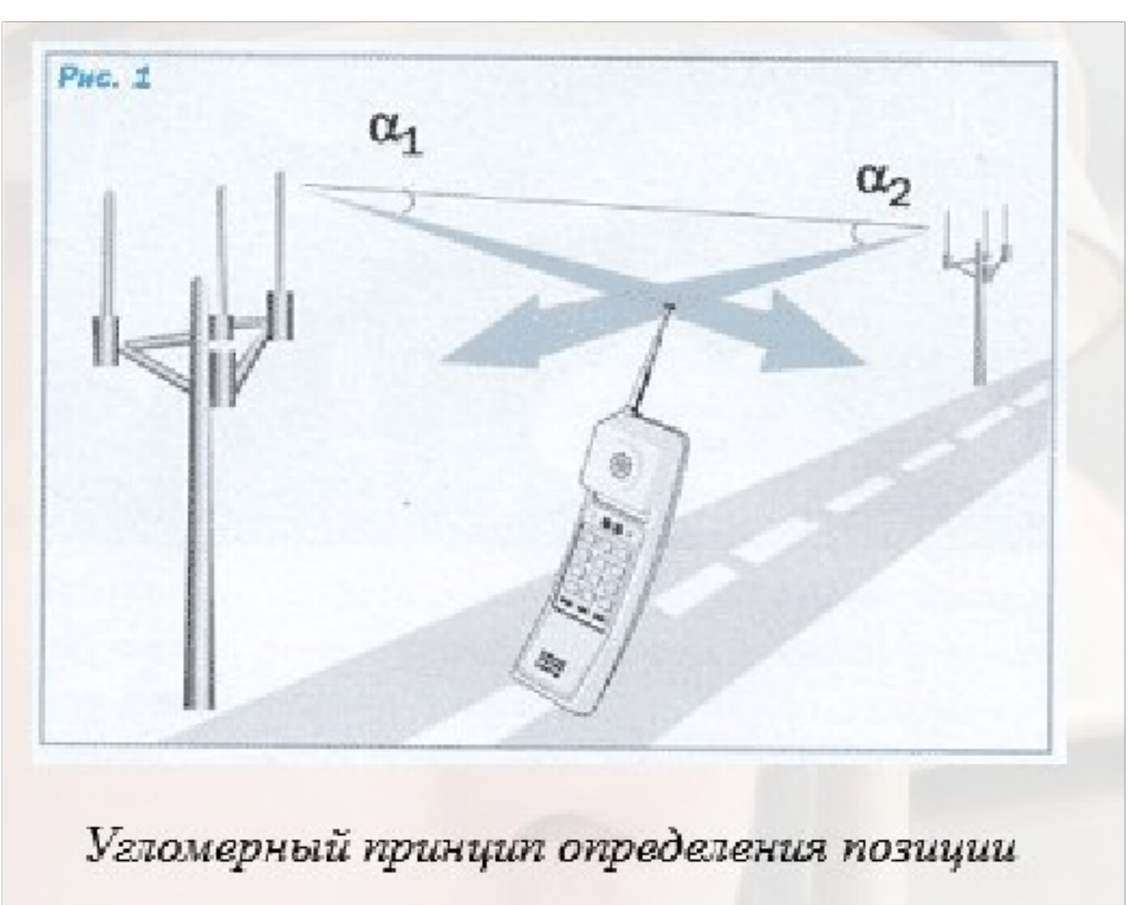
Цитата Хьюго Ландау, разработчика OpenSSL: «*Безопасных смартфонов не бывает. Вот простой факт, который удивительно часто упускается из виду. В современных смартфонах есть микросхема ЦП и микросхема основной полосы частот, которая управляет связью по радиосети (GSM/UMTS/LTE/и т. д.). Эта микросхема подключается к ЦП через DMA (прямой доступ к памяти). Таким образом, основная полоса частот имеет полный доступ к основной памяти и может произвольно скомпрометировать ее. Можно с уверенностью предположить, что эта основная полоса очень ненадежна. Это закрытый исходный код и, вероятно, вообще не проверен. Насколько я понимаю, современная прошивка основной полосы частот возникла в результате усилий по разработке основной полосы частот GSM, начиная с 1990-х годов, когда важность безопасных методов разработки программного обеспечения не была очевидна. Другими словами, как я понимаю, и это подтверждается исследованиями, эта прошивка имеет тенденцию быть чрезвычайно небезопасной и, вероятно, имеет множество уязвимостей удаленного выполнения кода. Таким образом, ни один смартфон нельзя считать защищенным от злоумышленника, способного скомпрометировать радиоканал. Это включает любую организацию, способную развертывать устройства, подобные Stingray, или любую организацию, способную получить контроль над базовой станцией путем взлома, юридического или иного принуждения. На мой взгляд, было бы вопиющим безумием не предположить, что полдюжины или более национальных государств (или связанных с ними подрядчиков) имеют в запасе эксплойты для выполнения кода против популярных базовых полос. В этом случае поиск «безопасных» телефонов и «безопасных» приложений для связи выглядит довольно странно.*»

Цитата: «*Разработчики Replicant нашли и закрыли лазейку в Samsung Galaxy. Работая над Replicant - полностью бесплатной версией Android, мы обнаружили, что проприетарная программа, работающая на процессоре приложений и отвечающая за обработку протокола связи с модемом, на самом деле реализует бэкдор, который позволяет модему выполнять удаленные операции ввода-вывода файлов в файловой системе. Современные телефоны поставляются с двумя отдельными процессорами:*

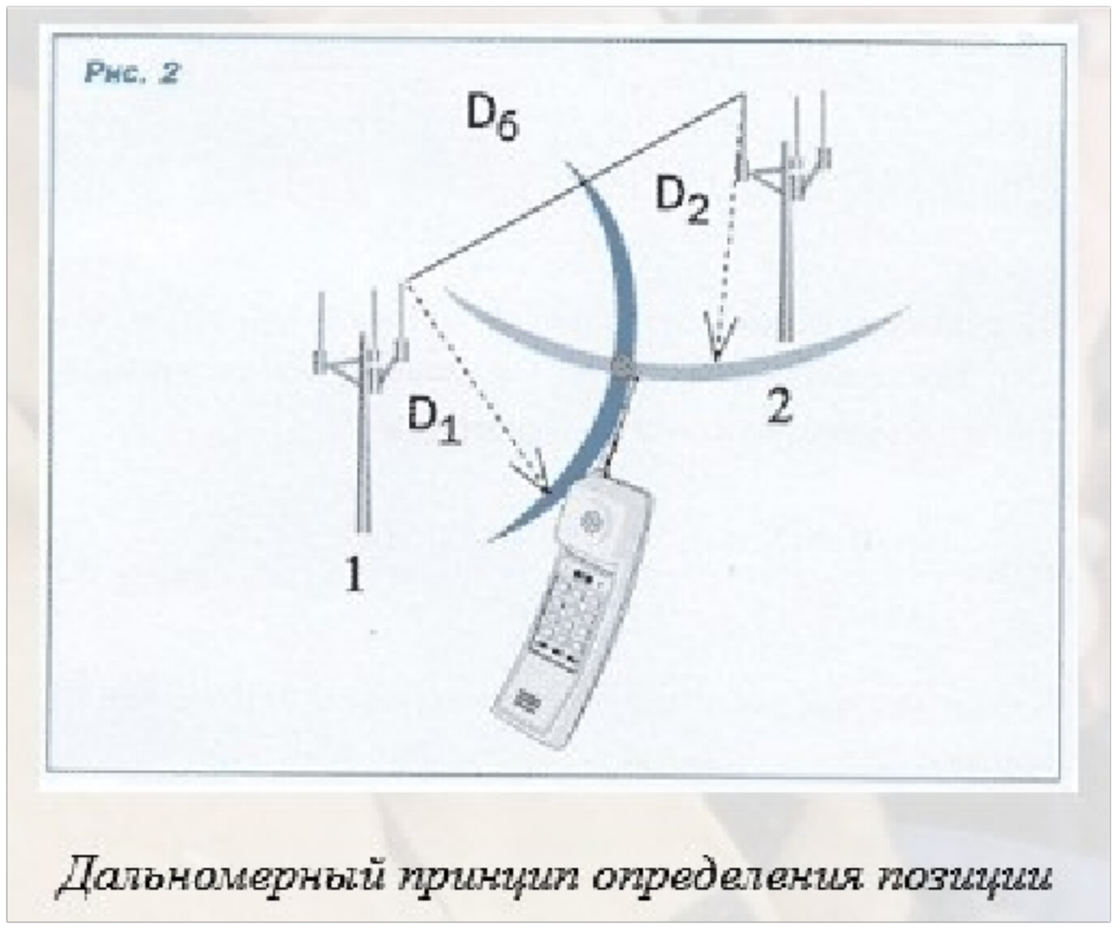
один из них представляет собой процессор приложений общего назначения, на котором работает основная операционная система, например Андроид; другой, известный как модем, основная полоса частот или радио, отвечает за связь с сетью мобильного телефона. На этом процессоре всегда работает проприетарная операционная система, и известно, что в этих системах есть лазейки, которые позволяют удаленно преобразовать модем в удаленное шпионское устройство. Шпионаж может включать в себя активацию микрофона устройства, но он также может использовать точное местоположение устройства по GPS и доступ к камере, а также пользовательские данные, хранящиеся на телефоне. Модемы большую часть времени подключены к сети оператора, что делает бэкдоры почти всегда доступными. Насколько нам известно, в большинстве устройств модем может иметь полный контроль над процессором приложений и системой, но в этом нет ничего нового. Replicant не сотрудничает с бэкдорами, но если модем может взять под контроль главный процессор и переписать программное обеспечение в последнем, система с главным процессором, такая как Replicant, не сможет его остановить»

Цитата: «*В целом доступ к данным, утечка которых опасна (сведениям о местонахождении; информации, получаемой от камеры и микрофона; журналам SMS-сообщений и звонков), запрашивают 89% приложений в Android и 39% — в iOS*».

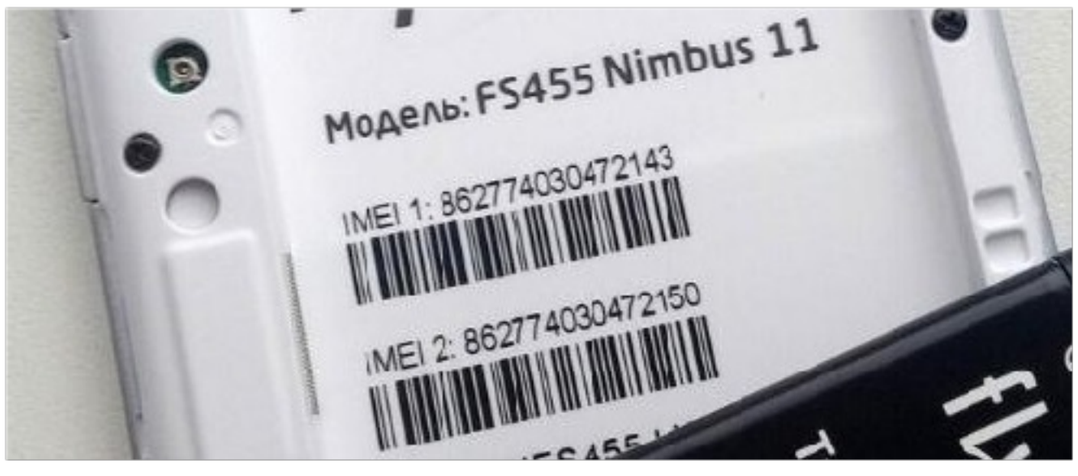
Отслеживание местонахождения мобильного телефона это рутинная процедура, используемая для задержания политических активистов перед митингами. Не берите с собой сотовые телефоны на важные мероприятия и переговоры. Отключайте его, а лучше не берите вовсе, если не хотите чтобы полиция наблюдала ваше перемещение и круг вашего общения в режиме online. Никогда не сообщайте важную информацию через разговор по сотовому телефону и по SMS. Телефоны всех оппозиционеров и всех их контактов прослушиваются, как вероятно и всех россиян. Современные вычислительные мощности и объемы носителей информации без труда позволяют хранить и обрабатывать такие объемы информации, в том числе распознавать слова и реагировать на ключевые фразы.



Угломерный принцип определения позиции



Дальномерный принцип определения позиции



Телефон имеет уникальный номер IMEI, который видит сотовый оператор, а значит и полиция. Его вы можете найти в отсеке аккумулятора или в меню операционной системы телефона в разделе информация о телефоне. Если в телефоне два отсека для SIM карты, то кодов IMEI у телефона тоже два. Отсюда следует вывод, что не имеет смысла вставлять левую SIM карту в телефон, в который раньше была вставлена SIM карта, зарегистрированная на ваш паспорт. Волею судьбы IMEI не только однозначно идентифицирует ваш телефон среди остальных сотовых телефонов планеты, но и сообщает марку вашего телефона. Это можно проверить на сайте www.imei.info/. Цитата из методички МВД РФ: «*Информация о конкретной модели и марке телефона облегчит работу при проведении обысков и осмотров, а также позволит определить стоимость телефона. Чем дороже телефон, тем меньше вероятность того, что злоумышленник избавится от него*».

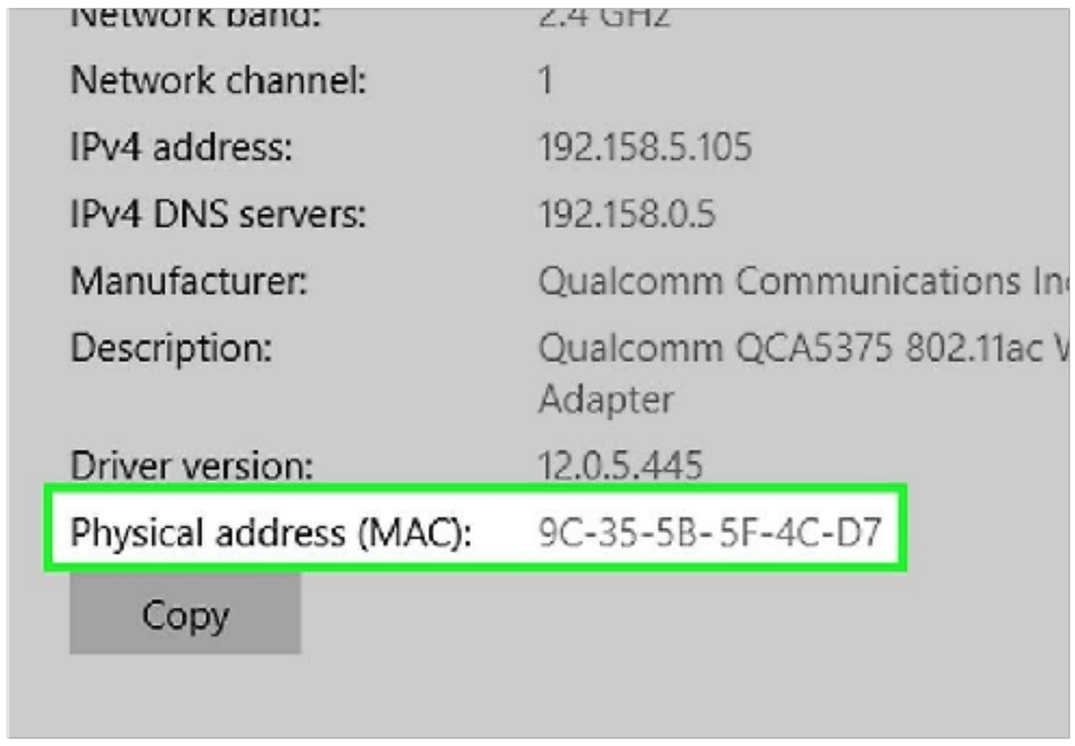
Мессенджер, который требует при регистрации аккаунта номер телефона, является частью всевидящего ока. Никогда не регистрируйтесь в мессенджерах на номер телефона, оформленный на ваш паспорт.

Цитата: «*Сотни уйгуров [в Китае] были заключены в лагеря или колонии за прослушивание "незаконных лекций" или установку зашифрованных приложений. Других* ***судят за неиспользование своих мобильных телефонов****, обвиняя в попытках скрыться от властей.*»

Лучше не пользуйтесь сотовым телефоном.

Сеть Интернет

Сайты и мессенджеры в сети Интернет идентифицируют вас по IP адресу, а ваш Интернет -провайдер по MAC адресу вашей сетевой платы компьютера, телефона или роутера.



В сети Интернет данные передаются пакетами, каждый из которых содержит всегда в незашифрованном виде IP адрес как получателя пакета информации, так и IP адрес отправителя. Кроме того, для преобразования символьных имен сайтов в IP адреса в интернете существует доменных имен (DNS). Запросы к DNS серверу о преобразовании символьных имен в IP адреса и ответы DNS сервера обычно передаются в незашифрованном виде. Следовательно, даже если содержимое пакета информации зашифровано, например по протоколу HTTPS, получатель пакета, а также все промежуточные узлы и ваш интернет провайдер видят кому и от кого отправлен пакет. Протоколированием посещенных вами сайтов занимается система слежки СОРМ.

В настройках сетевого подключения операционной системы, а также в браузере адрес DNS сервера стоит изменить на, например, DNS сервера Cloudflare 1.1.1.1, это может предотвратить утечку DNS при включенном VPN. В браузерах, как правило, присутствует опция включить DNS over HTTPS (DoH). По умолчанию запросы и ответы DNS отправляются по сети в незашифрованном виде, что означает, что адреса всех сайтов, которые вы посещаете, могут быть отслежены и запротоколированны вашим интернет-провайдером или любым промежуточным звеном в сети. Однако включение DoH не достаточно для защиты DNS запросов. На одном IP адресе может быть несколько сайтов. Для определения к какому именно сайту на IP адресе обращается браузер, протокол HTTPS отправляет при запросе имя сайта снова в незашифрованном виде. Ваш интернет провайдер и любые промежуточные звенья в сети снова могут видеть и протоколировать какие сайты вы посещаете. Чтобы обойти отслеживание DNS запросов используются технологии ESNI (Encrypted Server Name Indication) и ECH (Encrypted Client Hello). Эти технологии могут поддерживаться, а могут не поддерживаться вашим браузером и как правило отключены по умолчанию. В настоящий момент браузер FireFox поддерживает ECH.

Цитата: «*С августа 2020 в Китае блокируется ESNI- и TLSv1.3-трафик. С октября 2020 и ранее в России провайдеры так же начали блокировку ESNI-трафика*».

Для работы ECH и ESNI необходимо, чтобы сайт, к которому обращался браузер поддерживал TLS v 1.3. Вы можете использовать программу для анализа сетевого трафика вашего компьютера, например WireShark, чтобы убедиться, что включение ECH и ESNI часто не дает результата. Однако даже если зашифровать DNS запросы, IP адреса пакетов всегда остаются незашифрованными, следовательно ваш провайдер все равно видит, к каким IP адресам вы обращаетесь, т.е. с хорошей точностью все равно знает какие сайты вы просматриваете. Следовательно правильным будет отправлять ВЕСЬ трафик через туннель, например VPN и TOR. Естественно VPN сервер должен быть не на территории России или дружественных ей режимов, вроде Беларуси. Слишком многие программы любят отправлять данные в обход proxy, поэтому правильнее использовать Whonix для полного заворачивания трафика в сеть TOR.

Очевидно, что одного VPN сервера не достаточно, поскольку провайдер видит, что вы обращаетесь к IP адресу VPN сервера, а сайт, который вы посещаете, также видит запрос от того же IP адреса, и вас, если немного захотеть, можно идентифицировать, если к сайту, как например в случае Вконтакте, имеют доступ политическая полиция. Очевидно, что необходима цепочка серверов, что и обеспечивает TOR.

Очевидно, что нужно несколько уровней защиты, для того, чтобы отказ одного уровня не привел к фатальным последствиям. Даже одновременный отказ двух уровней защиты не является совсем большой редкостью, а может стать злым совпадением. У вас в жизни не бывало совпадений? Как известно системы управления самолетом имеют тройное дублирование.

Изучите самостоятельно, как работают SSL-сертификаты безопасности и криптосистема с открытым ключом. После этого вам станет ясно, что скачивать программное обеспечение вроде браузеров и мессенджеров следует только с официальных сайтов, иначе в них могут быть закладки, полностью вас деанонимирующие. После скачивания программного обеспечения следует сверить хэш-сумму скаченного файла с опубликованной его создателями, или сверить PGP подпись файла, чтобы убедиться, что файл не был изменен по пути к вам. Включите автоудаление cookie и данных из кэша при закрытии браузера. Отключите опцию WebRTC peer connection. Отключите опцию Send the referrer head. Включите в браузере опции HTTPS Everywhere.

Учитывая, что, во-первых, в обществе нет запроса против слежки за ним, и во-вторых учитывая, что браузеры могут сотрудничать со спецслужбами правительств, никто не может гарантировать, что в вашем браузере нет еще какой-то особенности, обнуляющей вашу безопасность, или что она не появится в следующем обновлении без вашего спроса, в виде какой-то новой опции, отключенной по умолчанию. Поэтому правильным будет использовать VPN в связке с Whonix, полностью отправляя весь трафик через зашифрованный туннель.

Никогда не открывайте непонятные ссылки, которые вам могут прислать. Важно понимать, что открытие такой ссылки в браузере это http запрос, в результате которого сторона на другом конце узнает как минимум ваш IP адрес, а вероятно и ваш fingerprint - «отпечаток пальца», содержащий множество вполне идентифицирующей вас информации, включая подробную версию браузера и операционной системы, установленное программное обеспечение, используемые шрифты, разрешение экрана, аудио и видео оборудование и множество другой технической информации о вашем компьютере.

Цитата: «*Злодей может скомпрометировать веб-приложения и поднять дорвеи, разместить там JS-код и составлять базу данных уникальных фингерпринтов. Например, он может выяснить, что пользователь с уникальным фингерпринтом c2c91d5b3c4fecd9109afe0e был замечен на сайтах sdfsdfsdfdrugs.onion (основная тематика — наркотики), gunsdfsdf.onion (основная тематика — оружие), linkedin.com/vasya и так далее. Результат: конкретная личность и ее психологический портрет.*»

Если ваш трафик не зашифрован, открытие такой ссылки полностью вас деанонимизирует на стороне провайдера, который видит DNS запрос по этой ссылке или обращение к IP адресу за ссылкой. Не следует просто так открывать сложные документы вроде pdf, docx и т.п., тем более исполняемые и не известные вам форматы, присланные вам или найденные в Интернете. Неизвестно, что внутри них. Открытие их может также привести к интернет запросу или исполнению зловредной программы на вашем компьютере. Вы знаете, что делают такие сложные программы, как Acrobat Reader или Microsoft Word? Такие документы следует открывать в «песочнице» - изолированной от интернета и чистой, т.е. не содержащей никакой персональной информации, операционной системе.

В интернет в идеале следует выходить с левой сим-карты, не связанной с вами, как и с левого телефона, в который никогда ранее не вставлялась сим-карта связанная с вами. Местоположение такого телефона разумеется всегда отслеживается с точностью до нескольких метров в городе, и вероятно до десятка метров в малонаселенной местности, и это стоит учитывать. В идеале следует менять свое местоположение после использования такого телефона.

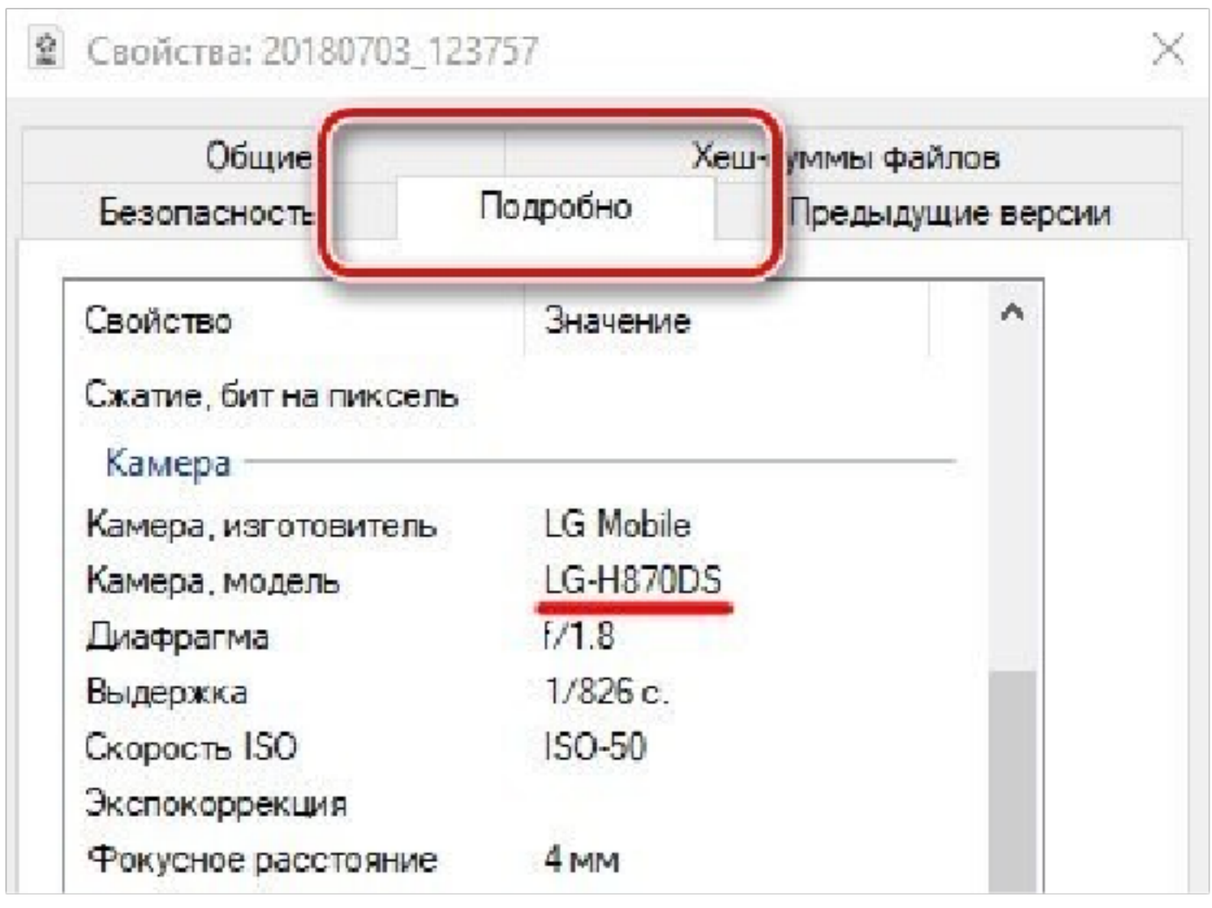
Для каждой отдельной задачи создавайте новую чистую цифровую личность, в частности используйте отдельный браузер, компьютер или операционную систему. Если дело примет серьезный оборот, при надвигающейся опасности избавьтесь от устройства, с которого осуществляли связь. В противном случае оно будет важной частью в материалах вашего уголовного дела и его название не раз прозвучит на вашем суде.

Метаданные

Волею судьбы, смартфоны, фотоаппараты и видеокамеры записывают в записываемые ими фото и видео файлы так называемые Exif метаданные, содержащие подробную информацию об устройстве, с которого осуществлялась фото или видеосъемка, в том числе марку устройства, размер матрицы, время съемки, а при возможности и местоположение, где производилась съемка. Тоже самое делают компьютерные программы: фото и видеоредакторы, записывая в метаданные время создания, *название программы-редактора*, *его версию.* Тоже самое делают и офисные пакеты программ и многие другие программы, зачастую сохраняя в метаданных файла имя автора файла и название компьютера.

Метаданные файлов позволяют вас идентифицировать. Так, например, Telegram оставляет без изменения Exif метаданные загружаемых видеофалов, что как известно позволило по дате создания видеофайла раскрыть ряд провокаций со стороны властей искусственных образований на территории Украины ДНР и ЛНР перед началом вторжения в Украину 24 февраля 2022.

Цитата: *Видеообращения главы ДНР Дениса Пушилина и главы ЛНР Леонида Пасечника, в которых они говорят о необходимости эвакуировать население из-за угрозы со стороны Киева, были записаны 16 февраля — за два дня до их публикации. Об этом свидетельствуют метаданные роликов. При этом Пушилин в своей речи акцентировал на том, что он говорит ее* «сегодня, 18 февраля» *Также Пушилин заявил, что «к сожалению, ситуация в Донбассе идёт к войне». Также старой оказалась и запись перестрелки, которую ДНР преподносила как атаку украинских ДРГ, намеревавшихся взорвать емкости с хлором на территории очистных сооружений в районе Горловки. Проект Gulagu. net обратил внимание на то, что и в метаданных этого видео дата не соответствует заявленной: оно было снято 8 февраля в 10:29:30, то есть за 10 дней до официальной публикации.*



Отсюда следует вывод, что при передаче фото и видео файлов необходимо удалять их Exif метаданные тем или иным способом. Это можно сделать с помощью бесплатных сайтов в сети Интернет, как и просматривать метаданные данные файлов, например https://www.adarsus.com/en/remove-metadata-online-document-image-video/ и https://www.metadata2go.com/ соответственно. В Linux существует утилита mat2 для удаления метаданных из файлов.

Метаданные содержатся не только в файлах фото и видео, но и в других документах, например Microsoft Office, Adobe Acrobat, аудиофайлах. Всю персональную информацию из них необходимо удалить, а лучше не использовать такие файлы. Отметим, что некоторые программы не отображают все метаданные файла, что может создать иллюзию безопасности. Цитата: «*как правило, фотоаппараты добавляют к файлу информацию, специфичную только для данной конкретной камеры. Правильно интерпретировать такую информацию могут только программы от изготовителя фотоаппарата.*»

Цитата: *«Метаданные – это данные слежки. Собирать метаданные о людях означает следить за ними»*. Брюс Шнайер, американский специалист по цифровой безопасности.

Цитата: «*С конца 70-х в штате Канзас орудовал жестокий убийца. Полицейские прозвали его BTK (bind, torture, kill – «связывать, пытать, убивать»). Жертвами маньяка становились одинокие женщины и семьи. Жажда славы подталкивала BTK отправлять сообщения в полицию, газеты, радиостанции. Убийца рассказывал о деталях своих жутких преступлений, прилагал доказательства-фотографии, писал безумные стихи. В 2005 году BTK подбросил коробку со своими сочинениями на автостоянку, и тут его машину зафиксировала дорожная камера. Увы, расстояние было слишком велико. Черный внедорожник Jeep Grand Cherokee – вот и все, что удалось установить следователям. Вскоре психопат сделал попытку перейти с бумажных сочинений в электронный формат. Он отправил в полицию дискету с файлом. Следователи принялись изучать диск с файлом. Помимо послания маньяка, они обнаружили удаленный файл Microsoft Word и восстановили его. Содержание файла ничего не дало. Но в метаданных документа была упомянута местная лютеранская церковь, а последняя редакция принадлежала некоему Деннису. Следователи быстро вышли на Денниса Рейдера, председателя церковного совета. Когда полиция подъехала к его дому, то увидела припаркованный черный Grand Cherokee. Анализ ДНК сделал возможным арест преступника. Сейчас Деннис Линн Рейдер, он же BTK, отбывает 10 пожизненных сроков в тюрьме строгого режима Эль Дорадо в Канзасе.*»

Вас также могут вычислить по дефектам матрицы вашей видеокамеры, например, если вы «анонимно» опубликуете фото или видео, демонстрирующие битые пикселы вашего телефона или видеокамеры, лежащей у вас в чулане. Вас также могут вычислить по особенностями используемого микрофона. Также для вашей индентификации могут быть использованы дефекты принтера, на котором вы печатаете «анонимные»

документы или листовки. Одной из разновидностей метаданных являются «желтые точки» - незаметные точки печатаемые принтерами, для их идентификации, рассмотренные ранее.

Уничтожение данных с носителей информации.

Удаление информации с носителей информации представляет собой не такую простую задачу, как думают многие. Выполнение команд операционной системы delete или shift delete, не удаляет данные физически, потому что после этого данные остаются на HDD (накопителе на жестких магнитных дисках) пока не будут перезаписаны другой информацией. Такие данные легко могут быть восстановлены любой программой для восстановления удаленных файлов. Для физического удаления файлов с HDD для системы Windows существует утилита sdelete (от слов secure delete), которая перезаписывает весь объем HDD случайными числами или нулями, на что уходит не мало времени. Команда для очистки диска нулями «./sdelete.exe -z E:», где «E:» - буква диска. По тому же принципу действуют специальные комманды для надежного удаления файлов с HHD в операционной системе Linux. При этом sdelete не удаляет с диска имена файлов и имена файлов могут быть восстановлены.

Ввиду сложных алгоритмов выравнивания износа, оптимизации быстродействия и коррекции ошибок у SSD дисков, строго говоря, с твердотельного носителя, в том числе и с flash карт, невозможно ни надежно удалить файлы, ни надежно их восстановить. После удаления файла операционная система обычно отправляет команду TRIM накопителю SSD (как и HDD с черепичной записью) и с этого момента контроллер накопителя возвращает нули при обращении к секторам накопителя, которые занимал соответствующий удаленный файл. Однако данные остаются в ячейках памяти SSD диска непредсказуемо долгое время и могут быть извлечены специалистами, минуя контроллер SSD диска. Поэтому правильным решением будет шифровать данные сразу при записи на диск. А надежным способом удаления информации с SSD дисков, SD карт и flash накопителей будет их физическое уничтожение. Еще одно затруднение при удалении данных с жесткого диска, в том числе с HDD, могут вызывать bad сектора, которые помечаются контроллером жесткого диска как поврежденные, но при этом могут нести на себе конфиденциальную информацию.

Неплохим решением для временного хранения файлов является использования RAM диска, т.е. эмуляция диска в оперативной памяти. После выключения питания информация в RAM диске бесследно уничтожается.

Компьютерные программы: браузеры, мессенджеры, графические\фото\видео редакторы, пакеты офисных программ и другие, сложны и пишут множество ваших приватных данных на жесткий диск. Cookie, история посещения страниц, логи, кэши, история переписки, временные файлы, эскизы изображений, все самое неожиданное, что вы и не могли предположить. Это еще раз показывает то, что производители

программ совсем не заинтересованы в вашей приватности. И все эти данные могут стать материалами в вашем уголовном деле.

Одно из первых, что сделает специалист, получив после обыска ваш компьютер, это анализ файлов подкачки и гибернации, в которые записывается содержимое оперативной памяти со всеми ключами шифрования, паролями и остальными вашими ценными данными. Файлы подкачки и гибернации представляют значительную опасность для вашей приватности и их можно отключить.

Шифрование носителей информации

Из вышесказанного следует вывод, что весь системный диск стоит полностью зашифровать. Это надежнее, чем заниматься поиском и удалением незашифрованных данных на диске. Используйте Open Source программы для шифрования, как например Vera Crypt. Не используйте закрытое программное обеспечение, поскольку, как вышесказанно все корпорации собирают ваши данные в коммерческих интересах, а также сотрудничают со спецслужбами, следовательно вероятность наличия «черного хода» в закрытом программном обеспечении недопустимо велика.

Никогда не оставляйте открытыми криптоконтейнеры, уходя например в магазин, или спать. Никто не знает, что в это время не придет группа захвата чтобы произвести ваше задержание и обыск.

Пока компьютер включен конфиденциальные данные находятся в оперативной памяти (RAM). В том числе в оперативной памяти находится ключ для расшифровки диска при использовании полнодискового шифрования. Существуют простые технологии для извлечения данных из оперативной памяти работающего компьютера, в том числе используя DMA (прямой доступ к памяти) некоторых устройств компьютера, вроде шины PCI и Thunderbolt, или быстрое принудительное выключение компьютера и загрузку программы злоумышленника, которая извлечет данные из RAM, поскольку данные в RAM сохраняются несколько секунд при исчезновении питания. Наконец возможно физическое извлечение предварительно охлажденных до низких температур модулей RAM из компьютера и последующее их чтение. Отсюда следует, что правильным будет полностью выключать компьютер, когда вы его оставляете без физического контроля.

Правовой основой для вашего права не сообщать пароли, не разблокировать устройства и не предоставлять какую либо информацию следствию, является 51 статья Конституции РФ (аналог пятой поправки к Конституции США) - «Никто не обязан свидетельствовать против себя самого, своего супруга и близких родственников». По этой, как и по многим другим причинам, предпочтительно использовать пароли вместо биометрических данных, поскольку ваш палец могут насильно приложить к сканеру отпечатка пальца или сфотографировать ваше лицо для разблокировки устройства. Биометрические данные также можно подделать, и их в отличие от пароля нельзя поменять.

Под пытками 100% людей меняют свои взгляды на жизнь, поэтому лучшим вариантом при обыске является физическое уничтожения носителей информации. Чтобы обеспечить необходимое для этого время укрепите помещение, где находится цифровая техника. Широко известен случай, когда штурм полицией хорошо укрепленного расчетно-кассового центра теневых банкиров, занял четыре часа. За это время его охраной в соответствии с инструкцией были уничтожены находящиеся внутри документация и цифровая техника. Если утром вам стучат в дверь, и вы спали, вам стоит потратить время, чтобы хорошенько проснуться, чтобы оценить ситуацию, прежде чем идти открывать дверь, поскольку в полусонном состоянии человек находится в состоянии неполного сознания и легко внушаем.

Уделите особое внимание запоминанию своих паролей. Опасность шифрования данных, с которой вы столкнетесь, состоит в том, что множество ценной информации было потеряно, просто потому, что ее владелец забыл пароль шифрования.

Физический доступ к компьютеру

Важно понимать, что шифрование жесткого диска может вас обезопасить, только в случае, когда ваш зашифрованный компьютер попадает в руки злоумышленника впервые. Ни одна программа для шифрования (ознакомьтесь с инструкцией VeraCrypt) не гарантирует защиты информации в случае физического доступа злоумышленника к компьютеру, прежде чем вы им воспользуетесь.

Имея физический доступ к вашему компьютеру, злоумышленник может установить программный или аппаратный keylogger, который будет записывать и\или отправлять по сети все нажатые вами на клавиатуре клавиши, т.е. похитит пароли и конфиденциальную переписку. Или будет записывать и\или отправлять по сети снимки экрана при вашей работе на компьютере.

Кроме того, как вы можете догадаться, запуск любого зашифрованного компьютера начинается с исполнения незашифрованного компьютерного кода, например загрузчика Vera Crypt или ядра Linux, которые в свою очередь запрашивают пароль и расшифровывают остальную информацию на жестком диске. Имея физический доступ к компьютеру, злоумышленник может модифицировать незашифрованную программу загрузчика, вставив внутрь код, который отправляет по сети и\или сохраняет ваш пароль для расшифровки диска, который вы вводите при включении «зашифрованного» компьютера. Разумеется, похитив введенный вами пароль по сети, злоумышленник может расшифровать зашифрованный диск, заранее скопированный им при первом физическом доступе к компьютеру.

Чтобы избежать физического доступа к вашему компьютеру, целесообразно, во-первых, не привлекать внимания злоумышленников, а также установить нестандартную сигнализацию в помещении, где хранится компьютер.

Компьютерные вирусы

Не открывайте сомнительные ссылки и сомнительные файлы присланные вам даже знакомыми людьми. Не посещайте сомнительные сайты. Не запускайте на компьютере сомнительные программы. В случае необходимости открывать такие файлы и ссылки следует в «песочнице» - отдельной чистой операционной системе, не содержащей персональных данных, по возможности отключенной от сети Интернет.

Устанавливайте программное обеспечение только из источников, заслуживающих доверия. Проверяйте хеш-суммы и PGP подпись скаченных исполняемых файлов, чтобы убедиться, что файл не был изменен при движении по маршруту в сети к вам. Следует использовать последнюю версию программного обеспечения, поскольку в программном обеспечении время от времени обнаруживаются «дыры», которые с течением времени устраняются разработчиками.

Для конфиденциального общения и для работы с конфиденциальной информацией стоит использовать отдельный компьютер или отдельную операционную систему, которые вы не используете в повседневной работе, и на которых установлен и запущен минимум компьютерных программ.

Следует включить в операционной системе технологию DEP (Data Execution Prevention) для всех программ. Для операционной системы Linux имеются средства для обнаружения атак и проверки целостности файлов компонентов операционной системы.

Камеры видеонаблюдения

«Мир на самом деле лучше, чем представлял Оруэлл, но в нем также гораздо больше слежки», Илон Маск.

Видеонаблюдение в современном городе с использованием машинного распознавания лиц носит почти тотальных характер. Без общественного запроса на запрет использования технологии распознавания лиц в общественных местах этот вид слежки будет только усиливаться. Используя множество камер видеонаблюдения прослеживают маршрут конкретного человека, особенно в случае преступления им закона. Удивительно, но люди сами стоят собственную тюрьму, устанавливая системы видеонаблюдения в подъездах своих многоэтажных домов, в том числе используя домофоны со встроенными видеокамерами. Не удивительно потом происходящее вмешательство в личную жизнь, наиболее частый пример которого — распад семей, из-за видефиксации супружеских измен. Такие системы видеонаблюдения в подъездах могут быть подключены к системе «безопасный город», во всяком случае компании, занимающиеся «системами безопасности», как правило, курируются ФСБ.

Машинное распознавание лиц позволяет идентифицировать человека даже в медицинской маске, хотя медицинская маска и снижает вероятность распознавания.

Наиболее важной для распознавания лица является область глаз и бровей. Также важен контур челюсти, форма носа и рта. Следовательно против распознавания лиц эффективно одновременное ношение медицинской маски и темных очков. Полезны также кепка и капюшон, поскольку могут скрыть ваше лицо при видеосъемке со множества ракурсов.

Цитата: «*Наиболее агрессивно технологии распознавания лиц внедряются в Китае. К 2019 г. в этой стране системы распознавания лиц были установлены в самых разных местах: на улицах городов, в магазинах, отелях, кафе и ресторанах, образовательных учреждениях, детских садах, зоопарках, транспорте, на банкоматах и даже в туалетах и на дверных замках. В марте 2020 г. сообщалось о планах властей КНР сформировать национальную систему, которая позволит идентифицировать человека за несколько секунд, получая данные с 626 млн камер. В декабре 2019 г. в Китае вступил в силу закон об обязательном распознавании лиц покупателей SIM-карт.*»

Цитата: *«Британский журналист протестировал систему видеонаблюдения в Китае, попросив добавить себя в список разыскиваемых лиц. После этого он попытался скрыться в Гуйяне, население которого превышает 4 млн человек, но уже через 7 минут был задержан полицейскими.»*

Видеозаписи с камер наблюдения хранятся обычно от трех дней до месяца. Обычно три-семь дней для уличных камер и тридцать дней для важных объектов, например банков. В случае важных переговоров скрывайте свое лицо от видеокамер наблюдения, используйте одежду и обувь, которые вы не используете в повседневной жизни, изменяйте свою походку и держитесь от видеокамер подальше. И никогда не берите с собой сотовые телефоны.

Важно иметь ввиду, что в России наказание невиновных и безнаказанность виновных скорее правило, чем исключение. Неискушенный человек, вследствие уверенности, что он не нарушает закон и осознания себя невиновным, может решить пренебречь мерами информационной безопасности, поскольку он может посчитать, что честные правоохранительные органы не тронут невиновного человека. К сожалению это не так, и это очень опасная ошибка. Дело не только в том, что не являясь опытным юристом вы можете не осознавать, что ваши действия на самом деле нарушают установленный закон, что сплошь и рядом происходит с комментариями в Интернете. Дело в том, что ваши действия даже не нарушающие установленный закон могут быть преподнесены следствием как доказательства вашего преступления, если на то есть «политическая воля» или желание полицейских во чтобы то не стало раскрыть преступление. Попав под видеокамеры в неподходящем месте в неподходящее время, или имея контакт по незащищенному каналу с человеком, находящимся в разработке органов, или написав комментарий в интересном чате в горячее время, например перед крупным митингом, можно легко стать свидетелем по уголовному делу, и подвергнуться не только допросу но и обыску с изъятием компьютерной техники, вербовке в стукачи, а возможно и пыткам с целью получения признательных показаний, и в результате попасть в тюрьму за чужое преступления. Особенностью работы политической полиции является то, что в

большинстве случаев следственные действия производятся в целях давления на политического активиста, чтобы он прекратил или изменил свою деятельность, или в целях вербовки в информаторы. Следовательно, политическая полиция будет только рада, если вы предоставите ей повод вызвать вас на допрос или провести обыск в вашем жилище. Политическая полиция особенно не знает никаких законных преград, если приходит разнарядка сверху, например в преддверии федерального протеста или выборов, кого-то наказать и притормозить. В этом случае не надо удивляться откровенному беспределу в виде фабрикации как административных арестов так даже уголовных дел. Все вышеперечисленное представляет собой тоталитарную практику и может привести вас к решению бездействовать, но я хочу сказать нечто совершенно иное, что хорошо продемонстрировать примером. Допустим вы в своем городе каким-то образом находите факт политической акции, например граффити или баннер. Не изучая уголовного кодекса РФ и не следя за практикой репрессий в России вы можете не определить по каким статьям уголовного кодекса РФ можно привлечь за выполнение обнаруженной вами политической акции (чаще всего вандализм, но может быть дискредитация армии, оскорбление чувств верующих и другие). Не будучи гэбней или скрепоносцем и не следя за практикой репрессий в России вы можете не оценить какой общественный резонанс и какую реакцию политической полиции вызовет данная акция. Возможно она настолько рушит духовные скрепы, что ее расследование возьмет на контроль глава Следственного комитета РФ или хотя бы региональная гэбня. И главное, что я пытаюсь донести. Справедливо считая себя невиновным вы можете с включенным сотовым телефоном и не скрывая своего лица подойти и сфотографировать эту политическую акцию. При этом человек, который исполнил эту политическую акцию, понимая что преступает закон, скорее всего максимально соблюл все меры безопасности. В результате только ваше нахождение в этом месте, особенно если вы публичный политический активист или журналист легко может привести к обыску и допросу вас как свидетеля, а возможно и к пыткам и фабрикации уголовного дела. Если вы, справедливо считая себя невиновным, выложите полученные фотографии акции в сеть со своего незащищенного аккаунта в социальной сети, это еще больше усугубит ситуацию. Как правило политическая полиция начинает расследование с выяснения, кто первым выложил фото и видео акции в сеть. Действительно зачастую тот кто совершает акцию сам же и выкладывает фото в сеть. Никогда не выкладывайте в сеть фото и видео материалы о серьезных и опасных политических акциях через каналы, которые сильно ассоциируются с вами. Как правило хорошая акция вообще не требует выкладывания вами материалов в сеть, поскольку за вас это сделают случайные очевидцы, не являющиеся ни публичными ни подпольными оппозиционерами, и затем СМИ, если акция действительно была удачной. Правильным поведением оппозиционера при обнаружении жесткой политической акции будет выключить или хотя бы перевести в режим полета мобильный телефон, закрыть лицо маской, например от коронавируса, в идеале использовать одежду, которую вы не используете в повседневной жизни, сфотографировать акцию, и по безопасному каналу связи отправить фото вашим соратникам за пределами России или в оппозиционные СМИ. Зачастую бывает полезнее вообще не публиковать такие фото, хотя бы в течение недели по двум причинам. Во-первых велика вероятность того, что по прошествии недели видеозаписи с камер наблюдения будут удалены, что увеличит вашу безопасность. Во-вторых, публикация

фото скорее всего приведет к уничтожению зафиксированного вами политического высказывания политической полицией. В том время как не будучи обнародованным в медиа это политическое высказывание могло длительно и массово оказывать воздействие на очевидцев.

Во всех штабах и помещениях политических, религиозных, и прочих общественных организаций, а также неформальных политически активных групп в России спецслужбы, как правило, устанавливает видео и аудио наблюдение. Современные видеокамеры легко могут иметь объектив размером менее 1 мм, и их тяжело заметить. Видео и аудио наблюдение могут устанавливать в жилых помещениях подозреваемых. В помещении целесообразно установить самодельную сигнализацию, фиксирующую проникновение. Это особенно важно для предотвращения физического доступа к вашему компьютеру. Как ранее было отмечено, в разделе «Физический доступ» шифрование может защитить ваши данные, только в случае, когда ваш компьютер попадает в руки злоумышленников впервые, но ни как ни после того, как они установили на него keylogger или изменили программный код загрузчика.

Аудио наблюдение осуществить еще легче, даже не проникая в помещение. Например аудио можно снимать лазером со стекла окна с большого расстояния или вмонтировав микрофон в стену. Никогда не обсуждайте важные вещи в таких помещениях. Специальные направленные микрофоны фиксируют речь на открытом пространстве на расстояниях до 30-100 метров. Но для того, чтобы к вам применяли такие методы, вы конечно уже должны быть «в разработке» и представлять интерес для спецслужб.

Информаторы и агенты спецслужб.

Информаторы, внедренные в общественно или политически активные группы, являются старым и неотъемлемым методом наблюдения за такими группами. Этот метод тоталитаризма пожалуй наиболее разрушителен для идей свободы, поскольку нападает на саму основу свободного общества — доверие между людьми и свободную кооперацию. Этот метод тоталитаризма испытан веками, следовательно очевидно, что он эффективен и представляет большую угрозу.

По-моему мнению, наилучшим способом борьбы с внедренными агентами является исследование мировоззрения и биографии этих людей. На самом деле, ни один человек не может скрыть от внимательного взгляда своего мировоззрения, особенно на протяжении длительного промежутка времени. Мировоззрение человека проявляется в мельчайших словесных оборотах и в мельчайших деталях поведения. Вряд ли хоть один человек станет на протяжении многих лет действовать вопреки своему мировоззрению. Это как минимум разрушительно для психики. Надежность человека значительно повышается с количеством лет вашего знакомства. «По плодам узнаете их» - неплохое правило. Вряд ли человек, из года в год приносящий пользу движению, будет агентом спецслужб. Скорее рано чем поздно противник свободы в группе совершит агрессивный поступок, вредоносное действие, или высказывание против сторонников свободы. Так можно выявить противников свободы и агентов гэбни. Агенты гэбни, как правило

стараются делать такие выпады завуалированно, преувеличенно вежливо и выбирая подходящий момент.

Как мы выяснили ранее, чтобы быть агентом гэбни не обязательно это осознавать. Чтобы молотком забивать гвозди, молоток не обязательно должен обладать сознанием для понимания своего предназначения. На порядок больше, чем агентов на зарплате или на крючке, или идейно сотрудничающих со спецслужбами, просто людей запрограммированных определенными ментальными программами, разрушительными для оппозиции. Я называю их Zombie агенты гэбни. Есть схожее но более широкое понятие - «полезные идиоты».

Zombie агенты гэбни это прежде всего провокаторы внутренней вражды с переходом от обсуждения идей на личности (в том числе на национальность, возраст, пол, сексуальную ориентацию, внешний вид, форму черепа, одежду и т.д.), распространители теорий заговоров, переводчики агрессии с власти на другой объект, размыватели повестки, а также скрытые сторонники тоталитаризма, люди испытывающие синдром жертвы (стокгольмский синдром, он же - ассоциация себя с агрессором) и подсознательно стремящиеся к поражению, следовательно целенаправленно совершающие ошибки, стремясь попасть в лапы противника. Все это дает практическое основание рассматривать всех людей с тоталитарным мировоззрением как агентов спецслужб, без разницы, непосредственные они агенты ФСБ или Zombie.

Действительно, можно представить политическую секту, которая может не являться непосредственным проектом ФСБ, но использует те же самые методы гэбни: теории заговора, мистику, имеет собственного вождя, и даже своих Интернет-троллей, например как секта Светланы-Лады-Русь. Такая политическая секта будет полным конкурентом гэбни в «ареале обитания» гебни, представляющем выдуманный мир тоталитарной иллюзии. В случае покушения на власть такая политическая секта будет подвергаться ожесточенным репрессиям в полном соответствии с формулой Чарльза Дарвина «самая ожесточенная борьба за существование происходит между самыми близкими видами». Но мы должны себя спросить, является ли такая политическая секта друзьями борцов за свободное обещество? Как я отмечал ранее, в искусственном мире тоталитарной иллюзии Путина может победить только еще больший Путин. Следовательно, борьба по правилам этого иллюзорного мира, т.е. с использованием теории заговора, мистики и вождизма, не имеет смысла, а имеет смысл только разрушение этого искусственного вудуманного мира. В то же время, политическая тоталитарная секта, например секта Светланы-Лады-Русь, как раз распространяет тоталитарную иллюзию, рассказывая, что во всем «виноваты Ротшильды», тем самым укрепляя иллюзорный мир, в котором властителями является именно Путин и гэбня. Таким образом, подобные «оппозиционные» секты, распространяющие теории заговора, являются Zombie агентами гэбни.

Zombie агенты редко становятся непосредственными агентами спецслужб, поскольку многие из них имеют нестабильную психику и им сложно держать себя в руках, но они

наносят не меньший вред. Они черпают свое мракобесие из источников, уже имеющих непосредственное отношение к спецслужбам. Последнее демонстрируется общей теорией тоталитаризма Арент Ханны, содержанием пропутинских групп в социальных сетях и тем, что в 2022 теории заговора — сатанистов, еврейских сект и пр. стали вещаться в России уже с государственных трибун. Мракобесные идеи имеют вирусных характер, следовательно при опасности взрывного распространения Zombie идей в группе необходимом как можно скорее пресекать это распространение, вплоть до удаления Zombie из группы. Иначе группа очень быстро превратится в кружок метафизической борьбы с мировым еврейским\рептилоидов\капиталистическим\ сатанинским заговором, а все адекватные люди из нее уйдут сами.

Zombie-агент ФСБ по определению это скрепоносец, занимающийся защитой или распространением духовных скреп тоталитаризма. Такое распространение духовных скреп почти всегда происходит в процессе мракобесия. Следовательно, Zombie-агент ФСБ это синоним слова мрабес. Существование ментальных вирусов духовных скреп, тем более их экспансия, являющаяся характерной чертой всех тоталитаризмов, не возможны без механизмов их репликации и защиты. Таким образом, мы приходим к выводу, что слова «скрепоносец», «ватник», «мракобес» и «Zombie-агент ФСБ» это все слова синонимы, обозначающие одно и тоже явление.

В противодействии информаторам спецслужб особенно настороженно следует относиться к сторонникам имперского национализма и советской диктатуры. Эти группы идейно близки путинскому фашизму. Они, как и любые другие тоталитаристы бессознательно испытывают между собой и путинским фашизмом симпатию, хотя и могут проявлять значительную агрессию друг к другу на сознательном уровне. Националисты всегда были в разработке спецслужб и наводнены агентами. С настороженностью следует относиться к людям, которые рассказывают, что у них есть друзья или знакомые в силовых органах, особенно в Следственном Комитете или ФСБ. Это как минимум может говорить о тайной симпатии такого человека к тоталитаризму, а может говорить и о том, что этот человек уже сотрудничает со спецслужбами по вашу душу. С большой настороженностью следует относиться к людям, особенно тоталитарных взглядов — коммунистических или националистических, которые не могут внятно и искренне сформулировать, зачем они примкнули к движению.

Информатор спецслужб более чем в половине случаев является также и провокатором — он будет провоцировать группу совершить незаконные действия, чтобы уголовное дело было сшито быстрее, а в работе политической полиции было меньше труда и больше результата.

Другим видом информатора является абсолютно неприметный человек. Это может быть немолодая женщина, о которой потом никто не может вспомнить ничего определенного. Зато в материалах уголовного дела появятся записи всех ваших разговоров. Это демонстрирует, что необходимо выяснять мировоззрение и историю людей в группе. Также это демонстрирует, что вести чувствительные разговоры в присутствии неизвестных вам людей просто глупо и это путь к получению вами «премии Дарвина».

Фатальной и распространенной ошибкой, как и доверение чувствительной информации неизвестным вам людям, является позиция, что все примыкающие к движению люди являются агентами ФСБ. Эта дегенеративная иллюзия является важной частью Всевидящего Ока и должна быть разрушена. Человек захваченный этой опасной иллюзией сам становится Zombie тоталитаризма. Не удивительно, что такую позицию часто можно слышать именно от сторонников тоталитарных националистических идей, которая у них доходит до абсурда, и представляет ни что иное, как «мозговой разжиж». Спецслужбы имеют ограниченные физические возможности для внедрения провокаторов, и если бы оппозиционных групп в России внезапно стало в три раза больше, я уверен, что политическая полиция испытала бы затруднения в наблюдении за ними. Как было отмечено, свободное общество и борьба за него, в принципе не возможны без доверия между людьми. Следовательно обеспечение безопасности от агентов тоталитаризма, накопление знаний в области методов оперативной работы политической полиции, и проверка людей, должны стать ежедневной практикой оппозиции, но ни как не отказ от любой деятельности. В противодействии агентуре ФСБ чрезвычайно полезно правило Бритвы Хэнлона — «никогда не приписывайте злому умыслу то, что можно объяснить человеческой глупостью».

Интересна одна особенность, как Zombie-агенты, они же - распространители скреп, относятся к сообществам в социальных сетях и персонам, пропагандирующим ценность свободы личности, освещающим коррупцию и вопиющий беспредел российской власти, а также освещающим в России достижения Свободного мира. Проводя аналогию, можно сказать, что Zombie агенты относятся к таким сообществам как лейкоциты крови к инородным телам, представляя собой иммунную систему тоталитаризма. Забавным образом, это поведение еще раз оправдывает определение «одноклеточные» в отношении скрепоносцев. Эта иммунная особенность Zombie-агентов может выводить из себя либеральных оппозиционных активистов, приводить к возникновению чувства вины или создавать представление о целом народе, как о неизлечимом. Дело в том, что Zombie-агенты начинают медленно собираться вокруг таких сообществ и на каждую новость о каком либо вопиющем и неоспоримом преступлении российской власти, как и на каждую новость о достижениях Свободного мира начинают произносить заклинания - «во всем виноваты», и далее по выбору: «жиды», «капитализм», «мировой сионизм», «педерасты», «педофилы», «предательство православной веры», «распад СССР», «не соблюдение традиций», «сатанисты», «буржуи», «Горбачев», «Ельцин», «либерасты», «англосаксы», «секта Хабад», «США», «коллективный Запад». Zombie-агенты не только пишут комментарии, но и пишут личные сообщения и письма, зачастую весьма объемные, с таким же содержанием. Тоже самое происходит не только в сети, но и на митингах, собраниях и при личных встречах.

Обладая человеческой эмпатией, хочется выслушать каждого такого Zombie, не удалять его комментарий или что-то ему ответить. В итоге это не приводит ни к чему хорошему. Дело в том, что такие заклинания, иногда представляющие многостраничные сочинения, есть не более чем рефлекторная реакция скрепоносца на разрыв ткани духовных скреп, защищающих его от реальности, точно такая же, как выделение

желудочного сока у собаки Павлова является реакцией на звук колокольчика. Как и выделение облака чернил головоногими моллюсками при поступлении сигнала опасности. Это поведение находится в согласии с ранее упомянутым утверждением, что угроза духовным скрепам для скрепоносца угроза экзистенциальная. Как только скрепоносец распознает в своем информационном поле присутствие угрожающего его миру разрыва духовных скреп, он начинает произносить заклинания, которые должны заделать дыру в тоталитарной иллюзии. Мы уже упоминали, что сознание скрепоносца это по сути первобытно-племенное сознание, не видящее границы между внутренним и внешним миром, для которого практика магии и заклинаний имеет первостепенное значение.

Эта иммунная функция по заделке дыр в ткани тоталитаризма и заставляет скрепоносцев состоять в либеральных группах. Иными словами, группа, пропагандирующая идеи индивидуальной свободы и есть дыра в теле тоталитаризма, а собрание вокруг нее мракобесов, это защитная воспалительная реакция тоталитаризма. Отметим, что репликация и иммунная защита это примитивнейшие механизмы, неотделимые от самого существования жизни и свойственные как одноклеточным организмам, так и духовным скрепам, как ментальному паразиту. Понимание этого должно уберечь вас от эмоционального выгорания, чувства вины, и бесполезной траты времени при столкновении с этим явлением.

Существует еще одна причина отравляющего огромного присутствия тоталитаристов в оппозиции. Как отметил, например, Фридрих Фон Хайерк в его книге «Дорога к рабству», социализм всегда тяготеет к тоталитаризму. В тоже самое время путинская Россия очевидно не является социальным государством. В результате, в российском обществе и в российской оппозиции существует сильный запрос к социализму. Сторонники национал социализма Гитлера, сторонники коммунизма, сторонники восстановления СССР, - все они, почти всегда из популизма, эксплуатируют социальную необустроенность и нищету России. Но в результате своей деятельности они не производят ничего кроме отравления российского общества тоталитарными идеями — советизма, сталинизма, империализма, жидоборчества. Антисоциальность путинского режима, ограбление им России и нищета России, приводят к распространению тоталитарных идей, антидемократических и имперских, парадоксальным на первый взгляд образом, только укрепляя Путинскую власть. В результате путинскй тоталитаризм, да и вообще «загадочная русская душа» описывается, даже не патернализмом государства, а по большому счету все го двумя словами — стокгольмский синдром. Или ассоциация себя с агрессором. Чистая мазохистская любовь россиян к своей власти. Это следует учитывать и очищать оппозицию от тоталитарных элементов, по-сути своей являющихся агентами кремля, которых используют «втемную».

Имитация и фетишизм.

<цитата вырезана цензурой>

Политика это не шутки. В странах с неразвитой демократией субъектов политики часто сажают в тюрьмы и иногда убивают. Убийство Бориса Немцова, отравление Литвиненко, попытка отравления Навального. Стоит ли приводить еще бесчисленные примеры политических убийств в России?

Политическая полиция действует подобно имунной системе, сначала распознавая, а затем уничтожая врагов политического режима. Помните, что самые фатальные для человека болезни, это болезни не распознаваемые имунной системой. Имитируя сопротивление политическому режиму, и коллекционируя у себя дома патроны, боеприпасы, оружие, запрещенные книги и символику, увлекаясь страйкболом, и тем более выкладывая что-либо из этого в социальные сети, обсуждая по незащищенным каналам связи, или в присутствии сомнительных лиц, вместе с декларацией своих оппозиционных взглядов, вы будете распознаны имунной системой тоталитаризма как опасный враг, даже если вы занимаетесь всем этим только для удовлетворения ваших психологических потребностей, а не для достижения какого либо иного результата. То, что выглядит как враг, для политической полиции врагом и является, со всеми вытекающими последствиями. Красной тряпкой в 2022 году для политической полиции в России является украинский флаг, какой бы это мелочью для вас не казалось.

<вырезано цензурой, не принципиально, но может вызвать неприятности>

Не храните ради фетишизма патроны, оружие, и т.п. Не изображайте из себя оппозиционного «Рембо». Не прославляйте насилие. Такое позерство в путинской России плохо для вас закончится.

Одиночка и группа.

Человек, действующий в группе всегда психологически испытывает ложное чувство безопасности. Настоящее групповое действие всегда является более сложным для осуществления и как правило более опасным. Напомним, что политическая полиция в России была сформирована из бывшего управления по борьбе с организованной преступностью (УБОП), т.е. изначально была заточена на борьбу с организованными группами.

Общеизвестно, что остановить деятельность одиночки на порядки труднее, а зачастую практически невозможно. Но такая деятельность редко приобретает большое политическое значение. Остановить деятельность группы из двух-трех человек на порядок труднее, чем группы из десяти человек. Старая народная мудрость гласит: «*Если хочешь идти быстро – иди один. Если хочешь идти далеко – идите вместе*». Вам следует только понять, надо ли вам идти быстро или вам надо идти далеко.

Когда скрытность вредна

Из самого определения тайной политической полиции, данного еще Арендт Ханной, и из принципа «крысы любят темноту» следует, что деятельность тайной политической полиции необходимо максимально предавать общественной огласке.

Весь опыт на протяжении многих лет показывает, что во всех случаях репрессий в отношении вас, в частности при всех следственных действиях и на всех судах необходима максимальная общественная огласка. Необходимо публично называть фамилии следователей, судей, оперативных работников, экспертов и стукачей. На судах необходимо максимальное присутствие слушателей и журналистов в соответствие с антитоталитарным принципом, формально все еще закрепленном в Статье 123 Конституции России- «Разбирательство дел во всех судах открытое».

Весь опыт на протяжении многих лет показывает, что чем больше придается общественной огласке ваше уголовное дело, в частности, чем больше слушателей приходят на судебное заседание, выполняя роль свидетелей репрессии, тем менее суров в итоге приговор. Тем меньше лет вам придется сидеть в тюрьме, или меньше будет штраф, как бы не казалось обратное. Чем больше предается огласке деятельность тайной политической полиции, в частности чем больше официальных жалоб отправляется на нее в прокуратуру, следственный комитет, отдел собственной безопасности МВД, правозащитникам и в иные инстанции, а также чем чаще вы оспариваете в судах ее деятельность, в частности незаконные обыски, тем больше тайная политическая полиция вынуждена держаться в рамках закона, и тем больше походить на обычную полицию, что разрушает саму суть тайной политической полиции. Именно по этой причине вам скорее всего будут поступать угрозы усугубления вашего положения, в случае жалоб и предания вами публичной огласке вашего преследования. Наш опыт показывает, что поддаваться таким угрозам всегда значит совершать серьезную ошибку. Зачастую политическая полиция оставляет в покое скандального человека, который при осуществлении давления на него сразу обращается в СМИ, пишет жалобы и обращается в суд. Разумеется последнее работает хорошо, если вы не совершили преступление, а целью следственных действий в отношении вас являлось просто оказание на вас давления, что и бывает в подавляющем большинстве случаев. Зато к тем, кто помалкивает, политическая полиция периодически ходит домой с обысками как в гости .

Признание вины

Весь опыт политических репрессий в России показывает, что признание своей вины еще никогда никому не помогло, и еще никому не облегчило приговор, а только облегчает работу системы репрессий — следователей и судей.

Цитата: *«Джесси Вашингтон был осуждён за убийство в зале здания суда Уэйко, заполненном пришедшими в ярость местными жителями. Он признал себя виновным, сказав «да, я сделал это» и тихо извинившись, и был быстро приговорён к смертной*

казни. После вынесения приговора он был вытащен из зала суда присутствовавшими там людьми и подвергнут казни прямо перед мэрией в Уэйко. Зверская расправа привлекла более 10 тыс. зрителей, в том числе представителей городских властей и полиции, которые также собрались, чтобы посмотреть на казнь, и не сделали никаких попыток вмешательства, хотя подобные самосуды и были запрещены в Техасе. По сохранившимся описаниям, на данном мероприятии царила праздничная атмосфера, и многие дети пришли на зрелище во время обеденного перерыва в школе. Толпа избила Вашингтона, затем подвесила его на цепи на дереве и развела под ним костёр. Его неоднократно опускали в огонь и через какое-то время поднимали, иногда делая паузы, во время которых отрезали ему пальцы на руках и ногах и кастрировали. Процесс казни продолжался около двух часов, причём палачи сознательно делали всё для того, чтобы продлить его страдания. После того как пожар был потушен, обугленное тело Вашингтона тащили по городу, а некоторые его части были проданы в качестве сувениров. Профессиональный фотограф снимал эти события, в результате чего появились и сохранились для истории редкие фотографии линчевания. Фотографии были напечатаны и позже продавались в Уэйко в качестве почтовых открыток.»

Фото с одной из американских открыток, показывающей тело Джесси Вашингтона после линчевания.

Напутствие

Абсолютной информационной безопасности, как известно, не бывает, но она возрастает пропорционально принятым вами мерам и строгости их соблюдения. Информационная безопасность во многом похожа на соревнование брони и снаряда, известное из военного дела, потому что эта область постоянно развивается. Информационная безопасность является чрезвычайно обширной областью. В этой книге мы не могли не рассмотреть ее, но рассмотрели лишь неопределенный минимум. Информационная безопасность в достаточном объеме вряд ли может быть изучена за короткий промежуток времени, вероятно на это у вас уйдет несколько месяцев. Обширность и сложность этой области часто привод к иллюзии, что компьютерная безопасность в принципе не возможна. Вам следует самостоятельно заняться обучением и совершенствованием в этой важной для практического применения области. Хорошим решением будет изучение документации Whonix и VeraCrypt.