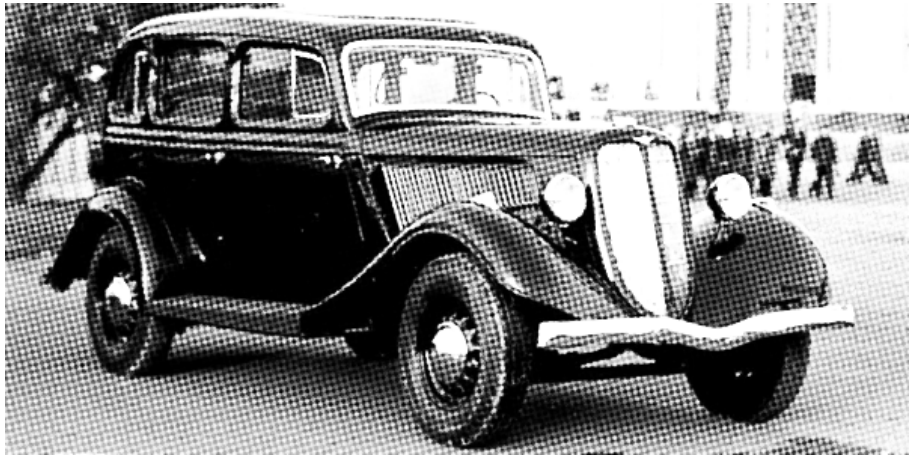
Публикация исчерпывающей инструкции по безопасности, к сожалению, невозможна. Тем не менее, мы совместно с Движением Иркутских Анархист_ок подготовили некоторые правила по информационной и физической безопасности для людей, занимающихся каким-либо активизмом в наше непростое время.

No Trace Project / No trace, no case. A collection of tools to help anarchists and other rebels **understand** the capabilities of their enemies, **undermine** surveillance efforts, and ultimately **act** without getting caught.

Depending on your context, possession of certain documents may be criminalized or attract unwanted attention—be careful about what zines you print and where you store them.

«Чёрный воронок не приедет»



Внимательно следите за действиями ментов и понятых, они могут что-то подкинуть.

- В первую очередь вас постраются лишить средств связи. Необходимо успеть заблокировать телефон до того, как он попадет в руки ментов.
- На все опасные, провокационные вопросы—51 статья и отказ говорить без защитника.
- (*) Спокойно проведите «экскурсию» по квартире, следите за действиями ментов, показывайте содержимое шкафов, тумбочек, ящиков и т.д. Это может помочь избежать агрессии в вашу сторону. Не препятствуйте проведению обыска—мусора уже у вас в квартире. При сопротивлении к вам могут применить силу или устроить полный погром в квартире с открыванием кафеля в ванной.
- (*) Все, что изымают, должно быть описано в соответствующем документе. Что изъято и не описано—украдено и не вернется к вам никогда. Внимательно проверяйте этот список, вносите свои правки, ставьте подпись, когда уверены, что все четко.
- (*) Скорее всего, вас задержат. Сопротивляться нет смысла, только заработаете ст.19.3. (неповиновение сотруднику полиции). Спокойно идите в машину, в участке требуйте звонок, донесите информацию о задержании до правозащитников или тех, кто может с ними связаться.

И помните самое главное о тюрьме:

- Не бойтесь ее.
- Не попадайте в нее.

«Чёрный воронок не приедет»

Original text in Russian

2024

abc38.noblogs.org/чёрный-воронок-не-приедет

Layout

No Trace Project

notrace.how/resources/ru/#chiornyi-voronok

- При осмотрах не жестят, но могут психологически давить, чтобы вы, например, разблокировали устройства.
- Если это обыск и просят разблокировать устройство, зайти в мессенджеры и прочее—отказывайтесь (51 статья, ничего не делать без защитника, забыли пароли—что угодно).
- Не открывайте дверь, если никого не ждете. Если ждете—спрашивайте по имени и смотрите в глазок. Договоритесь об этом с остальными людьми, проживающими в квартире.
- Если за дверью менты, сразу оповестите доверенных людей (товарищей, правозащитников/адвокатов, семью, других людей, проживающих в этой квартире и т.п.—список индивидуальный). Заблокируйте и выключите все устройсва, которые могут вас скомпроментировать.
- Если вы никак ранее не выдали свое присутствие дома, то ведите себя тихо. Возможно, они уйдут сами.
- Если переждать невозможно, то до того, как открыть дверь, попросите содрудника(ов) представиться и предъявить документы через глазок. Все данные фиксируйте (запишите и сразу отправьте доверенным людям, либо можно быть постоянно на звонке с кем-то из них, проговорите вслух, чтобы услышали и записали).
- Для любых дальнейших действий внутри вашего дома у ментов должны быть соответствующие документы. Это может быть осмотр или обыск. Осмотр—добровольное мероприятие, от него можно и нужно отказываться.
- (*) В любом случае, требуйте и читайте документы, которые вам предъявляют. По возможности фотографируйте.
- Если это обыск, то должны присутствовать понятые или видеосъемка. Второе лучше, потому что понятые зачастую подментованы.
- (*) Не позволяйте осуществлять обыск в помещении (например, в другой комнате) без вашего присутствия.

Публикация исчерпывающей инструкции по безопасности, к сожалению, невозможна. Тем не менее, мы совместно с Движением Иркутских Анархист_ок[1] подготовили некоторые правила по информационной и физической безопасности для людей, занимающихся каким-либо активизмом в наше непростое время.

«Сейчас же не 37-й год—что хочешь, то и говори, тем более в интернете, 'чёрный воронок' за тобой завтра не приедет. Чего прятаться-то?», сказал как-то Путин об анонимности в Интернете. Как видим, приезжает с завидной регулярностью.

Подготовка к репрессиям

Чтобы пройти через все испытания достойно, нам нужно к ним готовиться.

Испытывать страх перед обыском, полицейским насилием, тюрьмой—это нормально. Этот страх нужно принять, его можно обсуждать и работать с ним. Но действовать всё же нужно, исходя из своих убеждений и задач.

Спокойно обдумайте свои варианты, свою стратегию. Обсудите, к каким последствиям вы готовы. Задайтесь вопросом: что вам нужно, чтобы быть готовыми?

Желательно это делать в коллективе, если он есть, или с ближайшими друзьями и подругами.

Продолжайте то, что вы делаете, и ищите необходимую поддержку для этого. Если нужно—смените поле деятельности. Можно сменить место и регион жительства.

К задержаниям, обыскам и заключению в СИЗО также нужно готовиться. Вот некоторые шаги, которые можно предпринять заранее:

- Подготовьте своё место проживания—не держите дома ничего, что может хоть как-то использоваться против

[1] https://t.me/anhoirk

вас, вплоть до самых мелочей. Агитационные материалы, вещества, предметы—всё, что может вызвать вопросы, должно храниться в другом месте, не связанным с вами напрямую.

- Установите связь с медиа, и убедитесь, что если на вас хоть как-то будут воздействовать силовики, это будет передано огласке. Постарайтесь, чтобы анархистскому движению и таким группам, как Анархистский Чёрный Крест, Зона Солидарности и другим, была максимальна доступна необходимая информация о вас.
- Найдите себе адвоката или адвокатку, которым вы можете доверять, заключите с ними договор на защиту. Или, по крайней мере, выйдите на связь с правозащитными инициативами, составьте представление о том, к кому вы могли бы обратиться в случае необходимости.
- Ознакомьтесь с правовыми аспектами задержания, обыска, допроса. Знайте то, какие действия силовиков являются законными, а какие нет.
- Подготовьте свои устройства. Убедитесь, что ваши девайсы зашифрованы и храните всё, что может быть интересно силовикам, в зашифрованном виде в хранилищах, доступ к которым есть только через других товарищей и товарищек—желательно за границей. Найдите способ уничтожения информации в случае экстренной ситуации.
- Обговорите различные сценарии на случай ареста со своими близкими, определите планы действий. Задействуйте людей, которые не известны силовикам и не попадут под удар в случае задержания вас или людей из вашего сообщества, и смогут вести необходимую коммуникацию или выполнять другие задачи.
- Подготовьте так называемую «канарейку»: запишите видеообращение на случай ареста. Расскажите на этом видео, что вы ожидаете, что вас будут пытать и принуждать к записи видео, где вы будете отрекаться от анархистского движения и оговаривать себя, зачитывая

Офлайн

- Оглядываться по сторонам: неприметные, но малоприятные люди могут провожать вас домой или в другие места.
- Не открывайте двери никому. Ведите диалог только через дверь, если что, говорите, что родителей дома нет.
- 51 статья Конституции—не свидетельствовать против себя и своих близких.
- Помните о камерах. Особенно если хотите ускользнуть из-под чуткого взора Большого Брата.
- Не пользуйтесь доставкой еды, старайтесь не использовать сервисы такси или вызывать не со своего номера и не на свой адрес.

Обыск, Осмотр, Пришли менты

(То, что отмечено звездочками может быть невозможно осуществить при грубом проведении обысков и задержаний.)

- С теми, с кем живете вместе, можно договориться об условной фразе, которая оповестит, что с вами пришли менты.
- В особых случаях обыск может произойти, когда вас нет дома, но обычно его целью является в т.ч. задержание.
- Старайтесь поддерживать хорошие отношения с соседями, так они могут, например, не открыть подъездную дверь полиции, или, если их позовут в качестве понятых, быть на вашей стороне.
- Основание для обыска—уголовная статья (статус обвиняемого или свидетеля). Осмотр может проводиться у людей, которые даже не имеют процессуального статуса. От осмотра можно отказаться, но мусора не скажут вам этого сами и вряд ли произнесут слово «осмотр», поэтому читайте документы.

зоваться прочими мессенджерами с привязкой номера телефона, если нет возможности делать это с иностранной симкой.

- При звонках через любые мессенджеры лучше отключать P2P или звонить через прокси (Tor, VPN).
- Не пользоваться сервисами ВК-групп (никакими) для каких-либо активистских дел. В крайнем случае делать это анонимно и через Tor.
- Не подписываться своим именем и не ставить свою фотографию ни в каких соцсетях или мессенджерах, а также использовать уникальные никнеймы.
- Хорошие варианты мессенджеров: Element (желательно не на стандартном сервере, используйте, например Disroot),[6] Deltachat.
- Любой даже самый защищенный мессенджер не убережет вас от не надежных людей. Связывайтесь только с проверенными контактами, выработайте свой способ верификации людей.
- Используйте разные аккаунты для разных целей.

Прочее

Выбирайте открытые аналоги программного обеспечения, следите чтобы они проходили аудит (независимую проверку безопасности).

[4] *Примечание от No Trace Project:* Мы рекомендуем использовать Signal, а не Telegram. Все чаты в Signal шифруются сквозным шифрованием, в то время как в чатах Telegram оно не используется по умолчанию, а в групповых чатах не может быть использовано вообще. Кроме того, Signal использует стандартные протоколы шифрования, а Telegram нестандартные, которые в прошлом подвергались серьёзной критике[5] со стороны исследователей безопасности.

[5] https://words.filippo.io/dispatches/telegram-ecdh

[6] *Примечание от No Trace Project:* Мы рекомендуем использовать Signal, а не Element/Matrix. По сравнению с Signal, у Element/Matrix плохая защита метаданных[7] и множество других проблем.[8]

[7] https://anarc.at/blog/2022-06-17-matrix-notes/#metadata-handling

[8] https://telegra.ph/why-not-matrix-08-07

текст, написанный ментами. Объясните, что любые ваши заявления, сделанные на ментовском видео, являются сделанными под давлением, и их нельзя воспринимать всерьёз. Передайте это видео на безопасное хранение, и договоритесь—когда и где это видео будет публиковаться, если с вами что-то произойдёт. Убедитесь, что вы не сможете повлиять на публикацию «канарейки» из-за давления и пыток.

То, чем мы занимаемся—это борьба. Её нужно воспринимать соответственно, и готовиться к вероятности того, что борьбу придётся продолжить в неволе, в неблагоприятных условиях и под сильным давлением.

Устройства

Используйте устройства с безопасными операционными системами.

Для телефона: это GrapheneOS или свежий и обновлённый LineageOS (на момент написания инструкции актуальный LineageOS 20).

Для компьютера: это Tails,[2] Ubuntu 22.04 или 22.10 со всеми обновлениями. Также не стоит ставить приложения не из стандартного репозитория, если вы не уверены в их авторах.

Важно:

- Не пользоваться устройствами побывавшими в руках у полиции.
- Шифровать всё, что можно зашифровать.
- Если нельзя зашифровать—не пользуйтесь этим.
- Пользуйтесь VPN по умолчанию. В настройках VPN заблокировать приложения, соединения которых не идут через VPN.

[2] *Примечание от No Trace Project:* Tails это операционная система, разработанная так, чтобы не оставлять следов на компьютере, где вы её используете. Также она заставляет все ваши интернет-соединения проходить через сеть Tor.

- Используйте TAILS для всего, что требует большей аномнимости, к примеру, использование шифрованной почты, использования крипто-кошельков и хранение файлов, если у вас нет безопасного устройства с безопасной операционной системой.

Помните:

- Если телефон побывал в руках у ментов, то он больше не безопасен.
- Если нет шифрования, то устройство тоже не безопасно.
- Если на устройстве стоит стандартная прошивка—это не безопасно.
- Безопаснее использовать устройства со свежими обновлениями.

Пароли

- Используйте KeePassXC для хранения паролей.[3]
- Стоит их периодически (раз в 1-3 месяца) менять.
- Не используйте один и тот же пароль для разных сервисов.

Браузер

- Открывайте присланные ссылки только через Tor.
- Пользуйтесь Tor для всего, связанного с активисткими делами.
- Не заходите на сайты без шифрования. То есть, выбирайте сайты начинающиеся с «https» а не «http».

[3] *Примечание от No Trace Project:* Вы можете хранить большую часть своих паролей в KeePassXC, чтобы не запоминать их. Они могут быть очень длинными и случайными (например, состоять из 40 случайных символов). Однако вам придется запоминать пароли, которые вы вводите при загрузке зашифрованных устройств. Для них мы рекомендуем использовать пароли Diceware, состоящие не менее чем из 5 слов. Такие пароли можно сгенерировать с помощью KeePassXC (выберите вкладку «Парольная фраза» при генерации пароля).

- По возможности, установите расширения NoScript и DuckDuckGo для того, чтобы блокировать трекеры и скрипты.
- Разделяйте свою деятельность и посещение различных государственных сайтов (или сайтов, близких к государству: Сбербанк, Почта России, Госуслуги). Многие из этих сайтов будут предлагать вам использовать российский сертификат безопасности. Этот сертификат позволит перехватывать ваши данные на других сайтах (даже не российских).
- Для некоторых целей вам может потребоваться заходить на определённые государственные сайты (тот же список законопроектов, к примеру) и для них нужен этот сертификат, но его устанавливать нельзя. Если все же нужно зайти на подобный сайт, то лучше ставьте браузер со встроенным сертификатом и ни в коем случае не используйте его нигде, кроме таких сайтов. Пример браузеров со встроенным российским сертификатом—Яндекс-браузер и Хромиум гост.

Мессенджеры

- Не используйте в Телеграме российский номер, тем более зарегистрированный на вас или ваших близких. Раздобыть «левую симкарту» вы можете с помощью друзей и товарищей, которые сейчас за границей (желательно в «не дружественных странах»).
- Используйте Телеграм только с Tor или надёжным VPN. Как настроить: можете найти в интернете по запросу «настройка прокси Telegram». Вот, например, простая инструкция.
- Выставите в телеграме «Кто видит время моего последнего входа» на «Никто».
- Signal также имеет свои недостатки, которые могут привести к нарушению анонимности.[4] И у него так же, как у Телеграма, исходный код сервера закрыт. Не стоит поль-