Аноним
Уверенность. Отвага. Родство. Доверие
Рецепт культуры безопасности

Скопировано 27 мая 2025 с сайта БОЛЬШЕ ДВУХ дистро.
Оригинал опубликован 5 ноября 2019 на сайте North Shore Counter-Info.

ru.anarchistlibraries.net

Уверенность. Отвага. Родство. Доверие

Рецепт культуры безопасности

Аноним

номности, связности и анонимности, справедливы и по отношению к телеграму (но его критика — задача другого, обстоятельного текста).

Мне бы не хотелось, чтобы живой и ясный текст кроличихи оказался для вас очередной инструкцией, набором пунктов чтобы исполнить — или проигнорировать. Культура безопасности живёт в сообществе, углубляясь в неё, мы обрастаем не столько навыками, сколько привычками — к людям, к действию, к родству.

Сколько хозяек, столько и рецептов. Дерзайте!

Переводческий комментарий

Всё это время в знакомых мне российских контекстах едва ли находилось место для разговора о культуре безопасности: либо её запирали в быту, где она живёт нетронутой, «естественным образом», либо заменяли вопросами цифровой гигиены, ответы на которые всегда заключаются в индивидуальных решениях. Насколько всё же важна для движения информационная безопасность, критическая масса объясняющих её инструкций заслонила проблему, которой озабочены и организационная стратегия и культура безопасности сообществ. От этого (как и от репрессий) страдает совместное воображение: что мы считаем сложным, а что — уже даже невыполнимым.

Зин авторства анонимной крольчихи у вас в руках — не первая попытка запустить отдельный разговор о культуре безопасности на русском: в далёком 2009 московская группа АЧК издала *Руководство по культуре активистской безопасности и противодействию репрессиям*. Центральное место там занимал опыт западных товарищей и товарок начала 2000-х, что, конечно, не умаляет ценности извлечённых уроков. Дополнять и продолжать диалог, вносить в него свежие высказывания — лучшее, что мы теперь можем. Несомненно, этот текст так же требует поправок на времена и нравы.

Первое: держите в уме, насколько наш местный полицейский аппарат предпочитает практику пыток, а также какие дыры, недочёты и огрехи в системах надзора он ею закрывает — материальная основа государственного насилия должна объективно, насколько это возможно, отзываться в ваших моделях оперативной безопасности. Ещё одно замечание: фейсбук — не единственная, а у нас — и не самая популярная среди гнусных цифровых платформ. Практически все претензии к тому, как он вредит авто-

При обсуждении культуры безопасности чаще всего приходится слышать о двух видах опыта: в первом человек отгораживается от окружающих, во втором — сам оказывается объектом подозрений и его/её сбрасывают со счетов. Оба варианта оставляют неприятный осадок: первый порождает страх и подозрительность, второй — отстранённость и обиду. Я убеждена, что это две стороны одной медали, два типа переживаний одной плохо настроенной культуры безопасности.

В своей организационной работе[1] я хочу исходить из доброжелательности и открытости новым лицам. Но также я хочу по мере сил оберегать свою организационную работу от посягательств — в первую очередь, государства, но также боссов и ультраправых. Иными словами, мне нужны правила безопасности, которые приветствуют открытость и не лишают меня понимания, что я взвесила текущие риски и пытаюсь с умом их сократить. Задача культуры безопасности — вести́ к большей открытости, не наоборот.

Перед вами рецепт культуры безопасности, который опирается на практику переосмысления: он позволяет сместить акценты со страха на уверенность, с неприятия риска

[1] *Ориг.* organizing. В русскоязычных контекстах часто не делается различий между активизмом и организацией-как-действием и оба явления передают одним словом. «Активизм», кажется, в большей степени работает с реализацией прав в уже сложившихся властных отношениях, тогда как «организация» — с воплощением в жизнь собственной власти организующихся. Устоявшееся определение до сих пор не вошло в язык, потому описанные мною границы очень условны и служат скорее поводом к дискуссии нежели ответом. Чтобы не ломать язык об колено, здесь и далее в тексте периодически используются логически близкие, но более громоздкие варианты перевода: организационная работа, организующее действие, организация борьбы, самоорганизация. Также: в узком контексте истории синдикализма «organizing» передаётся на русский калькой, «органайзинг». — *Здесь и далее прим.пер.*

на отвагу, с оторванности и разобщённости на родство и с подозрительности — на доверие.

Страх оправдан: государство могуче, его репрессии вошли в норму и оно в силах поломать нас и все наши планы. Но жить в постоянном страхе я отказываюсь. Достоверные сведения и надёжные планы позволят обернуть страх в уверенность — раз наши правила безопасности соизмеримы рискам, с которыми мы сталкиваемся. Учитывая силу наших врагов, трудно представить, как мы вообще сможем приступить к действию, не преобразив собственный страх во что-либо ещё.

Вместо того, чтобы осторожничать, я хочу ставить такие задачи, которые окажутся полезны и уместны и которые отвечают моим принципам и моей оценке ситуации. Надёжная культура безопасности создаёт условия, чтобы сообща проявлять отвагу в тактике действий. Не преобразив практики избегать риска, мы держим себя в рамках установленного порядка, ни на шаг не отступая от спущенных сверху рамок дозволенного протеста.

Цель репрессий — в разобщении людей. Я не хочу, чтобы практики безопасности моих друзей и подруг способствовали нашему разобщению — культура безопасности должна укреплять наше общее родство. Организационная работа будет казаться хлопотной, если мы не преобразим разобщения и не начнём строить связи, которые позволяют разглядеть в нас самих проблески того мира, который мы стремимся воплотить в жизнь.

При встрече с новыми лицами я не хочу питать подозрений — они губительны для пространств совместного сопротивления. Вместо подозрений я хочу задаваться вопросом: «на чём мне выстроить доверие к человеку передо мной?», хочу сближаться с людьми — и оборачивать подозрение в доверие.

потому другой вариант неподотчётного доступа к сети — пользоваться VPN. Анархистки и активистки могут найти бесплатный VPN у *riseup.net*.

Ещё много чего можно предпринять для тех.безопасности, но перечисленные решения помогут закрыть львиную долю. Несколько лет назад на нас нагрянули с обыском — менты изъяли что-то около пятнадцати ноутбуков и телефонов, плюс кучу флешек и жёстких дисков. Один единственный ноутбук из всего списка оказался не зашифрован, оттого что был включенным. Но из всего остального набора техники им не удалось восстановить ни крохи информации. Аналогичным образом, и история звонков и сообщений, доступная от операторов связи, не дала им зацепок, потому как мы пользовались сервисами с оконечным шифрованием, которые скрывают метаданные. Мы не держим связь через соцсети или сервисы гугла, поэтому запросы к владельцам платформ тоже оказались безрезультатными. Перечисленные правила тех.безопасности помогут тем, кто пользуется ими грамотно и на постоянной основе — разница в практике даёт явную разницу в результатах. Они вселяют уверенность, не лишая нас чувства связности, и помогают развить доверие.

Спасибо, что дочли этот текст! На поверку он оказался объёмней, чем я рассчитывала, надеюсь, он вышел содержательным. Я взялась составить его, потому что дельной информации о культуре безопасности — раз, два и обчёлся. Надеюсь, он сподвигнет кого-то из вас проговорить, какие правила помогут руководствоваться духом уверенности, отваги, родства и доверия. Вместо страха перед наступающими врагами давайте сосредоточимся на образе мира, который пытаемся построить. В добрый час!

ной авторизации пользователей на любой чих, что сводит на нет идею анонимного доступа и больше напоминает пиар-ход.

2. Шифруйте хранилища данных. Следует немедля зашифровать память вашего телефона (если только нет осознанной потребности в обратном). В Android есть такая возможность, а у многих айфонов шифрование включено по умолчанию. Для компьютеров, жёстких дисков, флешек и облачных хранилищ я рекомендую *VeraCrypt* — он позволяет создавать зашифрованные «ниши», куда вы сбрасываете нужные файлы. Это, однако, вам не поможет, если устройством завладеют, пока хранилище находится в расшифрованном виде. Если рассчитываете, что вас могут задержать, старайтесь передвигаться между локациями с выключенным (то есть, зашифрованным) телефоном.
   Как правило, шифрование отключается при запуске устройства, поэтому советую обзавестись простым будильником, чтобы иметь возможность выключать на ночь телефоны и компьютеры — в особенности, если над вами нависла угроза обыска. Шифруйте резервные копии данных и храните их в другом месте.

3. По возможности скрывайте свою сетевую идентичность. Ваш IP-адрес известен каждому сайту и сервису, к которым вы обращаетесь, и он же даёт операторам связи и государству связную картину ваших действий, пусть бы вы даже стремились соблюсти приватность (например, пользуясь в браузере режимом инкогнито). Для исследовательских целей я рекомендую пользоваться *Tor*. Как правило, коммерческие соцсети его блокируют (среди исключений Reddit и ещё, по запросу — Twitter)[5], потому другой вариант неподотчётного доступа к сети — пользоваться VPN.

[5] Спустя пять лет с момента публикации этого текста многие коммерческие соцсети открылись трафику Tor, некоторые даже обзавелись специальными *onion*-адресами, но почти все они требуют обязатель-

Чтобы структурировать беседу, стоит поскорей ввести определение культуры безопасности. **Культурой безопасности называют набор правил для оценки рисков, контроля за каналами распространения информации и выстраивания прочных отношений в основе организации.** Вариантов культуры безопасности — бессчётное множество, но все они продиктованы ясными и однозначными обсуждениями существующих рисков и способностью реагировать на перемены. Пример ниже — рассказ о том, как систематическое обсуждение рисков намечает ход дальнейших действий и отражается на методах преследования. Позже я растолкую ряд упомянутых тут практических подходов к культуре безопасности.

> На протестах против строительства трубопровода мы хотели сделать упор на массовых акциях прямого действия на объектах нефтегазовой инфраструктуры. Обозначенные на первых порах риски были невелики — мы наращивали аудиторию среди местных и собирали информацию. Можно было без опаски привлечь к этому делу множество людей и открыто делиться информацией на любой доступной нам платформе. Наши оценки не поменялись с началом символических акций протеста, но эффекту неожиданности пришлось уделять больше внимания, когда мы перешли к планированию акций, где перекрывали дорожное движение и пикетировали отделения полиции. Даже если оставить за скобками вопрос уголовного преследования за подобное, акции просто-напросто потеряли бы в эффективности, знай все о них заранее. Потому мы отказались от средств коммуникации, подверженных слежке, и попросили наших сто-

ронниц и сторонников делиться информацией среди надёжных лиц с серьёзными намерениями.

Едва только начался этот этап протестной кампании, к защите трубопровода подключилась Объединённая следственная группа (JIG) — федеральный полицейский механизм, куда вошли силовые ведомства самых разных уровней. Подобные структуры концентрируют громадные ресурсы, чтобы препятствовать социальной организации, потому они представляют особую угрозу борьбе всякого рода. Пусть на курсе нашей работы это не отразилось, мы всё же вернулись к обсуждению рисков и стали вести планирование в небольшом закрытом кругу, чтобы оградить организаторов акций от уголовного преследования за участие в преступном заговоре. Мы всё ещё могли приглашать к участию тех, кому доверяли, и развивать доверие с другими, например, с помощью проверок личностей друг друга. Вместе с тем, мы решили прекратить строить планы в широком кругу всех, кто готов помогать информировать и привлекать местных. Так мы перешли к этапу блокад критической инфраструктуры. Нам предстояло лишь развить масштаб этого блока организации — подтолкнуть другие группы к таким же формам организующего действия, а работу групп с разных направлений координировать на встречах делегаций.

(Как и у всякой модели организации, у этой, безусловно, есть свои изъяны и преимущества. В мои планы не входит

Адаптацию к новым практикам использования соцсетей можно растянуть во времени: критически оценивая текущие практики, мало-помалу переходить, в первую очередь, на очные встречи и затем уже — на другие платформы. Подлые компании столько лет отнимали значительную часть нашей жизни — ожидаемо, нужно время, чтобы выработать новые устойчивые привычки и подходы к организации.

Напоследок скажу пару слов о технической безопасности. В этой теме достаточно легко увязнуть, она запутанная. Есть, тем не менее, несколько простых решений, которые позволят существенно усилить безопасность данных, — я ограничусь тремя короткими соображениями.

1. Пользуйтесь оконечным шифрованием, где это возможно, кроме, разве что, случаев, когда осознаёте потребность в обратном. Шифрование сообщений — это не всегда просто, но уже достаточно приложений, которые упростили эту технологию до уровня обычной переписки. Я рекомендую *Signal* от Open Whisper Systems[4]. *WhatsApp* использует аналогичный протокол шифрования сообщений, но без защиты метаданных. Их общий недостаток в том, что они не межплатформенные — в отличие от того же PGP, когда всё устроено в виде простых фрагментов текста, которые легко копировать и отправлять электронной почтой, сообщением в соцсети или даже смской. Но в него на порядок сложнее вкатиться, а опыт показывает, что мало кто готов посвятить столько сил техническим нюансам.

[4] На смену OWS пришла НКО-структура под названием Signal Technology Foundation, но для мессенджера и протокола это не меняет сути дела.

ваши странички и аккаунты. Как в этом случае вы можете продолжить вести организацию?

Проблему слежки, надеюсь, никто не возьмётся оспаривать. Всё, что вы сообщаете фейсбуку, навечно попадает в базу данных, к которой у полиции есть постоянный доступ. Приложения фейсбука (и гугла, и прочих) следят за вами и вашими устройствами, а полученные сведения также доступны разведывательным органам. Я не выдвигаю догадок — мои слова подтверждает всё растущее число дел, против активистов и активисток по всей Европе и Северной Америке, которые строятся на подобного рода информации.

Моё предложение относительно соцсетей заключается в следующем: отдавайте приоритет личным встречам, по возможности — регулярным, чтобы наперёд знать дату ближайшего собрания, если связь по сети прервётся. Я бы также предложила, пользуясь соцсетями, задаваться вопросом, есть ли в таком формате острая необходимость, и пытаться перенести беседу на другую площадку. Призываю вас относиться к соцсетям как к рупору, к способу разносить речь, а не как к пространству актового зала, где ведут беседы и ближе узнают друг подругу. Обращайтесь к ним для продвижения идей, анонсов и распространения информации, а беседы переводите в другие места. В нашей собственной организационной работе мы удаляем практически все комментарии со страничек, которые ведём, и уводим большую часть бесед на другие площадки сразу, как получили сообщение. Везде, где возможно, у нас общие аккаунты с минимумом персональных данных. Это лишь один из способов пользоваться преимуществами соцсетей, обходя уйму острых углов. Может быть, вы не захотите лезть в такие дебри, а может быть, наоборот, решите пойти дальше.

выступать за какой-то конкретный способ организовывать борьбу, но, как ни крути, с некоторыми методами я знакома лучше, нежели с другими.)

Прежде чем углубиться в конкретные задумки и порядки, хочу ответить на возражение, типичное для разговоров о культуре безопасности в организации: «Раз я ничего противозаконного не делаю, то и о безопасности мне думать нечего». Суть возражения всегда одна, хотя встречаются и более конкретные формы, допустим, «Раз я ничего деликатного не обсуждаю, то и о слежке мне беспокоиться нечего» или «Раз на таможне меня никогда не останавливают, то и о пачке анархистской литературы в моей машине мне беспокоиться нечего».

Государство ведёт репрессии и борется с организацией, его роль в этом исключительна, а поводам не обязательно быть противозаконными. Сама я провела почти год в тюрьме, два года под домашним арестом и около пяти лет под разными типами надзора. Весь этот срок я отбыла за непримечательные организационные задачи — государство задалось целью ответить на них репрессиями. К восьми месяцам тюрьмы меня приговорили за то, что я координировала собрания, а также сочинила и распространила воззвание организовать шествие в связи с проходившим большим саммитом. Спустя несколько лет меня также приговорили к году лишения свободы за то, что я раздавала листовки с анонсом шествия, а после на том шествии присутствовала. В обоих случаях на демонстрациях были факты уничтожения имущества, но в них меня так и не обвинили. Наоборот, государство решило вцепиться в тех, кто, как и я, занимался рядовой публичной организацией, и выдвинуло обвинения в преступном сговоре. В этом нет ничего необычного — похожим образом складывались и другие дела о преступных сговорах в США и Канаде.

Эти события я пересказываю не затем, чтобы изобразить из себя жертву. Я хочу, чтобы моя организационная работа угрожала власти, и осознаю, что в таком случае столкнусь с преследованиями. Важно тут, что государство решило наказывать за распространение листовок и координацию встреч в пример и в назидание другим. Пусть бы даже это задевало одного человека из ста, нам следует учитывать все случаи, когда мы строим модели безопасности нашей организации. Иначе только и останется что превентивно прекратить все проекты, усвоить репрессивные логики и впредь строить свою работу с позиций трусости и слабости — или ожидать худшего всякий раз, когда государство надевает ежовые рукавицы.

Однако культура безопасности не ограничивается противодействием уголовному преследованию, она также помогает не допускать помех нашим задумкам. Уголовка — исключительная, но далеко не единственная угроза.

Непосредственно в деле, по результатам которого я схлопотала обвинения в преступном сговоре на том большом саммите, были замешаны только двое из 16 внедрённых оперативников JIG. Остальные меняли пароли от аккаунтов и электронной почты, направляли автобусы по неверным адресам, крали наши медикаменты и санитарные средства, тиражировали опасные слухи, чтобы обострять социальные противоречия, и даже пытались подставить подростков на дикой затее с бомбой. Всё это причиняло колоссальный ущерб (вряд ли когда мы сможем его в полной мере оценить), и для этого ментам даже не нужно было привлекать кого-то к суду.

Выше я уже говорила, как важно с точки зрения безопасности сохранять эффект неожиданности. Например, при организации демонстраций в поддержку заключённых: тайная их подготовка позволит рассчитывать на свободу действий и передвижений до момента, когда появится по-

мы принимаем его цензурные ограничения наших мыслей и планов как свои собственные. Вот так заранее складывать лапки значит призывать на свою голову поражение.

Организация на подобных платформах также рискует попасть под шквал враждебных реакций. Нам не под силу управлять общественным мнением о наших действиях — они и не всегда найдут понимание и поддержку, раз уж мы стремимся к миру, стоящему на принципиально иных началах, где нет места капитализму. Гул, следующий по сети за нашумевшими акциями, способен выбить из равновесия. Не так давно ультраправым и массмедиа удалось разогнать волну негативных реакций на антифашистскую сходку в нашем городке, что вылилось в поток угроз и гневных комментариев в соцсети. Антифа в своей организации сильно полагались на фейсбук, а потому столкнулись с выбором: не выходить в сеть, избегая потока угроз, но оказаться отрезанными от товарищей и товарок — либо оставаться в сети и поддерживать связь, но позволить вражде и стрессу сопровождать их беседы. Такие тенденции сказываются на устойчивости организации и позволяют дурной молве фактически застопорить нашу работу.

В более широком смысле это проблема контроля корпораций над социальными платформами. Фейсбук — громадная, состоятельная корпорация, чьи интересы полностью противоречат нашим: что хорошо для нас, губительно для них. Полагаясь на их инфраструктуру, мы вверяем им право заткнуть нас в любой момент и на любом основании. Такого рода компании легко поддаются общественному давлению и, увы, не надо далеко ходить за примерами инициатив, которые навлекли на себя гнев и лишились страничек, а вместе с ними — и связи с костяком своей аудитории. Чересчур полагаться на подобные компании губительно. Задумайтесь, как поступили бы, пропади неожиданно все

вых органайзеров нередко пользуются псевдонимами при контактах с посторонними или разглашают информацию лишь в общих чертах. Кроме того, в таких организациях принято созывать небольшие стачечные комитеты под конкретные задачи, допустим, сбор на демонстрацию, а переговоры — скрывать от посторонних глаз или вести́ их в других каналах связи, не прибегая к помощи соцсетей и списков почтовой рассылки.

Я бы советовала включать развёрнутые обсуждения по темам риска и безопасности в самые разные направления, за которые берутся такого рода организации, потому как на каждом есть свои запросы. Подступиться к этому можно, вверив рабочим группам самим определять внутренние правила безопасности и общие основания для согласия. Также на пользу пойдёт, если привечать личную инициативу в кругу участников и участниц, объединённых схожими взглядами, — это обеспечит орг.структуре достаточную гибкость, чтобы в ней уживались разные виды организующего действия для разного рода занятий.

На деле, отповеди культуре безопасности чаще всего возникают в обсуждениях выгоды от использования соцсетей, среди которых до сих пор самая популярная — это Facebook. В связи с этим, хочу предложить несколько критических замечаний организационной работе с фейсбуком — и как следует поступать крупным организациям, которые зависят от платформы.

Один из решающих аргументов против коммерческих соцсетей — они сокращают пространство возможностей организации. Едва ли можно рассчитывать в соцсетях на бóльшую приватность, чем вам удастся себе обеспечить в проходной отделения полиции. И раз это практически уже ни для кого не секрет, сложились чёткие пределы, какие темы там безопасно и не безопасно затрагивать. Полагаясь на фейсбук в качестве основной площадки организации,

лиция. Другой пример: ячейка ИРМ [*ориг.* IWW, Industrial Workers of the World, Индустриальные Рабочие Мира] организует кампанию против начальства под лозунгом «Требуй заработанного» [*ориг.* reclaim your pay] — им придётся принять меры, чтобы уберечь себя от гражданских исков и внимания вневедомственной охраны. Антифашистам и антифашисткам, что работают над раскрытием личностей ультраправых, предстоит избегать атак на улицах и утечек собственных персональных данных. Наконец, множество частных охранных компаний работает в интересах частного бизнеса и помогает там, где полиция бессильна, — в последние годы они всё чаще противодействуют кампаниям в защиту земель коренных народов.

Вопросы безопасности уже включены в большую часть нашей организации, но, чтобы выстроить культуру безопасности, недостаточно подробно оценивать риски лишь в отдельных случаях, как недостаточно и внедрить чёткие правила собственной безопасности и эффективности наших действий, какие бы задачи перед нами ни встали. Добротная культура безопасности включает всё перечисленное — плюс уделяет внимание прочным связям, укреплению доверия и росту уверенности в собственных силах.

Вот пара базовых принципов культуры безопасности — как я её понимаю.

«Никогда-никогда» — насколько известный принцип, настолько и недостаточный — в самой примитивной форме его можно сформулировать так: «Никогда не болтай о чьём бы то ни было участии в противозаконных действиях. Никогда не болтай о чьём бы то ни было интересе к противозаконным действиям».

Явный недостаток проглядывает в том, что чаще всего мы не влезаем в однозначно противозаконные дела. *Никогда-никогда* стоило бы переосмыслить так: «Никогда не болтай о чьём бы то ни было участии в действиях, за

которые могут преследовать по закону. Никогда не болтай о чьём бы то ни было интересе к действиям, за которые могут преследовать по закону».

Но и этого мало, потому как у нас хватает беспокойств кроме уголовного преследования. Вне зависимости, в какой вы компании, стоит всем взять за правило — не трепать языком о чём угодно противоправном. Это касается и на первый взгляд ерундовых тем — болтовня о нападениях на ментов или имущество безобидна до тех пор, пока не попадает в текст доноса.

Чаще всего подозрения рождаются, когда кто-то склоняет собеседниц к обсуждению противозаконных методов. Чем предполагать: «передо мною мент и меня провоцируют», можно переформулировать проблему так: «Раз нам с этим человеком предстоит сотрудничать, нужно разъяснить ей свою интерпретацию культуры безопасности» — и тут могла бы помочь обновлённая формулировка принципа «*Никогда-никогда*». Она же подчёркивает, что строить теории и догадки об авторстве проведённых анонимных акций — забота не наша, но ментов. Если кто-то спрашивает об анонимной акции, можно намекнуть: неважно, кто её сделал, ведь она говорит сама за себя.

(Другое проявление негодной культуры безопасности, которому уделяют уже меньше внимания, — когда через претензии к культуре безопасности закрепляют пагубные модели властных отношений. Нам однозначно следует друг перед подругой проговаривать свои опасения относительно безопасности, но к этому всегда следует приступать с обоюдного согласия и, по возможности, с глазу на глаз. Расскажите, что узнали, изложите свое видение культуры безопасности, уточните, считает ли собеседница оправданными такие ограничения и будьте готовы услышать возражения. Мы стремимся к единодушию, которое позволит развить спектр совместного организующего действия, а не

Дарби. В тексте *Отчего из мизогинов выходят великолепные доносчики*[3] звучит мысль, что коллектив мог бы уделить больше сил решению ситуации с отвратительным сексистским поведением Дарби ещё до того, как тот пошёл на сотрудничество с ФБР, которое в конечном счёте позволило им поймать нескольких человек. Его случай — крайняя форма, однако же в наших кругах не редкость, когда окружающим в тягость патриархальное поведение со стороны мужчин. У людей могут крепнуть подозрения к тем, кто их так тяготит, но будет ошибкой искать засланных агентов, когда налицо проблема в сексизме. Дать бой деструктивному поведению ценно само по себе, а попутно избавиться от доносчиков вроде Дарби — станет приятным плюсом.

Теперь обратимся к **организациям с широким составом и официальным статусом**. Такого рода организации со скрипом вступают в разговор о культуре безопасности, потому как тяготеют к совсем другим формам организующего действия, которым едва ли свойственны подобные дискуссии. В их случае идея культуры безопасности больше походит на расплывчатую критику всего их принципа организации нежели на план, как её укрепить. Часть перечисленных мной правил, вероятно, не подойдёт официальным организациям с широким составом, но я убеждена, что все основные принципы на них распространяются. Более того, в них уже найдутся действующие правила безопасности — такой организации только нужно присмотреться, как она функционирует.

Например, в подразделениях ИРМ вполне обычное явление — тайно браться за организацию профсоюзных кампаний на предприятии. Вовлечённые в поддержку цехо-

[3] *Why Misogynists Make Great Informants*, текст Кортни Моррис, впервые опубликован в 2010 году в седьмом выпуске журнала *make/shift*, выдержал множество перепечаток и несколько зин-изданий от разных коллективов.

Всем, кто хоть немного времени провёл в активистских кругах, не составит труда продолжить список пагубных тенденций.

Как я уже говорила в разделе о тонкостях проверки личности, полиция и спецслужбы всё чётче распознают зоны, скрытые от обзора, которые возникают при сложностях в обращении с пагубными тенденциями и проявлениями угнетения в нашей среде. Я приводила в пример полицейскую, которая изображала жертву насилия, чтобы пробраться в чужие жизни, — её удалось подселиться соседкой к кому-то в квартиру. Был и другой случай с внедрённым агентом: полицейскому (темнокожему парню средних лет) долго удавалось переводить стрелки: любое замечание в свой адрес, что он смущает людей (в частности, нарушает правило «*Никогда-Никогда*»), он отвергал как проявления расизма. Он смог выйти на группу антирасистских активисток из другого района, чтобы заручиться их поддержкой, — и таким образом отбиться от череды попыток изгнать его из пространств организации. Его показания в итоге легли в дело, по которому шесть человек получили реальные сроки. Он, разумеется, сталкивался в наших кругах с расизмом. Это — вкупе с тем, как бесстыдно он пользовался антирасистскими убеждениями в своих целях, — должно послужить поводом нам оценить слабые стороны своих антирасистских позиций. Подобный фарс сработает с меньшей вероятностью, имей мы чёткую позицию по расовому, гендерному или любому другому типу угнетения (в том смысле, что каждой и каждому не сложно будет детально объяснить своё видение проблематики) и способы вплотную подойти к их решению.

Поводов человеку оказаться ненадёжным предостаточно — равно как и проявлений хищнических повадок кроме тайной работы на полицию. «А не мент ли передо мной?» — не самый насущный вопрос. Примером тому Брендон

затыкать и не стыдить людей (и уж тем более — не строить из себя отпетых радикалов). Одно из крайних проявлений пагубных тенденций — ложные обвинения в стукачестве [*ориг.* snitch-jacketing]. Эта тактика сыграла роль в ослаблении революционных движений 70-х, потому как обвинения обычно оборачиваются серьёзными последствиями. Другой пример — когда кто-то «бывалый» затыкает прочих участниц группы за разговоры об акциях, которые их вдохновляют, или за их «порочные» связи.)

Ещё один принцип: **отдавайте предпочтение личным встречам**. Вне зависимости, насколько надёжна ваша платформа коммуникации, крепкие доверительные отношения и взвешенные решения рождаются, когда мы находим время для личных встреч. Технические средства связи чаще порождают недопонимания, делают слежку легче, а сама возможность коммуникации оказывается заложницей решений и ошибок компаний с другого конца планеты. Каждый случай виртуального общения в вашей организации должен вызывать вопрос: подменяет ли это общение вживую? Если так, есть ли в этом нужда? Попробуйте сократить зависимость от таких форм в пользу личного присутствия. (Техническую сторону вопроса мы рассмотрим чуть позже…)

Встречаются возражения, что социально тревожным людям проще было бы общаться при помощи цифровых устройств. Для других препятствием станет невозможность передвигаться физически. Таким деликатным вопросам, которые возникают во время настройки культуры безопасности, стоит уделять отдельное внимание и предметно изучать варианты, как приспособиться к озвученным потребностям, сохраняя уклон на личные встречи. Всё же технологии эти достаточно новые и у людей с очень разными физическими ограничениями

есть долгий опыт поиска союзниц для организации совместного действия.

Репрессии неизбежны — нецелесообразно пытаться уйти от них любой ценой. Всякая борьба, развейся она достаточно бурно, окажется борьбой с ментами, этими поборниками выпавшего на нашу долю миропорядка. Держа в уме потребность избежать репрессий любой ценой, мы соглашаемся использовать только санкционированные полицией формы сопротивления, что фактически лишает нас возможности собрать достаточно сил, чтобы добиться коренных изменений. Тем же, кто отказывается от этих ограничений, следует быть готовым столкнуться с репрессиями.

Один из способов подготовиться — с самого начала сосредоточить организационную работу на полиции и тюрьмах. С этой целью можно перенимать опыт антирасистского движения, которое, даже когда вовлекалось в самый широкий круг проблем, всегда понимало насильственный и расистский характер этих структур. Сформировавшееся движение уже не впадает в ступор от полицейского насилия и трезво смотрит на тюрьмы, что идёт нам в преимущество. Можно не останавливаться на достигнутом и внедрить практики солидарности в собственную организационную работу. Кто занят организацией трудящихся — обращайте внимание на борьбу за трудовые права в других контекстах и ищите дельные способы показать солидарность с репрессированными. Кто ведёт организационную работу в квир-среде — ищите и поддерживайте квирных заключённых, это поможет вам сориентироваться в тюрьмах в вашем регионе, когда и если потребуется. Заинтересованным в защите земель и борьбе за среду обитания следует знать, что по всему континенту защитникам и защитницам земли, заключённым и под обвинением, грозит физическое насилие со стороны государства. Практики со-

вшит принцип служебной необходимости [*ориг.* need-to-know], когда только вовлечённые лица посвящены в детали и знают круг соратниц (если только последние сами не посчитают правильным кому-то раскрыться).

Подобную гибкость можно привнести и в другие организационные модели. Главное — уважать личную инициативу, не требуя, например, согласовывать каждую затею с какой-то руководящей инстанцией (что случается как в группах с уставом и строгим порядком принятия решений, так и в вольно устроенных активистских группах — как негласное правило). Не менее важно уважать свободу объединений — когда в порядке вещей работать закрытыми малыми группами, параллельно участвуя в широких открытых организациях. Формально это можно воплотить через организацию комитетов или рабочих групп с правом устанавливать собственные стандарты участия. Другие возможности: перенимать отдельные принципы организации аффинити-групп или однозначно проговаривать, какую информацию распространять по принципу служебной необходимости.

И, наконец, **упредительные обсуждения пагубных тенденций**. И сами по себе они — хорошая привычка, однако их вклад в безопасность так важен, что не грех сопровождать ими каждый разговор о культуре безопасности. Есть немало тенденций, что подрывают общее доверие и осложняют организацию — например, травля или деспотичное поведение, свойственное патриархату и культуре белого превосходства. В этот же список можно добавить: сосредоточение в одних руках связей и ресурсов (что позволяет возглавлять проекты лишь определённому кругу лиц), беспочвенные наезды, хвастовство и негодные практики безопасности (например, когда кто-то расспрашивает о чьей бы то ни было причастности к противозаконным акциям, тем самым нарушая принцип «*Никогда-Никогда*»).

штриховая — относительное доверие, пунктирная — что вы слабо знакомы. Такое совместное упражнение позволит подсветить тенденции в коллективе и выделить, над чем ещё предстоит потрудиться, чтобы развить доверие.

Может открыться, что лишь один-единственный участник в крепких отношениях со всеми, а между остальными сложилось сильно меньше родства. Следовательно, чтобы группа стала жизнеспособней, предстоит устранить такой дисбаланс — на случай, если того участника возьмут под арест, он заболеет или выгорит. Это же добавит группе равноправия, поскольку возможность протолкнуть инициативу напрямую зависит от объёма доверия окружающих к инициатору. По результатам упражнения может также оказаться, что к кому-то из участников никто не выработал доверия. Это указывает на необходимость ближе с ним познакомиться и поискать почву для доверия.

Среди внедрённых агентов сложилась практика — прибившись к одному сообществу, сыпать потом именами оттуда в других местах. Круги доверия и поручительство прекрасно от этого защищают. Однако, круги доверия — это не просто способ выявлять противников, но и отличная мотивация укреплять сети, превращая как можно большее число пунктиров в сплошные линии.

Гибкость орг.структуры — это свойство организации подстраиваться под потребности самых разных видов деятельности. Метод, который закрывает именно эту потребность, — организация в неформальные сети и аффинити-группы. Участников неформальной сети (то есть, не имеющей устойчивых очертаний) связывают идеи, а аффинити-групп — уже конкретные проекты или взаимное желание затеять таковой вместе с теми, с кем находишь общий язык. Преимущество в том, как легко приступать к проектам разной степени риска, потому что под каждый есть свои правила культуры безопасности. Сюда же по умолчанию

лидарности со всеми ними, включённые в вашу работу, послужат источником вдохновения для изобретательного и смелого сопротивления.

Ещё одно преимущество тут в том, что вам также ответят солидарностью. Тюрьмы — места потрясающего сплочения, где сходятся множество видов борьбы с господством и угнетением. Оберегать друг подругу на порядок легче, погрузившись в среду сопротивления, которая деятельно заявляет о своей солидарности перед лицом репрессий. И снова замечу, что достоверная информация — наше оружие в борьбе со страхом: чем больше нам известно об устройстве полиции и тюрем, тем скорее мы можем переменить страх на готовность и уверенность.

Учитывая всё изложенное, давайте разберём подробнее, **из чего состоит оценка рисков**. Главное — вести её открыто, систематически, и находить варианты эффективных действий, которые соответствуют вашим целям и которым эта оценка поможет воплотиться в жизнь. Достаточно легко выработать отвращение к риску и стать самим себе надзорной инстанцией похлеще, чем могло бы нам устроить государство. Ясность по вопросу рисков позволит вам сосредоточить усилия на собственных возможностях и отваге.

Принимаясь планировать демонстрацию, подумайте, какой она примет характер. Ожидаете, что всё пройдёт мирно и без происшествий — или выйдет безудержно и агрессивно? Если полиция перейдёт в оцепление, вы подчинитесь или попробуете прорваться? Какие действия, сопряженные с повышенным риском преследования (помимо самого факта выхода на улицу), вам приятно будет там увидеть? Битые окна, исписанные стены или, может быть, что-то пустяковое, вроде расклейки стикеров. Если вас лишат эффекта неожиданности, что грозит вашим планам? Кому их не стоит раскрывать? Как привлечь желанных лю-

дей, чтобы не пронюхали нежелательные? Чётко изложив своё видение характера акции, вы позволите остальным приспособить к ней самостоятельные планы.

Насколько при этом важно удерживаться от самонадеянности, показывает ситуация из 2018:

> Организаторы анархистской книжной ярмарки решили вечером после мероприятия собраться на марш. Другим сторонам организации они уделили гораздо больше сил и не потрудились оценить риски, связанные с маршем, потому что за плечами у них был опыт организации сотен демонстраций. Между тем, марш оказался на порядок агрессивнее прочих, с кучей случаев уничтоженного имущества. Они не проговорили явным образом риски и не нашли времени оценить ситуацию накануне. Они также не учли, что полиции выделили на них дополнительные ресурсы в рамках работы JIG при саммите G7, который проводили тем летом в соседней провинции. Вышло так, что их правила безопасности в преддверии событий оказались не приспособлены к уровню риска получившейся акции, и всех организаторов ярмарки по итогу обвинили в преступном сговоре.

Это пример крайнего случая, но неожиданные повороты событий — вообще-то обычное дело (что чаще всего нам на руку, поскольку никому не под силу спланировать повстанческую ситуацию[2] от и до). С меньшей вероятностью нас застанут врасплох, если в привычку войдёт оценивать

[2] С большой долей вероятности, отсылка к «революционной ситуации» Ленина с поправкой на инсуррекционизм. *См.* «Вооруженная радость».

веку по одному лишь предположению, что вас связывают знакомства, или по каким-то несущественным причинам — допустим, они соответствуют каким-то субкультурным нормам или в них видят носителей определённой идентичности.

Пример, как может выглядеть поручительство: «Мы знакомы уже пять лет, плотно сотрудничали на общественных проектах, я могу положиться на них в непростых обстоятельствах. Мы как-то устроили ужин дома у их отца, а ещё я регулярно подвожу их после работы». Или так: «Встретила её в том году на публичном мероприятии об изменениях климата и мы с тех пор регулярно видимся на всяком экологическом движе. Довелось обсудить много проблем, и я от неё в восторге. Знаю, что она хочет набраться опыта на организации акций, и думаю, отлично у нас впишется».

При обсуждении, почему вы доверяете человеку, всё же можно пренебречь принципом открытости, чтобы не нарушить правило «*Никогда-Никогда*». Принимать в свои ряды новых участниц или знакомить разные команды — это всегда щепетильная ситуация, если вы заняты организацией тайных операций, и причины для беспокойства там свои. Пользоваться поручительствами всё ещё желательно, но не стоит разговорами о прошлых акциях накручивать другим риски. Раз такие операции требуют прочной основы для доверия между сообщницами, допустимо принять поручительство и при этом не вдаваться в подробности отдельных действий.

Круги доверия главным образом впишутся в организацию неформальных сетей и аффинити-групп (на чём, к слову, строится почти весь мой организационный опыт). Речь идёт о том, чтобы, выписав по кругу имена участников вашей сети, строить между ними линии разного типа, которые описывают отношения: допустим, сплошная показывает крепкое родство с большим запасом доверия,

относительно поддержки пострадавших. Неловкость при встрече со сложными и болезненными темами порождает слепые зоны, в которых легко спрятаться тем, кто хочет нам вреда. Нужно не избегать таких хитросплетений, но искать в себе смелость распутывать их.

Подруга с опытом проверки личностей добавила к этому: в отдельных случаях уместно попридержать взаимность — когда есть повод не позволить человеку диктовать, в какой форме пройдёт проверка. Она также заметила, что в отличие от агентов под прикрытием это едва ли поможет со стукачами, которые ни за кого себя не выдают, а просто руководствуются скверными мотивами. Кроме того, вам стоит заранее чётко определиться с порядком действий на случай, если собеседник не пойдёт навстречу или даст вам повод сомневаться в себе.

Поручительство — один из подходов к привлечению новичков в существующие группы и пространства организации. Как и во всех прочих разобранных нами подходах, его потенциал раскроется, если пользоваться им открыто и на регулярной основе. Предварительное условие — заложить основу доверия между участницами группы. Быть может, в качестве основы достаточно схожих политических воззрений и возможности положиться на человека. А возможно, потребуется узнать, что он или она именно те, за кого себя выдают, имеют за плечами подходящий опыт организации, не расколются, если их возьмут в оборот, и спокойно относятся к акциям определённого типа. Как бы оно ни было, поручительство устроено следующим образом: один или несколько участников представляют новичка и явно проговаривают, что он или она отвечает основным принципам доверия. От каждого и каждой из присутствующих требуется в ясной форме принять или отклонить представленное поручительство. Подобная однозначность предотвращает риск слепо довериться чело-

степени риска, а сократить вред нам позволят надёжные и доступные правила безопасности. Добросовестная информационная безопасность, успешная маскировка, устоявшиеся традиции деятельной солидарности и отказа от сотрудничества с полицией, а также упорство — всё это позволило в тот раз сократить урон от непредвиденной ситуации, потому народ держал хвост пистолетом, пока всё не кончилось.

Ещё один пример: развитие какой-либо массовой организации — допустим, антифашистского движения. Какие вопросы, связанные с риском, станут на повестку, прежде чем вы приступите к сколько-нибудь серьёзному подбору сторонников? Чтобы добиться поставленных целей, какую степень доверия внутри организации стоит считать достаточной? Допустим, мы рискуем впустить в наши ряды агента полиции — тогда имеет смысл установить, что мы именно те, за кого себя выдаём. А если нас беспокоит возможность внедрения в организацию ультраправых, залогом доверия станет понимание убеждений друг подруги (укреплять его можно по ходу постепенной эскалации действия). И того и другого проще добиться, если отдавать в организации приоритет очной активности над онлайновой.

Если мы намереваемся развивать уличный фронт, разговор о безопасности коснётся тем дисциплины и планирования. Когда ситуация накаляется, чего мы ждём друг от подруги? Сложно оправдать ожидания, если они расплывчаты, и, наоборот, проще поступить по уму, когда вы заручились чётким планом действий и понимаете, работает он или нет. На вашей защищённости на улицах сильно скажется, какие привычки вы в своей организации выработаете относительно того, что считать достойным внимания вашей группы. Это отдельная от культуры безопасности тема, но у них много общего. Например, сходки антифашистов

и антифашисток связаны с риском нарваться на превосходящие силы противника, попасть в засаду или растерять один другую, зацепить слежку и быть опознанными ультраправыми или ментами, получить лишних травм или свинтиться.

Вот несколько правил для массовых сходок, которые снизят риски: порог значимости события (число участников и участниц, меньше которого акция либо отменяется, либо переходит к запасному плану, где требуется значительно меньше усилий), план отхода (когда вы покините позиции, как сообщите об этом остальным, где расстанетесь, как уйдёте от слежки и как узнаете, что остальные тоже в безопасности), точки сбора (откуда народ уже сообща выдвигается на место акции), адекватные уличные тактики (например, строй в две шеренги с дополняющими обязанностями между ними), простые и ясные правила связи (как переговариваться на улицах, брать ли с собой мобильники, какими именами пользоваться), плановые поверки (как убедиться, что все в безопасности, и как собраться для подведения итогов и поддержки тех, кому она нужна).

Испытанных в поле правил культуры безопасности великое множество — я не претендую на полноту. С большей охотой поделюсь здесь теми, что оказались нам полезны: это проверки личности, поручительства, круги доверия, гибкие орг.структуры и упредительные обсуждения пагубных тенденций.

Проверку личности проводят, чтобы установить, что человек именно тот или та, за кого себя выдает. В примере с трубопроводом нам потребовалось укрепить доверие и коллективную мощь в среде организаторов, когда мы решили сделать упор на прямом действии. Регулярное обсуждение рисков позволило понять, что в нашем случае непригодны те же практики безопасности, которыми мы

руководствуемся на протестах, митингах, временных сквотах или образовательных мероприятиях. Поскольку нас тревожила возможность внедрения агентов, мы решили проверять личности друг дружки. Выглядит это так: допустим, я вытащила человека попить кофе и, не предупреждая загодя, показала ему своё удостоверение личности и, например, семейное фото или школьный альбом. Затем я говорю, что стремлюсь заручиться доверием в его глазах, потому что хочу сообща с ним браться за более рискованные затеи. Мы обсуждаем, чем он мог бы поделиться со мной в ответ. Иногда я прошу позвонить на громкой связи кому-то из членов семьи или коллеге по работе, чтобы услышать от них какие-то подробности жизни или рабочих моментов. Порой можно обойтись одним удостоверением личности. Также можно зайти друг к другу домой. Принципиально важна как можно бóльшая взаимность (что не всегда просто на деле, раз кто-то должен проявить инициативу) и сосредоточенность на развитии доверия.

Нет смысла затевать проверку личности с теми, кому вы не доверяете или с кем вам будет некомфортно пойти на дело, как бы хорошо они ни справились. Не идёт речи о поиске ментов — мы лишь пытаемся упрочнить доверие и уверенность, так что такого рода проверки должны служить признаком уважения друг к дружке.

Сложности тут могут возникнуть по уйме причин. Например, у мигрантов может не оказаться как типовых документов, так и семьи поблизости. Нередко квир- и транслюди не пользуются именем по паспорту, и делиться им или старыми фотографиями им не с руки. Но подобные обстоятельства нужно, конечно же, учитывать и приспосабливаться к ним, а не делать из них повод избежать сближения. Был у нас случай, когда полицейская под прикрытием выдавала себя за жертву абьюзивных отношений и обрывала всякий разговор о её прошлом, пользуясь нашей позицией