ОВД-Инфо

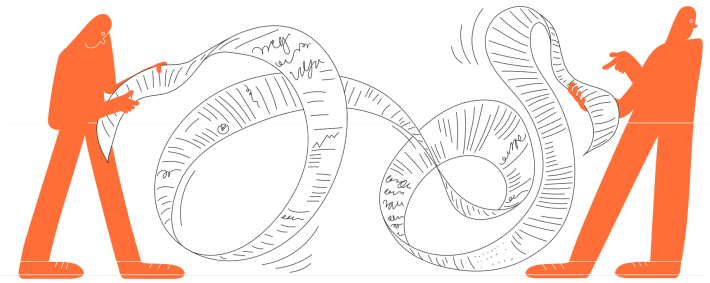
Гайд по общей безопасности для участников исследований

Основные положения по цифровой и общей безопасности

Введение

Насколько безопасно поучаствовать в соцопросе или дать интервью исследователю? А если они иностранцы, иноагенты или «нежелательные»? В этом гайде мы собрали основные положения по цифровой и общей безопасности, которые пригодятся в этом случае.

Если вам предлагают поучаствовать в исследовании и вы хотели бы понять свои риски и решить, стоит ли соглашаться, пишите нам в бот или на почту data@ovdinfo.org.



Оценка и минимизация ризков

Сотрудничество с организациями и физлицами, повышающее риск политического давления

Российское государство часто присваивает «неудобным» людям и организациям статусы, чтобы усложнить их работу. Это влияет и на людей, которые с ними взаимодействуют.
Многие правозащитные организации, независимые СМИ и люди, занимающиеся правозащитой, журналистикой и активизмом, признаны «иностранными агентами» — в том числе «ОВД-Инфо». Это касается и исследователей: например, иноагентами признаны Центр независимых социологических исследований и Лаборатория социальных наук. Существуют также статусы нежелательной и экстремистской организации: они подразумевают еще большие ограничения прав и свобод.

Иноагенты. Что касается иноагентов, то формально этот статус присваивается тем людям и организациям, которые «занимаются политической деятельностью» и при этом «получают иностранное финансирование» (подробнее об этом можно прочитать в материале

Фонда защиты прав СМИ). Если вы планируете сотрудничать с людьми и организациями-«иноагентами» (например, привлекать их в качестве респондентов, коллег по исследованию, подрядчиков или помощников в распространении результатов исследования или наоборот, участвовать в проводимых ими исследованиях), важно заранее продумать свою стратегию. Если вы планируете получать оплату за участие в исследовании от таких лиц и организаций либо от зарубежных организаций вообще, вы тоже оказываетесь в зоне риска «иноагентства». Если вы хотели бы избежать получения статуса, то финансирование лучше производить через третьи лица и организации либо в криптовалюте (об этом см. ниже).

Если деньги за участие в исследовании вы не получаете, то по закону такое сотрудничество ничем не грозит, и если вы не публичное лицо (и не собираетесь им становиться) и до этого не привлекали внимание правоохранительных органов, риски минимальны. При этом нужно быть готовым к тому, что если ваше участие будет публичным, то и вы «попадете на радар» к правоохранителям, что увеличит для вас и риски «иноагентства», и иные риски. То же самое касается репостов материалов, созданных «иноагентами», подписки и донатов: ответственности нет, но как будет на деле, мы не знаем. Так, журналистки Ольга Чуракова и Соня Гройсман формально получили «иноагентский статус» за репосты других «иноагентов», но, скорее всего, реальная причина была в их собственной работе.

Если хотите перестраховаться, не пишите о работе с «иноагентами» публично и в соцсетях. Если вы принимаете участие в исследовании организации-иноагента, также отказывайтесь от упоминания своих персональных данных в тексте. Вы всегда можете попросить людей, с которыми вы сотрудничаете, не упоминать ваше имя публично и не указывать вас в документах — вам должны пойти навстречу.

Нежелательные и экстремистские организации. Некоторые СМИ и проекты признаны «нежелательными» и «экстремистскими»; подробнее о том, как работает «нежелательность», читайте в нашей памятке. Здесь риски выше — их работа запрещена в РФ и за сотрудничество с ними грозит административная или уголовная ответственность. Мы не рекомендуем публично писать о сотрудничестве с такими проектами. Уточните у представителей этих организаций правила безопасности и четко следуйте им. Давать таким проектам интервью и писать для них статьи публично не стоит: нужно настаивать на анонимизации.

Если вы – гражданин РФ и находитесь на территории Евросоюза либо другой безопасной для пребывания стране, где рисков задержания и лишения свободы нет, осторожность тоже не помешает — например, вас могут оштрафовать на крупную сумму. Подробнее о взаимодействии с «иноагентами», «нежелательными» и «экстремистскими» организациями вы можете прочитать в наших карточках.

Криптовалюта для участников исследования

Если вы планируете получать оплату за свое участие, то есть несколько способов получать деньги от зарубежных организаций, а также от организаций и людей с негативным статусом («иноагентским», «нежелательным», «экстремистским»), которые можно назвать относительно безопасными. Вот они: оплата наличными, в криптовалюте (но не в любой!) и через стороннего человека или организацию, которые находятся на территории России и не попали на радары силовиков.

Оплата наличными – наиболее безопасный вариант, однако для этого получателю необходимо выехать за рубеж (например, в Грузию). Кроме того, в разных странах существуют разные ограничения на ввоз и вывоз валюты. Другая относительно надежная альтернатива – попросить исследовательскую организацию перечислить вам оплату не напрямую, а от российских юридических лиц (например, коммерческих), либо с карты частных лиц.

В случае, когда по тем или иным причинам другие способы оплаты недоступны, можно попробовать получать деньги в криптовалюте. На момент июня 2024 года у криптовалюты «серый» правовой статус в России: купить товары или услуги официально за «крипту» нельзя, но инвестирование на бирже криптовалют приравнивается разрешено (см. Федеральный закон от 31.07.2020 г. № 259-ФЗ). Поэтому покупка рублей за счет ваших активов в криптовалюте в России на данный момент законна; в будущем это может измениться.

Важно помнить, что сама по себе покупка, например, биткоина отправителем, перевод на кошелек получателя и последующая покупка рублей получателем не являются анонимными действиями: источник и назначение платежа можно отследить, и ФСБ это уже делали (см. дело о госизмене за донат ВСУ). Для того, чтобы анонимизировать ваши криптовалютные операции, необходимо использовать полностью анонимную валюту; на данный момент нам

известно лишь одна такая, и это Monero.

Вот алгоритм по анонимному получению криптовалюты «для чайников»:

- Завести любой удобный вам и отправителю «неанонимный» криптокошелёк – например, Trustee Wallet. Регистрация не должна требовать ваших паспортных данных; если требует почту – лучше указать специально созданную почту.
- Попросить отправителя купить удобной вам криптовалюты (например, привязанной к курсу доллара USDC ERC20), воспользовавшись какой-либо онлайн-площадкой. Для российских карт можно найти продавца, например, на бирже BestChange.ru.
- Получить на свой кошелёк оплату в криптовалюте (важно: если валюта работает на базе валюты Ethereum – «эфирах», то до того, как получить отправление, вам тоже понадобится купить немного «эфиров»).
- Установить программу Monero GUI Wallet с официального сайта Monero. Во время инсталляции выбрать «Простой режим bootstrap» и завести кошелёк Monero – он будет полностью анонимным.
- В своём «неанонимном» кошельке купить валюту Monero и переслать её на свой анонимный кошелёк.
- С кошелька Monero вывести деньги на свою банковскую карту или на оффлайн-банкомат снова через BestChange.ru.

Чтобы вас было труднее вычислить: базовая цифровая безопасность

Для того, чтобы ваши данные не утекли к силовикам, нужно, чтобы и вы, и исследователи, с которыми вы связываетесь, пользовались правилами цифровой безопасности. ОВД-Инфо составили памятку по цифровой безопасности для исследователей (ССЫЛКА), попросите тех, кто к вам обратился, подтвердить, что следуют её рекомендациям и защищают полученные от вас данные.

Если вас просят о проведении интервью онлайн, лучше всего воспользоваться для связи Telegram, Signal, WhatsApp, Google Meets и другими подобными мессенджерами; через VK, сервисы Яндекса и по мобильной связи с российской sim-карты лучше не рассказывать ничего сенситивного. Скройте номера телефонов в мессенджерах (доступно в Telegram и Signal), в настройках включите ретрансляцию звонков (Telegram: “P2P звонки — никогда”, в Signal и WhatsApp это так и называется — “ретрансляция звонков”). Если вам не повезет

созвониться с недоброжелателем с сильными техническими навыками — при включенном VPN и ретрансляции звонков он не сможет выяснить ваше местоположение. Также установите таймеры автоудаления на особенно чувствительные чаты.

Если вам требуется совершить звонок на номер мобильного телефона, помните, что звонок не будет приватным, так как проходит через сотовые вышки. Ничего опасного для вас в таком звонке обсуждать нельзя.
Мы всем рекомендуем отказаться от использования российских браузеров — они могут отслеживать каждое ваше действие в интернете. Также стоит избавиться от российских программ, которые имеют широкий доступ к вашей системе, например Алиса. Вам не обязательно постоянно работать в неудобных браузерах вроде Tor, вы вполне можете заменить Яндекс на Chrome или Firefox.

Основы безопасного хранения, передачи и удаления данных.

- Это понятие никак не расшифровывается, поэтому невозможно понять заранее, какие виды отношений с людьми или организациями за пределами России могут привести к статусу «иностранного агента».
- Все аккаунты для облачного хранения должны быть защищены сложным паролем и вторым фактором, а устройства и внешние диски зашифрованы, тогда хранение данных и файлов на них станет надежным. Если уж совсем трудно дается шифрование флешек и других носителей, старайтесь хранить файлы только в облаке не на российском сервисе и работать с ними там же.
- Если особенно сильно переживаете за конкретные файлы или папки, их можно отдельно зашифровать перед выгрузкой в облако — есть программы, которые не позволят расшифровать конкретный файл без пароля (если это звучит сложно, то посмотрите 5-минутное видео от Теплицы).
- Делитесь файлами и документами, давая к ним доступ в облаке. Доступ нужно предоставлять только по электронной почте, так как передача файла по ссылке делает ваш документ или файл общедоступным.
- Информация, попадающая на ваш компьютер или внешний носитель, никогда не исчезает с него бесследно, ее можно восстановить, если носитель не был зашифрован до того, как туда попали файлы. Это делается не чтобы навредить вам, просто современные диски стараются делать устойчивыми к износу. Если у вас есть файлы и документы, которые ни в коем случае никогда не должны найти на вашем устройстве, не удаляйте их обычным

способом. Воспользуйтесь программой Eraser (для Windows). Программа перезапишет нужные вам файлы случайными данными, и восстановить их станет невозможно. С macOS всё сложнее, надежные программы для такой перезаписи найти трудно. Опять же, хранение и работа с документами в облаке избавит вас от такой проблемы.

Если вы специалист по цифровой и правовой безопасности, этики проведения исследований во время войны, либо обладаете опытом исследовательской работы в современных российских условиях и обнаружили в этом тексте неточность – обязательно напишите нам на data@ovdinfo.org.