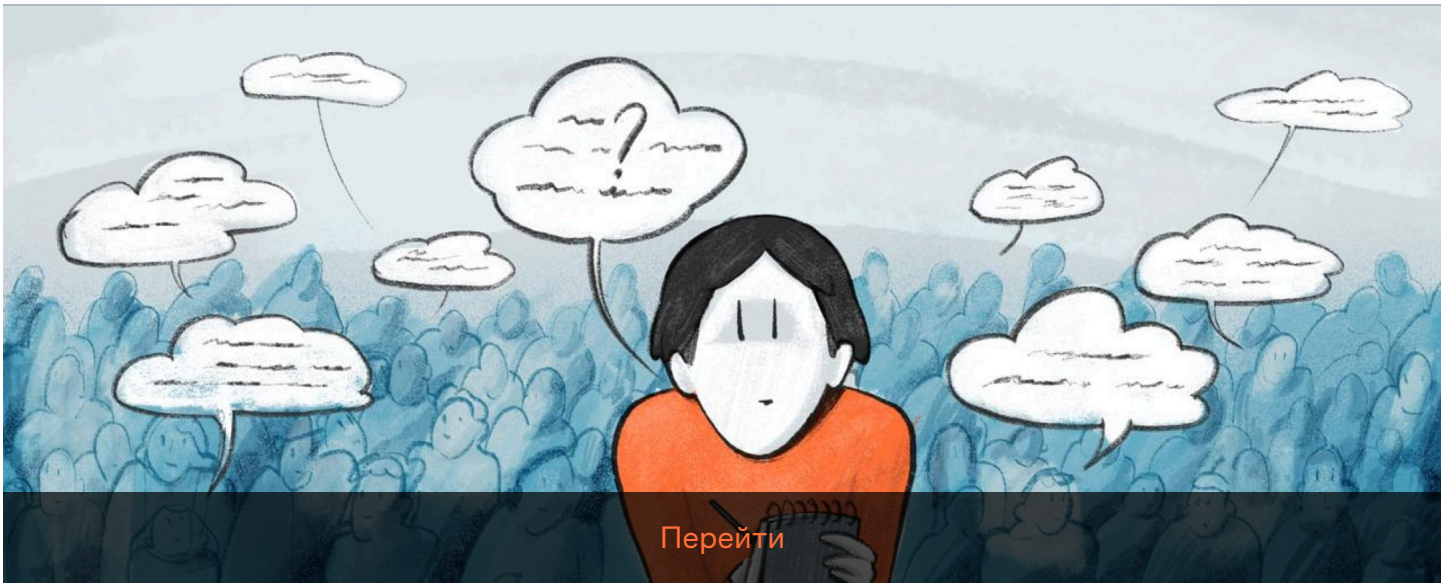


Иллюстрация: Настя Голикова для ОВД-Инфо

11.07.2024

# Памятка исследователям, работающим с российскими респондентами

English version

Аналитики ОВД-Инфо подготовили «Этический кодекс» для исследователей в области общественных наук, чьё поле находится в России. Здесь мы описали основные риски и сложности, с которыми можно столкнуться при проведении исследования такого исследования. Особое внимание мы уделяем безопасностью исследователя и респондента.
Если вы хотели бы провести исследование с участием российских респондентов с помощью этого гайда и нуждаетесь в дополнительной юридической, технической и этической поддержке ОВД-Инфо, заполните форму, и мы вам обязательно поможем.

## ЭТИЧЕСКИЕ РЕКОМЕНДАЦИИ

Большинство этических рекомендаций актуальны для любого поля, однако в России есть отдельная специфика:

во-первых, в России нет единой этической комиссии, которая бы утверждала дизайны исследований, а во-вторых, война и репрессии добавляют новые вызовы. Ниже мы сформулировали принципы, которыми руководствуемся сами.

1 Принцип добросовестности.

**1.1** «Не навреди» (non-maleficence). Исследование не должно быть направлено против конкретных людей, групп людей или общества в целом. При этом исследование может быть направлено на борьбу с социальной проблемой; риски для людей и групп людей в этом случае должны быть оправданы, минимизированы и уравновешены общественной полезностью (см. пункт 2).

**1.2** Less is more. Сбор данных респондентов должен быть обоснован; до сбора данных респондентов, следует изучить все существующие публикации и уже собранные массивы данных. Если данные респондентов собраны, они должны быть обработаны и использованы.

**1.3** Стандарты работы. Исследование должно быть выполнено в соответствии с международными методологическими стандартами и настолько качественно, насколько позволяют обстоятельства и возможности исследователей.

**1.4** Публичность. Где возможно, исследователи должны делать процесс сбора и анализа данных исследования прозрачным, а результаты и данные — публичными.

**1.5** Устойчивость. Исследователи не должны своими действиями закрывать доступ к респондентам для других исследователей или приводить к потере доверия к исследованиям в целом.

**1.6** Рефлексивность. Исследователи должны осознавать невозможность полной исследовательской нейтральности и принимать все усилия к эксплицитному выявлению и рефлексии собственных политических и гражданских позиций. Дискуссия в исследовательской команде и учитывание этих особенностей при планировании, проведении и презентации результатов исследования обязательны.

**2** Принцип полезности. Исследование должно приносить пользу исследуемой группе людей или обществу в целом.

**2.1** Под полезностью понимается защита и поддержка прав и свобод, в том числе права на информацию, восстановление правовой, социальной и исторической справедливости, повышение качества жизни и другие схожие цели.

**2.2** Gaze. Поскольку исследования общества не нейтральны и в центр исследовательской картины будут так или иначе поставлены те или иные люди или группы людей, исследователи должны по возможности давать голос наиболее уязвимым, маргинализованным, плохо представленным в общественной дискуссии людям и группам людей.

3. Принцип соблюдения прав. Исследование должно уважать и поддерживать права, свободы и человеческое достоинство респондентов.

**3.1** Несоблюдение прав респондента может принимать различные формы, в том числе:

**3.1.1** Прямое нанесение вреда здоровью респондента, в том числе, психологическому (в частности, через ретравматизацию)

**3.1.2** Раскрытие либо утечка персональных и сенситивных данных респондента, в том числе данных о самом участии в исследовании, приведшие к:

**3.1.2.1** Нанесению вреда здоровью респондента со стороны третьих лиц

**3.1.2.2** Политическому преследованию со стороны российского политического режима (инициирование или усиление репрессий)

**3.1.2.3** Потере миграционных, социальных и других прав и привилегий (как в России, так и за рубежом)

**3.1.2.4** Потере положения, трудоустройства, профессиональной либо личной репутации, материального капитала, ухудшению условий жизни

**3.1.2.5** Приобретению негативных, стигматизирующих статусов, ухудшению социального положения

**3.2** Чтобы избежать нанесения вреда респондентам и себе, исследователи должны:

**3.2.1** Где возможно, получать и фиксировать (письменно или под запись) информированное согласие респондента на сбор данных. Согласие должно быть получена в том числе на то, что сбор проходит именно таким образом (с аудио/видеозаписью, расшифровкой сторонними лицами, др).

**3.2.2** Пользоваться только безопасными локациями для встреч оффлайн, устойчивыми к взломам каналами и средствами связи, а также защищенными местами хранения и анализа информации; не хранить персональные данные респондента в одном хранилище с собранными сенситивными данными; разграничивать данные респондентов с личными данными исследователя; использовать для респондентов псевдонимы, и другие средства защиты данных.

**3.2.3** Не передавать данные респондентов третьим лицам. В случае, если для проведения интервью заключается договор с подрядчиком, нуждающимся в доступе к данным (интервьюером, расшифровщиком, редактором и проч.), данные необходимо выдавать в минимально возможном наборе и с соблюдением анонимности (т.е. не сообщая персональных данных респондента). Передача контактов третьим лицам допустима только с разрешения участника. Ответственность за верификацию благонадежности подрядчика целиком лежит на исследователях.

**3.2.4** Публиковать данные о респонденте исключительно в анонимизированном, обобщенном виде. Все данные, доступные публично, в том числе — цитаты, фотографии, артефакты и проч. — очищать от персональных данных либо таких данных, которые позволяют легко установить личность респондента (например, по участию в громкой медийной истории, проживанию в малом населенном пункте, редкому заболеванию и проч.).

**3.2.5** Заботиться о собственной цифровой, физической безопасности и психологической готовности работать с респондентами-членами несвободного общества, в особенности уязвимыми, пережившими насилие и проч. О способах заботы о себе см. ниже.

**3.3** В случае, когда участие в исследовании влечет за собой риски, описанные в пункте 3а., исследователи обязаны предупредить о них респондентов заранее (в случае с респондентами младше 14 лет — их родителей или опекунов).

**3.4** В случае нанесения вреда респондентам, исследователи, а также аффилированные с ними институции, несут за него полную моральную ответственность.

4 Равноценность прозрачность вашего исследования и будущей доступности данных для других исследователей. В некоторых ситуациях сообщение респондентам, что вы проводите исследование, может привести к потере их доверия и невозможности собрать данные — например, если вы проводите этнографический анализ в российских госструктурах. В этом случае исследователям необходимо взвесить такие аспекты:

**4.1** Важность информированного согласия. Везде, где это возможно, и всегда в случаях интервьюирования или опрашивания, а также сбора личных данных, как оффлайн, так и онлайн, перед сбором данных исследователь должен создать для респондента безопасное пространство и проинформировать (в случае с респондентами младше 14 лет — их родителей или опекунов):

**4.1.1** О цели исследования, о причинах рекрутинга на данное исследование данного респондента.

**4.1.2** О тематике вопросов интервью или опроса, и о возможности отказаться от ответов на тот или иной вопрос, прервать разговор или перенести его на другое время, в другой формат или другую локацию.

**4.1.3** О возможности отказаться от участия в исследовании на любом его этапе вплоть до публикации.

**4.1.4** О ведении фото/видео/аудио/письменной фиксации разговора, если они ведутся.

**4.1.5** О том, в каком виде будут использованы полученные данные.

**4.2** Доступ к данным. В случаях, когда общественная польза от проведения исследования особенно высока и в условиях низкой доступности данных в России, допустимо проведение включенного наблюдения, как онлайн, так и оффлайн, без предварительного согласования, особенно если такое согласование несет риски для исследователя или респондентов. При этом недопустим сбор персональных или сенситивных данных.

**4.3** Решение о приоритетности прозрачности либо доступа к данным принимается в каждом случае индивидуально, и за последствия несут ответственность исследователи и аффилированные с ними организации. Исследователи должны, где возможно, обсуждать такие решения коллегиально и аргументировать их.

## ЧТОБЫ ВАС БЫЛО ТРУДНЕЕ ВЫЧИСЛИТЬ: БАЗОВАЯ ЦИФРОВАЯ БЕЗОПАСНОСТЬ

1. Каждый аккаунт, который вы используете (личный или рабочий) должен быть защищен, даже если кажется, что он не слишком важен. Ваши переписки и файлы не должны попасть к силовикам, а соцсети и и аккаунты в государственных сервисах — к злоумышленникам.

**1.1** Пароли во всех ваших аккаунтах должны быть уникальные и длинные. Заведите парольный менеджер, сгенерируйте там пароли из случайных 16 символов и смените их во всех аккаунтах, которыми пользуетесь (полезно будет сначала вообще составить список всех аккаунтов, которые у вас есть: электронные почты, соцсети, телеграм, госуслуги, рабочие сервисы, даже неважные и неиспользуемые аккаунты). Вам не нужно знать эти пароли наизусть, их всегда можно скопировать из менеджера паролей. Мы можем посоветовать Bitwarden.

**1.2** Знать наизусть, как правило, необходимо всего два пароля: от парольного менеджера и от компьютера. 16 случайных символов запомнить очень тяжело, поэтому вы можете использовать парольные фразы.

**1.3** В каждом аккаунте должен быть второй фактор, вы можете найти его в настройках конкретного аккаунта. SMS — это не надежно, поэтому вместо него или в дополнение к нему используйте приложение для двухфакторной аутентификации. Мы советуем 2FAS, оно надежное и простое, попробуйте привязать к нему один аккаунт, и вы поймете, насколько это легко. Исключение составляют только мессенджеры, например, Telegram и WhatsApp — в них первым фактором является проверочный код, а вторым — облачный пароль (в Telegram) или PIN-код (в WhatsApp и Signal).

**1.4** 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.

**1.5** Постарайтесь минимизировать использование российских аккаунтов для работы — если связались с респондентом в VK, пригласите его общаться дальше в Signal или Telegram. Аккаунт в Яндексе — для доставок и такси, а для общения и хранения документов — Google.

**1.6** Если вам требуется совершить звонок на номер мобильного телефона, помните, что он не может быть приватным никаким способом, так как проходит через сотовые вышки. Ничего опасного для вас или респондента в таком звонке обсуждать нельзя. Если нужно просто скрыть номер от человека, которому звоните, воспользуйтесь любым сервисом IP-телефонии или Skype.

2 После аккаунтов важно защитить ваши устройства как от перехвата данных при подключении к интернету, так и для случаев, когда компьютер или телефон оказался в недобрых руках:

**2.1** Обновляйте все, что можно обновить: системы телефона и компьютера, программы и приложения. Злоумышленники (в том числе государственные) постоянно ищут новые пути для взлома, а разработчики постоянно стараются защитить от этого свои продукты. Новые меры безопасности приходят с каждым обновлением, вам нужно только их устанавливать.

**2.2** VPN шифрует данные, которые вы отправляете во время подключения к сети, а без VPN поставщик вашего интернета видит многое из того, что вы делаете в сети. Использование VPN в России все еще законно, незаконно только размещать о них информацию в открытом доступе. Старайтесь держать VPN включенным всегда, мы рекомендуем сервисы из списка vpnlove.me

**2.3** Установите короткое время блокировки экрана компьютера и смените простой пароль на парольную фразу. На телефоне также установите короткое время блокировки и код для разблокировки не короче 6 цифр. На многие приложения дополнительно можно установить пин-коды как на телефоне, так и на компьютере, например, в Telegram и Signal.

**2.4** Проверьте, нет ли в ваших устройствах российских сертификатов, при помощи которых можно перехватить и расшифровать то, что вы делаете в интернете. Здесь есть инструкция для macOS, на этой же странице в Notion можно найти инструкции для любой системы телефона или компьютера. Если сертификат Минцифры необходим вам (например, для использования электронной цифровой подписи), то лучше иметь отдельное устройство для таких манипуляций (либо отдельный браузер, но без сертификата в системе может работать не все, что вам нужно).

**2.5** Включите шифрование своего устройства. В современных телефонах шифрование, как правило, включено по умолчанию, а для компьютеров требуются специальные программы. В macOS есть встроенная программа FileVault, в Windows 10 и 11 Pro — BitLocker, в Linux — LUKS, а для Windows версий Home подойдет VeraCrypt. Шифрование — дело непростое, поэтому поглядите пошаговые инструкции здесь.

**2.6** Включите антивирусную программу на вашем компьютере. Встроенные программы не хуже платных, поэтому можно смело включать Firewall в macOS или Защитника Windows. Если вы хотите установить дополнительную антивирусную программу, присмотритесь к McAfee, Norton, Avast и Bitdefender. Но ни в коем случае не используйте российские антивирусные программы, такие как Касперский и Dr. Web.

**2.7** Откажитесь 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.

3 Основы безопасного хранения, передачи и удаления данных.

**3.1** 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.

**3.2** 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).

**3.3** 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**.

**3.4** 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.

**4** Программы для обработки данных.

**4.1** Программы для кодировки, которым можно доверять — **Atlas.ti**, **NVivo** (прозрачные политики безопасности, не сотрудничают с Россией), Taguette (работает локально и не собирает ваши данные), Qualcoder (создана энтузиастами, нет открытой политики безопасности, но разработчики охотно отвечают всем интересующимся).

**4.2** Вам может требоваться разное количество программ или онлайн-сервисов для разных целей, и каждую из них нельзя проверить и записать сюда. Перед использованием какой-либо утилиты ознакомьтесь с ее privacy policy, поищите там информацию о том, в зоне какого законодательства находится компания и ее сервера. Если нет России и стран СНГ — можно пользоваться. Если не получается найти нужную информацию, попробуйте связаться с разработчиком по контактным данным, представленным на сайте сервиса/программы.

## РАБОТА С ДЕНЬГАМИ

Во время проведения исследования может понадобиться работать с деньгами: например, если ваше исследование финансирует какой-то фонд или вам самим нужно перевести оплату за участие в исследовании вашим информантам. Есть несколько способов получения финансирования от зарубежных организаций, а также от организаций и людей с негативным статусом («иноагентским», «нежелательным», «экстремистским»), которые можно назвать относительно безопасными для получателя. 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); если речь идёт об оплачиваемом участии в исследовании, такой способ недоступен. Кроме того, в разных странах существуют разные ограничения на ввоз и вывоз валюты. Другая относительно надежная альтернатива — оплачивать услуги исследователей и респондентов, находящихся в России, через российские юридические лица (например, коммерческие), либо с карты частных лиц. Однако в этом случае проблема сдвигается дальше: как перевести деньги на счета этих финансовых «прослоек», если это нужно сделать из-за рубежа?

В случае, когда по тем или иным причинам другие способы оплаты недоступны, можно попробовать переводить 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»:
1. 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.

2. 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.

3. 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»).
4. Установить программу Monero GUI Wallet с официального сайта Monero. Во время инсталляции выбрать «Простой режим bootstrap» и завести кошелёк Monero — он будет полностью анонимным.
5. В своём «неанонимном» кошельке купить валюту Monero и переслать её на свой анонимный кошелёк.

6. С кошелька Monero вывести деньги на свою банковскую карту или на оффлайн-банкомат снова через BestChange.ru.

## ЕСЛИ ВЫ ПРИВЛЕКЛИ ВНИМАНИЕ СИЛОВИКОВ

Например, если вы исследуете «экстремистов», и теперь вас тоже хотят сделать экстремистом, либо если вы приняли участие в исследовании «нежелательной организации».

**Допрос**

Если вас вызвали на допрос — то вам будет присвоен процессуальный статус. Это ваша роль в уголовном деле — процессуальный статус определяет ваши права. Статус указывается в повестке. Если там указан один статус (например, «свидетель»), а вы приходите и вам говорят, что статус изменился (например, на «подозреваемого»), требуйте направления новой повестки, а также присутствия вашего адвоката.
Не соглашайтесь на адвоката, назначенного следователем.

## Допрос свидетеля

С одной стороны статус «свидетеля» наиболее безобидный, по сравнению с другими. С другой стороны при этом статусе меньше процессуальных прав и он может очень быстро поменяться. Помните, что любое слово может быть использовано против вас, а после допроса в статусе свидетеля можно перейти в статус подозреваемого.

Как правило, в начале допроса следователь устанавливает вашу личность: вы должны будете предоставить свой паспорт или иной документ, удостоверяющий личность. Следователь будет задавать вопросы, чтобы внести ваши анкетные данные в Протокол допроса (ФИО, адрес регистрации, место работы, др.). Ответить на эти вопросы надо.

Вам должны сообщить, по какому поводу и в каком статусе вас вызвали.

Следователь обязан разъяснить ваши права свидетеля по статье 56 УПК РФ. После этого Вам надо будет расписаться в соответствующей части протокола.

После этого начнутся вопросы по существу дела.
Главное — помнить, что вы не обязаны свидетельствовать против себя (**статья 51 Конституции)**

Старайтесь отвечать коротко, обдуманно и спокойно. Только на тот вопрос который был задан. Чего нельзя делать:

Не стоит рассказывать следователям историю своей жизни и пытаться «все объяснить»;

Нельзя отказаться от дачи показаний совсем. За это предусмотрена уголовная ответственность.

Однако, отвечая на вопросы следователя вы можете **применительно к каждому конкретному вопросу**:

- что-то забыть или не знать — можете спокойно так и ответить (не помню/не знаю).
- Пользоваться 51 статьей Конституции, если считаете, что ваши ответы могут вам навредить.
- Если вас спрашивают о ваших политических убеждениях, вы вправе отказаться со ссылкой на ч. 3 ст. 29 Конституции: «*Никто не может быть принужден к выражению своих мнений и убеждений*».

Нельзя противоречить себе и отрицать уже признанные в других делах факты, категорически нельзя говорить неправду, это моментально обнаружится и дальше допрос может пойти в непредсказуемом русле. Во всяком случае, любые ответы после этого будут восприниматься следователем критически.

По окончании допроса Вам дадут ознакомиться с протоколом. Внимательно прочитайте, попросите исправить недочеты/некорректно записанные ответы. Если следователь отказывается исправить протокол, напишите об этом в своих замечаниях к протоколу. Изложите в них кратко, о чем вы говорили на самом деле. Попросите следователя перечеркнуть все незаполненные строки, чтобы туда ничего не могли вписать постфактум, но сами этого не делайте.

В протоколе допроса может быть подобный пункт: «Я уведомлен и согласен с тем, что могу быть извещен о вызове для судебного разбирательства путем СМС-сообщения». Вы вправе согласиться на СМС-уведомление, но гораздо лучше, если все уведомления вам будут отправлять по почте.

**Только после этого подписывайте протокол.**

## Допрос подозреваемого/обвиняемого

Статус подозреваемого, разумеется, опаснее статуса свидетеля, однако (и именно поэтому) он дает вам больше процессуальных прав.

Допрос в статусе подозреваемого и обвиняемого должен обязательно происходить в присутствии адвоката. Очень важно являться на допрос исключительно со своим или правозащитным адвокатом — и не соглашаться на адвоката, назначенного государством. К сожалению, такие адвокаты не всегда действуют добросовестно и в интересах подзащитного.

Какие дополнительные права есть у **подозреваемого**:

- вы имеете право позвонить адвокату и быть допрошенным в присутствии адвоката. Поэтому если вы считаете, что можете стать фигурантом уголовного дела, то заранее заключите соглашение с адвокатом.
- вам должны обеспечить возможность конфиденциального разговора с адвокатом на срок не менее чем два часа.
- вы можете отказаться отвечать на вопросы следователя — это не повлечет за собой уголовного преследования (ч.2 ст. 46 УПК). Если вы в статусе подозреваемого Вы вправе общаться со следователями только в присутствии адвоката.

У **обвиняемого** есть все те же права. Кроме того, обвиняемый имеет право знакомиться со всеми материалами следственных действий по окончанию предварительного расследования.

**Обыск**

Как правило с обысками приходят около шести утра. По закону все следственные действия запрещены в ночное время с 22 до 6 утра (ч.3 ст. 164 УПК), кроме неотложных.

Если вам стучат в дверь рано утром полицейские, **не открывайте сразу дверь**! Сначала спросите их о причине визита. В случае, если они скажут, что пришли с обыском — попросите показать в глазок постановление об обыске. Скажите, что звоните своему адвокату и откроете полицейским дверь, как только приедет защитник. Учтите, что в постановлении об обыске должен быть указан номер дела и ваш адрес — если этого нет или адрес неверный, вы вправе не открывать. Но есть риск, что дверь могут выпилить при помощи болгарки.

Обязательно сообщите о происходящем родственникам и друзьям.

Вы имеет право только на один телефонный звонок — поэтому выучите наизусть или номер, адвоката или номер близкого человека, который сможет передать информацию и найти защитника.

Важно, что сейчас силовики стали приходить на обыски с государственным адвокатом по назначению. Надо требовать именно своего адвоката, так как адвокаты по назначению часто действуют в интересах полицейских и следователей.

## Ваши права при обыске

- пользоваться помощью адвоката;
- присутствовать при обыске;
- следить за действиями участников обыска;
- не свидетельствовать против себя и своих близких: это право вам дано статьей 51 Конституции РФ;
- ни в коем случае не  сообщать следователю пароли от компьютеров и мобильных устройств, а также почтовых сервисов, мессенджеров и соцсетей: это право тоже дано вам статьей 51 Конституции РФ;
- требовать неразглашения обнаруженных во время обыска подробностей вашей частной жизни, личной и семейной тайны;
- потребовать предъявления предметов, которые хотят изъять и внесения их в протокол;
- занести замечания в протокол;
- получить копию протокола обыска.

Помните, что Вы вправе ознакомиться с постановлением о производстве обыска, если нет возможности его сфотографировать, вы вправе его переписать.

По результатам обыска составляется протокол. Внимательно прочитайте протокол и укажите все возможные нарушения/злоупотребления со стороны следователей. В протоколе должны быть указаны:

- Дата и время начала и окончания обыска.
- Имена всех лиц, присутствующих при обыске.
- Описан ход обыска.
- Указан перечень изъятых предметов — требуйте описать вещи максимально подробно (не «коробка вещей», а список, модели и номера электронных устройств).
- Все пустые поля должны быть перечеркнуты.

**Указывайте ВСЕ замечания**. Особенно если во время обыска «нашли» что-то, чего у вас не было. Вы можете записывать замечания настолько долго, насколько вам нужно. Если замечания приложены на отдельном листе — укажите это в протоколе и кратко опишите.

Будьте готовы к тому, что вас задержат после обыска. Соберите минимально необходимые вещи (предметы первой необходимости), сообщите друзьям / родственникам и адвокату, куда вас везут.

## Советы при обыске

- Приготовьте блокнот/ежедневник, куда будете все записывать и ручку.
- Если адвокат не сможет прибыть лично — держите связь с адвокатом по телефону. Важно, что это должен быть **«пустой» телефон, не содержащий важной информации, потому что в какой-то момент его могут изъять следователи.**
- Если адвоката не допускают — сообщите об этом всем участникам обыска и позже внесите информацию в протокол.
- Не пытайтесь препятствовать проникновению следственной группы. Это может стать основанием для возбуждения в отношении вас уголовного дела.
- Перед началом обыска следователь должен представиться, сообщить, с каким уголовным делом связаны следственные действия, показать постановления и разъяснить вам ваши права.
- Перед обыском вам предложат добровольно выдать запрещенные предметы и/или информацию, необходимую следователю. Вы не обязаны это делать в соответствии со ст. 51 Конституции. Вы вправе выдать, но стоит помнить, что Вашу судьбу это не облегчит — не будет являться смягчающим обстоятельством. Поэтому подумайте прежде чем что-то отдавать.
- Обыск проводится в присутствии двух понятых. Запишите имена понятых, уточните у них, совпадают ли указанные ими адреса с адресами их проживания.

- Старайтесь контролировать действия следователей: по возможности требуйте чтобы обыск производился в разных помещениях поочередно. Все замечания записывайте в блокнот, после внесите их в протокол. Среди замечаний может быть грубость, неуважительное отношение к вашей собственности — что-то сломали/разбили, и тд. особенно, если следователи вошли в какую-то комнату или открыли какой-то ящик без вас, обязательно напишите это.

Что делать с устройствами с точки зрения цифровой безопасности до, после и во время обыска, можно прочитать тут.

## ДОСТУП К ГОСУДАРСТВЕННОЙ ТАЙНЕ, НАХОЖДЕНИЕ НА РЕЖИМНЫХ И ОПАСНЫХ ОБЪЕКТАХ

Что делать, если вы решили собирать информацию о режимных или опасные объектах — скажем, постройку дворца Путина или военного завода?

1. Для поиска информации в интернете используйте VPN и Tor-браузер, именно в таком порядке. Сначала включите VPN, он зашифрует и спрячет ваши данные от интернет-провайдера, затем запустите браузер Tor, который обеспечит максимум конфиденциальности при посещении нужных сайтов.

2. Во время такого поиска полностью откажитесь от использования аккаунтов в российских сервисах (VK, yandex и других), даже если это упростит работу, любой логин может вас деанонимизировать.

Если вы хотите физически посетить такое место:

**1** Когда мы говорим об опасных местах, в которых в принципе лучше не появляться, идеально — идти без устройств, подключающихся к мобильной сети (камеры и устройства для записи звука — ок).

**1.1** Если оставить свой телефон далеко от места невозможно, можно озадачиться запасным, но это трудный и ненадежный вариант: если ваш запасной и основной телефон находятся рядом, то они идентифицируются как устройства, принадлежащие одному человеку, то есть запасной телефон должен храниться где-то вне дома и работы, а такое место есть не у всех. Выключение запасного телефона не решает проблему.

**1.2** Неплохим вариантом может стать «клетка Фарадея» — специальный чехол для телефона, не пропускающий сигнал. Убрать телефон в такой чехол нужно сильно заранее до места и не открывать, пока не окажетесь в более безопасном пространстве. Купить «клетку Фарадея» можно в любом маркетплейсе, а проверить — просто убрав туда телефон дома и совершив звонок с другого. Если клетка работает, то дозвониться будет нельзя.

**2** Если вы идете в место, где появляться законно, но нужно сдавать устройство на входе в камеру хранения (госучреждения или режимные объекты вроде СИЗО), следует комплексно настроить безопасность телефона (об этом будет в следующих разделах). Отдельная важная настройка для таких ситуаций — **отключение управления заблокированным устройством при помощи USB**. Есть открытые инструкции по этой настройке для Android и iOS.

3. Также для похода в любое место, где телефон могут забрать на хранение или изъять, заведите отдельную учетную запись в своем телефоне (Apple ID или Google), чтобы можно было выйти из основной и не переживать за пароли, приложение второго фактора и другие данные.

4. Если вы сделали фото или видеозаписи на месте, то до передачи их кому-либо или выгрузки в облако стоит избавиться от метаданных. Хорошими вариантами программ для удаления метаданных являются ExifCleaner (на любой компьютер), Metapho (для iOS) и EXIF Fixer (для Android).

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.

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.