ARTICLE 19

МАТЕРИАЛЫ ПО ФИЗИЧЕСКОЙ И ЦИФРОВОЙ БЕЗОПАСНОСТИ

ДЛЯ ЛГБТ АКТИВИСТОВ

РОССИЙСКАЯ ЛГБТ-СЕТЬ
lgbtnet.org

GENDERDOC-M
gdm.md

ДОТЫК
dotyk.by

COMMUNITY CENTRE
communitycentre.by

JOURNALISTS 4 TOLERANCE
gaypress.eu/category/zhurnalistam/

DEFENDING FREEDOM OF EXPRESSION AND INFORMATION

ARTICLE 19 Free Word Centre 60 Farringdon Road London EC1R 3GA
T +44 20 7324 2500 F +44 20 7490 0566
E info@article19.org W www.article19.org Tw @article19org
facebook.com/article19org

ФИЗИЧЕСКАЯ БЕЗОПАСНОСТЬ

4. Что делать, если вам угрожают?
5. Вы собираетесь на встречу с человеком, с которым познакомились в интернете?
6. О чём нужно помнить, участвуя в публичных демонстрациях?
7. О чём нужно помнить, организуя публичное мероприятие?
8. Что делать, если вас задержали на публичном мероприятии?
9. В участке полиции
10. Подача заявления в полицию

ЦИФРОВАЯ БЕЗОПАСНОСТЬ

11. Как защитить свой смартфон?
12. Как защитить свой компьютер?
13. Безопасность в социальных сетях
14. Как защитить свою e-mail переписку?
15. Мобильные приложения, которые повышают безопасность

ВАМ УГРОЖАЮТ!

Что делать?

ФИЗИЧЕСКАЯ БЕЗОПАСНОСТЬ

ЕСЛИ ВАМ УГРОЖАЮТ

Зафиксируйте факт угрозы (видео или аудиозапись, скриншоты, запись телефонного разговора).

Проконсультируйтесь с юристом. Если вы не знаете, к кому обратиться, оставьте заявку на сайте **Российской ЛГБТ-сети** (www.lgbtnet.org), раздел «Получить помощь».

Подготовьте заявление в полицию.

Никому не отдавайте подлинники доказательств, к заявлению в полицию приложите копии.

Заявления обязаны принять в любом полицейском участке.

Если вам угрожают по гомофобным мотивам, **ОБЯЗАТЕЛЬНО** укажите это в заявлении.

Не забудьте получить от сотрудника полиции отрывной талон о том, что заявление принято.

После того как заявление будет зарегистрировано, сфотографируйте его.

ЗНАКОМСТВО В ИНТЕРНЕТЕ

О чём помнить, собираясь на встречу?

ФИЗИЧЕСКАЯ БЕЗОПАСНОСТЬ

ВЫ СОБИРАЕТЕСЬ НА ВСТРЕЧУ С ЧЕЛОВЕКОМ, С КОТОРЫМ ПОЗНАКОМИЛИСЬ В ИНТЕРНЕТЕ?

Назначайте первую встречу в безопасных местах (кафе, людный парк).

Не назначайте встречу у себя дома, не приезжайте домой к незнакомым людям, особенно на окраину города, за город, на дачу.

Не встречайтесь с человеком, если что-то вызывает у вас подозрения.

Предупредите кого-то из близких о том, куда направляетесь. Можете для этого использовать мобильное приложение **Companion** (https://www.companionapp.io/).

Позвоните со встречи, сообщите о том, ггде вы и все ли в порядке.

Не делитесь сведениями, которые могут быть использованы против вас (место работы, учебы или проживания).

После первой встречи возвращайтесь домой самостоятельно, откажитесь от предложений подвезти до дома или проводить до подъезда.

Если вам нужна помощь юриста, оставьте заявку на сайте **Российской ЛГБТ-сети** (www.lgbtnet.org), раздел «Получить помощь».

ПУБЛИЧНЫЕ ДЕМОНСТРАЦИИ

О чём помнить, участвуя в них?

ФИЗИЧЕСКАЯ БЕЗОПАСНОСТЬ

О ЧЕМ НУЖНО ПОМНИТЬ, УЧАСТВУЯ В ПУБЛИЧНЫХ ДЕМОНСТРАЦИЯХ?

Знайте свои права – если принимаете участие в публичной акции, митинге, убедитесь, что знаете, какие у вас есть права, а также какие ограничения существуют в вашей стране.

Узнайте как можно больше о мероприятии и его организаторах – убедитесь, что знаете, в какого рода мероприятии планируете принять участие.

Оцените контекст и риски – если вы знаете контекст и уровень риска, можно составить правильную стратегию действий.

Возьмите с собой заряженный телефон и паспорт.

Соберите группу друзей и договоритесь о плане действий во время мероприятия. Выберите место встречи и запасной выход в случае угрозы вашей безопасности и потери контакта с остальной частью группы.

Проверьте свои вещи – не берите с собой предметы, которые правоохранительные органы могут счесть опасными. Наденьте удобную обувь и одежду.

Оставайтесь на связи с близким человеком, который не принимает участия в мероприятии.

Вы имеете право снимать и фотографировать действия правоохранительных органов, даже если им это не нравится. Но это не касается участников мероприятия – они имеют право на это не соглашаться.

Если происходит провокация, на месте информируйте организаторов о всех угрозах и нарушениях, которые фиксируете.

ПУБЛИЧНЫЕ МЕРОПРИЯТИЯ

О чём помнить при их организации?

ФИЗИЧЕСКАЯ БЕЗОПАСНОСТЬ

О ЧЕМ НУЖНО ПОМНИТЬ, ОРГАНИЗУЯ ПУБЛИЧНОЕ МЕРОПРИЯТИЕ?

Определите координатора по безопасности мероприятия.

Ознакомьтесь с планом эвакуации из арендуемого помещения.

На случай срыва аренды запланируйте альтернативную площадку для проведения мероприятия.

Составьте список контактов юристов и правозащитных организаций.

Подготовьте основные медицинские препараты для оказания первой помощи.

Разработайте план реагирования на инциденты.

Поясните правила поведения участникам, например, что не приветствуется язык вражды.

Проинформируйте участников о намерении снимать мероприятие – участники должны дать согласие.

Не вступайте в конфликт с провокатором – вызывайте полицию или зафиксируйте провокацию/вандализм на фото и видео.

В случае провокации сохраняйте самообладание и отвечайте провокаторам в спокойном тоне, старайтесь снизить уровень агрессии в зале.

ПУБЛИЧНЫЕ МЕРОПРИЯТИЯ

Что делать, если вас задержали?

ФИЗИЧЕСКАЯ БЕЗОПАСНОСТЬ

ЧТО ДЕЛАТЬ, ЕСЛИ ВАС ЗАДЕРЖАЛИ НА ПУБЛИЧНОМ МЕРОПРИЯТИИ?

Выходя на публичную акцию, заранее узнайте, куда вы можете обратиться за помощью в случае задержания. Установите приложение **Red Panic Button**, которое позволяет каждые 5 минут сообщать о вашем местоположении установленному контакту.

Выясните фамилии, должности и звания лиц, которые производят задержания. Зафиксируйте информацию.

Не оказывайте прямого сопротивления.

Внимательно прочитайте протокол об административном задержании. Внесите все дополнения в соответствующее поле.

Удостоверьтесь, что в протоколе указано время фактического задержания, а не время доставления в отдел полиции.

По просьбе задержанного полиция обязана выдать копию протокола после его подписания задержанным и составителем. Распишитесь в получении копии протокола после того, как получите копию на руки.

По вашей просьбе полиция должна сообщить о задержании вашим родственникам и защитнику.

В случае жалоб задержанного на плохое самочувствие или состояние здоровья дежурный в обязательном порядке должен вызвать бригаду скорой помощи.

В рамках административного процесса или задержания никто не должен подвергаться насилию, другому жестокому или унижающему человеческое достоинство обращению.

Вы можете проводить фотографирование и видеосъемку должностных лиц органов внутренних дел и их действий при осуществлении ими должностных полномочий.

В УЧАСТКЕ ПОЛИЦИИ

ФИЗИЧЕСКАЯ
БЕЗОПАСНОСТЬ

В УЧАСТКЕ ПОЛИЦИИ

Личный досмотр производится лицом одного с вами пола в присутствии двух понятых того же пола и только после того, как административный процесс начат.

Дактилоскопия (снятие отпечатков пальцев) может проводиться только в том случае, если ваша личность не установлена.

Срок административного задержания не должен превышать три часа с момента доставления в отделение. Срок может быть продлен до 48 часов за мелкое хулиганство, неповиновение законному распоряжению сотрудника полиции.

Административное задержание может длиться не более 3 часов. Административное задержание свыше 3 часов оформляется протоколом.

Если задержание продолжается более 3 часов, вам должно быть предоставлено питание. Родственники или другие лица также могут передать вам продукты питания.

Все изъятые вещи в обязательном порядке должны быть указаны в протоколе с указанием их количества, степени износа и особенностей.

По вашей просьбе лица из дежурного наряда должны проводить вас в туалет.

Температура в помещении, где вы находитесь, должна быть не ниже +18 С°.

На ночь вам должны предоставить место для сна.

ПОДАЧА ЗАЯВЛЕНИЯ В ПОЛИЦИЮ

ФИЗИЧЕСКАЯ БЕЗОПАСНОСТЬ

ПОДАЧА ЗАЯВЛЕНИЯ В ПОЛИЦИЮ

Само заявление лучше написать дома, а в участке заполнить только «шапку».

Заявление обязаны принять в любом полицейском участке.

Заявление пишется в свободной форме. Старайтесь писать кратко и по делу.

Сотрудники полиции могут отговаривать вас от подачи заявления. Будьте к этому готовы.

Если на вас напали по гомофобным или трансфобным мотивам, **ОБЯЗАТЕЛЬНО** подробно опишите это.

Если есть такая возможность, возьмите с собой адвоката, или человека, имеющего опыт подачи заявлений.

Обязательно получите отрывной талон о том, что ваше заявление принято.

После приема заявления у вас должны взять объяснение. В нем нужно продублировать все сведения из вашего заявления.

СМАРТФОН

Как защитить?

ЦИФРОВАЯ
БЕЗОПАСНОСТЬ

КАК ЗАЩИТИТЬ СВОЙ СМАРТФОН

Если ваша SIM-карта по умолчанию не защищена PIN-кодом, установите его в настройках. Избегайте самых простых кодов – 0000, 1234 и т. п. Постарайтесь придумать сложный код, который не так легко угадать.

Установите пароль для заблокированного экрана. Это самое важное и базовое правило мобильной безопасности. Если ваш телефон включен, то без блокировки экрана любой человек сможет увидеть ваши сообщения, письма, контакты и фотографии, если его захватит.

Выключайте настройки отслеживания вашего местонахождения, когда оно вам не нужно.

Убедитесь, что Bluetooth и Wi-Fi работают только когда это необходимо. Это уменьшает риск потенциального взлома через другие устройства.

Не храните личных фотографий в альбомах на мобильном телефоне. В случае захвата или потери телефона вся ваша личная жизнь может стать доступна посторонним людям. Фотографии лучше хранить на зашифрованных жестких дисках или защищенном компьютере.

КОМПЬЮТЕР

Как защитить?

ЦИФРОВАЯ
БЕЗОПАСНОСТЬ

КАК ЗАЩИТИТЬ СВОЙ КОМПЬЮТЕР

Не используйте нелицензионную операционную систему. Это не только незаконно – такую систему легко взломать, так как нет возможности получать обновлений для исправления ошибок и уязвимостей в системе.

Установите антивирусное ПО для вашей операционной системы (**Avast**, **Avira**, **Malwarebytes**, **Windows Firewall**). Убедитесь, что имеете обновленную версию, и проверяйте диск по крайней мере раз в неделю.

Используйте разные, длинные пароли, включая заглавные буквы и цифры, для входа в операционную систему, на почту и другие аккаунты. Если боитесь забыть такое количество разных паролей, храните их в программе **KeePass**. Меняйте пароли каждые два-три месяца.

Не сохраняйте пароли в браузерах и регулярно чистите историю поиска и посещения сайтов. Чтобы полностью удалить файлы с диска, пользуйтесь шредером **CCleaner**, **BleachBit**.

Шифруйте уязвимую информацию, хранящуюся на вашем компьютере, используя программу **VeraCrypt**. Стоит также делать копии ваших документов – храните их в зашифрованном виде в интернет-облаках (например: **Mega**).

СОЦИАЛЬНЫЕ СЕТИ

Правила безопасности

ЦИФРОВАЯ БЕЗОПАСНОСТЬ

БЕЗОПАСНОСТЬ В СОЦИАЛЬНЫХ СЕТЯХ

Обязательно введите двухфакторную аутентификацию для входа в ваш аккаунт Facebook, VK, twitter.

Удаляйте все данные, включая пароли и историю поиска, если заходите на свой аккаунт с чужого или публичного компьютера.

Используйте защищенный протокол https. Это обеспечит шифрованность информации и невозможность слежки за тем, что вы делаете в социальной сети.

Чтобы скрыть вашу локацию и вход в социальные сети или любые другие сайты, используйте **VPN** или **Tor**. Использование VPN и Tor обеспечивает шифрование всех ваших действий и информации в социальных сетях.

Убедитесь, что лица тех, кто желает оставаться на групповых фото и видео инкогнито, заретушированы. Для этого пользуйтесь приложением **ObscuraCam**.

«Все, что попадает в интернет, остается там навсегда». Обращайте внимание на содержание ваших постов в соцсетях. Не публикуйте информацию, которая может быть использована против вас или ваших знакомых, коллег.

Ограничивайте доступ к вашему профилю (статусы, фотографии, персональные данные и посты) до лиц, находящихся в списке ваших друзей.

Добавляйте в друзья только тех людей, которых знаете лично.

Если хотите использовать соцсети для своей общественной деятельности, лучше создать отдельный публичный профиль, а свои личные фотографии и другие данные распространять только на знакомых друзей в закрытом профиле.

Не рекомендуется использовать чаты в социальных сетях для передачи уязвимой информации. Хотя Facebook ввел возможность шифровать чат (доступно только в мобильном приложении).

ПЕРЕПИСКА

Как защитить?

ЦИФРОВАЯ
БЕЗОПАСНОСТЬ

КАК ЗАЩИТИТЬ СВОЮ E-MAIL ПЕРЕПИСКУ

Бесплатные почтовые ящики, такие как **mail.ru** или **yandex.ru**, небезопасны. Они не защищают вас от взлома или перехвата сообщений. Из всех бесплатных ящиков на данный момент рекомендуется **Gmail**, **Protonmail**, **Riseup** і **Tutanota**, которые используют самую надежную защиту пересылаемых сообщений.

Если вы уже установили аккаунт Gmail, введите двухэтапную аутентификацию. Тогда даже если кто-то узнает ваш пароль, не сможет зайти на ваш ящик без кода, полученного на ваш телефон.

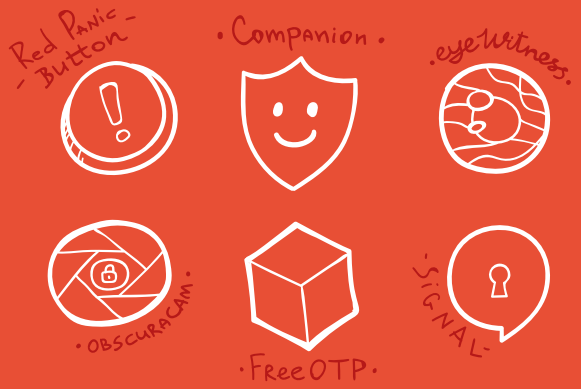
Научитесь шифровать письма. Это несложно! Для этого существует много программ, таких как **Mozilla Thunderbird**. Ее нужно установить на компьютере вместе с приложением **Enigmail** и можно использовать как основную почтовую программу.

Обращайте внимание на возможный фишинг. Злоумышленники часто пытаются получить наши данные и пароль с помощью фейковых писем. Никогда не нажимайте на ссылки в таких письмах без проверки адреса отправителя – несложно заметить, когда он поддельный.

При всем этом не забудьте, что недостаточно того, чтобы только вы соблюдали правила безопасности. Их должны соблюдать и люди, которым вы отправляете сообщения, в противном случае защита не сработает.

МОБИЛЬНЫЕ ПРИЛОЖЕНИЯ

которые повышают безопасность



ЦИФРОВАЯ БЕЗОПАСНОСТЬ

МОБИЛЬНЫЕ ПРИЛОЖЕНИЯ, КОТОРЫЕ ПОВЫШАЮТ БЕЗОПАСНОСТЬ

Red Panic Button
Помогает активистам связаться со своими сторонниками в случае опасности.

Companion
Друзья или родственники виртуально наблюдают, как вы добираетесь домой, и реагируют в случае опасности.

Signal
Зашифрованные звонки и переписка.

eyeWitness
Безопасное хранилище ваших фото и видео, фиксирующих нарушения прав человека.

ObscuraCam
Помогает сделать ретуш лиц, зафиксированных на групповых фотографиях и видео.

FreeOTP
Создает одноразовые пароли для входа в аккаунты Google, Facebook и другие.

Приложения Viber, Skype, Facebook Messenger, Google Hangouts не используют межабонентское шифрование (end-to-end encryption)