



FOR EMBATTLED CIVIL SOCIETY ORGANIZATIONS

ОЦЕНКА РИСКОВ ОРГАНИЗАЦИЙ ГРАЖДАНСКОГО ОБЩЕСТВА

Следующая информация представляет собой отрывок из пособия «Lifeline», Фонда помощи организациям гражданского общества в ограниченном пространстве (www.csolifeline.org/advocacy-toolkit). Это краткий обзор того, как организации гражданского общества могут думать о своей цифровой безопасности в контексте участия в информационно-просветительских кампаниях.

Управление рисками в рамках подхода слежения за ситуацией

Угрозы могут быстро меняться или нарастать. Поэтому вам имеет смысл уделить внимание тому, чтобы обнаружить проблемную ситуацию, понять ее и приспособиться к ней. Слежение за **социально-политической обстановкой**, например, может включать идентификацию властных людей, на которых ваша работа (например, публикация отчета) скажется отрицательно. Подумайте, какими ресурсами они могут располагать для преследования вашей организации (например, преследование с помощью юношеских вооруженных группировок). Точно также **оценка географической ситуации** может включать в себя планирование маршрутов протеста, чтобы в случае опасности, если власти перейдут к чрезмерному применению силы, протестующие могли бы быстро и бесшумно разбежаться. Дополнительную информацию об этом подходе см. у **Front Line Defenders**.

Вопросы для организаций по оценке риска

- Если решения принимает преимущественно один человек или несколько людей, то каков план Б на случай их ареста?
- Есть ли у вас документы о процедурах охраны безопасности и было ли проведено обучение сотрудников? Проводили ли вы тестирование, чтобы убедиться, что сотрудники следуют предписанной процедуре?
- Есть ли процедура, которая в ходе найма новых сотрудников позволяет убедиться, что нанимаемые сотрудники или волонтеры не являются агентами правительства или враждебной группировки? Есть ли правила на случай, когда сотрудник покидает организацию, особенно обиженный сотрудник (например, смена паролей или замков)?
- Есть ли особые процедуры обеспечения безопасности в отношении случайных волонтеров или посетителей офиса организации?
- Ериняли ли вы особые меры, чтобы снизить угрозы в отношении жертв и свидетелей нарушений прав человека, чьи рассказы вы документируете?
- Можете ли вы и ваши сотрудники получить помощь в случае стресса или выгорания?
- Есть ли в организации особые процедуры на случай ареста или физического нападения?
- Есть ли у вас список внутренних и международных контактов (например посольств, СМИ, лидеров общин и других инфлюенсеров), которых можно было бы уведомить в случае нападений?

ПРИМЕР: КАК СТРУКТУРИРОВАТЬ ОЦЕНКУ РИСКА

Риск: Арест при обыске на дому и конфискация документов/ телефона/ ноутбука

Вероятность, что это случится: Средне-высокая

Возможное влияние: Средне-высокое влияние на меня, моих родственников и организацию

Оценка угрозы: Полиция обычно врывается с обыском рано утром; об этом свидетельствует опыт правозащитников, которые пострадали недавно.

Уязвимые места:

- Предписанные процедуры закона не соблюдаются; не стоит ожидать ордера на обыск или разрешения пригласить адвоката
- Организация работает с информацией деликатного характера
- Со мной живут маленькие дети

Профилактические меры:

1. Обсудить риск с супругой/ супругом и объяснить, кому нужно позвонить, если придет полиция, и что делать после этого.
2. Договориться, что в моменты наибольшего риска дети будут спать у тети.
3. Рассмотреть возможность установки в доме камеры наблюдения для регистрации происшествий.
4. Узнать о том, какие права есть при задержании, чтобы с полным основанием требовать их соблюдения (даже несмотря на то, что эти требования могут остаться без ответа).
5. Заранее переговорить с адвокатом, на случай если будет можно обратиться к адвокату.
6. Не хранить дома информацию деликатного свойства.
7. Удалять информацию с компьютера и телефона или шифровать ее.
8. Убедиться, что все личные дела (например, налогообложение) улажены, чтобы не давать повода для политического преследования.

(Источник: *Front Line Defenders*)

- Есть ли у вас контактные данные организаций, которые могут оказать срочную помощь правозащитникам/ организациями гражданского общества в опасности, и знаете ли вы, какого рода информацию они могут запросить? (например **Front Line Defenders**, **Lifeline**, Фонд быстрого реагирования)

Lifeline, Фонд помощи организациям гражданского общества в тяжелом положении, предоставляет неотложную финансовую помощь организациям гражданского общества (ОГО), подвергающимся угрозам или нападениям, а также гранты по обеспечению устойчивости, чтобы помочь ОГО отвечать на общие угрозы, ведущие к сужению гражданского пространства. За подробными сведениями обращайтесь на вебсайт нашей организации <https://www.csolifeline.org> или по адресу info@CSOLifeline.org. Найдите нас в Twitter [@CSOLifeline](https://twitter.com/CSOLifeline).



FOR EMBATTLED CIVIL SOCIETY ORGANIZATIONS

КОНТРОЛЬНЫЙ СПИСОК ПРАКТИЧЕСКИХ МЕР БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ ГРАЖДАНСКОГО ОБЩЕСТВА

Это краткое изложение некоторых практических шагов по обеспечению безопасности для организаций гражданского общества. Для получения более подробных инструкций см. ссылки на ресурсы ниже.



Дом

- Оцените, в каких местах ваш дом может оказаться уязвимым, а затем подумайте, как можно снизить риск. Не забывайте, что есть множество мер, которые не требуют или почти не требуют финансовых затрат (планирование действий семьи на случай чрезвычайных обстоятельств, самообразование онлайн, обеспечение защиты общины, обеспечение постоянного использования физических мер безопасности (например, постоянно закрывать двери и окна)).
- Если вы задумываетесь о том, чтобы установить дополнительное оборудование для охраны безопасности, постарайтесь не привлекать внимания соседей, поскольку это может усилить опасность.
- По возможности, пусть у вас будет отдельный вход и отдельный аварийный выход.
- Постарайтесь не брать работу на дом, если вы работаете с материалами деликатного содержания.
- Убедитесь, что вы тщательно исполняете все другие законы и правила, такие как налоговое законодательство, правила дорожного движения, законы о наркотиках и лекарственных средствах, чтобы не привлекать к себе нежелательного внимания.
- Уделите время и внимание тому, чтобы завязать крепкие отношения с соседями, которые могли бы вас предупредить, если они заметят в районе что-то подозрительное.



Офис

- Разработайте план защиты данных и не храните ненужные данные.
- Используйте безопасные платформы коммуникации, например, Сигнал, и шифруйте переписку по электронной почте по мере возможности.
- Примите меры, чтобы сотрудники не оставались в офисе в одиночку; всегда безопаснее работать вдвоем или в компании.
- Если вы опасаетесь проникновения в офис, сначала рассмотрите решения, которые не требуют серьезных финансовых инвестиций. Камеры видеонаблюдения полезны для сбора фактов и для того, чтобы заставить людей отказаться от взлома, но у них есть и недостатки. Наличие камер безопасности может давать ложное чувство безопасности; их легко взломать и на их содержание постоянно требуются деньги.
- Обдумайте безопасные маршруты с работы/ на работу и найдите безопасное место для проведения встреч.
- Подготовьте план безопасных поездок, чтобы сотрудники, подвергающиеся наибольшему риску, могли воспользоваться самыми безопасными вариантами. Может потребоваться изменить время или место встреч; изменить вид транспорта; в некоторых случаях понадобятся средства на пользование частными автомобилями, которые нельзя отследить.

- Ограничивайте число людей, у которых есть доступ к деликатным сведениям, даже если речь идет о сотрудниках, которым вы доверяете.



Путешествия

- Придумайте кодовое слово для обозначения внезапной опасности и договоритесь о ежедневной свертке с коллегой, которому вы доверяете.
- Избегайте повторения одних и тех же действий, чтобы этим не могли воспользоваться те, кто за вами следят.
- Выбирайте место для встреч с учетом требований безопасности; посмотрите, сколько входов у помещения и подумайте, не будет ли безопаснее провести встречу в более публичном месте.
- Следите за сроком действия паспорта и других документов, разрешающих выезд (в том числе виз), сделайте копии всех документов и раздайте их коллегам, которым вы доверяете.



Задержания/аресты/похищения

- Придумайте кодовое слово для обозначения внезапной опасности и договоритесь о ежедневной свертке с коллегой, которому вы доверяете.
- Избегайте повторения одних и тех же действий, чтобы этим не могли воспользоваться те, кто за вами следят.
- Выбирайте место для встреч с учетом требований безопасности; посмотрите, сколько входов у помещения и подумайте, не будет ли безопаснее провести встречу в более публичном месте.
- Следите за сроком действия паспорта и других документов, разрешающих выезд (в том числе виз), сделайте копии всех документов и раздайте их коллегам, которым вы доверяете.



Демонстрации

- Попробуйте объединить демонстрантов в четверки и попросите их присматривать друг за другом.
- Рассмотрите возможность окружения демонстрации людской цепью.
- Не выводите на демонстрацию всех ключевых сотрудников.
- Рассмотрите возможность работы с т.н. «сопроводителями» (с пользующимися уважением религиозными лидерами, сотрудниками из посольств тех стран, которые считают беспристрастными).

Пособие **Front Line Defenders** по охране безопасности <https://www.frontlinedefenders.org/en/resource-publication/workbook-security-practical-steps-human-rights-defenders-risk>

Пособие по обеспечению защиты <https://www.frontlinedefenders.org/en/resource-publication/protection-handbook-human-rights-defenders>

Цифровая безопасность <https://securityinabox.org/en/>

