



**ПРАКТИЧЕСКОЕ РУКОВОДСТВО ПО
РЕАГИРОВАНИЮ НА КИБЕРПРЕСЛЕДОВАНИЕ
ДЛЯ ЖЕНЩИН-ЖУРНАЛИСТОВ**

REUTERS/ Raheb Homavandi

В сотрудничестве с

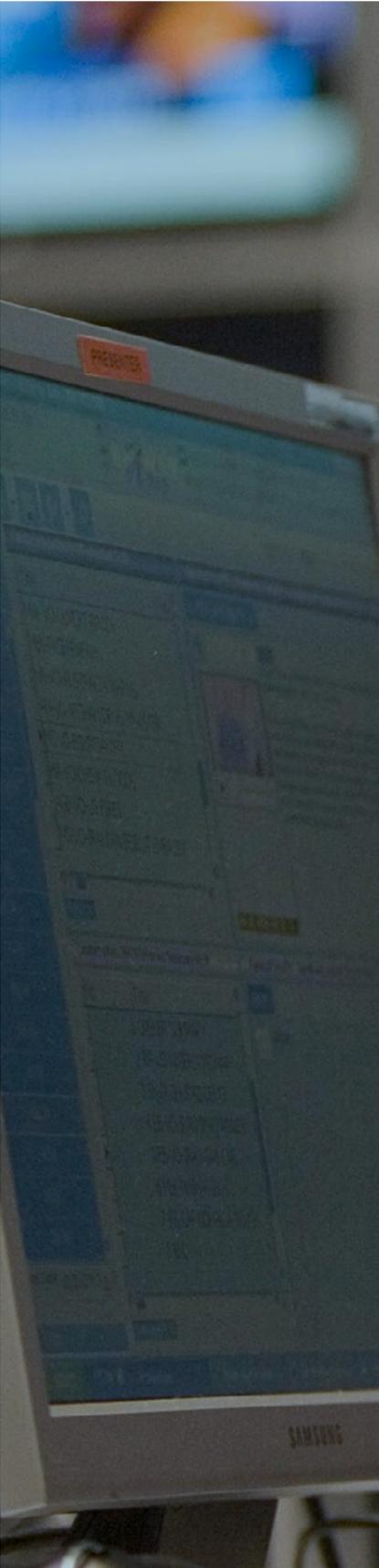


TrustLaw



При поддержке





ПРЕДИСЛОВИЕ

Публикация настоящего руководства стала возможной благодаря поддержке шведского фонда Postcode Foundation. Его содержание было разработано Элой Стэпли (Международный фонд женских СМИ) при координации фонда Thomson Reuters. Компания Dechert LLP щедро предоставила исследование на безвозмездной основе. Однако не следует считать, что содержание данного доклада отражает точку зрения Dechert LLP или юристов, внесших в него свой вклад.

Редакционная коллегия ЮНЕСКО: Сэорла Маккейб, Тереза Чорбахер

Поддержка в реализации проекта: Йоханн Бир, Сара Боньяди, Аннина Клаессон

Графическое оформление: Паула Фигероа

Данные, представленные в документе, приведены исключительно в информационных целях. Они не являются «юридическим советом». Читателям настоятельно рекомендуется обратиться за советом к квалифицированному юристу в связи со своими конкретными обстоятельствами. Авторы-составители доклада постарались сделать содержание доклада правильным и актуальным на момент публикации, но они не гарантируют его точность или полноту, тем более что обстоятельства могут измениться после публикации. Ни ЮНЕСКО, ни авторы и составители не несут никакой ответственности за предпринятые или непредпринятые действия, а также за любые убытки, возникшие в результате доверия к данному изданию или любым содержащимся в нем неточностям. Фонд Thomson Reuters не занимает позицию в отношении содержания или мнений, выраженных в данной публикации, в соответствии с принципами Thomson Reuters Trust в области независимости и свободы от предвзятости.



ВВЕДЕНИЕ



Эта онлайн-насилие имеет серьезные последствия для свободы прессы, такие как ограничение права голоса женщин-журналистов в Интернете.

Рост социальных сетей привел к тому, что участие журналистов в цифровом публичном пространстве стало одной из их профессиональных задач. Это создало новые возможности для журналистов, включая женщин-журналистов, такие как более широкий охват аудитории, возможность общения с журналистами на международном уровне и возможность создания специализированных изданий. Вместе с тем такое присутствие в Интернете несет в себе ряд рисков. Иногда, сами того не осознавая, женщины-журналисты поделились личной информацией о себе. Эта информация теперь используется против них. Злоумышленники ищут в Интернете данные, которые можно использовать для запугивания и преследования работников СМИ, а также для того, чтобы помешать им выполнять свою работу. Это не единственная проблема; журналисты часто получают угрозы смерти, угрозы сексуального насилия, угрозы, направленные на их семьи, и становятся мишенью кампаний по дезинформации. Исследования показали, что от этих нападений непропорционально страдают женщины-журналисты.

В 2020 году ЮНЕСКО и Международный центр журналистов (ICFJ) провели опрос среди 714 женщин-журналистов из 125 стран, в результате которого было установлено, что 73% из них сталкивались с онлайн-насилием, связанным с их работой. Согласно данным опроса журналистки, пострадавшие от других видов дискриминации, таких как расизм и гомофобия, еще чаще становились мишенью, причем с более серьезными последствиями.

Такое онлайн-насилие имеет серьезные последствия для свободы прессы, такие как ограничение права женщин-журналистов на свободу выражения мнений и информации в сети. В то время как онлайн-платформы стараются предотвратить онлайн-атаки, а государства — привлечь виновных к ответственности, журналисты могут предпринять определенные шаги для того, чтобы лучше защитить себя и своих сотрудников. Данное руководство составлено для поддержки женщин-журналистов, которые сталкиваются с проблемами онлайн-насилия.

- 
ПОНИМАНИЕ
- 
ПЕРЕДАЧА
ИНФОРМАЦИИ
- 
ИНФОРМИРОВАНИЕ
- 
РЕАГИРОВАНИЕ
- 
ПОДДЕРЖКА

REUTERS/ Carlos García Rawlins

ПОДГОТОВКА К КИБЕРПРЕСЛЕДОВАНИЮ

Принятие мер для самоподготовки и подготовки своих коллег к киберпреследованию является важной частью минимизации риска. Чем больше вы можете сделать заранее, тем лучше вы будете защищены в случае нападения.

УПРАВЛЕНИЕ ОНЛАЙН-КОНТЕНТОМ

Управление онлайн-контентом и защита данных может быть сложной задачей. Это требует вложения времени и необходимых знаний в области информационных технологий. Поэтому наше руководство направлено на то, чтобы ознакомить вас с некоторыми ключевыми шагами, которые вы можете предпринять для снижения рисков для себя и своих источников информации. Понимание того, какой информацией можно делиться, а какие данные лучше держать в секрете, является ключом к лучшей защите. Информацию, которая может быть использована для проверки вашей личности, контактной информации или определения вашего местонахождения, лучше хранить в автономном режиме. К ней относятся такие данные, как дата вашего рождения, личный номер телефона и адрес. Важным первым шагом является составление карты ваших онлайн-данных и мест их хранения. Курс Международного фонда женских СМИ (IWJF) **Keep it Private** дает более подробное представление о персональных данных и способах их защиты. Найдите свое имя в Интернете с помощью всех поисковых систем и просмотрите видео и фотографии, а также веб-сайты. Онлайн-злоумышленники часто нападают на женщин-журналистов, выискивая их фотографии на пляже или в спортзале, которые затем распространяют в Интернете, сопровождая угрозами и женоненавистническими оскорблениями. Ведите записи обо всех материалах, которые вам неприятно иметь в сети. Затем приступайте к их удалению.



Если информация хранится на ваших сайтах в социальных сетях или на сайтах родственников и друзей, то вам следует удалить ее или сделать приватной. Следует иметь в виду, что настройки доступа в некоторых социальных сетях автоматически устанавливаются таким образом, что третьим лицам разрешается воспроизводить любой контент, размещенный в сети, при условии, что авторы дали предварительное согласие. Поэтому настоятельно рекомендуется всегда проверять правовые положения и условия пользования и, при необходимости, изменять настройки доступа, применяемые к контенту, размещенному в аккаунтах социальных сетей. Имейте в виду, что копии этих данных могут продолжать существовать где-то еще в Интернете, например, на сайтах интернет-архивов, таких как **Wayback Machine**.

Управление онлайн-контентом имеет решающее значение, поскольку ваши данные могут оказаться на стороннем сайте, например, в публичной базе данных или социальной сети, и удалить информацию может быть непросто. Для этого может быть необходимо судебное решение, предписывающее сайту или провайдеру доступа удалить личную информацию или всю страницу, на которой она отображается. Журналисты должны изучить свои права в отношении удаления своих данных из публичных баз данных, поскольку это часто зависит от законодательства страны, в которой они живут и работают. Комитет по защите журналистов разработал более подробное **руководство** по удалению данных из Интернета.

БЕЗОПАСНОСТЬ УЧЕТНОЙ ЗАПИСИ

Обеспечение безопасности ваших учетных записей в Интернете — важный шаг, позволяющий вам лучше защититься от преследования.

Злоумышленники в Интернете могут попытаться взломать ваши учетные записи, завладеть ими и разместить контент, который может нанести вам профессиональный вред. Они также могут искать данные, такие как фотографии или видео, которые могут быть использованы, чтобы дискредитировать или шантажировать вас и ваших источников информации. Чтобы обезопасить свои учетные записи, убедитесь, что вы используете менеджер паролей и создаете длинные пароли, состоящие более чем из 16 символов. Не следует использовать пароли повторно, так как если злоумышленник получит доступ к вашему паролю, он сможет войти в несколько учетных записей. Убедитесь также, что вы включили **двухфакторную аутентификацию (2FA)** для всех своих учетных записей. Это дополнительный уровень безопасности, который снизит риск того, что кто-то получит доступ к вашим учетным записям. **Фонд имени Рори Пека (Rory Peck Trust)** **предлагает подробное руководство**, из которого можно узнать больше о безопасности учетных записей.



REUTERS/ Anushree Fadnavis

ПОДУМАЙТЕ, КТО И ПОЧЕМУ МОЖЕТ ВЫБРАТЬ ВАС В КАЧЕСТВЕ ЖЕРТВЫ

Существует много различных типов онлайн-злоумышленников, и они используют различные стратегии для нападения на журналистов. Понимание того, кто и почему может захотеть выбрать вас в качестве мишени, поможет вам лучше подготовиться. Прежде чем публиковать статью, полезно попытаться предугадать возможную обратную реакцию в Интернете и какую форму она примет. Это поможет вам психологически подготовиться к киберпреследованию, а также разработать стратегии борьбы с ним. Может быть полезно составить схему различных видов групп, которые проявляют враждебность в Интернете, и стратегий, которые они обычно используют. Новостным редакциям рекомендуется предусмотреть подготовку к онлайн-насилию в рамках процесса оценки рисков. В **руководстве PEN America по защите от киберпреследования** есть пособие по стратегиям, которые используют злоумышленники в Интернете, а **IWMF разработал подробный курс «Know your Trolls» («Знай своих троллей»)** для журналистов, желающих узнать больше о том, кто такие злоумышленники в Интернете и почему они нападают

● ДОКСИНГ

Доксинг — это все более распространенная тактика, используемая против журналистов в качестве способа запугивания, которая заключается в сборе и раскрытии личных данных в Интернете, таких как домашний адрес или персональные контактные данные, с призывом к пользователям Интернета использовать эти данные для преследования или причинения вреда жертве, будь то в Интернете или реальной жизни. Если ваше местонахождение опубликовано в Интернете и распространяется с угрозами в ваш адрес, то вы подвергаетесь риску физического нападения. Новостные редакции должны планировать действия на случай доксинга и предпринимать шаги по защите журналистов, ставших жертвами этой тактики из-за своей работы. Это должно включать обсуждение возможности стать жертвой доксинга при оценке рисков и, если возможно, наличие плана экстренного перемещения на новое место. Журналисты должны обязательно ставить своих редакторов в известность, если они обеспокоены тем, что та или иная новость несет в себе риск доксинга. Внештатные журналисты должны обсуждать угрозы доксинга с коллегами, журналистскими сетями, а также со своими редакторами-заказчиками, которые могут оказать им поддержку в случае инцидента. В газете New York Times есть подробное [руководство](#) о том, как лучше защитить себя от доксинга. В зависимости от юрисдикции, в которой это произошло, доксинг может преследоваться по закону за нарушение неприкосновенности частной жизни или домогательство.



● ИСКАЖЕНИЕ ИЗОБРАЖЕНИЙ

Злоумышленники часто ищут в Интернете изображения женщин-журналистов, которые могут быть использованы для их дискредитации или причинения им вреда. Эта стратегия нападения в Интернете предполагает использование изображения вне контекста, часто с сексуальным подтекстом. Злоумышленники могут также переделывать изображения, накладывая лицо женщины на порнографические материалы. Они часто находят фотографии или видео из социальных сетей журналиста, поэтому важно, чтобы журналисты проверяли, какие изображения находятся в открытом доступе. Некоторые видео и фотографии могли быть опубликованы с их (подразумеваемого) согласия, например, когда они были сделаны в ходе их публичной профессиональной деятельности, т.е. во время интервью или репортажа, или для статьи. Журналисты должны предпринять шаги, чтобы удалить или ограничить доступ к любым фотографиям или видео, которые, по их мнению, могут быть использованы против них. Онлайн-злоумышленники могут также взламывать учетные записи или устройства в поисках изображений, которые могут быть использованы для шантажа женщин-журналистов. Журналисты должны следовать рекомендациям по защите учетных записей в Интернете (см. стр.5). Они могут обратиться в суд по поводу любого использования и/или представления их изображения, не связанного с их публичной профессиональной деятельностью, и/или любого искаженного изображения, в котором они могут быть легко идентифицированы, если содержание публикуется без их предварительного согласия и может причинить им вред.

РАЗГОВОРЫ С ДРУГИМИ ЛЮДЬМИ

Бывает важно говорить с другими людьми о насилии в Интернете и его последствиях. Если вы сообщите другим о том, что с вами происходит, это поможет вам лучше защитить себя и своих близких.

РАЗГОВОРЫ С РЕДАКЦИЕЙ И КОЛЛЕГАМИ

Если вы чувствуете в себе силы, поговорите со своим редактором или руководителем редакции о киберпреследованиях. Полезно заранее подумать о том, как ваше СМИ может поддержать вас и что бы вы хотели, чтобы произошло. За рекомендациями обращайтесь к **руководству** PEN America, содержащему информацию о том, как говорить с работодателями об онлайн-насилии. Разговоры с коллегами о насилии, с которым вы столкнулись, также могут быть полезны. Создание сетей взаимопомощи и обмен стратегиями борьбы с киберпреследованием полезны, особенно для фрилансеров и молодых сотрудников, которые могут чувствовать себя не очень комфортно, обращаясь за помощью. Женщинам-журналистам может помочь вступление в группы поддержки как на рабочем месте, так и вне его. Они могут оказать столь необходимую поддержку, когда речь идет о противодействии онлайн-насилию. Редакция должна поощрять создание сетей взаимопомощи, внутренних механизмов передачи информации, с помощью которых сотрудники могут безопасно и конфиденциально сообщать об онлайн-насилии, а также иметь план поддержки журналистов, столкнувшихся с онлайн-

насилием. Это может включать стратегии реагирования на онлайн-насилие, план действий в случае доксинга, а также предоставление психологической поддержки тем, кто в ней нуждается. PEN America подготовила информационное **руководство** для работодателей о том, как поддержать сотрудников, столкнувшихся с киберпреследованием. ЮНЕСКО и фонд Thomson Reuters также недавно разработали руководство под названием **«Гендерно-чувствительная политика безопасности для редакций»**, которое может быть полезно в этом контексте. Если в вашей редакции нет политики безопасности или она неадекватна, необходимо развивать коллективную адвокацию, чтобы изменить эту информацию.



РАЗГОВОРЫ С СЕМЬЕЙ И ДРУЗЬЯМИ

Члены семьи и близкие друзья журналистов также могут стать мишенью для злоумышленников в Интернете, поэтому важно поговорить с ними о преследовании и о том, как оно может повлиять на них и на вас. Объясните им важность конфиденциальности в Интернете и сообщите им, распространение какого контента в Интернете вы не одобряете. Возможно, члены семьи не обеспечили защиту собственной информации в Интернете, поэтому полезно поработать с ними над удалением данных и включением настроек безопасности. Помогите им составить карту их «цифровых следов» и добиться удаления контента. PEN America предлагает информационное [руководство](#) о том, как говорить с семьей и друзьями об онлайн-насилии.

ПСИХОЛОГИЧЕСКАЯ ПОДДЕРЖКА

Киберпреследование имеет последствия в офлайне для тех, кто стал его жертвами. Столкнувшись с насилием журналисты часто сообщают, что чувствуют страх, изоляцию и подавленность. В результате опроса, проведенного в 2020 году ЮНЕСКО и ICJF, выяснилось, что 26 процентов опрошенных женщин-журналистов признались, что онлайн-насилие негативно сказалось на их психическом здоровье, а 12 процентов обратились за медицинской помощью. Справиться с этими трудностями помогает обращение за профессиональной помощью. В идеале редакции должны оказывать психосоциальную поддержку журналистам. Тем, кто не имеет доступа к профессиональной помощи, может быть полезно поговорить с друзьями и коллегами. Комитет по защите журналистов предлагает это [руководство](#) со ссылками на ресурсы, которые могут помочь. В Dart Centre есть исчерпывающий [обзор](#) о киберпреследовании с рекомендациями по реагированию на него.



ЧТО ДЕЛАТЬ ВО ВРЕМЯ И ПОСЛЕ ПРЕСЛЕДОВАНИЯ

Если вы стали жертвой продолжительного онлайн-насилия, может быть трудно понять, как защитить себя.

ПЕРВЫЕ ШАГИ

Журналистам, которые не приняли превентивных мер, следует ознакомиться с разделом «[Подготовка к киберпреследованию](#)» в начале данного руководства. Все журналисты должны проверить свои учетные записи и убедиться, что они используют надежные пароли и имеют включенную 2FA. Сотрудники СМИ должны поговорить со своими редакторами о насилии, а редакция должна оказать поддержку в соответствии со своими рекомендациями касательно киберпреследования. Для некоторых журналистов может оказаться полезным уйти в офлайн и позволить коллеге или доверенному другу следить за их учетными записями, пока преследование не утихнет. Онлайн-поддержка от других журналистов или сообществ тоже может помочь. Их можно попросить написать сообщения поддержки в Твиттере. Также важно документировать любые сообщения, которые вызывают беспокойство. Подробную информацию о том, как документировать преследование, можно найти в заключительном разделе данного руководства.

РЕАГИРОВАНИЕ НА НАСИЛИЕ

Знать, когда и как реагировать на онлайн-насилие, может быть непростой задачей. Это связано с тем, что существует множество типов злоумышленников в Интернете, и может быть сложно определить мотив преследования. Реакция на киберпреследование может усугубить ситуацию; однако бывают случаи, когда она может помочь. Журналисты, ставшие объектом скоординированных кампаний по дезинформации, которые ставят под сомнение честность их репортажей, могут отреагировать, прикрепив ответ к верхней части своей ленты в социальных сетях. В идеале они должны делать это при поддержке СМИ. Новостным редакциям рекомендуется разработать политику реагирования на онлайн-насилие и ознакомить с ней сотрудников. Такие организации, как HeartMob и TrollBusters, также предлагают советы и поддержку по реагированию на насилие.

ДОКУМЕНТИРОВАНИЕ И ПЕРЕДАЧА ИНФОРМАЦИИ О ПРЕСЛЕДОВАНИИ

Невозможно документировать все случаи онлайн-насилия, но рекомендуем вам задокументировать конкретные сообщения, чтобы показать их редакторам, передать властям или поделиться с организациями, занимающимися вопросами свободы прессы. Журналистам следует рассмотреть возможность документирования угроз от рецидивистов, особенно если они используют свое настоящее имя, а также сообщений, содержащих угрозы смерти или изнасилования. Если возможно, сообщайте о насилии на платформах социальных сетей через специальные каналы сообщений. Делайте скриншоты как можно большего количества сообщений, включая содержание, дату, время и имя злоумышленника. Рекомендуется создать электронную таблицу для отслеживания преследований с указанием их даты и времени, а также платформы, на которой они произошли. Более подробную информацию от PEN America о документировании преследования можно найти [здесь](#).



ПРЕСЛЕДОВАНИЕ ВИНОВНОГО(-ЫХ) И ПОИСК ПРАВОВЫХ ИНСТРУМЕНТОВ ДЛЯ ЗАЩИТЫ

Привлечение к ответственности за киберпреследование женщин-журналистов может происходить по различным правовым нормам, начиная от домогательств и угроз и заканчивая положениями о защите свободы прессы. В зависимости от юрисдикции сексизм или гендерно-мотивированное поведение могут считаться отягчающим обстоятельством, если они послужили мотивом для совершения преступления или правонарушения.

На практике, столкнувшись с киберпреследованием, женщины-журналисты могут принимать различные меры, чтобы остановить или избежать дальнейшие преследования, а также для создания аргументов в пользу судебного иска:

- во-первых, особенно в случае выдача себя за другое лицо в Интернете и/или доксинга, поддерживать связь с источниками информации и контактами, чтобы они могли предвидеть дальнейшее преследование и защитить себя;
- во-вторых, собирать доказательства, такие как свидетельские показания и скриншоты сообщений и изображений, полученных или размещенных в Интернете;

- в-третьих, связаться с веб-сайтами, на которых размещены соответствующие страницы, и попросить удалить информацию, и, возможно, потребовать более активных действий по фильтрации атак и постоянному удалению злоумышленников с платформ социальных сетей;
- наконец, сообщить о преследовании, используя механизмы, установленные местными властями, и, в соответствующих случаях, подать жалобу в местную полицию, прибегнув при необходимости к помощи адвоката.
- Рассмотрите все «за» и «против» передачи информации о насилии в новостях или тематической статье для поднятия этого вопроса в общественной повестке дня.



04

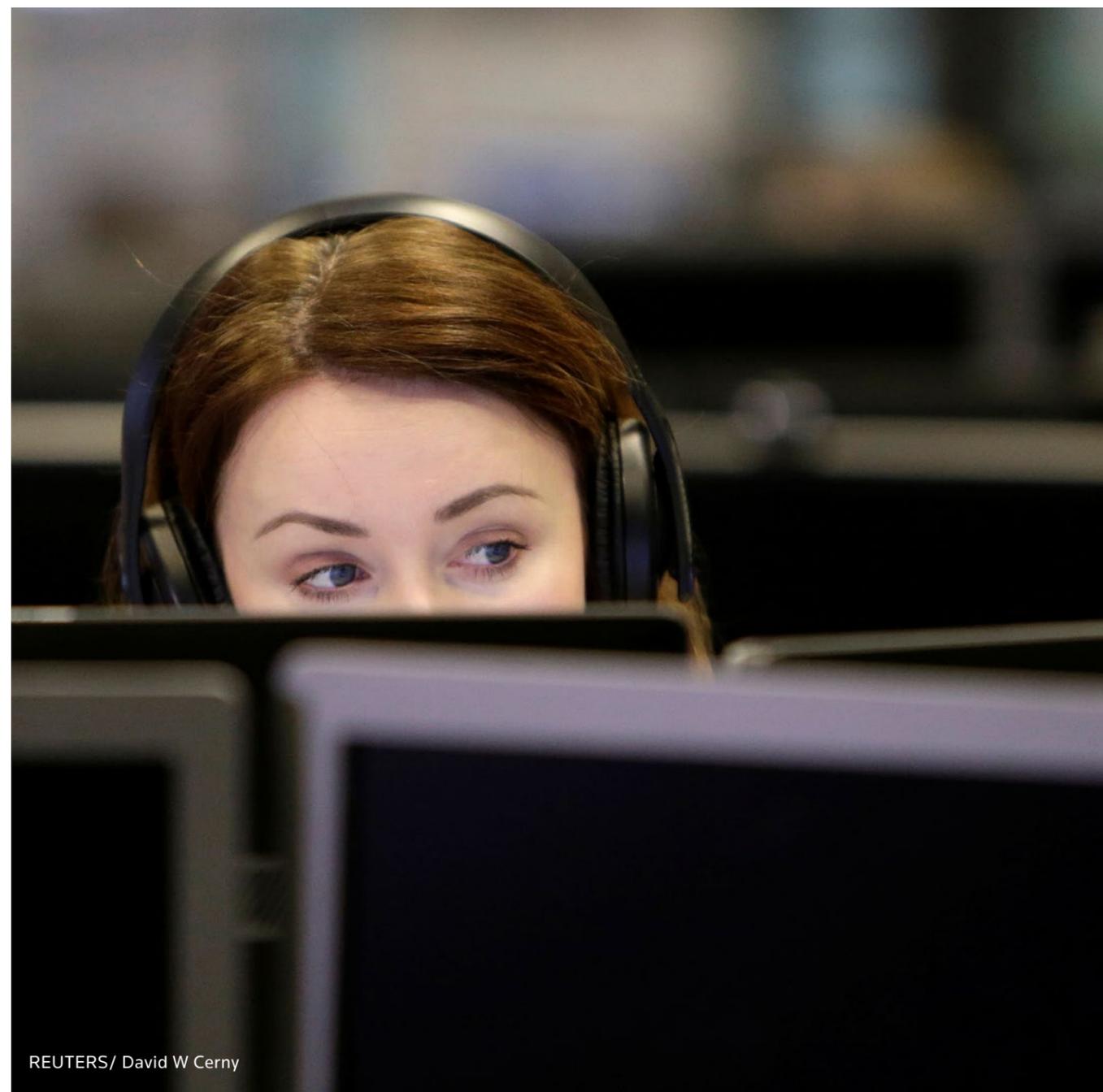
ОРГАНИЗАЦИИ И РЕСУРСЫ

Существует множество организаций, разработавших полезные ресурсы для поддержки женщин-журналистов в борьбе с киберпреследованием.

01	Access Now	Поддержка по цифровой безопасности доступна на следующих языках: <u>английском, испанском, французском, немецком, португальском, русском, арабском, тагалоге и итальянском</u>
02	Dart Center	<u>Руководство по самозащите</u> для преодоления психосоциального воздействия киберпреследования
03	Electronic Frontier Foundation (Фонд «Электронная граница»)	Основные руководства по самозащите Surveillance Self Defense доступны на <u>английском, испанском, французском, арабском и португальском</u> языках.
04	Digital Rights Foundation (DRF)	DRF проводит исследования <u>исследования и тренинги</u> в области онлайн-безопасности
05	Frontline Defenders and Tactical Tech Security in a Box («Безопасность в коробке»)	Набор инструментов и тактик по цифровой безопасности доступен на <u>английском, испанском, французском, арабском и португальском</u> языках.
06	HeartMob	<u>Онлайн</u> -поддержка и ресурсы
07	Online SOS	Ресурсы по борьбе с <u>онлайн</u> преследованиями для американской аудитории
08	PEN America	Подробное руководство по борьбе с киберпреследованием доступно на <u>английском и испанском</u> языках.

09	SMEX	Руководство по самозащите в Интернете для женщин на <u>арабском</u> и <u>английском</u> языках.
10	Tactical Tech	Руководство, включающее информацию о «самодоксинге», на <u>испанском</u> языке.
11	Комитет по защите журналистов	Индивидуальная помощь и ресурсы по цифровой безопасности, доступные на разных языках
12	Комитет по защите журналистов	«Удаление личных данных из Интернета» на <u>английском, испанском и французском</u> языках
13	Комитет по защите журналистов	«Защита от целенаправленных атак в Интернете» на <u>английском, испанском и французском</u> языках.
14	Международный фонд женских СМИ (IWMF)	Программа борьбы с онлайн-насилием на <u>английском, французском и испанском</u> языках, предлагающая индивидуальную помощь в обеспечении цифровой безопасности для женщин-журналистов и ресурсы для борьбы с киберпреследованием.
15	Международный фонд женских СМИ (IWMF) и Free Press Unlimited	Know your Trolls доступен на английском, испанском, французском и арабском языках.
16	Международный фонд женских СМИ и Международный центр для журналистов	<u>Онлайн-насилие</u> Центр реагирования

17	Международный фонд женских СМИ (IWJF) и Free Press Unlimited	Keep it Private доступен на английском, испанском, французском и арабском языках.
18	Международный фонд женских СМИ (IWJF) и Центр развития журналистики в Северной и Южной Америке имени Джона С. и Джеймса Л. Найта (Knight Centre for Journalism in the Americas)	<u>«Киберпреследование: стратегии защиты журналистов»</u>
19	The NYT Open team	<u>Руководство по защите от «самодоксинга»</u>
20	Фонд имени Рори Пека	<u>Руководство по цифровой безопасности</u> включает в себя руководства по защите от киберпреследования и троллинга в Интернете (доступно на нескольких языках).
21	Troll Busters	<u>Ресурсы</u> по борьбе с киберпреследованием на разных языках
22	UNESCO	С дискуссионным документом ЮНЕСКО можно ознакомиться <u>здесь</u> . Дополнительные ресурсы, инструменты и исследования ЮНЕСКО и партнеров можно найти на сайте <u>https://en.unesco.org/themes/safety-journalists/women-journalists</u> .



REUTERS/ David W Cerny



REUTERS/ Damir Sagolj

Опубликовано в 2021 г. Организацией Объединенных Наций по вопросам образования, науки и культуры, 75352 Paris 07 SP, France. ©UNESCO

Данная публикация предлагается в открытом доступе под лицензией Attribution ShareAlike 3.0 IGO (CC-BY-SA 3.0 IGO) (<http://creativecommons.org/licenses/by-sa/3.0/igo/>). Используя содержание данной публикации, пользователи соглашаются с правилами пользования Репозиторием открытого доступа ЮНЕСКО. Репозиторий (<http://en.unesco.org/open-access/terms-use-ccbysa-en>).



Использованные названия и представление материалов в данной публикации не являются выражением со стороны ЮНЕСКО какого-либо мнения относительно правового статуса какой-либо страны, территории, города или района или их соответствующих органов управления, равно как и линий разграничения или границ. Ответственность за взгляды и мнения, высказанные в данной публикации, несут авторы. Их точка зрения может не совпадать с официальной позицией ЮНЕСКО.

В сотрудничестве с



TrustLaw



При поддержке



При поддержке

