INSI

Цифровая защита

Противодействие онлайн-насилию внутри редакции и за ее пределами

JOURNALISM | SAFETY | RESPONSIBILITY | COMMUNITY

Оглавление

Введение

Медиаиндустрия сталкивается с непрекращающейся волной онлайн-атак на журналистов — со стороны государственных структур, организованных преступных сетей, ботов и обычных пользователей, воодушевленных анонимностью. Слова ненависти, дезинформация и угрозы физического насилия стали повседневной реальностью для многих наших коллег. Одни вынуждены покинуть профессию, другие испытывают длительное психоэмоциональное напряжение — и всё это происходит в то время, когда независимая и глубоко проработанная журналистика особенно необходима как никогда.

Цифровое насилие крайне трудно сдерживать. Одно остается очевидным: журналисты ожидают от своих работодателей ответственности на всех этапах — до, во время и после атак, — выражающейся не только в поддержке, но и в конкретных действиях.

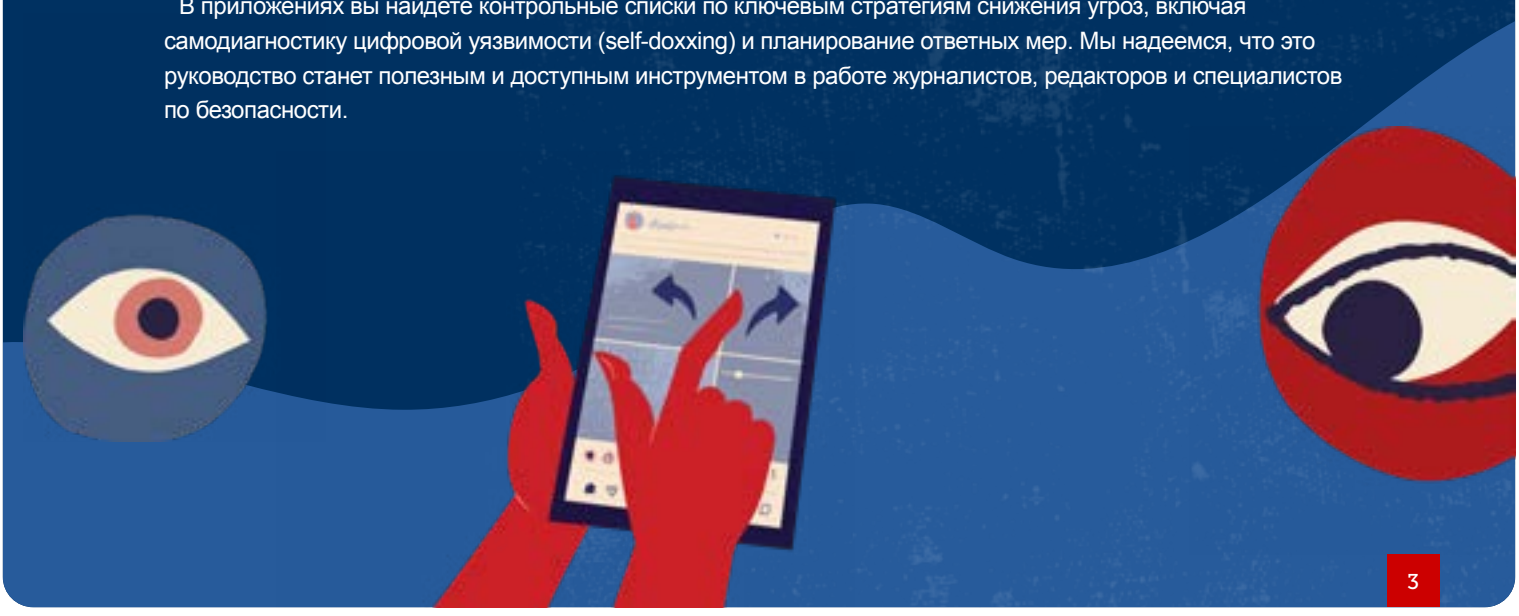
С 2020 года организации — члены INSI регулярно встречаются, чтобы обменяться опытом и наработанными подходами. На начальном этапе реализация инициативы осуществлялась при поддержке Google News Initiative и Facebook, которым мы выражаем особую признательность за содействие и участие.

Настоящее руководство, подготовленное для INSI Майком Кристи — ключевым участником данной работы, основано на проведенных встречах и последующих обсуждениях. В качестве глобального руководителя по безопасности в Reuters он заложил стандарты того, как медиакомпании могут защищать своих сотрудников от физических, цифровых и эмоциональных угроз. Его вклад стал важным элементом в формировании лучших отраслевых практик. Руководство предназначено для руководителей редакций — как в редакционных, так и в подразделениях по работе с персоналом и службах безопасности. Его цель — помочь выстроить практическую систему по снижению воздействия онлайн-угроз и подготовке к ситуациям, когда цифровое насилие может перерасти в физическую угрозу.

Каждая редакция сталкивается с собственным уровнем рисков, обладает уникальной культурой и разным объемом ресурсов. Но с цифровым насилием не стоит бороться в одиночку. Куда более действенным является отраслевое сотрудничество — включая взаимодействие с цифровыми платформами по вопросам соблюдения правил и привлечения к ответственности, а также государственными структурами в сфере эффективного регулирования. INSI призывает все организации-члены активно участвовать в этих совместных инициативах и внедрять принципы коллективной устойчивости в свою политику реагирования.

Мы понимаем, что многие редакции уже хорошо осведомлены о масштабах и характере онлайн-угроз, но при этом испытывают дефицит времени. Поэтому руководство начинается с самых срочных и практичных шагов. Вначале представлена рабочая схема действий против цифровых атак, специально разработанная для менеджеров, отвечающих за безопасность и поддержку персонала, после чего рассматриваются более широкие аспекты проблемы.

В приложениях вы найдете контрольные списки по ключевым стратегиям снижения угроз, включая самодиагностику цифровой уязвимости (self-doxxing) и планирование ответных мер. Мы надеемся, что это руководство станет полезным и доступным инструментом в работе журналистов, редакторов и специалистов по безопасности.



Профилактические меры

В современном высокотехнологичном мире журналисты сталкиваются с растущими рисками: злоумышленники используют устройства, подключенные к облаку, а также объединенные базы данных на разных платформах. Неопределенная угроза уже вызывает тревогу, — но если в сообщении упоминается, например, школа ребёнка или фото спальни, найденное на сайте агентства недвижимости, — угроза становится вполне реальной. Чтобы защитить сотрудников, редакции необходимо планировать меры по защите своих сотрудников заранее.

1. Оцените масштаб проблемы

Проведите опрос среди сотрудников редакции, чтобы понять, насколько серьезной является проблема онлайн-угроз и цифрового насилия. Обязательно включите в исследование женщин и представителей меньшинств — именно они чаще становятся мишенью для таких атак.

2. Организуйте обучение

Включите основную информацию об онлайн-угрозах, их последствиях и действиях компании в такие курсы, как:

- тренинги по безопасности в условиях враждебной среды;
- тренинги по информационной безопасности.

Также можно проводить специальные воркшопы, целиком посвящённые теме цифрового насилия.

3. Создайте каналы для подачи жалоб

Расскажите сотрудникам, как они могут сообщить о случаях онлайн-угроз — особенно если они поступают через личные сообщения или социальные сети. Это может быть:

- канал в Slack или Microsoft Teams;
- отдельный адрес электронной почты;

Также можно создать пространство, где журналисты смогут анонимно делиться опытом, выявлять тенденции и поддерживать друг друга.

Важно: редакционная служба безопасности должна заранее знать, если готовится материал, способный вызвать негативную реакцию онлайн. Не стоит дожидаться последствий.

4. Проведите самопроверку уязвимости (self-doxxing)

Предложите журналистам самостоятельно проверить, какие данные о них имеются в открытом доступе. Полностью удалить информацию, накапливавшуюся десятилетиями в интернете, невозможно — например, в США адрес собственности зачастую доступен в публичных реестрах. Однако значительная часть информации может утекать из социальных сетей при недостаточно защищенных настройках конфиденциальности. Включите это задание в программу адаптации новых сотрудников.

5. Проведите углубленный анализ для уязвимых групп

Особое внимание стоит уделить журналистам с высокой публичностью или тем, кто работает с деликатными или потенциально конфликтными темами. Такую работу может взять на себя:

- внутренний IT-отдел или отдел по управлению рисками,
- либо внешний подрядчик.

6. Используйте сервисы удаления данных

Такие сервисы, как DeleteMe, позволяют автоматически направлять запросы на удаление персональных данных из баз данных брокеров, торгующих информацией о пользователях. Хотя такие инструменты доступны не во всех странах, все же рекомендуется:

- оформить корпоративную подписку,
- либо предоставить индивидуальные аккаунты журналистам, находящимся в зоне риска.

Важно понимать: эти сервисы не удаляют сам источник утечки, но позволяют ограничить дальнейшее распространение.

7. Подключите сервисы мониторинга угроз

Многие медиакомпании уже используют решения для мониторинга бренда и репутации. Такие системы отслеживают:

- нарушение авторских прав,
- поддельные сайты и аккаунты,
- оскорбительный контент, наносящий ущерб репутации.

Кроме того, существуют специализированные системы, которые могут выявлять:

- цифровые угрозы, направленные против организации;
- персональные угрозы в адрес отдельных журналистов;
- активность в закрытых каналах, включая Telegram и даркнет.

8. Удалите старые публикации

Рекомендуется рассмотреть возможность удаления ранних постов в социальных сетях, которые могут показаться легкомысленными или иметь политическую окраску. Например:

- прежние политические взгляды могут вызвать сомнения в объективности журналиста при освещении выборов;
- Фотографии с вечеринок могут быть использованы против журналистов, работающих с ультра консервативными группами, и представлять угрозу для их безопасности.

Включите эту проверку в стандартную процедуру для новых сотрудников.

9. Сделайте публичные профили менее информативными

Для тележурналиста фото в профиле может служить частью имиджа. Однако журналисту, занимающемуся расследовательской финансовой журналистикой, стоит задуматься: действительно ли необходимо размещать свое фото в профиле? Женщинам особенно рекомендуется использовать гендерно-нейтральные изображения. Фото может быть использовано для отслеживания через программы распознавания лиц.

10. Разделяйте личные и профессиональные аккаунты

Создайте:

- отдельный личный аккаунт — только для семьи и друзей, с максимально строгими настройками конфиденциальности;
- отдельный рабочий аккаунт — с минимальным количеством личной информации и исключительно профессиональным контентом.

Рабочий аккаунт следует вести с пониманием того, что всё опубликованное может стать достоянием общественности и использоваться злоумышленником.

11. Обучение работе на публике

Организуйте тренинги для журналистов по правилам поведения на публичных мероприятиях, конференциях и в прямом эфире. Это особенно важно, поскольку:

- ультраправые группы нередко пытаются спровоцировать журналистов публичными вопросами, записывают их реакцию и распространяют вырванные из контекста фрагменты в сети с целью дискредитации;
- некоторые агрессивно настроенные лица выдают себя за информаторов и предлагают «сенсационные» сведения, чтобы спровоцировать журналиста на предвзятую реакцию и использовать ее против него.

12. Определите сотрудников, которым требуется повышенное внимание

Некоторые журналисты нуждаются в дополнительной подготовке и защите. Особое внимание стоит уделить следующим категориям:

- политическим обозревателям и фактчекерам;
- сотрудникам, работающим в странах, где государственные структуры используют онлайн-угрозы как инструмент давления;
- женщинам, а также представителям расовых, этнических и ЛГБТК+ сообществ;
- журналистам с активным присутствием в социальных сетях;
- журналистам, публично упомянутым или подвергнутым критике со стороны влиятельных лиц или лидеров;
- репортерам, освещающим острые международные и геополитические темы.

13. Модерация комментариев

Поддержание безопасного и корректного общения в комментариях — серьёзная задача, требующая выделенных ресурсов. Некоторые новостные организации просто отключают возможность комментирования. Другие используют автоматизированные инструменты или сочетание автоматизации на базе ИИ и модерации вручную.

Важно помнить: даже если комментарии направлены не лично на журналиста, а в адрес редакции, их необходимо отслеживать — в них могут содержаться завуалированные угрозы или призывы к насилию.

14. Создание межфункциональной группы реагирования

В случае серьезных онлайн-угроз может потребоваться скоординированное участие нескольких отделов. Рекомендуется заранее сформировать группу быстрого реагирования, куда должны входить:

- **Редакционное руководство** — принимает решения о перемещении сотрудника, усилении охраны или обращении в правоохранительные органы;
- **Служба безопасности редакции** — отвечает за физическую, цифровую и эмоциональную безопасность журналиста;
- **Специалисты по информационной безопасности (IT)** — отслеживают атаки, выявляют их источники и ведут журнал угроз;
- **Корпоративная служба безопасности —** не допускает известных преследователей в редакционные помещения или на объект;
- **Юридический отдел** — оценивает возможности правового реагирования на угрозы с учетом законодательства о свободе слова;
- **Отдел по работе с персоналом (HR)** — организует психологическую поддержку и консультирует по вопросам временного перевода сотрудников;
- **Отдел по связям с общественностью —** при необходимости выступает с официальными заявлениями от имени организации в СМИ или социальных сетях;
- **Группа поддержки коллег** — оказывает моральную и практическую помощь пострадавшему журналисту внутри коллектива.

15. Разработка редакционных рекомендаций по онлайн-безопасности

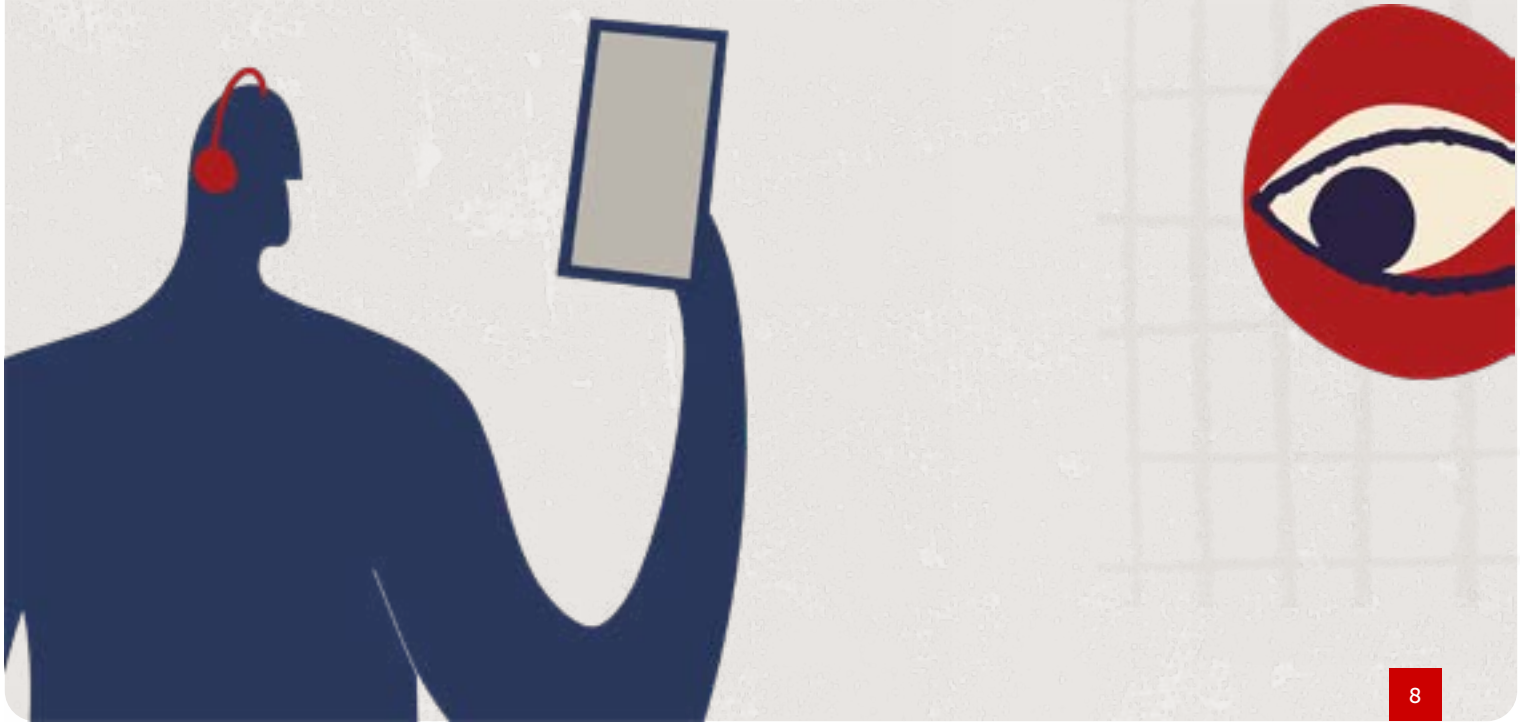
База рекомендаций по безопасности в новостной организации должна включать материалы о природе онлайн-агрессии, её последствиях и о том, какую поддержку компания оказывает журналистам. Основные инструкции по информационной безопасности также должны охватывать тему онлайн-преследования.

16. Снижение рисков в условиях слабой цифровой защиты

Политика BYOD (Bring Your Own Device — использование личных устройств) и широкое привлечение внештатных сотрудников затрудняют сокращение поверхности атаки на редакции и журналистов. Защищенное приложение для общения с конфиденциальным источником может быть установлено как на рабочем, так и на личном ноутбуке. Переписка может сохраняться в облаке в небезопасном виде — в аккаунтах, к которым корпоративная служба информационной безопасности не имеет доступа.

Способы снижения рисков:

- Рассмотрите возможность публикации особо спорных материалов без указания авторства. Это часто вызывает возражения со стороны журналистов, и их мнение следует учитывать.
- Пересмотрите политику публикации подробных профилей журналистов на сайте и размещения ссылок на их профили в самих новостных материалах. Такие профили могут быть полезны для развития личного бренда, но также увеличивают объем потенциально конфиденциальной информации в открытом доступе. Большинство профилей содержат фотографии, что позволяет злоумышленникам отслеживать журналистов с помощью программ распознавания лиц.
- Настройки, позволяющие контенту широко распространяться и становиться вирусным, могут использоваться и для онлайн-агрессии. Редакции стоит разработать рекомендации по безопасному использованию этих настроек и стратегически подходить к их применению.



Механизмы подачи жалоб

Формируйте доверие у журналистов

Онлайн-угрозы часто поступают не через официальные каналы, контролируемые компанией — не в виде комментариев под статьями или писем на корпоративную почту.

На практике большинство угроз и оскорблений поступает в личные сообщения через персональные профили в социальных сетях.

Чаще всего они приходят:

- личными сообщениями в социальных сетях;
- на персональные аккаунты;
- через мессенджеры, не контролируемые IT-отделом.

Причины, по которым журналисты не сообщают об угрозах:

- считают это «частью профессии»;
- боятся, что это подорвет доверие к ним как к профессионалам;
- опасаются, что редакция отстранит их от освещения темы;

Журналистов необходимо поощрять сообщать о таких угрозах. Способы поощрения включают в себя:

Обучение и повышение осведомленности. Каждая обучающая программа должна чётко пояснять:

- какие меры принимает компания для предотвращения онлайн-угроз;
- какую поддержку получит пострадавший сотрудник;
- уверенность в том, что журналист не будет отстранен от освещения, если он сообщит о факте домогательств или угроз.

Создание каналов обратной связи. Эффективные и доступные способы подачи жалоб:

- Используйте удобные платформы для сбора информации и жалоб — например, Slack или Microsoft Teams, онлайн-формы или электронную почту.
- Важно: все обращения должны своевременно отслеживаться и обрабатываться. Если журналисты видят, что жалобы игнорируются — доверие будет утрачено.

Жалобы

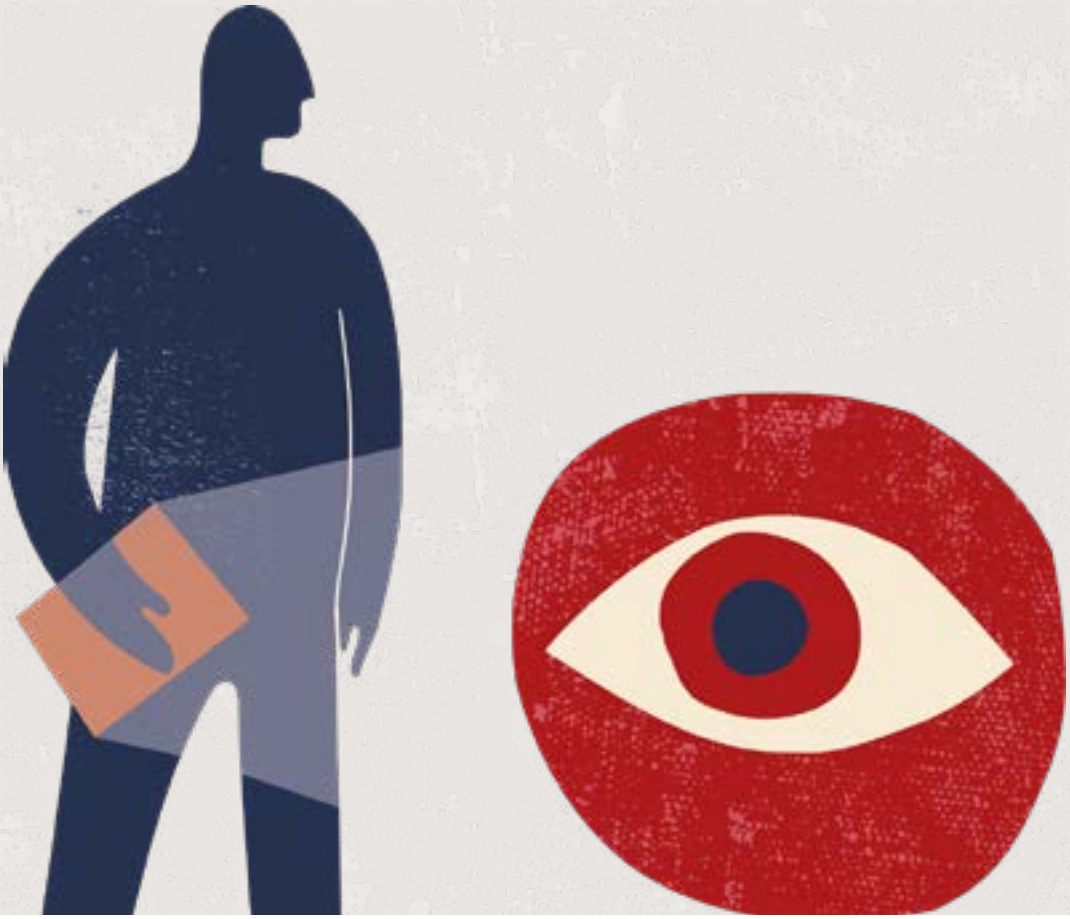
Некоторые социальные платформы предоставляют специальные порталы для партнеров, а также назначают представителей, через которых организации могут подавать жалобы и экстренные запросы.

Через эти каналы можно:

- сообщить о взломе аккаунта;
- пожаловаться на кражу учетных данных;
- передать информацию о травле, домогательствах или подделке профилей;
- запросить удаление контента, нарушающего правила.

В других случаях отдельные пользователи может потребоваться самостоятельно сообщать о случаях преследования или других проблемах напрямую в социальную сеть.

Руководители должны понимать, какие платформы используют их журналисты и как эти платформы рассматривают жалобы.



Мониторинг публичных угроз

Для отслеживания публичных проявлений онлайн-агрессии новостные организации используют специальные инструменты, позволяющие выявлять потенциальные угрозы для редакций и объектов. Большинство таких систем направлены на защиту репутации бренда. Некоторые из них анализируют не только открытый интернет, но и тёмную и глубокую сеть, а также групповые чаты в приложениях вроде Telegram.

Современные решения могут отслеживать угрозы и нападения, которые поступают через личные сообщения, однако для мониторинга личных аккаунтов журналистов требуется их согласие.

Также существуют автоматизированные фильтры, которые помогают защитить журналистов и других пользователей от токсичных и оскорбительных сообщений. Они скрывают из поля зрения сообщения с определенным содержанием или словами.

Такая модерация помогает минимизировать эмоциональный вред, но в то же время может затруднить выявление серьезных угроз, требующих реакции со стороны организации. Новые системы на базе искусственного интеллекта способны одновременно блокировать оскорбления и анализировать сообщения, чтобы обнаруживать потенциально опасные угрозы.

Механизмы реагирования

После того как редакции наладили эффективные механизмы подачи жалоб и мониторинга, им может потребоваться анализировать сотни сообщений, чтобы определить, могут ли какие-либо из них повлечь серьезные последствия в реальности. Сортировка онлайн-преследования с целью выявления действительно серьёзных агрессоров, имеющих криминальное прошлое или склонность к насилию, может быть похожа на поиск иголки в стоге сена.

Рассмотрите следующее при принятии решения о том, как реагировать:

1. Идентификация нападавших

Иногда достаточно начать с обычного поиска в Google — результаты могут оказаться неожиданно информативными. Пользователи часто используют одни и те же никнеймы или псевдонимы на разных платформах, что может помочь установить личность отправителя. Онлайн-сервисы, такие как Social Catfish, можно использовать для обратного поиска по адресам электронной почты, в то время как PeekYou может искать по именам пользователей.

Отдел информационной безопасности медиакомпании также может иметь возможность определить, где расположены IP-адреса. Многие онлайн-агрессоры используют VPN, чтобы скрыть свое местоположение, и создают фальшивые одноразовые аккаунты, когда предыдущий блокируется.

2. Анализ и оценка угроз

Признаки того, что онлайн-угроза может перерасти в физическое насилие, включают:

- **Содержит прямую угрозу, такую как «Я убью тебя».** В отличие от этого, косвенная угроза, такая как «тебя следует казнить за измену», может рассматриваться как свобода выражения мнения, а не как намерение причинить вред.
- **Создает повышенный риск для журналиста.** Был ли обнародован его домашний адрес? Будет ли он в опасности, если его местоположение станет публичным?
- **Нападающий скрывает свою личность.** Это может указывать на то, что он понимает, что его действия неправильны. Нападающие, использующие свои настоящие имена, вопреки ожиданиям, могут быть более опасны, потому что они могут не осознавать, что делают что-то неправильное.
- **Месторасположение.** Человек, живущий рядом, может представлять большую угрозу, чем тот, кому нужно лететь через полмира, чтобы добраться до цели.

- **Судимость или история насилия.** Есть ли у нападающего связи с насильственными группами или разрешение на владение оружием?
- **Эскалация.** Перешли ли атаки с одной платформы на другую и увеличились ли они по объёму и агрессивности?
- **Организованность.** Вовлечено ли в атаки правительство или другой субъект? Проявляли ли они ранее готовность применять насилие? Может ли правительство также применить юридические меры или задержать журналиста?
- **Боты.** Обратите внимание на новые аккаунты без очевидной истории или те, которые уже участвовали в подобных кампаниях.

3. Защита журналистов

Блокировка онлайн-нападающих может показаться заманчивой с целью защиты эмоционального состояния журналистов. Однако блокировка также может спровоцировать эскалацию, которая останется незаметной. Злоумышленники часто создают новые аккаунты и просто продолжают преследование.

В качестве альтернативы, команда редакционной безопасности или отдел информационной безопасности могут взять на себя мониторинг личных аккаунтов в социальных сетях. Однако журналисты могут не захотеть передавать пароли или предоставлять доступ к сообщениям из конфиденциальных источников.

В такой ситуации коллега или редакционный руководитель могут отслеживать сообщения, при необходимости подключая специалистов по безопасности и информационной защите.

4. Принятие мер

Редакции должны действовать быстро, если в ходе анализа установлено, что онлайн-преследование может перерасти в реальную угрозу. Возможные действия включают:

- **Обращение в правоохранительные органы.** О прямых угрозах всегда следует сообщать в полицию или или другие уполномоченные органы. Журналистам, возможно, придется подать заявление самостоятельно.
- **Закрытие** офисов.
- **Внесение известных нападавших в списки лиц, которым запрещен вход в офисы** компании, и информирование об этом внешних подрядчиков и арендодателей.
- **Обеспечение безопасности дома или временного жилья журналиста** — установка системы охраны или подключение к охранной службе.
- **Перемещение журналиста и его семьи в отель с хорошей системой безопасности** на время оценки угрозы.
- **Назначение телохранителей** для известных медийных персон.
- **Перенаправление корпоративной электронной почты и блокировка** агрессоров в личной почте.
- **Назначение ответственного за мониторинг поступающих угроз** от имени журналиста.
- **Жалоба на нарушителя через платформу.** Журналистам, возможно, придётся самостоятельно подать жалобу с помощью доступных инструментов.
- **Принятие юридических мер.**
- **Обращение к коллегам из других редакций**, которые могут обладать информацией, помогающей оценить серьезность угрозы.

- **Публичная поддержка журналиста** для укрепления его устойчивости и морального духа.
- **Освещение случая преследования**. Это может стать эффективным способом привлечь внимание к атаке, особенно если она является частью более широкой тенденции.

5. Поддержка журналиста

Массовое преследование может оказать серьезное эмоциональное воздействие. Поддержка со стороны редакции крайне важна для устойчивости и способности журналиста продолжать работать без страха.

Следует рассмотреть следующие меры поддержки:

- **Предоставление поддержки внутри редакции** со стороны коллег и консультаций с психологом.
- **Открытое заявление позиции редакции о том, что она не обвиняет журналиста** или материал над которым он работает и поддержит его в продолжении освещения темы.
- **Помощь в подаче жалобы** на платформу или заявлении в полицию.
- **Глубокий анализ цифровых уязвимостей журналиста**, чтобы исключить возможности для дальнейших атак.
- **Проверка и усиление системы безопасности в доме журналиста.** При необходимости — решение о временном переселении журналиста и его семьи в более безопасное место.
- **Перенаправление давления со стороны агрессоров на компанию** — размещение официальных заявлений в комментариях или публикация отдельного заявления.

6. Чрезвычайные случаи

Некоторые случаи онлайн-преследования могут перерасти в угрозу физической безопасности всей редакции. Организованная и целенаправленная кампания со стороны влиятельного политического деятеля с целью разжигания гнева и ненависти, может сделать невозможной безопасную работу журналистов — на публике, на отдельных мероприятиях или в некоторых регионах. Службы безопасности, должны быть готовы к такому развитию событий и при необходимости передавать отдельные случаи преследования на уровень высшего руководства.

7. Ведение записей и извлечение уроков

Каждый новый случай онлайн-преследования может отличаться, и в каждом из них можно извлечь уроки для будущего. Ведение записей поможет организации выявлять возникающие тенденции. Это будет крайне важно для убеждения высшего руководства и финансовых директоров в необходимости выделения средств на борьбу с этой проблемой.

Чек-лист для руководителей редакций

Упреждающие меры	Оцените масштаб проблемы	Проведите опрос среди сотрудников
	Организуйте обучение и мероприятия по повышению осведомленности	Включите эту тему в базовые курсы по безопасности для всех журналистов
	Наладьте каналы коммуникации	Teams, Slack, электронная почта
	Проведите самопроверку уязвимости (self-doxxing)	Включите в программу адаптации и сделайте доступным для сотрудников в формате обучающего модуля на внутреннем портале
	Проведите углубленный анализ ситуации	Рассмотрите возможность привлечения внешнего специалиста
	Использование сервисов по удалению данных	Подпишитесь на сервисы удаления информации для журналистов, находящихся в группе риска
	Мониторинг угроз	Внешние специалисты могут отслеживать даркнет, глубокий веб и труднодоступные площадки, такие как чаты в Telegram.
	Удаляйте старые публикации	Добавьте это в адаптацию новых сотрудников
	Создавайте профили с минимальной личной информацией	Это необходимо включить в обучение и вводный курс по безопасности
	Создайте отдельные личные и рабочие профили	Обсуждайте с журналистами и редакционными командами разделение личных и профессиональных аккаунтов.
	Следите за уязвимыми группами или отдельными сотрудниками	Проведите дополнительный тренинг по безопасности для команд фактчекинга и политического направления; возможно привлечение внешнего специалиста
	Организуйте обучение навыкам публичных выступлений	Обеспечьте журналистов тренингами по правильному поведению на публике.
	Модерируйте комментарии	Внешний специалист может помочь с этим
	Сформируйте меж функциональную команду быстрого реагирования	Включите представителей руководства редакции, специалистов по безопасности, редактора по соцсетям, юристов и сотрудников, оказывающих коллегам поддержку
	Опубликуйте рекомендации по безопасности	Разместите их во внутренней сети
	Снижайте риски	Удалите фото из профилей журналистов

Чек-лист для руководителей редакций

Механизмы для подачи жалоб	Создайте канал для журналистов, через который они смогут сообщать о случаях травли	Рассмотрите использование платформ Teams, Slack или электронной почты
	Используйте каналы для отправки жалоб на платформах	К возможным вариантам относятся партнёрские порталы, прямые контакты с представителями платформ или самостоятельная подача жалоб журналистами
Механизмы мониторинга	Осуществляйте мониторинг публичных угроз	Рассмотрите возможность привлечения внешнего специалиста
	Осуществляйте мониторинг личных сообщений	Рассмотрите возможность привлечения внешнего специалиста, если журналист даст согласие
	Используйте программное обеспечение, которое защищает журналистов от оскорбительных сообщений	Это помогает снизить эмоциональное воздействие на пострадавших, но может затруднить обнаружение серьезных угроз
	Модерируйте и отслеживайте комментарии	Рассмотрите возможность привлечения сторонней организации
Механизмы реагирования	Разработайте метод выявления онлайн-агрессоров	Сервисы Social Catfish и PeekYou помогут провести обратный поиск по адресам электронной почты и псевдонимам соответственно
	Проведите анализ и классификацию угроз	Эту работу выполняет команда по безопасности, при необходимости с поддержкой внешнего специалиста
	Защищайте потенциальных жертв	По возможности привлекайте редакторов и коллег для мониторинга сообщений
	Действуйте при серьезных угрозах	Проверьте безопасность журналиста, на которого направлена угроза; проинформируйте администрацию здания; взаимодействуйте с правоохранительными органами; помогите журналисту подать заявление об угрозе; связывайтесь с платформами; принимайте решения по юридическим мерам; организуйте помощь от коллег в поддержку пострадавшему журналисту и сотрудникам, затронутым атакой
	Предлагайте поддержку	Наиболее эффективную поддержку журналисту, подвергшемуся атаке, могут оказать непосредственный начальник или сотрудники из его окружения
	Ведите учет записей	Этим процессом может управлять отдел информационной безопасности

Приложение 1. Определение онлайн-агрессии

Онлайн-преследование и травля могут принимать разные формы и преследуют цель запугать, подавить или заставить журналистов замолчать. Они могут выходить за рамки виртуального пространства и причинять эмоциональный вред, который может иметь долгосрочные последствия.

По мере развития технологий и совершенствования искусственного интеллекта мы будем сталкиваться с новыми формами онлайн-преследования, распространяемыми через каналы, о существовании которых сегодня мы почти ничего не знаем. Те платформы, на которых сейчас сосредоточено наибольшее количество токсичной травли и оскорблений, скорее всего не будут вызывать сильное беспокойство в ближайшие годы.

Принятие более оборонительной позиции и использование проактивных стратегий, направленных на повышение устойчивости оказывается более эффективными, чем сосредоточение внимания на отдельных платформах или надежда на то, что они сами будут реагировать на сообщения о травле. Онлайн-преследование также может затрагивать вопросы свободы слова, что осложняет вмешательство правоохранительных органов и делает компании социальных сетей менее склонными брать на себя ответственность за модерацию контента.

Некоторые другие определения онлайн-преследования можно найти здесь: PEN America; Школа общественного здравоохранения им. Т.Х. Чана при Гарвардском университете; Центр журналистики и травмы Dart.

Почему это важно

- Редакциям необходимо защищать своих журналистов от онлайн-преследования чтобы:
- Гарантировать, что они могут освещать события свободно, свободно, без страха и объективно.
- Защищать самих журналистов и их рабочие места от физических угроз.
- Поддерживать их психическое здоровье и эмоциональное благополучие в долгосрочной перспективе.

Одной из основных целей онлайн-травли является попытка запугать журналистов, заставить их замолчать, отказаться от освещения острых тем или вовсе покинуть профессию. И часто такие попытки оказываются эффективными.

По данным исследования ЮНЕСКО, проведённого в 2020 году среди женщин-журналистов, 30 % респондентов сообщили, что начали заниматься самоцензурой в социальных сетях после того, как подверглись онлайн-атакам. Другое исследование, проведённое Международным фондом женщин в медиа (IWMF), показало, что 40 % респондентов женщин-журналистов перестали писать на темы, способные спровоцировать нападки, а треть из них задумывалась о том, чтобы уйти из профессии.

Онлайн-преследование становится разрушительной угрозой свободе слова и экзистенциальным вызовом для журналистов и редакций, чья миссия — добиваться правды и разоблачать злоупотребления власти через качественную журналистику и бескомпромиссные расследования. Во всех случаях онлайн-преследование несет риск причинения значительного психологического и эмоционального вреда, нередко оставляя продолжительные ментальные последствия.

В некоторых случаях онлайн-атаки перерастают в физическое насилие и прямые угрозы. По данным опроса ЮНЕСКО, 20 % респондентов по всему миру сообщили, что подвергались нападениям в реальной жизни вместе с онлайн-агрессией. На Ближнем Востоке эта цифра еще выше: более половины женщин-журналистов, рассказавших в опросе о случаях онлайн-абьюза, также стали жертвами физического насилия.

Использование онлайн-агрессии как оружия

В ряде стран онлайн-агрессия была превращена в инструмент цензуры и подавления. Авторитарные правительства, экстремистские группы, политические деятели и влиятельные беспринципные личности используют её для мобилизации интернет-натиска против предполагаемых оппонентов или критиков. Влияние тысячи угрожающих или оскорбительных сообщений значительно сильнее, чем нескольких единичных.

Женщины-журналисты и журналисты из групп меньшинств

Женщины-журналисты, журналисты из меньшинств и небинарные журналисты получают значительно больше онлайн-оскорблений, чем их белые коллеги-мужчины, при этом многие из этих нападок имеют женоненавистнический или расистский характер. Когда редакция хочет оценить, в какой мере ее сотрудники подвергаются онлайн-агрессии, ей следует обязательно опросить женщин, представителей меньшинств и ЛГБТК-журналистов, так как именно они чаще всего становятся основными мишенями.

Темы, провоцирующие волну агрессии

Наиболее чувствительные и опасные направления:

- политика — особенно в странах с высокой степенью поляризации, например, США;
- авторитарные режимы и темы, связанные с ними;
- конфликтные вопросы — этнические, религиозные и территориальные споры;
- свободное выражение мнений, включая дискуссии о цензуре.

Наиболее Неожиданно высокий уровень токсичности может проявляться в таких сферах, как:

- игровая индустрия;
- инвестиции, криптовалюта, мем-акции;
- поп-культура, спорт и музыкальные фан-сообщества.

Другие темы, провоцирующие онлайн-насилие:

- Радикально правые и левые движения;
- Мизогиния;
- Антисемитизм;
- Культурные войны
- Дезинформация
- Расизм
- Свобода слова и цензура
- Геополитическая напряженность

ВИДЫ ЦИФРОВЫХ АТАК

Угрозы насилием

• Угрозы расправы, преследования, изнасилования, убийства, «возмездия» в адрес семьи, включая детей. Некоторые из них представляют собой прямые угрозы, требующие вмешательства правоохранительных органов;

• Часто подобные высказывания балансируют на грани между угрозой и выражением мнения, что усложняет своевременное реагирование.

Атаки толпой (dogpiling)

• Десятки или сотни аккаунтов скоординированно нападают на жертву;

• Массовое направление жалоб с целью блокировки аккаунта;

• Часто организуются тролль-фабриками или партийными сетями.

Кибersталкинг

• Навязчивая и длительная онлайн-слежка;

• Может включать шантаж, взлом и отслеживание активности в сети;

• Часто подпадает под определение уголовного преступления

• Журналистам необходимо обратиться за помощью к адвокату

Doxxing

публикация личной информации, такой как:

• Домашний адрес;

• Номер телефона;

• Место учёбы детей;

• Фото, документы, паспортные данные с целью провоцирования домогательства, слежки, физического нападения и тд.

• Доксинг может произойти во время работы журналиста в опасных регионах или при выполнении рискованных заданий.

Имперсонация

создание фейковых аккаунтов от имени журналиста, распространение фальшивых или компрометирующих публикаций,

может использоваться для:

• подрыва репутации;

• введения в заблуждение аудитории;

• вымогательства.

Swatting

агрессор сообщает в полицию о якобы происходящем преступлении (например, «заложник» или «убийство»),

на место выезжает спецназ или вооружённые силы.

В США были зафиксированы случаи, когда такие инциденты приводили к гибели людей.

Приложение 2. Практическое руководство для журналистов, столкнувшихся с цифровым насилием

Онлайн-угрозы и травля создаются с целью:

- запугать;
- заставить замолчать;
- подорвать уверенность в себе;
- вынудить отказаться от темы или профессии.

Что делать при серьезной атаке

- Немедленно сообщите о происходящем своему редактору или руководителю;
- Не оставайтесь наедине с проблемой: попросите поддержки.

Как повысить личную устойчивость к онлайн-атакам

Сократите объём доступной информации о себе:

- Удалите из открытых источников лишние личные данные;
- Проведите самодиагностику цифровой уязвимости (self-doxxing);
- Убедитесь, что ваш домашний адрес, номер телефона, информация о членах семьи и личные фото не доступны публично.

Разделите личную и профессиональную онлайн-жизнь

Создайте отдельные аккаунты:

- рабочий — с минимумом персональных данных, исключительно для профессионального общения;
- личный — закрытый, доступный только для узкого круга доверенных людей.

Не смешивайте личные контакты с профессиональными: не добавляйте коллег, редакторов или источников в личные аккаунты.

Информационная безопасность

Обновляйте программное обеспечение и приложения.

Уязвимости регулярно обнаруживаются в:

- операционных системах (Windows, macOS, Android, iOS);
- мессенджерах и браузерах;
- офисных и облачных сервисах.
- Обновления закрывают важные уязвимости в системе. Не откладывайте их установку.

Остерегайтесь фишинга

Более 75 % кибератак происходит через фишинговые электронные письма, содержащие ссылку или вложение, которые могут поставить под угрозу безопасность вашего компьютера.

Фишинг — основная причина взлома. Будьте бдительны, если:

- сообщение вызывает тревогу или требует немедленных действий;
- вас просят перейти по ссылке и ввести личные данные;
- письмо пришло от незнакомого отправителя;
- в тексте есть грамматические ошибки или подозрительное оформление.
- Используйте инструмент, такой как Dangerzone, чтобы открывать вложения в защищенной среде.

Используйте менеджер паролей

Программы для взлома паролей способны подбирать сотни миллионов комбинаций в секунду и использовать персональную информацию, собранную из ваших аккаунтов в социальных сетях. Поэтому крайне важно использовать менеджер паролей — специальную программу для создания надежных паролей и их безопасного хранения.

Примеры таких программ:

- 1Password;
- Dashlane;
- KeePassXC.

Они помогают:

- создавать уникальные пароли;
- хранить их в зашифрованной форме;
- использовать сложные фразы вместо простых дат рождения.
- Важно: придумайте надежный и уникальный мастер-пароль.

Проверьте, не были ли ваши данные скомпрометированы

Откройте сайт haveibeenpwned.com. Введите свой email и проверьте, не утекли ли ваши пароли при прошлых взломах. Если да:

- немедленно смените пароль;
- если использовали тот же пароль где-либо ещё — замените его везде.

Используйте двухфакторную аутентификацию

Активируйте двухфакторную аутентификацию. Она отправляет дополнительный код доступа через SMS или через приложение, такое как Google Authenticator или Symantec VIP Access. Предпочтительнее использовать приложение, поскольку SMS-сообщения могут быть перехвачены в случае клонирования вашей SIM-карты.

Регулярно оценивайте риски для информационной безопасности

Возможно, на первый взгляд ваша история не кажется чувствительной, но заранее предсказать, не приведёт ли она к появлению информации, требующей защиты, невозможно. Думайте об информационной безопасности с самого начала работы над материалом и применяйте основные меры защиты, описанные в этом документе, еще до того, как обычная новость станет более чувствительной и потребует дополнительных мер безопасности.

Используйте временный телефон

Подумайте, стоит ли брать с собой обычный телефон на встречи с источниками, если вы работаете над деликатным материалом. Опытные специалисты могут отслеживать ваш телефон и определить, что вы и источник находились в одном месте, что может поставить под угрозу их безопасность. Обсудите с руководителем, редактором или IT-специалистом, нужно ли использовать временный телефон.

Подключайтесь через VPN

Используйте VPN — он шифрует ваше подключение к интернету — когда вы выходите в сеть с рабочих или личных ноутбуков и телефонов через слабо защищённые публичные сети Wi-Fi в отелях, аэропортах и других местах. В качестве бесплатного варианта можно использовать Proton VPN.

Используйте зашифрованные приложения для чувствительной переписки

WhatsApp, Signal и Wire — хорошие варианты. Однако следует учитывать, что компания Meta, владеющая WhatsApp, сохраняет так называемые метаданные — кто с кем и когда общался, хотя содержимое переписки остается недоступным. В Telegram переписка по умолчанию не шифруется — чтобы обеспечить конфиденциальность, необходимо выбрать режим «секретного чата».

Зашифруйте жёсткий диск

Жёсткий диск на вашем ноутбуке должен быть зашифрован по умолчанию. Если это не так, доступ к данным на устройстве может получить любой. При включенном шифровании и выключенном устройстве информация остается в безопасности. То же самое касается и смартфонов.

Используйте защищенные версии сайтов

Всегда проверяйте, что сайты, которые вы посещаете, работают через защищённое соединение. Установите расширение HTTPS Everywhere, чтобы автоматически переходить на безопасную версию сайта. Избегайте ресурсов, адрес которых начинается с http://, а не https://.

Шифруйте конфиденциальные файлы и документы

Для шифрования папок и файлов можно использовать бесплатные программы с открытым исходным кодом, такие как VeraCrypt и 7-Zip.

Избегайте зарядки через общественные USB-станции

Заряжайте телефон от розетки, а не от общественных USB-станций. Например, во время чемпионата мира по футболу в 2014 году в Бразилии некоторые USB-точки в аэропорту Рио были установлены преступной группой и использовались для кражи данных с телефонов путешественников. Чтобы защититься, используйте USB data blocker — специальный адаптер, который блокирует передачу данных и позволяет передавать только питание.

Защищайте свои устройства

Держите телефоны и ноутбуки при себе, особенно если работаете с конфиденциальной информацией. Если вы оставите ноутбук в гостиничном номере, невозможно узнать, получил ли кто-то к нему доступ в ваше отсутствие.

Установите приложения, которые помогут определить, подвергался ли ваш телефон атакам вредоносного ПО. Например, iVerify позволяет проводить бесплатную глубокую проверку раз в месяц, а F-Secure Mobile Security (ранее Lookout Lite) обеспечивает постоянную защиту. Вредоносные программы, загруженные во временную память, зачастую можно удалить, просто перезагрузив устройство.

Будьте особенно осторожны при пересечении границ

Заранее перенесите важную информацию в облачное хранилище. Выйдите из аккаунтов и приложений — на случай, если сотрудник пограничной службы потребует доступ к вашему телефону или ноутбуку. Полностью выключите устройства, чтобы усложнить доступ к хранящейся на них информации.

Как защититься от доксинга

Информация, размещенная о нас в интернете, может сделать нас уязвимыми перед людьми, которым не нравятся наши материалы. Агрессоры ищут старые публикации в соцсетях, чтобы подорвать нашу репутацию как журналистов, или пытаются найти личные данные — например, домашний адрес. Иногда цель таких действий — спровоцировать других на реальные нападения.

Тролли также могут пытаться раскопать чувствительную или компрометирующую информацию, чтобы запугать или наказать журналиста.

Вот с чем вы можете столкнуться:

- Так называемый swatting — ложный вызов полиции, например, сообщение о захвате заложников по вашему адресу.
- Женщина-критик, выступавшая против доминирования мужчин в игровой индустрии, получала угрозы изнасилования, убийства и взрыва.
- Онлайн-тролль может выйти из виртуального пространства и стать настоящим преследователем.

Что можно предпринять:

Иногда полезно «задоксить» себя самостоятельно (т. е. провести self-doxxing), чтобы узнать, какая информация о вас уже есть в открытом доступе — и что могут использовать тролли.

Поиск в интернете

Проверьте своё имя в разных поисковых системах — Google, Bing, Yandex, DuckDuckGo и Baidu. Разные платформы могут показывать разные результаты, особенно если вы жили или работали за границей.

“Имя Фамилия” или “имя пользователя”	Используйте кавычки, чтобы искать точное слово или словосочетание. Ищите разные варианты вашего имени, часто используемых имен пользователей и адресов электронной почты.
1.“Имя Фамилия” - “НазваниеСМИ” 2.“Имя Фамилия” “НазваниеСМИ” -site:НазваниеСМИ.com	1.Это исключит результаты, содержащие вашу медиакомпанию “НазваниеСМИ”, показывая при этом другие результаты, которые обычно скрыты на последующих страницах. Знак минус также хорошо подходит для удаления результатов о других людях с таким же именем. 2. Ищите страницы, где упоминаются вы и ваша медиакомпания, при этом фильтруя страницы с сайта НазваниеСМИ.com.
“Имя * Фамилия»”	Звёздочка (*) выступает в роли подстановочного знака для любых промежуточных слов, например, вашего отчества или инициалов.
“(650) 656-5656” или “6506565656”	Ищите ваш номер телефона, включая альтернативные форматы.
“имяпользователя@gmail.com” filetype:pdf	Это покажет любые PDF-файлы, в которых указан ваш личный электронный адрес, например, выпускные издания или прошлые презентации.
“Имя * Фамилия” 101 Main St Los Angeles CA	Ищите упоминания, связанные с прежними адресами, городами, учебными заведениями, местами работы и публикациями.
Имя Фамилия site:reddit.com	Ищите на конкретных сайтах, чтобы найти результаты, не индексируемые поисковыми системами.

Используйте обратный поиск по изображениям

- Загрузите свое фото в Яндекс.Картинки, чтобы увидеть, где ещё в интернете оно используется.
- Загрузите фотографии из своих профилей в X (бывший Twitter), Facebook, LinkedIn и Instagram на сервис TinEye, чтобы проверить, где ещё встречаются эти изображения.

Настройте конфиденциальность в соцсетях

Социальные сети собирают данные о вас для таргетированной рекламы. Управляйте тем, какую информацию они могут использовать и сколько данных собирают, с помощью настроек конфиденциальности. Помните, что настройки регулярно обновляются, и их нужно проверять и корректировать.

Facebook

Начните с инструмента самостоятельной настройки конфиденциальности Facebook:

- В строке поиска на главной странице введите “Privacy Checkup” и нажмите “Перейти”.
- Проверьте, кто может видеть данные вашего профиля, — убедитесь, что ни один из пунктов не установлен как “Доступно всем” (Public).
- Ограничьте круг лиц, имеющих доступ к вашим публикациям, выбрав “Друзья”, “Некоторые друзья” или “Только я”.
- Учтите, что обложка профиля всегда общедоступна; замените её на изображение, на котором не видно вашего лица.

Дополнительно выполните следующие шаги в разделе Журнал действий (Activity Log):

- Нажмите “Использовать журнал действий” (Use Activity Log), чтобы просмотреть вашу хронику. Скрывайте или удаляйте всё, что вы не хотите оставлять в открытом доступе. Убедитесь, что в разделе “Проверка фотографий” (Photo Review) нет изображений. Фотографии могут появляться там, если у вас включено распознавание лиц — при желании эту функцию можно отключить.
- Перейдите в раздел “Материалы с вашими отметками” (Activity You’re Tagged In), чтобы посмотреть, кто вас отмечал. В зависимости от настроек конфиденциальности автора публикации, такие отметки могут быть видны всем пользователям.

Далее

- Вернитесь на страницу настроек “Конфиденциальность” и нажмите “Ограничить аудиторию прошлых публикаций” (Limit Last Posts).
- Проверьте, кто может видеть приложения, которые вы используете, и насколько вас могут найти по ним.
- Ознакомьтесь с настройками приватности своих друзей: ваши комментарии и лайки, а также их активность на вашей странице (комментарии и лайки) могут быть доступны другим. Даже если вас не отмечали, заинтересованные пользователи могут просматривать круг ваших контактов (семью, коллег) или тех, кто взаимодействовал с публичными элементами вашего профиля (например, лайкнул обложку или фото профиля).
- Убедитесь, что вас устраивают параметры в разделе “Реклама” (Ads).
- В разделе “Профиль и отметки” (Profile and Tagging) включите опцию “Просматривать публикации, в которых меня отмечают, прежде чем они появятся в хронике”.
- С помощью функции “Просмотр как” (View As) посмотрите, как ваш профиль выглядит для других пользователей.

Instagram

- Создайте профессиональный аккаунт и заведите отдельный личный профиль, ограниченный только друзьями и семьей.
- Переведите личный аккаунт в режим “Закрытый аккаунт” (Private Account), чтобы видеть ваши публикации могли только одобренные вами подписчики.
- Отключите отображение статуса активности (Show Activity Status) в личных сообщениях и при ответах в историях, чтобы никто не видел, когда вы онлайн.
- В разделе “Редактировать профиль” (Edit Profile) снимите галочку с опции, которая предлагает ваш аккаунт в рекомендациях других пользователей.
- В настройках приложения на телефоне откройте “Конфиденциальность и безопасность” (Privacy and Security) и отключите или ограничьте доступ к геолокации: включайте его только когда действительно хотите поделиться местоположением.
- Проверьте параметры “Отметки и упоминания” (Tags and Mentions) и “Комментарии” (Comments), чтобы контролировать, кто может отмечать вас, упоминать и комментировать ваши публикации.

LinkedIn

LinkedIn — профессиональная сеть, и ваш профиль с фотографией по умолчанию открыт для всех. Однако разведслужбы нередко создают фальшивые аккаунты, добавляются к вам в контакты и изучают вашу сеть. Также на LinkedIn активны мошенники, предлагающие фиктивные вакансии.

Чтобы обезопасить себя, выполните следующие настройки:

- В разделе “Настройки и конфиденциальность” → “Видимость вашего профиля и сети” (Visibility of Your Profile & Network) проверьте, насколько широко вы делитесь своим именем, списком контактов и регионом.
- Ограничьте круг лиц, которые могут видеть ваши контакты. Если среди ваших собеседников есть чувствительные источники, выберите “Только я” (Only You).
- Переведите себя в “Приватный режим” (Private Mode), чтобы люди, чьи профили вы просматриваете, не узнали об этом.
- Ограничьте доступ к вашему email только первому уровню связей (1st Degree Connections).

Затем

- В разделе “Показывать профиль за пределами LinkedIn” (Profile Visibility off LinkedIn) выберите “Нет”, если вы не хотите, чтобы ваш профиль отображался на платформах-партнерах.
- Настройте, кто может найти ваш профиль по адресу электронной почты или номеру телефона, если эти люди не находятся у вас в контактах.
- В разделе “Видимость ваших действий в LinkedIn” → “Подписчики” (Followers) решите, будут ли все пользователи LinkedIn видеть ваши публичные обновления или только подписчики.

Кроме того

- Будьте осторожны при синхронизации контактов, особенно если среди них есть люди, чью конфиденциальность нужно сохранить; при необходимости удалите все синхронизированные события календаря.
- Проверьте, не публиковали ли вы старое резюме с указанием домашнего адреса.
- Удалите из профиля информацию о своей средней школе.

X

X (ранее Twitter) — одна из основных площадок для онлайн-агрессии в отношении журналистов и одно из первых мест, куда злоумышленники обратят внимание в поисках уязвимостей вашей приватности. Чтобы усилить защиту профиля, выполните следующие шаги:

- Решите, стоит ли использовать в профиле фото, которое может пригодиться программам распознавания лиц, и насколько подробно заполнять раздел “О себе”.
- Не указывайте дату рождения и отключите отображение местоположения в разделе “Ваши публикации”.
- В меню “Конфиденциальность и безопасность” выберите “Защитить публикации” (Protect Your Posts) в разделе “Аудитория, медиа и отметки” (Audience, Media and Tagging), чтобы ограничить круг лиц, которые могут видеть ваши публикации. Отключите “Отметки на фото” (Photo Tagging).
- В разделе “Личные сообщения” (Direct Messages) задайте, кто может отправлять вам сообщения.
- В разделе “Видимость профиля” (Discoverability) настройте, могут ли люди, имеющие ваш адрес электронной почты или номер телефона, находить вас на X.
- Будьте осторожны при синхронизации контактов вашего телефона с X, особенно если среди них есть люди, чья конфиденциальность должна быть защищена.
- В разделе “Обмен данными и персонализация” (Data Sharing and Personalization) отключите “Персонализированную рекламу” (Personalized Ads).
- В тех же настройках снимите галочку с опции персонализации на основе “Inferred Identity” и запретите “Обмен данными с бизнес-партнерами” (Data Sharing With Business Partners).
- Примите решение, разрешить ли использование вашего контента для обучения искусственного интеллекта Grok.

Личные сайты

Если у вас есть личный сайт, домен может быть привязан к вашему адресу, номеру телефона, имени и электронной почте — это лёгкий способ узнать ваши контактные данные.

- Перейдите на сайт DomainTools, введите URL вашего сайта и проверьте, не доступна ли ваша личная информация.
- Подумайте о скрытии данных через сервис защиты приватности, например Who is Guard.
- Ознакомьтесь с предложениями вашего регистратора доменов: возможно, у него есть бесплатные или платные опции для сокрытия ваших персональных данных.

Смените пароли на взломанных аккаунтах

Если ваш аккаунт был взломан, имя пользователя и пароль могли попасть в продажу и оказаться в даркнете.

- Сервис Have I Been Pwned? поможет проверить, не были ли скомпрометированы ваши данные в известных утечках. Как только вы это выясните, немедленно измените пароль в затронутом аккаунте, а также во всех других сервисах, где вы использовали ту же комбинацию логина и пароля.
- При помощи программ вроде Keeper Security генерируйте длинные случайные пароли или фразы-пароли и храните их в надежном зашифрованном хранилище.
- Настройте 2FA через приложение-генератор кодов вместо SMS — так безопаснее.
- Выбирайте проверенный почтовый сервис например, Gmail и усилите его защиту аппаратным ключом безопасности YubiKey.
- Создайте новый, не скомпрометированный логин на основе отдельного email-адреса, который используется только для одной конкретной цели — например, для покупок в онлайн-магазинах.

Компании по сбору и продаже данных

Существует множество компаний-посредников, которые собирают ваши личные данные и сводят их в отчеты для последующей продажи. Вы можете попросить об удалении своих данных из их баз, но это зачастую сложно и требует периодического повторения, что отнимает много времени.

- Подпишитесь на сервис автоматического удаления данных, например DeleteMe или Optery — они возьмут всю рутинную работу на себя.
- Используйте приложение Permission Slip для отправки автоматических запросов на удаление. Платная версия предоставляет расширенные функции.

Приложение 3. Инструменты и ресурсы для журналистов и руководителей

Инструмент	Назначение
Tall Poppy	Комплексная защита от онлайн-преследования: обучение, реагирование, поддержка VIP
PEN America	Ресурсы и курсы по борьбе с цифровой травлей
Troll Busters	Консультирование по реагированию на онлайн-преследование
Theseus	Анализ цифровых угроз и рисков
DeleteMe	Удаление персональных данных из баз брокеров и агрегаторов
Permission Slip app	Автоматизация запросов на удаление персональных данных (расширенный функционал — в платной версии)
Mark Monitor	Защита бренда, управление доменами, борьба с фальсификацией
Proofpoint	Защита от фишинга и подмены личности
ZeroFox	Мониторинг даркнета и цифровая безопасность
Elv.ai	Автоматическая модерация комментариев, мониторинг угроз
Memetica	Выявление угроз
Interfor	Мониторинг соцсетей, выявление угроз
Ontic	Анализ угроз и расследования
Dataminr	Мониторинг угроз
JustDeleteMe	Удаление старых аккаунтов с различных платформ
TweetDelete	Массовое удаление твитов и постов в X (Twitter)
tweeteraser	Массовое удаление твитов и постов в X (Twitter)
Google's PerspectiveAPI	Автоматическая фильтрация и модерация токсичных комментариев

Дополнительные ресурсы

- PEN America — Практическое руководство по работе с онлайн-угрозами
- Zebra Crossing — Контрольный список цифровой безопасности
- IWMF — Индивидуальные консультации Международного фонда женщин в СМИ
- Reporters Without Borders (RSF) — Отчет об онлайн-преследовании журналистов

INSI

INTERNATIONAL
NEWS SAFETY
INSTITUTE

International News Safety Institute
C/O Thomson Reuters Foundation
5 Canada Square
Floor 8
Canary Wharf
London E14 5AQ

info@newssafety. org
www. newssafety. org
@INSInews