ГИБРИДНЫЕ УГРОЗЫ И ЦИФРОВАЯ БЕЗОПАСНОСТЬ ДЛЯ АКТИВИСТОВ

ARTICLE 19

КІБЕР БАБЕР

МАТЕРИАЛ ПОДГОТОВЛЕН В ПАРТНЁРСТВЕ С ARTICLE 19 И КІБЕРБАБЁР

ARTICLE 19 Europe — один из ведущих голосов в защите свободы выражения мнений и доступа к информации в Европе и Центральной Азии. Являясь региональным офисом международной организации ARTICLE 19, мы формируем общественную дискуссию и разрабатываем новаторские ответы как на новые, так и на давние угрозы правам человека. Мы работаем на пересечении прав человека, технологий и политик, чтобы добиваться системных изменений, противостоять цензуре и защищать независимые медиа, свободу выражения мнений онлайн и офлайн, а также гражданское пространство, одновременно поддерживая силу общественной солидарности в противодействии злоупотреблениям властью.

КіберБабёр — это инициатива по цифровой безопасности, созданная в 2021 году специалистами по кибербезопасности. Мы бесплатно и конфиденциально консультируем беларусов, предоставляем инструменты и проводим тренинги, которые помогают людям, организациям и сообществам защищаться от цифровых угроз. Через доступный контент, экспертное сотрудничество со СМИ и индивидуальные консультации мы продвигаем комплексный подход к безопасности, который объединяет цифровые, психологические, физические, информационные и правовые аспекты.

ARTICLE 19
Europe Nieuwe Achtergracht 164
1018 WV Amsterdam
The Netherlands

Email: europeoffice@article19.org
Web: www.article19.org
X: @article19europe
Bluesky: @article19europe

КіберБабёр
Web: www.cyberbeaver.help
Instagram: cyberbeaver_help
Telegram: t.me/cyberbeaver

Цифровая трансформация ускоряется, и вместе с этим растут и риски. Для активистов, НГО, независимых медиа и инициатив это ежедневная реальность: заблокированный сайт, фейковый Telegram-бот, фишинговое письмо, странная DDoS-атака в день важной кампании или публикация личных данных в провластном канале.

Мы провели исследование, в котором опросили русскоязычных активистов, журналистов, правозащитников и юристов, вынужденно находящихся в эмиграции и обнаружили ряд гибридных угроз и проблем, с которыми они сталкиваются. В результате исследования мы разработали эту методичку, чтобы помочь тем, кто может находится под угрозой. Она призвана помочь вам найти первую помощь в ситуации цифровых угроз и проблем. Пожалуйста, обращайтесь к ней в случае вопросов.

ЧТО ЭТО

Гибридные угрозы — это когда давление и атаки происходят не только через физическое вмешательство, суды или законы, но и через цифровые инструменты: интернет, соцсети, инфраструктуру. К гибридным угрозам в цифровой среде можно отнести:

- кибератаки на сайты и сервисы;
- блокировки и фильтрацию интернета;
- DDoS-атаки, выводящие сайт из строя;
- фейковые страницы и чат-боты, работающие от имени НГО;
- фишинг — письма и сообщения, выманивающие данные;
- целенаправленные взломы и утечки баз данных;
- доксинг — публикацию персональных данных;
- шпионское ПО, которое следит за телефоном или ноутбуком;
- давление через платформы: цензура, удаление контента, блокировка аккаунтов.

Отдельно каждый эпизод может выглядеть как «случайность», но в совокупности это складывается в систему давления: доступ к информации сужается, люди боятся читать и делиться материалами, команды тратят силы на тушение пожаров вместо работы.

ПОЧЕМУ ЭТО ВАЖНО

Активисты, правозащитники, независимые медиа и НГО — удобная мишень. У них часто нет дорогой инфраструктуры, а работа — чувствительная: права человека, миграция, ЛГБТК+, политические репрессии, война, коррупция. Например, в Беларуси к июню 2025 году было заблокировано более 18 тысяч информационных ресурсов, из которых 7 тысяч признаны «экстремистскими».

После 2020 года блокировались независимые медиа, правозащитные ресурсы, инициативы солидарности. В России после 2022 года под блокировки попали сотни независимых сайтов: международные СМИ, правозащитные организации, расследовательские проекты и антивоенные платформы. При этом их работа необходима в ухудшающихся условиях и наша задача — перевести сложное на простой язык и дать понятный план действий: как распознать угрозу, что она значит для вас и что можно сделать уже сейчас.

КАКИЕ УГРОЗЫ МЫ РАЗБИРАЕМ

В следующих главах мы поговорим о том, с чем русскоязычные активисты в Украине, Литве, Грузии, Польше, Беларуси и других странах сталкиваются регулярно. Каждая тема — отдельная глава:

- блокировка сайтов и интернет-цензура;
- фейковые страницы, поддельные боты и доксинг;
- фишинг — как не попасться на поддельные письма и формы;
- DDoS-атаки на сайты гражданских инициатив;
- минимизация рисков утечек данных в НГО;
- шпионское ПО и целевые атаки на телефоны и компьютеры;
- базовая защита учётных записей;
- удаление идентифицирующей информации из файлов и метаданных.

КАК ЧИТАТЬ ЭТУ МЕТОДИЧКУ

Представьте, что это не «научный отчёт», а набор дорожных карт.
PDF-версию можно использовать как:

- личную памятку;
- материал для тренингов;
- основу для внутренних инструкций команды;
- чек-лист в ситуации атаки

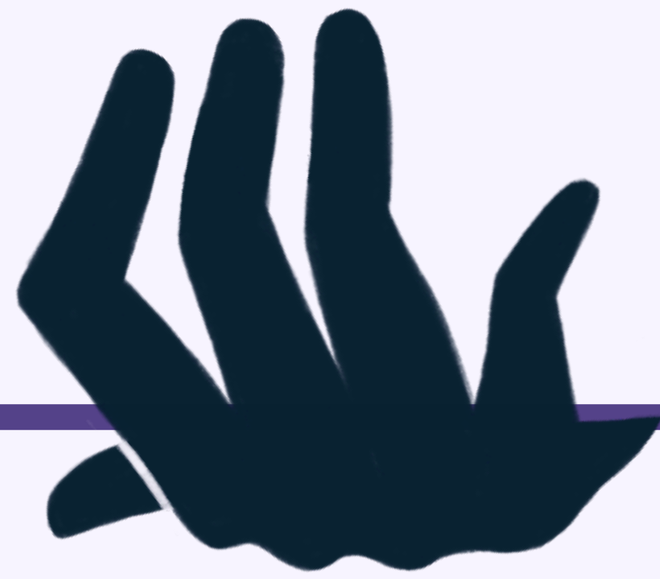
Более подробные технические детали, ссылки на инструменты и расширенные руководства вы найдёте в веб-версии или по гиперссылкам.

ЧТО МОЖНЕО СДЕЛАТЬ УЖЕ СЕЙЧАС

«Стартовый пакет», который уменьшит риски ещё до того, как вы дочитаете остальную методичку:

- вспомните и выпишите, какие у вас есть цифровые активы: сайт, соцсети, рассылки, формы, боты;
- проверьте, включена ли двухфакторная аутентификация хотя бы на основных аккаунтах (почта, соцсети, домен, хостинг);
- составьте короткий список официальных каналов организации (сайт, Telegram, Instagram и т.п.) — он пригодится и вам, и аудитории, если появятся фейки;
- договоритесь внутри команды, кто будет главным контактным лицом по цифровой безопасности: не «админ на всё», а человек, который хотя бы координирует реакцию, если что-то случится.

Это базовый уровень, который усилит эффект от всего, о чём мы будем говорить дальше.



ФЕЙКОВАЯ СТРАНИЦА

В условиях политического давления и ограничений свободы слова часто создаются фейковые страницы активистов и организаций. В Беларуси также встречались поддельные чат-боты, которые использовались для выявления и преследования активистов.

РИСКИ И ПОСЛЕДСТВИЯ

- распространение ложной информации от имени НГО или активиста;
- потеря доверия подписчиков и общественной поддержки;
- риск деанонимизации и преследования сторонников;
- угроза безопасности данных и репутации организации;
- усиление пропаганды и дискредитации.

Фейковые аккаунты — один из инструментов давления на активистов и НГО. Они позволяют властям и противникам гражданского общества не только дискредитировать организации, но и собирать данные для дальнейших репрессий.

Быстрое реагирование критически важно: чем раньше подписчики узнают о фейке, тем меньше у него шансов распространить ложную информацию или навредить людям.Важно не только блокировать такие страницы, но и укреплять доверие аудитории, подтверждать подлинность своих каналов и повышать прозрачность. В долгосрочной перспективе именно это помогает сохранять поддержку и защищать сообщество от манипуляций.

ЧТО ДЕЛАТЬ?

Заявить о фейке в своих соцсетях и предупредить аудиторию;

Написать жалобу на платформе через официальную форму (Facebook, Instagram, Telegram и др.);

Зафиксировать доказательства: скриншоты, ссылки, даты публикаций;

Повышать узнаваемость: регулярно напоминать, как отличить оригинальные страницы от фейков;

Верифицировать по возможности аккаунты, настроить оповещения о новых упоминаниях через Google Alerts или Mention.

МЕТАДАННЫЕ В ФАЙЛАХ

Почти каждый файл — фотография, документ, аудио или видео — содержит метаданные: скрытую служебную информацию. Это могут быть имя автора, дата и время создания, модель устройства, версия программы, история правок и даже географические координаты. Чаще всего мы не видим эти данные и не задумываемся о них, но именно они могут выдать человека или организацию.

Для НГО, журналистов и активистов, особенно работающих в условиях репрессий (Беларусь и регион), метаданные — это реальный риск. Фотография без лиц может содержать GPS-координаты места съёмки. Документ Word или PDF — имена авторов, коллег и внутренние комментарии. Аудиофайл — данные об устройстве записи. Такая информация может использоваться для деанонимизации, давления или преследования.

МЕТАДАННЫЕ МОГУТ ПРИВЕСТИ К:

- раскрытию личности автора или участников инициативы;
- слежке и угрозам для активистов и их семей;
- компрометации организации через «невидимые» данные в файлах и отчетах;
- юридическим последствиям: власти могут использовать такие файлы как доказательства в административных или уголовных делах.

ЧТО ВАЖНО ДЕЛАТЬ

1. Отключайте геолокацию и не сохраняйте координаты в фото и видео
2. Всегда проверять и очищать метаданные перед публикацией файлов
3. Работать с копиями, сохраняя оригиналы отдельно
4. Очищать документы (Word, PDF, Excel) от авторов, комментариев и истории правок
5. Использовать офлайн-инструменты для очистки: MAT2, ExifTool, функции LibreOffice и MS Office
6. Помнить, что Google Docs и другие облачные сервисы полностью метаданные не удаляют — «чистую» версию нужно готовить офлайн

Удаление метаданных — это не паранойя и не сложная техническая мера, а базовая цифровая гигиена. Простая привычка проверять файлы перед публикацией может существенно снизить риски и защитить вас, вашу команду и людей, с которыми вы работаете

DDoS-АТАКА ГРАЖДАНСКИХ ИНИЦИАТИВ

DDoS-атака (Distributed Denial of Service) — кибератака, перегружающая сайт миллионами искусственных запросов, из-за чего ресурс становится недоступен. Цель: блокировать работу сайта, мешать доступу к информации, деморализовать команду и отвлечь внимание для других атак. Такое воздействие особенно опасно для НГО и гражданских инициатив с ограниченными ресурсами.

DDoS-атаку можно назвать формой цифровой репрессии против гражданских инициатив. Даже кратковременная недоступность сайта может сорвать сбор донатов, сорвать голосования, заблокировать публикацию материалов или остановить онлайн-мероприятия. Для малых организаций и независимых проектов такие атаки создают серьёзные трудности из-за ограниченных ресурсов.

ЧТО ДЕЛАТЬ

- настроить защищённый хостинг в нейтральной юрисдикции (не РФ/РБ);
- подключить CDN и DDoS-защита, например: Cloudflare Free или Project Galileo для правозащитников;
- ограничить частоты запросов (Rate Limiting, Bot Fight Mode);
- делать резервное копирование данных в облаке и офлайн;
- устранить уязвимости: отключить лишние плагины, настроить двухфакторную аутентификацию и CAPTCHA;
- отслеживать уведомления: UptimeRobot, Wordfence, Telegram/email оповещения;
- поддерживать связи с аудиторией через безопасные альтернативные каналы (соцсети, рассылки).

РИСКИ И ПОСЛЕДСТВИЯ

Недоступность сайта, потеря доступа к важной информации, финансовые потери из-за остановки сервисов или сбора донатов, репутационные риски и снижение доверия аудитории, деморализация команды и давление на активистов, угроза информационной свободе и возможности донесения данных о нарушениях прав человека.

Комплексная защита помогает минимизировать последствия и сохранять доступность информации, а постоянный мониторинг позволяют организациям действовать быстро, защищать команду и аудиторию, а также сохранять доверие гражданского общества даже в условиях постоянных угроз.

ДОКСИНГ: КАК СНИЗИТЬ РИСКИ

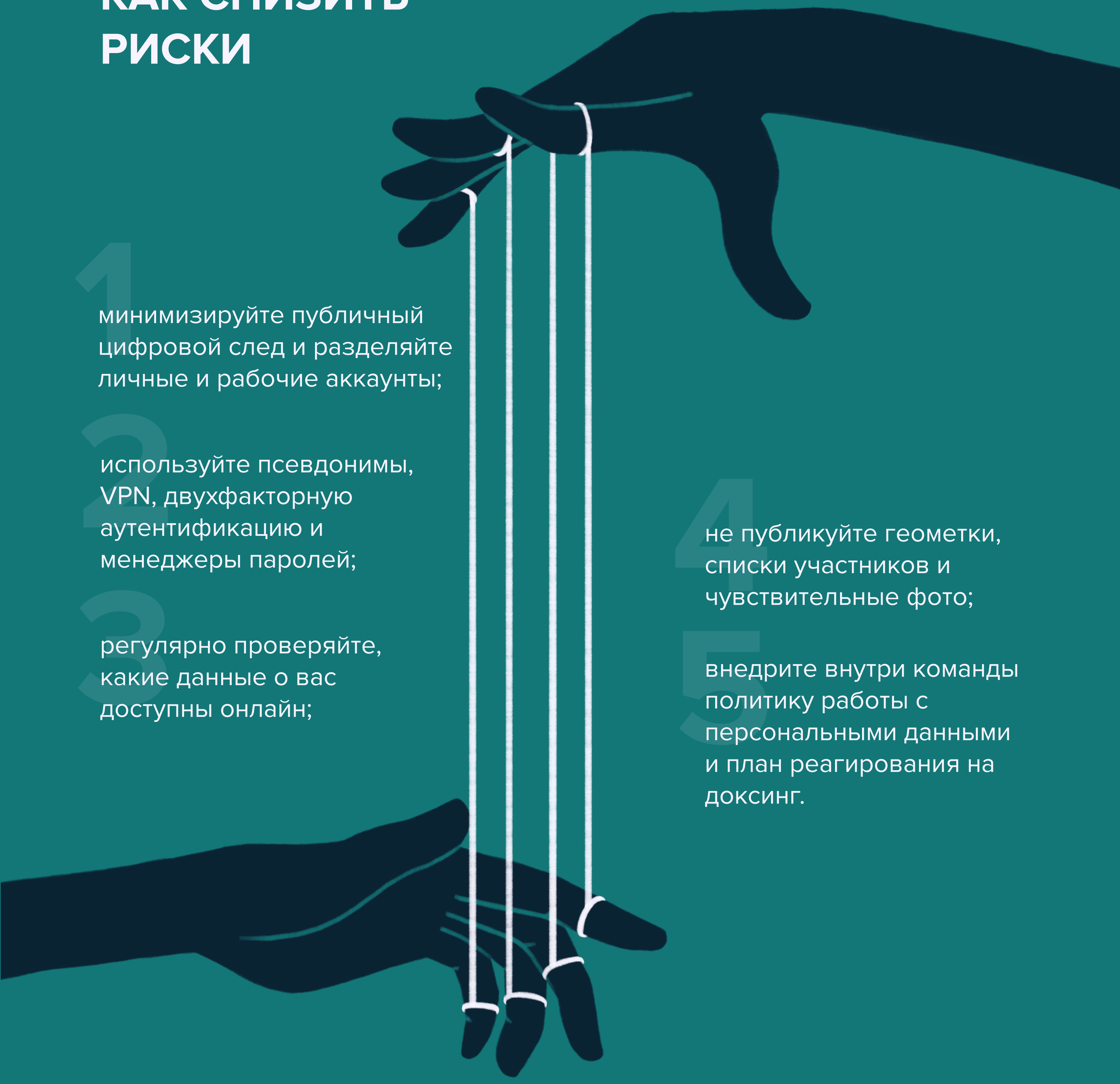
Доксинг — это умышленный сбор и публикация личной информации без согласия с целью давления, запугивания или дискредитации. Это могут быть имена, адреса, телефоны, данные родственников, фото, геолокация, архивные публикации и информация из открытых реестров.

Для НГО, правозащитников, журналистов и активистов доксинг — это реальная угроза безопасности, а не только репутационный риск. Он используется для травли, давления на семью и коллег, организации доносов, фабрикации административных и уголовных дел, а также для срыва работы и запугивания участников инициатив.

В Беларуси и регионе доксинг широко применяется как инструмент репрессий: персональные данные публикуются в Telegram-каналах и соцсетях, часто в сочетании с фишингом, взломами, фейками и информационными атаками.

Профилактика всегда дешевле реагирования. Поэтому внедряйте культуру цифровой безопасности внутри своей команды. Даже простые меры уже существенно снижают риск.

КАК СНИЗИТЬ РИСКИ



1 минимизируйте публичный цифровой след и разделяйте личные и рабочие аккаунты;

2 используйте псевдонимы, VPN, двухфакторную аутентификацию и менеджеры паролей;

3 регулярно проверяйте, какие данные о вас доступны онлайн;

4 не публикуйте геометки, списки участников и чувствительные фото;

5 внедрите внутри команды политику работы с персональными данными и план реагирования на доксинг.

БЛОКИРОВКА САЙТОВ ГРАЖДАНСКИХ ИНИЦИАТИВ

В странах с ограниченными гражданскими свободами власти блокируют сайты независимых медиа, правозащитников и активистов. Например, в Беларуси к 2023 году заблокировано около 2000 сайтов, признанных «экстремистскими». Это делается для контроля информации и подавления критики.

Блокировка сайтов не только техническая проблема, но и удар по гражданским инициативам и независимым организациям. Власти используют её как инструмент давления: сначала ограничивают доступ через провайдеров, затем угрожают хостингам, а в итоге сайты удаляются или навсегда теряют аудиторию из-за риска наказания за посещение «запрещённых» ресурсов. Когда сайт становится недоступен, организации также теряют возможность вести открытый диалог, распространять важную информацию и привлекать новых сторонников. Это ослабляет гражданское общество и подрывает доверие людей к независимым источникам.

Чтобы противостоять цензуре, важно действовать комплексно: сочетать технические решения (зеркала, VPN, Tor, современные веб-технологии) и работу по укреплению сообщества. Если пользователи знают, как обходить блокировки, и имеют доступ к информации через альтернативные каналы, блокировка становится лишь временной преградой.

СПОСОБЫ ОБХОДА БЛОКИРОВКИ

- зеркала сайта: создать копии ресурса на других доменах;
- VPN и прокси: поможет обойти региональные блокировки и защитить трафик;
- Tor и .onion-сайты: дает устойчивость к цензуре и высокий уровень анонимности;
- SPA и PWA: сайты, сохраняющиеся в браузере и работающие даже при блокировке;
- альтернативные каналы: соцсети, мессенджеры, e-mail рассылки, RSS.

РИСКИ И ПОСЛЕДСТВИЯ

- потеря доступа к независимой информации;
- снижение вовлечённости аудитории и поддержки инициатив;
- репутационные и технические проблемы для организаций;
- риски штрафов и уголовного преследования за «экстремизм»;
- падение охватов и исчезновение доменов из поисковиков.

ПОДОЗРИТЕЛЬНОЕ ПИСЬМО?

Фишинг — это целенаправленное интернет-мошенничество, при котором злоумышленники маскируются под банки, государственные органы, доноров, платформы (Google, Telegram, Meta), партнёров или коллег, чтобы заставить вас перейти по ссылке, открыть файл или ввести данные

Для НГО, активистов и журналистов фишинг — одна из самых частых и опасных цифровых угроз. Его цель — не только деньги, но и доступ к переписке, документам, базам контактов, спискам доноров и участников. Один скомпрометированный аккаунт может привести к утечке данных всей команды и поставить под угрозу безопасность других людей, включая тех, кто остаётся в Беларуси или других репрессивных странах

ЧАЩЕ ВСЕГО ФИШИНГ ВЫГЛЯДИТ ТАК:

- «служебное» письмо о блокировке аккаунта;
- сообщение от «коллеги» с просьбой срочно открыть файл;
- поддельный Google Doc, платёжная форма или бот помощи;
- запароленный PDF «в целях безопасности».

ОСНОВНЫЕ КРАСНЫЕ ФЛАГИ:

- срочность, давление, запугивание или обещания выгоды;
- странный или слегка искаженный адрес отправителя;
- ссылки, которые ведут не на официальный домен;
- вложения (ZIP, PDF, EXE), которых вы не ожидали;
- просьбы сообщить пароль, код 2FA, данные карты;
- отсутствие персонального обращения.

ЕСЛИ ВЫ ПОЛУЧИЛИ ПОДОЗРИТЕЛЬНОЕ СООБЩЕНИЕ:

- Не торопитесь — фишинг работает на спешке.
- Проверьте отправителя и ссылку (наведите курсор).
- Не открывайте вложения напрямую.
- Если сомневаетесь — уточните через другой канал связи.

ЕСЛИ ФИШИНГ УДАЛСЯ:

- срочно смените пароли и включите 2FA;
- проверьте активные сессии и устройства;
- предупредите коллег, если аккаунт рабочий;
- свяжитесь с банком при финансовых рисках;
- сохраните доказательства (письма, скриншоты).

Ключевая защита — регулярное обучение команды, простые правила цифровой гигиены и привычка всё перепроверять без страха «показаться параноиком»

КАК ЗАЩИТИТЬ УЧЁТНЫЕ ЗАПИСИ

Учётные записи — это ключи к вашей цифровой жизни: почта, соцсети, рабочие инструменты, облака и мессенджеры. Для НГО, активистов, журналистов и правозащитников компрометация аккаунта может привести не только к потере доступа, но и к утечке чувствительной информации, угрозам безопасности людей, дискредитации проектов и срыву работы организации.

На практике атаки чаще всего начинаются с одного взломанного аккаунта — особенно электронной почты — и быстро распространяются на другие сервисы через восстановление паролей или «вход через Google/Facebook».

В деятельности правозащитников, активистов, волонтёров и сотрудников НГО защита учётных записей особенно важна, так как приходится работать с чувствительной информацией, взаимодействовать с уязвимыми группами и вести коммуникацию в контексте, где утечка данных может повлечь не только технические, но и этические или даже физические риски.

Важно: даже базовые меры значительно снижают риски. Учётная запись с уникальным паролем и включённой 2FA в разы сложнее для взлома и часто останавливает атаку на раннем этапе.

ЧТО ОБЯЗАТЕЛЬНО СДЕЛАТЬ

- используйте уникальные и длинные пароли для каждого сервиса (12–15+ символов). Лучше — парольные фразы. Не используйте личную информацию;
- применяйте менеджер паролей (например, Bitwarden или 1Password), чтобы безопасно хранить и генерировать пароли;
- включите двухфакторную аутентификацию (2FA) везде, где возможно. Сохраните резервные коды офлайн. По возможности используйте аппаратные ключи безопасности;

- защитите электронную почту в первую очередь: 2FA, резервный email, уведомления о входах, проверка сторонних доступов;
- не используйте вход через соцсети, если есть альтернатива. Блокировка одного аккаунта не должна лишать вас доступа ко всем сервисам;
- регулярно проверяйте старые и редко используемые аккаунты: удаляйте ненужные, меняйте пароли, проверяйте утечки (например, через haveibeenpwned.com);
- проверьте настройки конфиденциальности в ключевых сервисах (Google, Apple ID, соцсети, мессенджеры), ограничьте видимость данных и отключите лишние разрешения.

ЦЕНЗУРА В ИНТЕРНЕТЕ:

ограничение свободы слова

Цензура в Интернете является системным ограничением свободы слова: блокировка независимых СМИ и НГО, давление на активистов и журналистов, контроль за онлайн-активностью граждан.
Цель: подавление критики, контроль информации и влияние на общественное мнение.

РИСКИ И ПОСЛЕДСТВИЯ

- недоступность независимых СМИ и правозащитных ресурсов.
- угроза преследования активистов и журналистов.
- самоцензура на не заблокированных ресурсах.
- ограничение доступа к альтернативной информации для граждан.
- усиление контроля за цифровым пространством и личными данными.

Цензура в Интернете — это не только техническая блокировка ресурсов, но и инструмент давления на гражданское общество. Она влияет на свободу слова, уменьшает доступ к альтернативной информации и создаёт психологическое давление на активистов.

Чтобы противостоять цензуре, важно сочетать технические меры (VPN, Tor, защита сайтов, шифрование) с организационными и социальными действиями: поддержкой независимых медиа, обменом безопасной информацией и документированием нарушений. Только комплексный подход позволяет сохранять доступ к важной информации, защищать аудиторию и поддерживать устойчивость гражданских инициатив в условиях цифрового давления.

КАК С ЭТИМ БОРОТЬСЯ

- Использовать VPN и Tor для обхода блокировок и обеспечения анонимности;
- Обучаться цифровой безопасности: защита аккаунтов, проверка источников информации, сохранение
- Шифровать устройства: BitLocker для Windows, FileVault для macOS;
- Защищать сайты от DDoS и других кибератак (например, Project Galileo от Cloudflare);
- Выражать солидарность и поддержку независимых медиа: делиться информацией, участвовать в международных инициативах;
- Документировать нарушения и фиксировать давления на активистов.

ШПИОНСКОЕ ПО

Шпионское программное обеспечение (spyware) — это вредоносные программы, которые скрытно устанавливаются на телефон или компьютер и позволяют третьим лицам получать полный доступ к данным пользователя.

Spyware может читать переписку и почту, отслеживать местоположение, записывать звонки, включать камеру и микрофон, перехватывать пароли и коды доступа. Часто такие инструменты используются для целенаправленной слежки за журналистами, правозащитниками, активистами и сотрудниками НГО.

КАК ПРОИСХОДИТ ЗАРАЖЕНИЕ

1-click: если вы перейдете по вредоносной ссылке на сайте, мессенджере, почте, соцсетях и невольно установите вредоносное приложение или откроете вложенный файл.

Zero-click: шпионское ПО внедряется без каких-либо действий пользователя, часто через уязвимости системы.

Продвинутое spyware сложно выявить, но тревожными сигналами могут быть быстрый разряд батареи, перегрев устройства, необъяснимые сбои, подозрительная активность камеры или микрофона, а также уведомления от Apple о целевой атаке. При подозрении на заражение важно не пытаться чинить устройство самостоятельно, прекратить чувствительную коммуникацию и обратиться к специалистам по цифровой безопасности (например, в Amnesty International Security Lab или к партнёрским инициативам).

Чтобы снизить риски, важно регулярно обновлять операционные системы и приложения, использовать встроенное шифрование и режим повышенной безопасности (например, Lockdown Mode на устройствах Apple), скачивать приложения только из официальных источников и быть крайне осторожными с ссылками и вложениями. Для НГО и инициатив критически важно также обучать команды цифровой гигиене, разделять личные и рабочие устройства и иметь заранее продуманный план реагирования.

Программы-шпионы — одна из самых серьёзных цифровых угроз для гражданского общества, но системный подход к безопасности, внимательность и базовые защитные меры могут существенно снизить риски и ограничить последствия атак.

КАК СНИЗИТЬ РИСК УТЕЧЕК ДАННЫХ

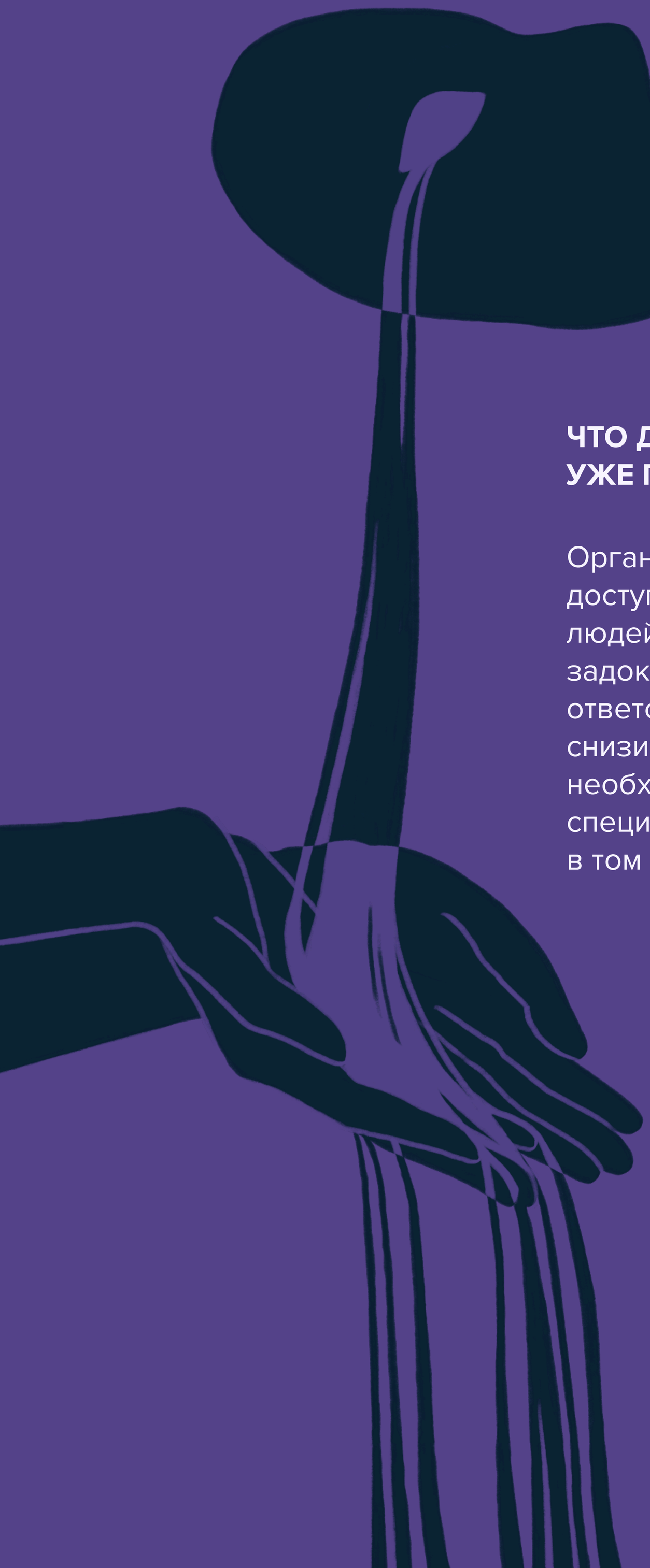
Некоммерческие и гражданские организации часто работают с чувствительными данными: персональной информацией сотрудников и волонтёров, сведениями о бенефициарах, донорах, внутренних процессах и свидетельствах нарушений прав человека. В условиях давления и репрессивных практик такие организации становятся приоритетной целью цифровых атак, слежки и попыток дискредитации.

Утечка информации — это несанкционированный доступ, раскрытие или передача конфиденциальных данных. Речь может идти о персональных данных, списках доноров, внутренней переписке, финансовой информации, логинах и паролях, а также о данных людей, находящихся под риском преследования. Утечки происходят из-за взломов, фишинга, ошибок сотрудников, утери устройств или действий инсайдеров.

Для НГО и доноров последствия утечки могут быть серьёзными: давление и преследование людей, подрыв доверия, репутационные потери и срыв программ помощи. В авторитарных контекстах даже один скомпрометированный файл может поставить под угрозу безопасность десятков людей.

Как снизить риски утечек

Ключевые меры защиты включают минимизацию объёма хранимых данных, чёткое разграничение доступов, использование уникальных паролей и двухфакторной аутентификации, шифрование данных, регулярное обновление программного обеспечения и обучение команды. Важно также заранее проводить оценку рисков и иметь план реагирования на инциденты.



ЧТО ДЕЛАТЬ ЕСЛИ УТЕЧКА УЖЕ ПРОИЗОШЛА

Организации должны немедленно ограничить доступы, оценить масштаб утечки и риски для людей, уведомить пострадавших и задокументировать инцидент. Открытая и ответственная коммуникация помогает снизить вред и сохранить доверие. При необходимости стоит обращаться к специалистам по цифровой безопасности — в том числе за внешней поддержкой.

Людям, чьи данные могли пострадать, важно сменить пароли, включить двухфакторную аутентификацию, быть осторожными с сообщениями и звонками и обращаться за помощью при угрозах безопасности.

Важно помнить: ответственность за защиту данных лежит на организации, а не на людях, чья информация оказалась под угрозой. Открытое и своевременное реагирование на утечки — ключевой элемент цифровой и этической устойчивости НГО.