Ежемесячный информационно-правовой бюллетень «СМИ и право», №89 (100), октябрь, 2013г.

Издается Национальной ассоциацией независимых СМИ Таджикистана (НАНСМИТ)

Республика Таджикистан, г. Душанбе, проспект Рудаки, 137.

тел/факс: (992 37) 221-37-11, 224-88-23;

Электронная почта: coordinator@nansmit.tj

Предназначен для всех журналистов, нуждающихся в юридической поддержке, а также для всех лиц, заинтересованных в развитии свободных СМИ и журналистики в Таджикистане.

Поддержка данного издания осуществляется Национальным фондом в поддержку демократии (NED, США) в рамках Проекта поддержки независимых СМИ Таджикистана.

В этом номере:

Как обезопасить себя и свои данные в социальных сетях?

- How-To Booklet

Можно сказать, что онлайновые сообщества родились вместе с самим интернетом. Сначала были BBS (bulletin board systems, "электронные доски объявлений") и дискуссии в списках e-mail. Люди радовались возможности общаться друг с другом, минуя государственные границы, через страны и континенты. Появились тематические конференции Usenet, чаты, веб-форумы, блоги. А затем наступило время социальных сетей. В основе социальной сети — сам человек, его личность. Вы можете выложить информацию о себе в интернете, включая фотографии, текст, файлы, даже информацию "где я сейчас нахожусь и чем занимаюсь". В социальной сети можно отыскать затерявшихся в прошлом друзей и одноклассников, поболтать о том и сем в группе по интересам, сыграть вместе в какую-нибудь онлайновую игру, пофлиртовать с незнакомкой (или незнакомцем), узнать, какие хорошие фильмы недавно вышли на экраны, и так далее. В принципе, эта информация доступна и без социальных сетей. Людей привлекает возможность получить все сразу, в одном месте, в атмосфере, пропитанной духом неформального общения.

Много слов сказано о том, что суррогатная "сетевая жизнь" угрожает в будущем заменить существенную часть обычной человеческой жизни. Но мы сейчас не об этом. Вряд ли такая подмена грозит современным гражданским активистам, людям, у которых в жизни есть много более важных задач. Главное — социальная сеть (по определению) предполагает обмен информацией между людьми. Информацией о самих себе. "Кто вы? Ваш пол? Возраст? Где живете? Кем работаете? Какую музыку предпочитаете? Какие фильмы любите смотреть? Есть ли семья, дети, домашние животные? Как проводите свободное время? — настойчиво интересуется социальная сеть. — Найдите новых друзей! Расскажите им больше о себе!" Удивительно, сколько людей готово искренне и во всех подробностях выкладывать свою личную жизнь всему миру. А ведь среди незнакомцев может оказаться кто угодно.

— Что ж, — рассудит человек осторожный и здравомыслящий. — Буду держаться подальше от социальных сетей, всех этих фейсбуков и твиттеров.

Однако социальные сети — не мода и не игрушка. Не стоит относиться к ним легкомысленно. Сегодня это мощный инструмент распространения информации, общения с аудиторией, поиска союзников и получения помощи. Их владельцы — коммерческие фирмы. Для них больше людей — значит, больше аккаунтов. Досье, если хотите. А больше аккаунтов — значит, больше потребителей рекламы. И больше денег. Иногда мы об этом забываем. Нам кажется, что социальная сеть — своего рода "продолжение интернета", этакое свободное сообщество. Между тем, у каждой сети есть свой хозяин. Именно ему вы доверяете всю информацию. А он волен поступать с ней по-всякому. Например, круг ваших знакомых. Сегодня вы своими руками добавляете аккаунты друзей и родственников в свой личный список. Завтра к владельцу социальной сети явятся правоохранительные органы и потребуют передать им этот список. Может ли такое случиться? Вполне.

Это не значит, что социальные сети нужно отбросить и забыть об их существовании. Они могут быть очень полезны. Давайте поговорим, как сделать работу с ними более безопасной.

Общие рекомендации по безопасности

Зададим себе несколько ключевых вопросов.

- Я размещаю информацию в сети; кто будет иметь к ней доступ?
- Кто, кроме меня, контролирует мою информацию?
- Какая информация обо мне касается также других людей?

- Насколько значимым для этих людей было бы разглашение этих данных?
- Кому из тех, с кем я откровенно общаюсь и передаю информацию, я на самом деле доверился бы полностью, а кому нет?

Таковы общие вопросы. Они важны, когда речь заходит о любой социальной сети или подобной службе. Что касается начала работы, то первым делом следует вспомнить о **надежном пароле**. Самый короткий способ все разрушить (включая доверие коллег) — допустить, чтобы кто-нибудь посторонний получил доступ к вашему аккаунту. Будь это случайный человек или злоумышленник, он станет обладателем информации о вас и тех, с кем вы связаны. Поэтому пароль нужно правильно создавать, аккуратно хранить и регулярно менять.

Вот еще несколько полезных советов.

- Отыщите на веб-сайте социальной сети **политику приватности** (иногда ее называют "политикой конфиденциальности") и прочтите то, что относится к безопасности ваших данных. Скажем, оставляет ли владелец сети за собой право использовать эту информацию в маркетинговых исследованиях?
- Выясните, **какие программные способы предлагает владелец сети для защиты данных.** Например, если вы заполните свой профиль, можно ли поставить нужную галочку, чтобы эта информация не показывалась другим пользователям?
- Если вы собираетесь провести какую-нибудь онлайновую акцию, возможно, следует завести для этого **другой аккаунт**, а не тот, который был использован в предыдущей акции. Или хотя бы другой псевдоним (ник).
- Будьте осторожны, если вынуждены пользоваться своим аккаунтом **с чужого компьютера.** Не забывайте очищать историю и кеш браузера и удалять сохраненный им пароль. По возможности используйте **защищенный (SSL) доступ** (https://...). Таким образом можно шифровать сеансы связи между вашим браузером и сетью.
- Так ли необходимо заполнять все поля вашего профиля, особенно если вы предполагаете использовать его в рабочих целях? Возможно, вы готовы поделиться фотографией, но **вряд ли нужно сообщать миру о деталях личной жизни,** например, о детях, или о том, как вы привыкли проводить свободное время.
- Социальная сеть может содержать инструменты для интеграции с другими подобными сетями или сервисами. К примеру, вы публикуете что-нибудь в Twitter, и эта новость автоматически появляется на вашей страничке в Facebook. **Будьте осторожны с интеграцией!** На каком-либо ресурсе вы можете действовать анонимно и чувствовать себя защищенным, но лишь до поры и до времени; интеграция-автоматика может раскрыть вашу личность.
- **Никогда не используйте социальную сеть или иной подобный сервис в качестве основного хранилища информации**. Это не ваш личный сайт, он вам не принадлежит, а резервное копирование обычно не входит в набор стандартных инструментов. Если решением владельца (а может, и под давлением правительства) ваша страница окажется заблокирована или удалена, жаловаться будет поздно. Помните, что владельцу сети проще избавиться от "неудобного" пользователя, чем вступать в конфликт с правительством, рискуя потерять гораздо больше.

Личная информация

Социальные сети и прочие подобные сервисы устроены так, что пользователи оставляют в них массу личной информации. Основная цель — найти старых знакомых и приобрести новых друзей. Личная информация помогает установить, что Михаил Петрович — тот самый Мишка, с кем вы учились на одном курсе в институте, а не однофамилец. Но чем больше информации о себе вы оставляете в сети, тем проще составить на вас досье. Даже если вы не волнуетесь за себя лично, в "пиковой" ситуации давление на гражданского активиста может возникнуть с неожиданной стороны, например, через родных и близких. А круг этих людей, включая деликатную информацию, иногда может быть восстановлен до малых подробностей с помощью интернета.

Другая проблема, которая со временем становится все более заметной и тревожной — подмена личности. Некто, собрав о вас достаточную информацию, может попробовать прикинуться вами. Так иногда поступают мошенники, чтобы оформить кредит или выудить какую-нибудь важную информацию из ничего не подозревающего онлайнового собеседника. Этим же приемом нетрудно воспользоваться и злоумышленнику, который, например, вознамерился сорвать запланированную правозащитную акцию.

- Даты рождения.
- Контактные номера телефонов.
- Фактические адреса проживания.
- Данные о членах семьи.
- Сексуальная ориентация.
- Вероисповедание.
- Данные о состоянии здоровья.
- Данные об образовании.

Так ли необходимо делиться с владельцами социальной сети этой информацией?

Друзья и контакты

Попадая в социальную сеть или иной подобный сервис, вы рано или поздно столкнетесь с предложением найти друзей — тех, кто зарегистрировался до вас и сообщил свои личные данные. По смыслу, это люди, которым вы доверяете. Довольно скоро вы обнаружите, что в сети есть группы по интересам. Их участниками могут быть не только ваши друзья, но и незнакомые люди. Очень важно четко представлять себе, какой информацией вы готовы поделиться с таким сообществом.

Когда используете сеть "ВКонтакте" или другой сервис, где хранится много ваших личных данных, не связывайтесь с людьми, которыми не можете вполне доверять.

С одной стороны, это хороший способ завязать новые контакты, познакомиться с единомышленниками, а может быть, получить какую-нибудь поддержку в будущем. С другой стороны, незнакомые люди хотят влиться в твой круг общения. Среди них могут быть и

такие, кто вовсе не желает добра ни тебе, ни твоей организации.

Чем ты сейчас занимаешься?

В Twitter, Facebook и других подобных местах существует возможность сообщать о себе самую актуальную информацию. Чем я сейчас занят? Что планирую сделать? Что происходит вокруг? Но давайте зададим себе еще один вопрос: "Кто может это увидеть?" Оказывается, во многих сетях такая возможность по умолчанию предоставлена всем желающим. Подумайте, не стоит ли ограничить этот список своими друзьями?

Так, социальная сеть "ВКонтакте" позволяет настроить объем передаваемых данных в меню "Мои настройки" — "Приватность". Для разных типов данных предлагается несколько вариантов на выбор. Например, на вопрос "Кто может видеть мои адреса" можно выбрать варианты: "Все пользователи", "Только друзья", "Друзья и друзья друзей", "Только я", а также два более тонких фильтра "Некоторые друзья" и "Все, кроме...".

Попробуйте договориться с коллегами об общем подходе к раскрытию информации. Попробуйте встать на точку зрения коллеги. Хотел бы он, чтобы вы распространяли о нем информацию?

На Западе уже были случаи, когда за излишнюю открытость (если не сказать — болтливость) в социальных сетях люди терпели неприятности. Это были учителя, которые в сердцах выражались о нерадивых учениках; официантки, язвившие насчет клиентов; офисные сотрудники, проклинавшие работодателей. 18-летний королевский гвардеец Кэмерон Райли приобрел мировую известность после того, как на своей страничке в Facebook обозвал нелестными словами Кейт Мидлтон, невесту (а ныне супругу) принца Уильяма. Импульсивного гвардейца отстранили от служебных обязанностей, а затем собрали о нем досье на основе его же собственных высказываний в Facebook. Если случай Райли кажется вам неубедительным, обратите внимание на трех граждан Ливана, которые подверглись преследованию за критику президента этой страны в Facebook.

Что новенького в интернете?

В социальной сети легко переслать другу ссылку на понравившийся веб-сайт. Вопрос лишь в том, кто еще получит копию этой информации? Возможно, человек или целое учреждение, для которого такая ссылка (даже не написанная вами статья, а обычная гиперссылка) покажется красной тряпкой.

Если хотите, чтобы о ваших интересах и предпочтениях знал только избранный круг друзей, не забудьте отметить соответствующий пункт в настройках.

Где ты?

Большинство социальных сетей с готовностью покажут ваше местонахождение, если только вы сообщите им эти данные. Обычно такое случается, когда вы пользуетесь мобильным телефоном с GPS-модулем. Но необязательно. Сеть, к которой подключен ваш компьютер, также может передавать данные о местонахождении. Не забывайте об осторожности на сайтах, которые позволяют обмениваться фото- и видеоматериалами. Проверьте настройки.

Американская правозащитная организация Electronic Frontier Foundation даже выпустила специальное пособие под названием On Locational Privacy, and How to Avoid Losing it Forever ("Где вы находитесь: как не потерять приватность навсегда").

Обмен фото и видео

Фотографии и видеоматериалы позволяют легко идентифицировать человека. Известный российский режиссер и публичный деятель Никита Михалков пополняет свой блог только выступлениями, снятыми на видео. Когда его спросили, зачем он это делает (а не пишет обыкновенным текстом, как другие), режиссер ответил, что не желает искажений и пересудов типа "это сказал не Михалков". Для гражданского активиста все может быть наоборот. Если постараться, можно сохранить анонимность, рассказывая в интернете о нарушениях прав человека (в частности, об этом глава "Как сохранить анонимность и обойти цензуру"). Но видео или фото — убедительное свидетельство. Будьте осторожны, отбирая материалы для размещения в сети. И, конечно, не публикуйте ничье изображение без предварительного согласия.

Обратите внимание: многие камеры "снабжают" материал всевозможной технической информацией. Даже если камера не впечатывает дату прямо в кадр, нередко по фотографии можно узнать, когда был сделан снимок. А некоторые сайты и вовсе отображают эту информацию всем желающим.

Чаты

Во многих социальных сетях можно пообщаться с друзьями в реальном времени. Пожалуй, нет менее безопасного способа обмениваться информацией в интернете, чем этот. Если все-таки без чата не обойтись, убедитесь, что все участники разговора вошли на сайт с использованием защищенного протокола (https://...). А лучше воспользоваться какой-нибудь независимой программой для обмена мгновенными сообщениями.

События, группы, сообщества

Итак, вы сделали следующий шаг и присоединились к сообществу (группе). Какая информация о вас окажется доступной членам этого сообщества?

Как минимум, люди узнают, что вы не равнодушны к теме. Если сообщество достаточно четко формулирует свои цели и задачи, вас могут

причислить к его сторонникам (даже если вы просто зашли посмотреть). Информация о том, какие сообщества вы посещаете, может быть доступна и другим людям, не входящим в сообщества. Так, всякий пользователь интернета может легко увидеть, какие сообщества ЖЖ вам по душе, и на этом основании сделать вывод о ваших интересах и политических взглядах.

Кроме того, вступая в сообщество, вы часто оказываетесь среди малознакомых людей. Большинство объединено какой-нибудь благой целью (хотя это по-прежнему очень разные люди). Некоторые заглянули случайно или по ошибке. Кто-то черпает информацию для оппонентов. И вот на пороге появляетесь вы — под настоящим именем, с настоящей фотографией. Не так ли?

Иногда создание сообщества на острую социальную тему может быть расценено как провокация. Представьте, что вы открыли группу "Андижанские события" (в 2005 году в Ферганской долине, в городе Андижан произошли массовые беспорядки, жестоко подавленные узбекскими властями). Какие последствия может иметь призыв к жителям Андижана, участникам и очевидцам событий 2005 года, присоединиться к вашей группе и активно участвовать в дискуссии?

Особенности разных сетей

Facebook

Facebook — крупнейшая в мире социальная сеть. Если ваш новый знакомый или собеседник признается, что он активный пользователь интернета, с большой вероятностью у него есть аккаунт в Facebook. К сожалению, об этом известно и нашим недоброжелателям. Поэтому если кто-нибудь решил использовать интернет для составления досье или просто для сбора информации о человеке, он, скорее всего, начнет с Facebook.

Основатель Facebook Марк Цукенберг (Mark Zuckerberg) известен тем, что заявил: "Онлайновой приватности пришел конец". В определенном смысле это правда. Частной жизни на Facebook места мало. Даже если вы (казалось бы, чего проще!) отметили все нужные пункты в настройках, чтобы личная информация была доступна только друзьям, она все равно откроется любому, кто захочет воспользоваться поиском. Свои возможности доступа есть и у разработчиков игр и приложений для Facebook.

Стоит вам создать аккаунт в Facebook, вы не сможете его удалить. Facebook позволит лишь "деактивировать" аккаунт (по запросу), но в любой момент его можно восстановить со всей находящейся там информацией и настройками. Проще говоря, ваши данные из Facebook не удаляются.

"Условия использования" Facebook гласят, что для любых загруженных вами фотографий и видео вы передаете Facebook неисключительное право использовать эти материалы без географических ограничений. Facebook утрачивает это право, лишь когда вы удаляете свой аккаунт (см. выше) или сами материалы. Однако если вы были настолько добры, что поделились материалами с кем-нибудь, и этот пользователь Facebook не удалил их, право сохраняется.

Известно, в частности, что Департамент обороны США осуществляет мониторинг Facebook и другие социальные сети. Может быть, правительство вашей страны это не делает. Пока...

Советы:

- Проверьте настройки своего аккаунта в Facebook.
- Обращайте внимание на политику конфиденциальности Facebook. Бурный рост этой сети и пристальное общественное внимание привело к тому, что политика конфиденциальности Facebook часто меняется.
- Слышали такое слово: "зафрендить"? Это значит — присоединить к списку друзей. При этом вы открываете новому человеку доступ к информации о себе и своих интересах в рамках Facebook. Хорошая идея — "френдить" только тех людей, которым вы вполне доверяете в жизни.
- Возможно, имеет смысл деактивировать аккаунт всякий раз, как вы выходите из Facebook. Таким образом, аккаунт окажется "замороженным", никто не будет иметь к нему доступ, в том числе когда вы не в интернете. Восстановить аккаунт нетрудно, а все ваши данные и настройки, как мы уже говорили, сохранятся.

Советуем также почитать материал, подготовленный администрацией Facebook, который называется "Управление уровнем конфиденциальности".

Twitter

Twitter появился как служба обмена информацией типа "Что я сейчас делаю". Данные передавались с мобильных телефонов в интернет. Каждое сообщение укладывалось в 140 символов. Twitter называли "SMS для интернета". Система позволяет другим пользователям следить за вашей жизнью, а вам, соответственно, интересоваться, как идут дела у других людей. В отличие от социальной сети, "интересующиеся" — вовсе необязательно друзья. Этот список мало даст тому, кто захочет установить ваш круг общения. С другой стороны, в Twitter проще манипулировать личностью, выдавать себя за другого человека.

Хотя Twitter технически реализован как веб-сайт, многие люди не заходят на него, а пользуются отдельными приложениями (Twitter-клиентами). Если хотите попробовать такой клиент, убедитесь сначала, что он соединяется с сайтом безопасным образом.

Как и в случае с Facebook, американские власти проявляют интерес к Twitter, и ничто не мешает правительствам других стран последовать их примеру.

Советы:

- Не забывайте: то, что вы говорите в Twitter, по умолчанию может просмотреть любой человек.
- Если передаете информацию не столь публичного характера, лучше защитить ее: ограничить читательскую аудиторию своими последователями. Впрочем, они могут переслать вашу информацию другим пользователям, и об этом тоже полезно помнить.
- Если говорите о том, что способно поставить вас (или еще кого-либо) под удар (например, критикуете чиновников, нарушающих права человека), делайте это анонимно, под вымышленным именем.

YouTube

YouTube — наиболее известная служба для публичного размещения и обмена видеоматериалами. Владелец этого сервиса — компания Google. YouTube очень удобно использовать, когда видеофайл нужно сделать доступным самой широкой аудитории. Однако, если сотрудники Google посчитают ваше видео противозаконным или даже спорным, его могут удалить. Таким образом, нельзя считать YouTube удачным местом для хранения видеоархива. Google известен своей готовностью к компромиссу в этом смысле: компания старается избежать претензий и блокировки сервиса.

Google фиксирует имена пользователей для всех загружаемых материалов, а также информацию, откуда поступил тот или иной ролик. Это может быть потенциально использовано для отслеживания пользователей.

Хотя вы сохраняете право собственности на материалы, выложенные в YouTube, компания Google автоматически получает разрешение распространять эти материалы.

В разное время YouTube был заблокирован в Турции, Китае, Иране, Ливии, Тунисе и Туркменистане.

Советы:

- Никогда не публикуйте видео с участием какого-либо человека без его предварительного согласия. А если такое согласие имеется, все-таки подумайте, каким образом это видео может навредить ему и, в конечном счете, вам.
- Храните у себя копии выложенных на Youtube видеороликов.
- Если хотите поделиться видео лишь с ограниченным числом пользователей, используйте соответствующие настройки сервиса.

Flickr

Flickr — сервис для размещения, в первую очередь, фотоматериалов — принадлежит компании Yahoo!.

То, что вы размещаете на Flickr, остается вашей собственностью и может "облагаться" разными лицензиями и копирайтами. В свою очередь, вы даете Yahoo! разрешение распространять ваши материалы, выложенные на Flickr.

Flickr можно использовать не только для размещения фото, но и для поиска изображений с целью использования в работе. Многие лицензии так или иначе позволяют это делать.

Советы:

- Flickr может показывать спрятанную информацию, такую как дату съемки и модель камеры.
- Никогда не публикуйте фото с участием какого-либо человека без его предварительного согласия. Убедитесь, что лицензия (разрешения), которой вы "снабжаете" фотографию, не ущемляет ничьих прав.

То, что было сказано про активность властей США в отношении Facebook и Twitter, относится и к Flickr.

ВКонтакте

ВКонтакте — самая крупная российская социальная сеть. Она была основана в 2006 году с целью предоставить пользователям интернета возможность искать и находить одноклассников, сокурсников и т.д. Сегодня ВКонтакте является одним из самых популярных онлайновых сервисов не только в России, но и в ряде стран бывшего СССР. По своей идеологии ВКонтакте напоминает Facebook. Сеть бурно развивается, то и дело появляются новые функции, дополнения, изменения. Они нередко затрагивают и вопросы приватности. Так, в феврале 2011 года пользователи ВКонтакте лишились возможности ограничивать доступ к записям на своей страничке ("стене"); с этих пор записи могут быть прочитаны кем угодно, включая тех, кто не зарегистрирован в социальной сети. Объявления такого рода могут происходить без предварительного уведомления пользователей. Администрация ВКонтакте запрещает пользователям сети "искажать сведения о себе, своем возрасте или своих отношениях с другими лицами или организациями". Пользователям также запрещено "размещать... информацию, которая, по личному мнению Администрации, является нежелательной". Система содержит довольно гибкие настройки, позволяющие ограничить доступ к тем или иным материалам на странице пользователя. Администрация ВКонтакте заявляет, что не занимается цензурой, а в программном обеспечении отсутствуют какие-либо технические решения для контроля содержимого пользовательских страниц. В последнее время проект значительно расширился за пределы "обычной" социальной сети, например, была создана собственная платежная система. Это ставит вопросы безопасности и приватности на новый уровень.

Одноклассники

Также известна как "Одноклассники.ру". Вторая по значимости социальная сеть в России, ближайший отечественный конкурент

"ВКонтакте". "Одноклассники" созданы в том же 2006 году с той же целью. Вопросы, связанные с безопасностью и приватностью, "традиционны" для социальных сетей. В частности, если пользователь "Одноклассников" добавил друга или загрузил фотографию, всякий другой пользователь может отследить эти действия в "Ленте активности".

Живой Журнал

"Живой Журнал" (сокращенно ЖЖ) — не социальная сеть, а система ведения блогов, международная по статусу и крупнейшая в своем роде для России. ЖЖ несет в себе черты социальной сети (например, можно "зафрендить" другого пользователя). Пользователи ЖЖ, как правило, выступают под псевдонимами (никами), а не под настоящими именами. С другой стороны, будучи блоггерской системой, ЖЖ предназначен для регулярных публикаций и общения в т.н. сообществах. Из-за этого объем информации о частной жизни (взглядах, привычках, интересах) в ЖЖ очень велик. В последние годы ЖЖ играет все более серьезную роль как инструмент для обсуждения и решения социально значимых проблем. Современные блоггеры не только публикуют собственные мнения и организуют дискуссии, но и проводят общественные акции и целые кампании. Влияние блогосферы на медийное пространство с каждым годом увеличивается. ЖЖ привлекает людей, которые считают себя далекими от онлайновых технологий, включая известных фигур политики, журналистики, культуры и т.д., а также общественные организации, политические партии и другие структуры.

Поскольку блоги в ЖЖ открыты самому широкому кругу читателей, публикуемая информация может стать темой конфликта и даже предметом судебного разбирательства. Самым нашумевшим делом последних лет, связанным с ЖЖ, стал процесс над российским блоггером Саввой Терентьевым, который в своем блоге довольно грубо и зло высказался о милиционерах. Следствие посчитало эту публикацию разжиганием вражды к социальной группе — милиции. Терентьев был осужден условно.

(Адаптировано из https://securityinabox.org/ru/)

Четыре инструмента для обеспечения безопасности журналистов и их информации

Автор Margaret Looney

Многие журналистские расследования начинаются с информации, полученной либо по электронной почте, либо другими, связанными с использованием цифровых технологий, способами. В этом случае более, чем когда бы то ни было, вероятно, что информация может попасть в чужие руки. Поэтому сейчас так важно искать способы обеспечения безопасности как самих журналистов, так и информации.

Именно поэтому Фонд за свободу прессы (Freedom of the Press Foundation) начал краудфандинговую кампанию в поддержку четырех новых цифровых инструментов, которые журналисты могут использовать для безопасной работы с данными.

Это не первые инструменты, получающие поддержку фонда. Не так давно фонд взял на себя организацию работы "последнего дара журналистике" Аарона Шварца, борца за свободное распространение в Интернете любого контента. SecureDrop — это хранилище информации для анонимных источников, позволяющее безопасно загружать документы и другие материалы.

Инструменты разрабатываются "проверенными экспертами в области безопасности, которым мы действительно доверяем. Мы считаем, что создаем инструменты, которые будут очень полезны журналистам и редакциям", - сказал член правления Фонда Джош Стернс в разговоре с корреспондентом MediaShift.

Вот четыре инструмента для обеспечения безопасной работы в Интернете, которые поддерживает Фонд:

Tails - это операционная система, которую можно запустить с USB диска, карты памяти или DVD. Вы можете использовать Интернет анонимно, так как каждое интернет-соединение будет проходить через серверы защищённой сети Tor. Журналисты могут использовать операционную систему, чтобы общаться анонимно и обмениваться документами, и все файлы, электронные письма и сообщения будут зашифрованы. Кампания по сбору средств поможет профинансировать улучшения для Talis 1.0

LEAP Encryption Access Project сосредоточен на безопасности электронной почты. Стандартные почтовые клиенты могут подключаться к локальному прокси-серверу и LEAP берет на себя обеспечение шифрования всей почты, таким образом позволяя зашифровывать все входящие письма так, что только получатель письма может прочесть его.

RedPhone/TextSecure - два инструмента, созданные Open WhisperSystems, позволяющие организовать безопасную связь между конечными абонентами мобильных телефонов. Red Phone автоматически шифрует звонки с телефонов Android, а TextSecure шифрует текстовые сообщения. Оба инструмента работают скрыто, не нарушая нормальной работы телефона.

Цель организации **Tor Project** - с помощью реализации ряда проектов способствовать цифровой безопасности для каждого. Журналисты часто используют Tor Browser Bundle, позволяющий им работать в Интернете, не оставляя следов и не раскрывая своего местонахождения. Это бесплатное приложение с открытым исходным кодом, оно доступно для Windows, Mac, Linux/Unix и пользователей Android.

По материалам PBS MediaShift.

Маргарет Луни, помощник редактора IJNet, пишет статьи в блоге о последних тенденциях в сфере СМИ, инструментах для журналистов и ресурсах в области журналистики.

(Источник: https://ijnet.org/ru/blog/238734)

Журналисты и терроризм: американский опыт

По данным Комитета защиты журналистов (Committee to Protect Journalists), после 11 сентября и во время вторжения в Ирак появилась очевидная тенденция атаки американских властей на конфиденциальность источников журналистов, включая случаи длительного содержания под стражей нескольких журналистов, которые сопротивлялись решению судей по уголовным делам. Согласно исследованиям Комитета, определились три категории атак на американскую прессу:

1. попытки ограничить поток информации, которая озвучивается на финансируемых правительством США радиостанциях, и попытки убедить частные телесети, а также по крайней мере одну иностранную телекомпанию цензурировать новости;

2. нападения американских войск на известные им офисы иностранных телеканалов, а также как удар по отелю, где находились иностранные журналисты;

3. длительное тюремное заключение иностранных журналистов американскими силами, что практикуется на зарубежных военных базах.

Вторжение в право на защиту своих источников наиболее очевидно проявилось в широко известном ныне деле Джудит Миллер, журналистки The New York Times, которая отказалась раскрывать свои источники по делу об утечках информации из ЦРУ. Но еще до того, как Миллер была заключена под стражу, федеральный судья отправил под домашний арест другого американского журналиста - за его отказ сотрудничать в другом уголовном деле. В декабре 2004 года Джим Тарикани (Jim Taricani), корреспондент принадлежащей NBC телестанции WJAR-TV (Род-Айленд), пробыл 121 день под домашним арестом, он не был отправлен в тюрьму только из-за медицинских противопоказаний. Судья также запретил ему работать, давать интервью СМИ и использовать Интернет даже для личных нужд.

В том же 2004 году еще больше журналистов обвинялись по гражданскому иску, в котором ученый, ранее работавший в лаборатории правительства США, Вен Хо Лии (Wen Ho Lee) обвинял правительственных чиновников в утечке информации в прессу его персональных файлов. Несмотря на то, что дело было в конце концов разрешено, постановления суда в этом гражданском деле, если считать их с теми, что были в том же году приняты по уголовным делам, ослабили способность журналистов защищать свои источники.

1 августа 2006 года федеральный судья Сан-Франциско отправил журналиста видео-блоггера Джоша Вольфа (Josh Wolf) в тюрьму без права внести залог из-за того, что он отказался предоставить видеозапись по другому уголовному делу. Спустя тридцать дней федеральный апелляционный суд отпустил журналиста под залог, заявив, что аргумент журналиста, что у него есть общая законная привилегия не отдавать кассету, имеет смысл.

Соединенные Штаты также стремились ограничить прессу дома и за границей. Спустя меньше месяца после терактов 11 сентября тогдашний американский госсекретарь Колин Пауэлл обратился с предложением к эмиру Катара использовал свое влияние, чтобы обуздать вещание телекомпании Al-Jazeera, финансируемой властями Катара.

Этот запрос был озвучен из-за предполагаемого антиамериканского уклона телеканала, а также решения Al-Jazeera повторить в эфире эксклюзивное интервью 1998 года с Осамой бин Ладеном. 10 октября, тогдашний советник по национальной безопасности Кондолиза Райс попросила группу руководителей американских телеканалов проявлять осмотрительность, показывая сообщения от Бен Ладена и его соратников. Райс утверждала, что такие сообщения являются в лучшем случае пропагандой и могут содержать закодированные инструкции для террористических ячеек. Руководители телеканалов согласились цензурировать будущие кассеты от Бен Ладена, изымая текст, так как в нем может содержаться пропаганда ненависти к американцам.

Спустя три месяца после 11 сентября финансируемая правительством США радиостанция «Голос Америки» выпустила новый сборник правил, запрещающий интервью от «государств, спонсирующих терроризм». Изменения появились в ответ на давление Госдепартамента после того, как работающая на «Голос Америки» журналистка пуштунской службы сделала эксклюзивное интервью с лидером талибов Муллой Омаром. Журналистку также заставили уйти с работы.

Зафиксированы также случаи атак на СМИ в виде физических нападений со стороны американских сил. В ноябре 2001 года, во время американской кампании в Афганистане, ракета попала в здание афганского бюро Al-Jazeera в Кабуле.

Американские военные обозначили это здание как «известное» убежище для «Аль-Каиды», не приведя никаких доказательств. В ответ на письмо Комитета защиты журналистов Дональду Рамсфельду глава объединенного комитета начальников штабов Ричард Майер заявил, что ВС не знали о том, что здание использовалось Al-Jazeera, хотя журналисты работали в нем к тому времени около двух лет, и крыша здания была утыкана спутниковыми тарелками. Спустя четыре года, в июне 2006 года, известный американский журналист Рон Саскинд (Ron Suskind) заявил CNN, что атака на офис телеканала в Кабуле «была сделана специально, исключительно для того, чтобы послать мессадж Al-Jazeera».

Еще три медиацентра попали под удар в течение одного дня - 8 апреля 2003 года - во время вторжения сил коалиции в Ирак. В этот день войска США разрушили багдадский офис Al-Jazeera, а также находившийся рядом офис Abu Dhabi TV. Позднее тем же утром американский танк выпустил снаряд по багдадскому Palestine Hotel, центр для иностранных журналистов. В результате атак 8 апреля два журналиста были убиты и три ранены. CPJ позже провел собственное расследование удара по отелю, в результате которого стало ясно, что жертв вполне можно было избежать - он не был необходимой целью.

Наконец, Соединенные Штаты обратились к практике задержания журналистов на длительный срок без обвинения, и в одном случае была предпринята попытка завербовать репортера как информатора. В октябре 2005 года CPJ попросил Пентагон ответить на сообщения о том, что военные следователи пытаются завербовать пребывающего в заключении журналиста в качестве шпиона. Оператор Al-Jazeera Сами Мухидин аль-Хадж (Sami Muhyideen al-Haj) был арестован пакистанскими властями вблизи афгано-пакистанской границы в декабре 2001 года во время выполнения профессиональных обязанностей. Он был переправлен в Гуантанамо на Кубу, где содержался без обвинения четыре года. В сентябре 2005 года британская газета The Guardian написала, что следователи заявили аль-Хаджу, что он будет отпущен, если согласится стать информатором внутри Al-Jazeera. Однако особую озабоченность вызывает ситуация в Ираке. Только во второй половине 2005 года Комитет зафиксировал семь случаев с местными репортерами, фотографами и операторами, которые были задержаны американскими силами на длительные сроки без обвинения. По крайней мере три задокументированных случая тюремного заключения превышали 100 дней, другие продолжались неделями. Эти случаи касались журналистов, работающих на CBS News, Reuters, The Associated Press, и Agence France Presse.

Комитет отмечает, что длительное содержание под стражей журналистов без предъявления обвинений является типичным для многих

репрессивных режимов. Заявления американских сил, что условия в Ираке специфичны, а местная правоохранительная система работает медленно - не более чем эхо заявлений, которые делаются в подобных случаях такими режимами.

При этом Комитет отмечает, что репрессивные режимы по всему миру обратили внимание на американские ограничения прессы после 11 сентября, пытаясь оправдать таким образом свои нарушения прав журналистов.

Уже в первую годовщину 11 сентября Комитет отметил, как авторитарные режимы оценили риторику «войны с террором», пытаясь оправдать ограничения свободы прессы в своих странах. В России советник президента Владимира Путина заявил, что он планирует изучить американские ограничения на публикации о террористах, чтобы использовать этот опыт для разработки правил для российских СМИ. В Эритрее и Зимбабве власти начали называть террористами журналистов, критикующих тамошние режимы.

А в 2005 году, по данным Комитета, заключение под стражу Джудит Миллер по делу об утечке из ЦРУ было использовано как пример правительствами Венесуэлы, Камеруна, Непала и Египта - чтобы оправдать свои репрессивные меры. /Источник: Доклад Фрэнка Смайта «Свобода СМИ в США: изменения после 11 сентября»./

Комментарий Дэвида Уайза

Дэвид Уайз - один из самых известных и авторитетных журналистов в США, пишущих о спецслужбах. Сорок лет назад он вместе с Томом Россом выпустил книгу «Невидимое правительство», а недавно опубликовал книгу о советском кроте Роберте Ханссене. Много лет он занимается проблемой давления со стороны правительства на журналистов-расследователей, публикуя об этом статьи в Los Angeles Times:

- Великобритания уже на протяжении 100 лет имеет Закон о государственной тайне, предотвращающий утечки в СМИ и карающий нарушителей, включая журналистов. Часть чиновников администрации Буша и членов Сената смотрит с вожделением на британское законодательство. Если США примет подобный закон, это приведет к тому, что тех, кто разоблачает тюрьмы ЦРУ в Восточной Европе и прослушивание без ордера подозреваемых в терроризме, будут преследовать вместо награждения Пулитцеровской премией.

Однако Конституция (речь идет о 1-й поправке) остается барьером для тех, кто хотел бы ограничить поток информации для СМИ и общества. Но политика администрации постепенно урезает эту защиту. Нация стоит перед опасностью получить Закон о гостайне, утвержденный не через законную процедуру, хотя все это еще только возможность, но постепенно на практике. Количество таких фактов (я их перечислял в своей статье в Los Angeles Times 30.04.2006) нарастает:

Джудит Миллер (Judith Miller), репортер The New York Times, провела 85 дней в тюрьме, отказавшись назвать свой источник в расследовании специального прокурора Патрика Фицжеральда (Patrick J. Fitzgerald) по утечке имени агента ЦРУ Валери Плайм.

Два бывших сотрудника Американо-израильского комитета по общественным вопросам (AIPAC) попали под расследование федерального суда по обвинению в заговоре с целью нарушения антишпионских законов за получение информации от чиновников Пентагона. Оба лоббиста являлись гражданскими лицами, и правительство не обвиняло их в получении засекреченных документов.

Национальная архивная служба (The National Archives and Records Administration) с удивлением обнаружила, что по меньшей мере 55 000 документов, прежде доступных исследователям, были изъяты и засекречены заново по секретному соглашению с военными и ЦРУ. Это сделали тайно, так, что документы просто исчезли с полок. Историк Мэтью Эйд (Matthew Aid), который и раскрыл эти факты засекречивания, обнаружил, что, поскольку он обладает некоторыми из таких документов, его могут наказать по Закону о шпионаже (Espionage Act). Аллен Вайнштейн (Allen Weinstein), руководитель Национальной архивной службы, остановил засекречивание документов.

ФБР искала доступ к бумагам покойного колумниста Джека Андерсона (Jack Anderson) для того, чтобы изъять оттуда любые засекреченные документы. Андерсон обнародовал много историй, которые правительство пыталось держать в тайне. Его семья, ссылаясь на 1-ю поправку к Конституции, отказалась отвечать на запрос ФБР. Неясно, как далеко собирается в этом вопросе продвинуться ФБР и будет ли правительство пытаться изучить файлы других журналистов, мертвых или живых.

Портер Госс, директор ЦРУ, засвидетельствовал, что «его цель и надежда», чтобы репортеры, пользующиеся утечками по теме шпионажа и разведки, были доставлены в Большое жюри, где бы их заставили раскрыть имена тех, кто слил эту информацию.

ЦРУ отчислило Мэри Маккартни (Mary O. McCarthy), высокопоставленную сотрудницу, за возможные неразрешенные контакты со СМИ и раскрытие секретной информации журналистам. Агентство позволило распространиться мнению, что она передала историю о секретных тюрьмах ЦРУ в Восточной Европе Дане Прист из The Washington Post, которая якобы перечислила вознаграждение от Пулитцеровской премии на ее счет. Адвокат Маккартни заявил, что она не являлась источником этих сведений и никогда не разглашала секретную информацию.

Конгресс предложил сенаторам рассмотреть вопрос о том, чтобы сотрудников разведывательных агентств, допускающих неразрешенные утечки информации, лишать пенсии. А также позволить ЦРУ и Агентству национальной безопасности (NSA) арестовывать подозреваемых без ордера.

Хотя обвинительный акт против двух лоббистов из Американо-израильского комитета по общественным вопросам (AIPAC) переполнен ссылками на «засекреченную информацию», антишпионское законодательство за единственным исключением упоминает только «информацию, касающуюся национальной обороны».

Антишпионские законы были приняты в 1917 году во время Первой мировой войны. В 1951 году президентским указом была создана существующая сейчас в США система засекречивания документов. Но не существует законов, специально запрещающих утечки, таким образом правительство использовало антишпионское законодательство, чтобы бороться с практикой утечек.

Президент Клинтон наложил вето на закон против утечек в 2000 году, по которому раскрытие засекреченной информации правительственным чиновником считалось бы преступлением. Создавать преступление из утечек информации из правительства только потому, что она была помечена как секретная, по его мнению, было абсурдным.

В 2004 году правительство засекретило 15 294 087 документов. Необоснованное засекречивание документов - это факт из жизни

Вашингтона. Правительственная теория наказания лоббистов может изменить практику сбора новостей в Вашингтоне и взаимодействия лоббистов и экспертов с правительством. Чиновники в Вашингтоне рассказывают ежедневно репортерам о чем угодно, что может оказаться впоследствии засекреченной информацией. Кроме того, откуда журналист должен знать, кто является носителем засекреченной информации и что все это должно наказываться по закону, по которому должны ловить шпионов?

Правительство США по крайней мере до последнего времени считало, что антишпионское законодательство обращено против чиновников, которые разглашают информацию, но не против тех, кому ее разглашают.

Если говорить в целом, то администрации Буша пока не удалось наказать журналистов, но было достаточно угроз сделать это, и атмосфера после 11 сентября привела к росту секретности и давления на журналистов. Например, некоторых журналистов, в том числе таких известных, как Тим Рассерт (Tim Russert) из NBC, заставили давать свидетельские показания в недавнем судебном процессе по делу Льюса Либби (об утечке из ЦРУ). Это то же дело, по которому в тюрьме оказалась Джудит Миллер. В целом, я думаю, правительство с помощью различных акций пытается сделать журналистов более осторожными, и это оказывает негативное действие на свободу прессы.

(Источник: http://www.library.cjes.ru/online/?a=con&b_id=802&c_id=10926)