Руководство по проверке новостей

Tom Trewinnard

Supported by:

Nordic Council of Ministers' Office in Latvia

© The Centre for Media Studies at SSE Riga, 2017

Содержание

Распространенные видынедостоверной информации

Неверное время/неверное место **5**

Фотошоп и монтаж **7**

Подделка **8**

Постановочное видео 8

Сайты с поддельными новостями 9

Местечковые вирусные истории 11

Верификация сообщений

01 Это оригинал? **13**

Что такое: обратный поиск изображения? **14**

Что такое: EXIF данные? 15

02 Кто источник? **15**

Что такое: подставной аккаунт? 17

03 Где? **17**

04 Когда? **19**

05 Почему? **20**

Введение

Использование смартфонов и высокоскоростных мобильных сервисов привело к распространению фото- и видео-контента в социальных сетях. Первые сообщения с международными и срочными новостями, а также видео и фото-свидетельства, теперь все чаще появляются в социальных сетях.

Для журналистов это отличная возможность и вместе с тем вызов. Мы получаем из первых рук срочные новости со всего света и можем сообщать новости, о которых раньше бы не узнали. В то же время, в социальных сетях публикуется недостоверная информация и слова, вырванные из контекста, — чтобы ввести пользователей в заблуждение.

Чтобы использовать информацию из социальных сетей, журналистам необходимо проверять достоверность фотографии, видеозаписи или источника. В этом руководстве собраны чек-листы, которые помогут вам проверить информацию, найденную в сети. После каждого чек-листа приведены полезные советы, о которых следует помнить при проведении расследований.

Помните: лучше быть правым, чем первым

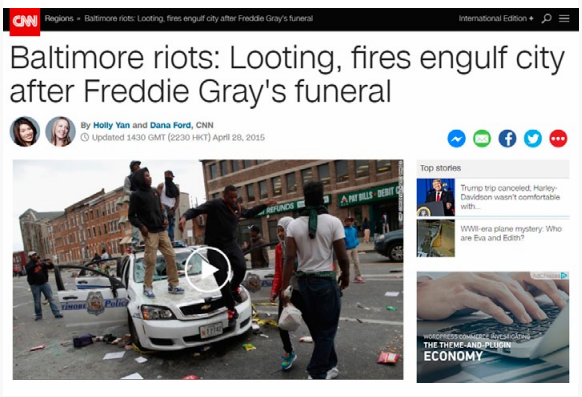
Распространенные видынедостоверной информации

При работе с социальными сетями важно знать о том, какие виды недостоверной информации встречаются чаще всего.

Неверное время/неверное место

Самый распространенный вид недостоверной информации – это вырванные из контекста фотографии или видео, которые повторно публикуются в сети с связи с актуальными событиями. Такие сведения часто распространяют в социальных сетях без злого умысла. Обнаружить фальсификацию, как правило, легко, если следовать некоторым правилам.

- **Пример**. Член парламента Латвии от националистической партии "Отечеству и свободе/ДННЛ" Александрс Кирштейнс, выступающий против размещения беженцев с Ближнего Востока и из Африки на территории ЕС, 20 июня 2016 года опубликовал в Twitter язвительный комментарий по поводу высококвалифицированных специалистов среди прибывших. В качестве иллюстрации Кирштейнс выбрал фото темнокожих протестующих, прыгающих на крыше автомобиля.



На самом деле, фото не имело отношения к тысячам беженцев, приехавших в Европу тем летом. Фотография была сделана во время столкновений в Балтиморе, США, после смерти местного жителя, задержанного полицией.

(http://edition.cnn.com/2015/04/27/us/baltimore-unrest/)

■ Похожий случай произошел 13 декабря 2015 года. Еще одна сторонница объединения “Отечеству и свободе/ДННЛ”, мать депутата, написала в Twitter, что в деревне с единственным в стране центром временного размещения беженцев мигранты ограбили на автобусной остановке 17-летнюю девушку. По словам Элиты Добравы, нападавшие украли у девушки мобильный телефон, а полиция не стала выезжать по вызову. Твит сопровождался изображением, которое часто используется на сайтах движения белых националистов в США, чтобы выразить негативное отношение к иммигрантам из Мексики.

■ Изображение не имело отношения к описанной ситуации, которая, к тому же оказалась выдумкой, перекочевавшей из другой соцсети (полиция опровергла информацию о произошедшем). На самом деле фотография была сделана в Лонг-Айленде, штат Нью Йорк, в 2004 году.

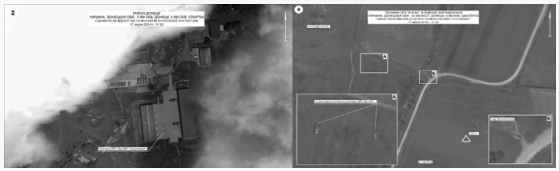
Фотошоп и монтаж

Более редки случаи с подделкой изображений в фотошопе или видео-монтажом. Такие материалы часто публикуются намеренно, для того, чтобы ввести людей в заблуждение. Обнаружить подделку такого типа может быть сложнее, чем установить недостоверную ошибку вида “неверное время/ неверное место”.

- Известный пример подделки видео связан с делом самолета Малайзийских авиалиний, который сбили над Востоком Украины. В результате катастрофы MH17 погибли 298 человек. После того, как появились видео-свидетельства причастности российских военных, Министерство обороны РФ опубликовало скриншот из видео с ракетной пусковой установкой БУК, из которой предположительно стреляли по самолету. Изображение содержало утверждение о том, что рекламный щит находился на территории страны, подконтрольной украинским властям.

- Житель Луганска сделал хорошую фотографию рекламного щита, доказав, что скриншот из видео подвергся манипуляциям (позднее к рекламному щиту приезжали журналисты из Correctiv и 60 Seconds Australia, однако к этому моменту билборд уже был испорчен вандалами).

- Другие группы, изучавшие инцидент, также предъявляли доказательства того, что российская сторона неоднократно подвергала манипуляциям фотографии со спутников, утверждая, что Россия не имела отношения к катастрофе MH17.



These slides release by the Russian Federation purport to show a Buk missile launcher absent from a Ukrainian military base (left), and a pair of Buk missile launchers in a field on the day of the shootdown (right).

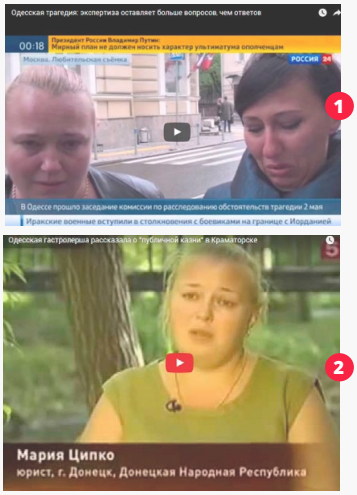
https://medium.com/@DFRLab/lie-in-the-sky-224186b6e98c#.87e60968x

Подделка

Подделка встречаются реже всего, поскольку для ее производства требуются большие усилия. Такие материалы специально публикуют для того, чтобы ввести людей в заблуждение. Встречаются разные типы подделок.

Постановочное видео

Постановочное видео может выглядеть как настоящая запись — как, например, в случае с видео с сирийским мальчиком-героем. Его снимал профессиональный режиссер, а в съемке участвовали актеры.



Во время конфликта Украины с Россией, кульминацией которого стала аннексия Крыма в 2014 году и который сопровождался агрессивной пропагандистской кампанией на подконтрольных Кремлю телеканалах, на Украине получила известность Мария Ципко. Ее назвали "гастролершей" за то, что она сыграла несколько ролей в новостях на российском телевидении.

- 21 июня 2014 года на канале "Россия 24" вышел репортаж о трагедии в Одессе, где после стычки пророссийских активистов с украинскими националистами при пожаре погибли больше 40 человек. В нем Ципко сыграла роль местной жительницы, рассказывающей о государственных репрессиях против пророссийских активистов.

■ 4 августа 2014 года на российском “5-м канале” Ципко выступала уже в качестве юриста, находящегося в зоне конфликта (в самопровозглашенной Донецкой Народной Республике на Востоке Украины); теперь она рассказывала репортеру о том, как украинские вооруженные силы казнили семью пророссийского повстанца. В сюжете не было представлено доказательств ее слов, не появилось их и позднее.

■ Кроме того, Ципко представляли как члена избирательной комиссии на так называемых референдумах о независимости в Луганске и Донецке в 2014 году; ее также называли представителем православного церковного фонда — правда, уже под другим именем.

3

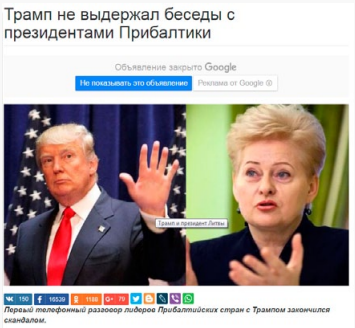
Сайты с поддельными новостями

Сайты с поддельными новостями имитируют реальные новостные издания. Их успешно используют для того, чтобы запустить виральные истории в сеть. Эти сайты могут повторять внешний вид реальных изданий; отличить их можно с помощью информации в URL или записях WHOIS.

■ Сайт Эстонского национального телерадиовещания находится по адресу err.ee (русскоязычная версия — rus.err.ee). Однако существует еще и ресурс eer.ru, который может ввести в заблуждение неопытных интернет-пользователей, поскольку визуально сайты очень похожи (как и многие новостные сайты в целом). Сайт eer.ru называет себя информационным агентством “Внешнеэкономические связи” и управляется негосударственной организацией “*Международный институт проблем устойчивого развития*”. На портале Spravkaforme.ru в описании компании сказано, что “*Международный институт проблем устой-*

чивого развития" работает в сфере медиа-бизнеса, и что ему принадлежит пять новостных сайтов с аудиторией более миллиона уникальных пользователей в месяц. Там также отмечается, что компания "тесно сотрудничает" с российским Министерством иностранных дел. Они нанимают фрилансеров, зарплата которых привязана к количеству просмотров каждой заметки.

- Сайт следует внешней политике Кремля. По запросам "Латвия", "Эстония" или "Литва" ресурс выдает не экономические новости, а сообщения о том, что в странах Балтии опасаются развала НАТО из-за победы Дональда Трампа на выборах президента США, о том, что жители Прибалтики — националисты или имеют антирусские настроения. В качестве источников информации используются государственные новостные агентства ТАСС или РИА Новости, сайт http://inosmi.ru/, публикующий переводы материалов иностранных СМИ на русский язык (оба входят в государственное агентство "Россия сегодня"), а также другие маргинальные веб-сайты.



- Еще один пример – выдуманное сообщение о первом разговоре между избранным президентом США Трампом и президентами трех стран Балтии, который якобы произошел 28 ноября. Сообщалось, что Трамп крикнул "Заткнитесь!" и закончил разговор. В истории стоит ссылка на американский новостной телеканал CNN, но у них никогда не выходило такого сюжета. Дипломатические представители всех трех стран заявили, что описанного разговора никогда не было. В качестве источника истории был указан сайт, который также называет себя "информационным агентством", однако там в основном публикуются новости о российской республике Хакасия и прогноз погоды в столице Хакасии Абакане.

- Эта же новость была опубликована на сайте, авторы которого утверждают, что они публикуют новости о регионах России. На сайте не указаны контакты редакции, но их московский адрес и руководитель редакции Максим Федоренко, те же, что и у eer.ru.

- Та же команда людей из EER.RU указана в качестве редакции интернет-сайта "МК-Лондон", который называет себя представителями газеты Московский Комсомолец.

Местечковые вирусные истории

Местечковые вирусные истории – это новый тренд. Сайты с вымышленными новостями публикуют новости о событиях, произошедших в конкретных населенных пунктах: от террористических атак до ссор знаменитостей. Источники этих историй всегда крайне сомнительны, но иногда местные СМИ подхватывают эти истории и публикуют как настоящие.

- В 2013 году в России началась кампания против усыновления детей иностранцами. Среди прочего, в ходе кампании норвежцев изображали как педофилов, а также высмеивали толерантное отношение к правам ЛГБТ в Скандинавии. Появился особый термин "Гейропа" — как противопоставление христианской верующей России, которая защищает консервативные ценности от влияния "прогнившего" Запада.

- Была создана ГОНГО (Государством организованная негосударственная организация) "Русские матери". Их координатор Ирина Бергсет утверждала, что норвежцы насиловали ее маленького сына, надев на него маску Путина (у нее были большие семейные разногласия после развода в норвежском суде).

- В Москве при содействии окологосударственных структур был организован массовый митинг, на который пришли 12 тысяч человек. В июне зарегистриро-

ванное в России интернет-издание "Segodnia.ru" опубликовало материал о том, что норвежский министр якобы предложил ввести инцест в качестве предмета школьной программы, так как это норвежская "социальная традиция". Материал не передал смысла высказываний министра: что дети надо научить распознавать домогательства и сообщать о них. Источником этой информации был пресс-релиз ГОНГО.

https://rg.ru/2013/03/07/voina.html

■ В 2013 году в Латвии были созданы три такие организации, все они копировали бытующие в России идеи. Их поддержали латвийские националистические и про-российские партии. В латвийских СМИ начали повторять идею “инцеста как социальной нормы" в Норвегии. Уважаемые представители общественности — например, известный детский врач — повторили это в интервью для газеты, которое быстро распространилось в социальных сетях и на семейных сайтах. Идея всплывала в интервью пророссийских и консервативных членов латвийского парламента, ее распространяли на русскоязычных сайтах и в YouTube, а также на российских телеканалах.

■ Некоторые примеры гораздо проще: в декабре 2016 года на латвийских страницах с псевдоновостями в Facebook распространилось мрачное видео с подростком, который называл Латвию – несостоявшимся государством. В течение недели на одном только YouTube это видео просмотрели 155 тысяч раз. Оно повторяло американский ролик “Дорогие будущие поколения, простите", который на момент написания этого текста набрал почти 5.7 миллионов просмотров. Беглый поиск на YouTube показал, что автор ролика претендует на статус видеоблогера (как правило, его ролики набирают около 5 тысяч просмотров). Тем не менее, этот ролик распространялся в латвийских социальных сетях и на сайтах псевдоновостей как правдивое и распространенное мнение.

Верификация сообщений

01 Это оригинал?

Как мы видим, наиболее распространенные виды подлога – это старые видео и фото, которые распространяют в привязке к актуальным событиям и новостям. При проверке важно убедиться в том, что материал является или оригинальным (то есть он не публиковался в интернете раньше и не подвергался обработке) или настолько близким к оригиналу, насколько можно найти.

Найти оригинал можно, воспользовавшись следующими способами:

- обратный поиск изображений через Google Image Search или TinEye;
- проверка “содранного” видео через Amnesty’s Data Viewer;
- проверка теней и отражений;
- при общении с источником попросите его прислать исходный файл (с EXIF данными);
- используйте инструменты анализа изображений — например, Izitru или Forensically, чтобы выявить признаки обработки (лучше всего проверять исходники изображений, а не файлы, найденные в социальных сетях).

СОВЕТЫ

- “Содранное”/видео – это видео, которое скачали с одного аккаунта и опубликовали в другом. Очень часто встречаются "содранные" видео крупных новостных событий, при этом бывает трудно найти исходник.

- Ищите признаки обработки изображения — например, зеркального отображения картинки и перекрашивания.

Что такое: **обратный поиск изображения?**

- Обратный поиск изображения позволяет проверить, встречалось ли уже изображение в сети и найти все веб-страницы, где это изображение уже присутствует. Обратный поиск изображения – это **первая проверка** фотографии из социальных сетей, которую вам следует провести: для нее требуются 30 секунд и 2 щелчка мыши, и это самый быстрый и эффективный способ избежать дальнейшего распространения контента **"неверное время/неверное место"**. Существуют два основных поисковика для обратного поиска изображения: Google Images и TinEye. Стоит проверить по обоим, так как они используют самостоятельные системы индексирования, в каждой из которых миллиарды изображений.

- Если по изображению нет ни одного совпадения в обратном поиске, это **не значит**, что это непременно оригинал или аутентичное изображение: необходимо провести дальнейшие проверки (смотрите далее).

- Free Chrome Extension RevEye делает быстрый поиск по ряду обратных поисковиков изображений, включая Google, TinEye, Yandex, Bing и Baidu.

Что такое: EXIF данные?

EXIF данные – это метаданные, закодированные в фотографии, которые могут предоставить множество информации, как то ID устройства, время и заснятия изображения. Однако EXIF данные удаляются с фото, опубликованных в социальных сетях (например, Twitter и Facebook) или переданными с помощью приложений для сообщений (например, WhatsApp, Viber). Просите ваш источник прислать вам оригинал фотографии по электронной почте, чтобы посмотреть EXIF данные с помощью бесплатно доступных онлайн-инструментов.

02 Кто источник?

Помимо проверки подлинности текстовой записи, фото или видео, необходимо также проверить источник. В некоторых случаях качественную подделку удавалось выявить, лишь обратившись к источнику материала.

Найти его след в сети можно с помощью нескольких техник:

- при анализе информации из профиля обращайте внимание на подозрительные моменты (недавно созданный аккаунт, аккаунт с небольшим числом записей/подписчиков/подписок, опубликованные записи свидетельствуют о смене географического положения автора и т.д.);
- попробуйте найти этого человека в других социальных сетях (ищите через Google имя пользователя или полное имя, если оно указано), соберите все подходящие данные или информацию;
- проверьте ссылки, указанные в профиле (также проверьте информацию о регистрации домена WHOIS);

- проверьте фото из профиля с помощью обратного поиска изображения (совет: обратите внимание на небольшие изменения, например, зеркальное отображение и изменение цвета);
- поищите сообщение из Twitter, чтобы проверить, были ли такие же твиты опубликованы в других микроблогах;
- проверьте, не является ли автор записи ботом. Для этого используйте специальные инструменты, например, BotOrNot;
- общаясь с источниками, просите их предоставить дополнительную информацию (например, уточните погоду и проверьте ее через Wolfram Alpha; запросите EXIF-данные, если они есть).

СОВЕТЫ

- Человек, загрузивший фото или видео, не всегда сам снимал материал. Попробуйте найти автора.

- Вычислить троллей и ботов можно проверив список аккаунтов, на которые автор подписался первым делом, или список тех, кто подписался на него. Как правило, боты и подставные аккаунты добавляют друг друга, чтобы повысить уровень доверия к своим страницам.

- Полезную информацию о человеке или аккаунте в социальной сети можно получить с помощью таких инструментов как Pipl, PeekYou, Spokeo и Foller.me, однако количество полученной информации зависит от страны.

Что такое: **подставной аккаунт?**

Подставные аккаунты или виртуалы – это сетевые аккаунты, используемые с целью обмана. Мотивации этих виртуалов бывают очень разными, но одной из тенденций стала растущая популярность спонсируемых государством виртуалов: настоящие люди получают деньги от правительства за то, что создают аккаунты в социальных сетях и на платформах для публикаций под ложными именами для того, чтобы распространять дезинформацию и создавать искусственное впечатление общественного мнения за или против конкретных лиц или политических стратегий (это называется астротерфинг). Подставные аккаунты можно вычислить техниками расследования (например, анализ соцсети конкретного аккаунта) и более техничнми методами (например, анализ IP адреса).

03 Где?

Проверка места, где была сделана запись, фото или видео, - это эффективный способ разоблачения дезинформации. Этот процесс известен как геолокация, он включает проверку карт, спутниковых снимков, изображений улиц и гео-меток на фото и видео.

Попробуйте определить по карте место, где было сделано фото или видео, следующим образом:

- внимательно проанализируйте фото/видео, обращая внимание на визуальные ориентиры. Это могут быть заметные здания, уличные знаки, номерные знаки машин, или характерный ландшафт – горы, реки;
- попробуйте найти эти визуальные ориентиры или здания на карте, используя изображения со спутников, изображения с гео-метками (например, Panoramio) или карты с аннотациями (например, WikiMapia);

- если у вас есть оригинал файла, проверьте EXIF-данные. Возможно, среди них есть данные о геолокации;
- проверьте другие записи источника в социальных сетях. Возможно, они помогут определить, где был пользователь в момент съемки фото или видео.

СОВЕТЫ

- Сообщения в Twitter и Facebook, YouTube-видео и фотографии в Instagram могут иметь геотеги, проставленные пользователем при размещении фото, видео или записи. Эти метки могут оказаться полезными, однако их необходимо верифицировать, поскольку пользователь может править геотеги при загрузке изображения. Это значит, что пользователь мог сделать фото в Риге и сопроводить его геотегом из любого другого места на планете (впрочем, такие случаи нельзя назвать распространенным явлением). Большая часть контента в социальных сетях публикуется без геотегов, поэтому необходимо проверять местоположение вручную и проводить геолокацию.

- Для видео – сделайте стоп-кадры (для этого можно использовать инструменты на YouTube, программы монтажа для работы с оффлайн-видео). Соберите из них сборные изображения, они могут дать более четкое представление о ландшафте. Четко пометьте эти изображения с соответствии с тем, что видно на карте с аннотациями или на спутниковых снимках.

https://www.bellingcat.com/news/2016/10/22/exit-corridor-shelling-west-aleppo-open-source-analysis/

04 Когда?

Определить когда была сделана запись, фото или видео очень важно для установления их достоверности. Это особенно важно еще и потому что в качестве подделки часто используются старые фотографии и видео с привязкой к актуальным новостям.

Чтобы узнать, когда было снято фото или видео, надо:

- провести обратный поиск изображений через Google Image Search или TinEye;
- проверить видео с помощью Amnesty's Data Viewer, чтобы выяснить, не было ли оно скачано из другого источника;
- если у вас есть оригинальный файл, найдите в EXIF-данных сведения о времени, когда было сделано изображение;
- посмотрите старые записи о погоде в нужном месте в конкретный отрезок времени с помощью Wolfram Alpha;
- если вы установили точную дату и точное местоположение, используйте SunCalc. С его помощью вы можете примерно определить время съемки, оценив направление и длину теней на фото или видео.

СОВЕТЫ

- Обращайте внимание на часовые пояса в соцсетях, где вы нашли контент. YouTube и Instagram используют тихоокеанское время США. Twitter использует время, соответствующее установкам вашего профиля. В записях Facebook проставляется время, соответствующее установкам вашего компьютера.

- В некоторых случаях подделку можно обнаружить по изменениям в городском ландшафте. Например, в ходе конфликта в Сирии в некоторых городах были

разрушены определенные здания и мечети, поэтому фото или видео с этими зданиями, якобы показывающие события уже после разрушений, скорее всего, помещены в неправильный контекст.

05 Почему?

Для установления достоверности бывает важно понять, почему пользователь социальной сети опубликовал определенный материал. Некоторые пользователи – случайные очевидцы, некоторые – туристы. Некоторые из них, возможно, профессиональные журналисты, другие – активисты, кто-то может быть чиновником. Бывает важно определить мотивацию источника: активисты или чиновники могут использовать социальные сети, чтобы рассказать только одну сторону истории или выставить своих оппонентов в дурном свете.

- При анализе информации из профиля обращайте внимание на подозрительные моменты (недавно созданный аккаунт, аккаунт с небольшим числом записей/подписчиков/подписок, опубликованные записи свидетельствуют о смене географического положения автора и т.д.).

- Попробуйте найти этого человека в других социальных сетях (ищите через Google имя пользователя или полное имя, если оно указано), соберите все подходящие данные или информацию.

Дополнительные ресурсы

Дополнительную информацию о том, как верифицировать данные, примеры и подробные гайдлайны можно найти на этих ресурсах:

First Draft News: объединение журналистов и специалистов из сферы технологий, которые разрабатывают обучающие материалы, анализируют случаи из практики, исследуют процесс поиска и верификации новостей в социальных сетях. На First Draft News собраны ресурсы для работы с видео, а также интерактивные обучающие упражнения, с помощью которых можно проверить и улучшить свои навыки.

Verification Handbook: первый комплексный ресурс для верификации новостей, включает описание случаев из практики. У книги есть два приложения, одно из них посвящено журналистским расследованиям, другое — верификации цифрового контента при работе в экстремальных условиях.

Supported by :

Nordic Council of Ministers' Office in Latvia

© The Centre for Media Studies at SSE Riga, 2017