

АНАЛИЗ МЕТАДАННЫХ ПОЛЬЗОВАТЕЛЬСКОГО ФОТО- И ВИДЕОКОНТЕНТА КАК МЕТОД ЕГО ВЕРИФИКАЦИИ

И. А. Королев

*Белорусский государственный университет,
ул. Кальварийская, 9, 220004, г. Минск, Республика Беларусь,
Iakorolev1996@gmail.com*

*Научный руководитель – В. П. Воробьев,
кандидат филологических наук, доцент*

В статье рассматривается изучение метаданных фото- и видеоконтента, снятого пользователями социальных медиа, как метод установления его достоверности. Проанализированы преимущества и ограничения метода анализа метаданных.

Ключевые слова: верификация; пользовательский контент; анализ метаданных.

STUDYING METADATA OF USER-GENERATED CONTENT AS A METHOD OF ITS VERIFICATION

I. A. Korolev

*Belarusian State University,
9, Kalvariyskaya Str., 220004, Minsk, Republic of Belarus
Corresponding author: I. A. Korolev (Iakorolev1996@gmail.com)*

*Scientific adviser – V. P. Vorobiev, Candidate of Philology,
Associate professor*

The article deals with metadata analysis of photo and video content taken by users of social media as a method of establishing its reliability. The advantages and limitations of the metadata analysis method are studied.

Key words: verification; user-generated content; metadata analysis.

Основной задачей журналиста при верификации созданного пользователями социальных медиа контента является определение «проис-

хождения (оригинальность контента), источника (кто загрузил), даты/времени его создания (когда создан) и локации (где создан)» [1]. Получение ответов на данные вопросы является базовым требованием для установления достоверности пользовательского контента.

Исходя из этого, можно утверждать, что процесс верификации фото- и видеоконтента включает в себя два направления: подтверждение соответствия контента действительности (установление его подлинности) и подтверждение соответствия контента сопровождающей его информации (установление даты, времени, места его создания), что необходимо во избежание использования соответствующего действительности контента в ложном контексте.

Наиболее эффективным способом подтвердить совпадение контента и контекста верифицируемого объекта является изучение его метаданных. Метаданные, также называемые EXIF-данными (exchangeable image file format), представляют собой информацию о файле, которая появляется на цифровом устройстве (в частности, смартфоне, фотоаппарате) автоматически при его создании и передается вместе с ним. Это встроенная в файл информация о его свойствах и признаках. Данный цифровой отпечаток остается с изображением или видеозаписью до тех пор, пока кто-то или какая-то программа не удалит его.

Метаданные хранят информацию о том, когда было выполнено изображение или видеозапись, на какое устройство и при каких его настройках (в случае фотографий). Метаданные также могут содержать информацию о геолокации и сведения о том, «как изображение было отредактировано в редакторе» [2, с. 61]. Узнать метаданные можно как при помощи детального просмотра информации о файле через функцию ПК «свойства файла – детальные», так и через специализированные инструменты: программное обеспечение, например, Photoshop (для фотографий) или Sony Vegas Pro, Adobe Premiere Pro (для видеозаписей), и онлайн-сервисы, в частности, View Exif Data (для фотографий) и Metadata2go (для видеозаписей).

Метаданные фотографий могут содержать информацию о том, в какой программе, а иногда и каким образом изображение подвергалось редактированию. Однако такая информация не всегда является прямым указанием на манипулирование, так как «многие фотографии обрабатываются в Photoshop или какой-либо другой программе редактирования для стандартной обработки, в частности, коррекции цвета или изменения размера» [3].

Главным ограничением метода анализа метаданных является факт того, что метаданные можно извлечь далеко не из всех изображений и видеозаписей. В частности, множество популярных платформ социальных медиа удаляют эту информацию для экономии трафика. Также, согласно исследованию Digital Security, при отправлении фотографии через популярные мессенджеры Telegram, Viber, WhatsApp из «галереи» или при помощи функции «камера» метаданные снимка стираются полностью. При этом если фотография передается «как файл», то все выше-названные мессенджеры оставляют метаданные нетронутыми [4, с. 11].

Специалисты рекомендуют проявлять осмотрительность к найденным метаданным, так как существуют инструменты, например, онлайн-сервис Imgonline.com.ua (в случае фотографий), позволяющие автору контента изменять EXIF-данные. Особого внимания заслуживает верификация даты и времени снимка, так как в устройстве могут быть установлены заводские настройки или другой часовой пояс.

Данные о геолокации являются важной информацией, однако «с учетом усиления тенденций борьбы за приватность пользовательских данных, во многих смартфонах настройки, связанные с дополнительной информацией о фото, например, GPS, могут быть отключены по умолчанию» [5]. Зачастую для включения функции сохранения геоданных фотографий и видеозаписей пользователю смартфона недостаточно только включить геолокацию, необходимо также выбрать специальную функцию привязки геоданных к снимкам и видеозаписям.

Данные о геолокации могут стать известны журналисту из самого фото/видео, если ему знакома изображенная местность, или она имеет характерные, значимые для определения локации, детали, в частности достопримечательности, номерные знаки на транспорте, вывески магазинов, граффити на стенах. Для того чтобы найти конкретное место по имеющимся деталям или убедиться в естественности окружающей среды, расположении домов, достопримечательностей или иных распознанных журналистом объектов, специалисты рекомендуют обратиться к инструментам, позволяющим оказаться на изображенном на видео/снимке месте, например, Google Map's или Google Earth.

Если журналисту известна геолокация, а в комментарии к фотографии/видеозаписи указано время ее создания, журналист может соотнести архивные данные о погоде со сведениями из комментария к файлу. Такую возможность дает инструмент WolframAlpha, позволяющий узнать, какая погода была в определенный день в указанной местности.

Данный инструмент может работать и в обратном направлении. Так, в 2012 году пользователь по имени Рита Крилл загрузила на YouTube видео удара молнии на ее заднем дворе. Журналисты не смогли связаться с Ритой, однако имеющейся у них информации (имя пользователя и дата загрузки) оказалось достаточно для того, чтобы верифицировать достоверность видеозаписи. Для начала при помощи сервиса Spokeo журналисты нашли всех обладательниц имени «Рита Крилл» с указанием их места жительства. Затем журналисты при помощи инструмента Wolfram Alpha установили, в каком из городов проживания пользователей с данным именем в указанный день были активные грозы. После чего журналисты убедились в том, что внешний вид дома Риты Крилл в Google Map's совпадает с домом на видеозаписи [6].

Таким образом, сегодня анализ метаданных является одним из наиболее эффективных и часто применяемых журналистами методов установления достоверности пользовательского контента. При этом данный метод имеет существенные ограничения, в частности, метаданные автоматически стираются у загружаемого в социальные медиа фото- и видеоконтента, а также поддаются редактированию в специализированных программах.

Библиографические ссылки

1. *Silverman C., Tsubaki R.* Verification handbook: An ultimate guideline on digital age sourcing for emergency coverage [Electronic resource]. Verification handbook. URL: <https://verificationhandbook.com/downloads/verification.handbook.pdf> (data of access: 27.08.2022).
2. *Карнов Д. С., Ибрагимова З. А.* Способы и средства обеспечения анонимности в глобальной сети Интернет // Правовая информатика. 2021. №. 3. С. 60–67.
3. *Horaczek S.* Spot faked photos using digital forensic techniques [Electronic resource]. Horaczek. 2017. URL: <https://www.popsoci.com/use-photo-forensics-to-spot-faked-images> (data of access: 27.08.2022).
4. Метаданные файлов: Невидимая информация, раскрывающая вашу личность [Electronic resource]. Digital Security. URL: <https://dsec.ru/useful-materials/analysis/metadannyye-fajlov-nevidimaya-informacziya-raskryvayushhaya-vashu-lichnost> (дата обращения: 27.08.2022).
5. *Баловсяк Н.* Как проверить достоверность фотографии [Электронный ресурс]. Stopfake. 2021. URL: <https://www.stopfake.org/ru/kak-proverit-dostovernost-fotografii> (дата обращения: 27.08.2022).
6. *Нолан М.* Маркхэм Нолан: Как отделить правду от вымысла онлайн [Электронный ресурс]. YouTube. URL: <https://www.youtube.com/watch?v=LjaqH5JogGo> (дата обращения: 27.08.2022).