Адміністрація Facebook була більш стриманою, заявивши, що вони самі активно видаляють повідомлення екстремістського змісту і готові до перемовин із урядом.

Використовуються ІТ-технології як для пошуку мародерів, так і в якості доказової бази в судах. Активно використовуються так звані «дігі‑вени» [5] («digi-van» – машини, які обладнано великим телеекраном, на якому демонструються фото мародерів, знятих CCTV – розгалудженої системи відеокамер, призначеної для візуального контроля чи автоматичного аналізу зображень).

Британські парламентарі вимагають від представників основних соціальних мереж блокувати доступ користувачів під час масових заворушень. Менеджери основних соціальних мереж Facebook, Twitter та BlackBerry та представники поліції сьогодні зустрінуться з міністром внутрішніх справ Великобританії Терезою Мей. На засіданні будуть підняті питання щодо ролі соціальних мереж під час масових акцій громадської непокори, а також їх відповідальність за зміст повідомлень, які публікуються на сайтах. Серед іншого буде обговорюватись можливість заборони доступу підозрюваних бунтівників до соціальних мереж. Мей пропонує провести конструктивну дискусію щодо того, як соціальні мережі можуть допомогти уряду під час заворушень замість обговорення закриття сайтів взагалі.Депутати від Консервативної партії Тім Голдвін та Луїза Менш запропонували закривати сайти на час надзвичайного стану.У свою чергу Twitter та Facebook оприлюднять заходи, які вже вживаються, для видалення повідомлень, які потенційно підбурюють до насильства.Нагадаємо, суд англійського міста Честер засудив до чотирьох років в’язниці двох молодих людей за заклики до насильства в соціальній мережі Facebook під час недавніх вуличних безладів в Британії.

Список використаних джерел:

1. Почепцов Г. Г. Інформаційна війна як інтелектуальна війна [Електронний ресурс] / Г. Почепцов. – Режим доступу: http://osvita.mediasapiens.ua/material/13303

2. Дубов Д. В. Мобільний зв’язок та соціальні мережі під час «BlackBerry-бунту» у Великобританії. [Електронний ресурс] Дубов Д. В. – Режим доступу: http://www.niss.gov.ua/articles/553/

Харицька О.М.

студент,

Навчально-науковий інститут інформаційної безпеки

Національної академії Служби безпеки України

МЕТОДИ ВЕРИФІКАЦІЇ ЗОБРАЖЕНЬ В МЕРЕЖІ ІНТЕРНЕТ

Сьогодні цифрове середовище сповнене чуток та недостовірних фактів, що змушує користувачів активно відсортовувати правдиву і справжню інформацію від брехні.

Як зазначає І. Грабовська: верифікація це (від лат. verus – істинний і *...фікація*) – методологічне поняття, що визначає процес встановлення істинності наукових положень у результаті їхньої емпіричної перевірки [1].

В мережі Інтернет знаходиться велика кількість невідфільтрованих даних. В процесі пошуку інформації користувачі часто стикаються з фейковою інформацією, яка може нести небезпечний характер та розповсюджуючи яку, вони несуть шкоду та створюють паніку в суспільству.

За допомогою неправдивої інформації, з використанням зображень «сайти-рекламники» підвищують свою відвідуваність шляхом зацікавлення користувачів вигаданою «пліткою», побачивши яку, не кожен зможе стриматись від відвідування цього сайту. Також інші сайти розповсюджують неперевірені зображення, які описують надзвичайні події та катастрофи. Побачивши такі зображення спільнота підпадає під вплив вмісту зображення, цим самим вводить в оману себе і оточуючих.

Для того щоб уникнути подібних ситуацій, користувач Інтернет повинен використовувати інструменти перевірки зображень:

1. Встановлення автора/першоджерела зображення.

Перш за все потрібно встановити автора зображення, і дізнатись від нього безпосередньо, чи він дійсно є тою людиною, яка його створила. Контакт з особою, яка завантажила зображення, через акаунт в соціальний мережі або адресу електронної пошти, з якої було поширено зображення, є наступним кроком. Також важливо спробувати дізнатись як можна більше про особу завантажувача. Ці деталі можуть допомогти визначити, чи насправді він є першоджерелом зображення.

У багатьох випадках люди можуть намагатись бути не байдужими та корисними, поширюючи зображення, які вони бачили де-небудь, та зізнаватися в тому, що вони є їх авторами. Але багато людей можуть видавати себе за автора в своїх інтересах, в таких випадках розшук джерела зображення може затягнутися на довгий період. Також існують випадки коли людина, яка завантажила зображення не є автором і розшук продовжується до встановлення людини яка фактично зробила зображення.

Важливим кроком є використання таких сервісів, як Google Reverse Image Search чи TinEye. Необхідно вставити URL зображення або копію зображення у будь-який з них, і вони просканують мережу на наявність збігів. Якщо декілька посилань покажуть на те саме зображення, натисніть «переглянути в інших розмірах», для подальшого аналізу.

Особливо корисним для підтвердження автора є Pipl.com, оскільки він дозволяє перевірити за допомогою перехресних посилань імена людей, імена користувачів, адреси електронної пошти і номери телефонів та, з іншого боку, онлайн-профілі осіб. Для пошуку в міжнародному масштабі додатковим корисним ресурсом є WebMii. LinkedIn також є чудовим способом верифікації людей і часто надає додаткові шляхи перевірки та відслідковування.

2. Підтвердження місця, дати і приблизного часу, коли зображення було отримано або зафіксовано.

Є декілька корисних журналістських і технічних засобів встановлення такої інформації як дата, місце, де зробили фотографію та інші важливі деталі. Основний спосіб зібрати цю інформацію – поговорити з автором/тим, хто завантажив зображення.

Із досвіду BBC, люди, які насправді знаходяться на місці подій, будуть надавати візуальні відповіді, часто описуючи деталі в теперішньому часі. («Я знаходжуся посеред вулиці X; я можу бачити і почути Y»). Чим більш невизначеною є відповідь, тим більше застереження виникає щодо того, що повідомляє джерело.

Інша корисна техніка – попросити, щоб людина надіслала будь-яке додаткове фото, зроблене в той самий час. Рідко буває так, щоб хтось робив тільки один знімок в ситуації, що заслуговує висвітлення у пресі. Наявність більше, ніж одного зображення, допомагає вам дізнатися більше про те, як розгорталися події. При цьому важливо звертати увагу на деталі, зображені на фотографії, такі як: державні номерні знаки на транспортних засобах, погодні умови, місцеві пам'ятки та визначні споруди, інші подібні орієнтири, вивіски, позначки, написи, будівля або магазин, які можна ідентифікувати, тип ландшафту та довкілля в знімку. Ці деталі допоможуть переконатися в тому, що людина справді була на місці подій та скоріш за все є автором зображення.

Підтвердження, що зображення є саме тим, що позначено/запропоновано до розгляду. Зображення може бути справжнім, але маркування чи підпис можуть бути некоректними. Наприклад, може бути зроблене фото звичайного дощу, а підписане як ураган чи шторм з великими жертвами. Також, фотографії можуть бути зроблені не в тому місці, яке вказано в надписі над зображенням. Тому, підтверджуючи дату, час і приблизне місце, де було зроблене фото, також важливо, упевнитись, що на зображенні – саме те, що стверджується. Зображення, яке є справжнім, може бути розміщено чи подано в неправдивому контексті.

Необхідно використовувати Google Maps, Bing Maps чи Wikimapia, які допоможуть вам перевірити місце зйомки. Зображення, які надсилають користувачі, дуже серйозно індексуються цими сервісами, мають там відповідні теги. І це дає додаткові корисні напрямки та ідеї, які варто відслідковувати, так само як і додаткові кути погляду на місця, де відзнято світлини, які ви досліджуєте.

Сервіси локації, які надають соціальні медіа, такі як Geofeedia та Ban.jo, можуть допомогти встановити, звідки було завантажено зображення. Якщо фото було викладено в Україні, а надпис над фотографією свідчить про події в іншій країні, то правдивість даної інформації піддається великому сумніву.

Окрім зазначених інструментів і методів, також корисно перевірити, чи подібні зображення розповсюджуються офіційними службами новин або агентствами. Чи є якісь зображення з того самого місця, що завантажуються на соціальних медіа іншими? Якщо вони показують подібну сцену з різних кутів, це також допоможе підвищити довіру до автентичності зображення.

3. Отриманий дозвіл від автора/першоджерела на використання зображення.

Найкращим рішенням завжди є отримання дозволу від власника авторських прав на зображення. До того ж, у багатьох країнах закони про авторське право стають все більш ясними щодо отримання автором компенсації, якщо в нього попросили дозволу на використання зображення.

Положення і умови авторського права щодо контенту, який ви завантажуєте собі з соціальних мереж, для різних сайтів є різними. Деякі, наприклад Flickr, чітко вказують біля зображення, чи залишив фотограф за собою усі права як автор, чи дозволяє використання за правилами Суспільної Творчості (Creative Commons) [2].

Отже, процес верифікації зображень є трудоємким, але дуже важливим для підтримання стабільності в суспільстві та забезпечення користувачів правдивою інформацією. Існує велика кількість людей які мають політичний або інший інтерес в тому щоб порушити стабільність у суспільстві, шляхом розповсюдження фейкової інформації. В той же час, є люди не байдужі та зацікавлені в донесені до суспільства правдиву інформацію. Тому необхідно вміти розрізняти ці дві групи людей, шляхом використання вище зазначених методів.

Список використаних джерел:

1. Грабовська І. Енциклопедія сучасної України / І. Грабовська // [Електронний ресурс] // Режим доступу: http://esu.com.ua/search_articles.php?id=33591

2. Сільверман К. Посібник з верифікації / К. Сільверман // [Електронний ресурс] // Режим доступу: http://verificationhandbook.com/downloads/verification.handbook_ua.pdf