

https://www.researchgate.net/publication/319449165_The_Al_Jazeera_effect_How_the_new_global_media_are_resaping_world_politics

ШИЯН Р. В.

студент, Університет економіки та права «КРОК»,
м. Київ,
shyianrv@krok.edu.ua

ВОВЧЕНКО О. В.

к.е.н., доцент кафедри міжнародних відносин та журналістики,
Університет економіки та права «КРОК»,
м. Київ,
VovchenkoOV@krok.edu.ua
<https://orcid.org/0000-0001-7502-5702>

БЕЗПЕКА ЖУРНАЛІСТА У ВІРТУАЛЬНОМУ ПРОСТОРІ

Актуальність теми дослідження обумовлена розвитком технологій, які формують віртуальним простір, де існують дещо інші загрози для журналістської діяльності. Спостерігаючи за порушеннями прав журналістів в Україні, можна помітити стрімке зростання Інтернет-погроз, онлайн-булінгу, втручання у особисте життя та інших видів порушень прав людини в Інтернеті стосовно представників журналістської діяльності через публічний характер їхньої роботи. Також, журналісти доволі часто стають жертвами хакерських атак, взлому електронної пошти та викриття особистих даних задля поширення дезінформації. Нехтуючи базовими знаннями цифрової безпеки, журналіст ризикує залишитися без важливої для нього інформації. Для журналіста проблема забезпечення цифрової безпеки є набагато актуальнішою, порівняно зі звичайним інтернет-користувачем. Оскільки основи професії журналіста полягають у пошуку, зборі, обробці інформації, яку у подальшому доносять до аудиторії. Буває так, що журналіст знаходить дані завдяки джерелам, які мають ризик бути розкритими через недостатній захист мобільних приладів, комп'ютерів, облікових записів журналіста [1].

Більшу частину соціальних мереж використовують задля людського самовираження. І це, як не дивно, є однією з небезпек у віртуальному просторі для журналістів. В Інтернеті люди підсвідомо поводять себе більш відкрито та сміливо, не боячись висвітлювати суб'єктивні думки. Такою можливістю користується більшість сучасних журналістів. Однак, деякі іноді переходять рамки дозволеного в соцмережах, не зважаючи на втрату репутації, яку ризикують зазнати журналістські редакції через таку поведінку. Варто пам'ятати, що кожна вашу викладену думку можуть використати проти вас. Потрібно бути обачним та обережним у своїх висловлюваннях, перш ніж публікувати їх у мережу. Адже, журналіст є головним ретранслятором великої кількості важливих даних, тож неодмінно важливо завчасно впевнитися у тому, що інформація є достовірною і, що вона не принесе шкоди читачам. «Велика небезпека соціальних медіа в тому, що тепер значно легше сказати щось погане чи непристойне у фейсбуці чи твітері, це може зробити кожен журналіст, і контролю тут немає. Я думаю, це одна з найбільш серйозних проблем, яку необхідно обговорювати. Як журналіст, я вважаю так: все, що я кажу у твітері чи фейсбуці, – це публічний простір, тому я б ніколи не написав там не лише неперевіреної інформації, але й певних звинувачувальних чи недоброзичливих речей на чийсь адресу» [2].

Наступним фактором ризику для журналіста є особисті дані. Для зловмисника викриття конфіденційних даних є основною метою, завдяки якій можна завдати значної шкоди журналісту та перешкоджати робочому процесу. Експерти Комітету із захисту журналістів дають наступні поради: необхідно видалити особисті дані з Інтернету; використовувати двофакторну аутентифікацію та менеджера паролів для захисту облікових записів; слід подумати про психологічний аспект (хакерські атаки та онлайн-переслідування не повинні похитнути моральний стан журналіста). Варто завчасно розуміти усі ризики та бути до цього підготовленим [3].

Журналісти використовують Інтернет для збору інформації, що може зробити їх самих та їхні джерела вразливими, якщо вони не вживатимуть заходів, щоб захистити себе. Інтернет-провайдери, уряди, компанії та злочинці збирають дані про користувачів Інтернету, які можуть бути використані для їх переслідування, у тому числі для порушення проти них судових справ. Комітет із захисту журналістів (CPJ) сформував чіткі дії, які робитимуть віртуальне середовище більш безпечним для людей, працюючих у журналістській сфері:

1. Дізнайтеся, кому належить ваш Інтернет-провайдер і які юридичні зобов'язання компанії щодо передачі ваших даних урядам. Подивіться, які дані зберігають про вас і як довго.

2. Коли ви відвідуєте веб-сайт, він збирає дані про вас, у тому числі вашу IP-адресу, яка видає ваше приблизне місцезнаходження, відомості про ваш пристрій. Розгляньте можливість встановлення безкоштовного браузера Tor Browser Bundle для анонімного використання Інтернету. Його особливо рекомендують журналістам, які займаються такими тонкими питаннями, як високорівнева корупція у країнах із розвиненими технічними можливостями.

3. Встановіть додаток для блокування реклами. Це захистить від шкідливих програм, які часто приховані у рекламі. Також, блокувальники реклами дозволяють звільняти від блокування певні сайти, у тому числі й ресурси новин.

4. Злочинці та інші особи можуть створювати підроблені веб-сайти, які можуть використовуватися для збирання ваших особистих даних, таких як паролі та дані кредитних карток тощо. Переконайтеся, що адреса веб-сайту справжня, а не підроблена. URL-адреса повинна бути написана правильно і включати https.

5. Не варто використовувати загальнодоступні комп'ютери, особливо ті, що знаходяться в Інтернет-кафе, прес-центрах або інших закладах. Загальнодоступні гаджети можуть бути заражені шкідливим або шпигунським програмним забезпеченням. У разі використання такого

гаджету слід уникати входу у свої особисті облікові записи. Обов'язково вийдіть з усіх сеансів та очистіть історію переглядів [4].

Тобто, Інтернет-мережа хоч і є досить зручним ресурсом для отримання, обробки та подачі інформації, але водночас він наділений власними недоліками, які можуть завдати значної шкоди журналістській діяльності. Сформовані правила безпечної роботи у віртуальному просторі допоможуть тримати у безпеці конфіденційні дані.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Цифрова безпека журналістів та інших працівників медіа. URL: https://courses.prometheus.org.ua/courses/course-v1:Prometheus+DSJ101+2022_T1/about
2. Дорош М. Марк Літл: Журналісти в соцмережах мають поводитись як на місці події. URL: <https://ms.detector.media/onlain-media/post/5991/2012-10-10-mark-littl-zhurnalisty-v-sotsmerezkhakh-mayut-povodytys-yak-na-mistsipodii/>
3. Essential journalist safety information for 2022. URL: http://support.cpj.org/site/MessageViewer?dlv_id=6182&em_id=2863.0
4. Digital Safety Kit. URL: <https://cpj.org/2019/07/digital-safety-kit-journalists/>

ШЛАПАК С. О.

студентка, Університет економіки та права «КРОК»,

м. Київ,

shlapakso@krok.edu.ua

ВОВЧЕНКО О. В.

к.е.н., доцент кафедри міжнародних відносин та журналістики,

Університет економіки та права «КРОК»,

м. Київ,

VovchenkoOV@krok.edu.ua

<https://orcid.org/0000-0001-7502-5702>