

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Інформаційна незалежність держави. URL:
<https://osvita.ua/vnz/reports/politolog/17286/>
2. Дзьобань О. П., Пилипчук В. Г. Інформаційне насильство та безпека: світоглядно-правові аспекти : монографія. Х : Майдан, 2011. 244 с.
3. Уханова Н. С., Бойко О. В. Проблеми інформаційного протистояння і додержання прав людини в контексті розбудови інформаційного суспільства. *Інформація і право*. 2011. № 2(2). С. 71–77.
4. Про національну безпеку України : Закон України від 21 червня 2021 р. № 2469-VIII / Верховна Рада України. URL:
<https://zakon.rada.gov.ua/laws/show/2469-VIII#Text>
5. Стратегія інформаційної безпеки : Указ Президента від 28 грудня 2021 року № 685/2021. URL: <https://www.president.gov.ua/documents/6852021-41069>
6. Інформаційно-психологічні війни. URL:
<https://osvita.ua/vnz/reports/psychology/28792/>

СИТНИК А. Д.

студентка, Університет економіки та права «КРОК»,
м. Київ,
sytnykad@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>

ЦИФРОВА БЕЗПЕКА ЖУРНАЛІСТА-РОЗСЛІДУВАЧА

Регулярні дослідження порушень прав журналістів в Україні демонструють істотне зростання онлайн-погроз, онлайн-булінгу, втручання у

201

приватне життя та інших форм порушень прав людини в Інтернеті щодо журналістів, блогерів та громадських активістів через публічний характер їхньої роботи. Окрім цього, журналісти щодня стикаються з ризиками зламу електронної пошти, акаунтів у соціальних мережах тощо, зокрема для поширення дезінформації. Найчастіший ризик від нехтування основами цифрової безпеки – втрата важливої інформації. Для журналіста це часто набагато серйозніше, ніж для пересічного інтернет-користувача, адже основа професії журналіста – пошук, збір, перевірка інформації, яку потім доносять до суспільства. Нерідко журналісти збирають інформацію завдяки джерелам, що можуть бути розкриті через недостатній захист мобільних приладів, комп'ютерів, облікових записів журналіста [1].

Актуальність теми зумовлена зростанням значення цифрової безпеки журналістів-розслідувачів як виду журналістської діяльності в умовах інформатизації суспільних відносин, розвитком відкритих інформаційних джерел, впровадження інформаційно-комунікаційних технологій.

Злам електронної пошти, профілів у соціальних мережах, месенджерах, вітік та зловживання становить особливу небезпеку для журналіста-розслідувача, що розслідує гострі суспільно важливі та конфліктні теми. Тому, спеціалісти у сфері цифрової безпеки дають журналістам важливі рекомендації.

По-перше, для того, щоб захистити від зламу свою поштову скриньку, профілі у месенджерах та соцмережах, потрібно встановити двофакторну авторизацію, яка забезпечує додатковий захист на випадок, якщо пароль потрапить до чужих рук. Також, не варто заходити до своєї поштової скриньки чи профілю з чужих пристроїв. Найважливішим є використання надійних паролів, які не повинні повторюватися з паролям на інших сервісах.

По-друге, для уникнення витоку інформації під час розмов зі своїми джерелами краще не використовувати звичайні телефонні розмови, тому що вони найменш захищені, а комунікація за допомогою різноманітних

месенджерів (наприклад, WhatsApp, Facebook Messenger, Telegram тощо) є більш надійною, але також варто налаштувати двофакторну авторизацію.

По-третє, якщо телефон чи комп'ютер вкрадено, то для уникнення витоку та втрати важливої інформації, необхідно всі пристрої (ноутбуки, смартфони, флешки) зашифровувати за допомогою спеціальних програм (для Windows – Bitlocker, для MacBook – FileVault, для смартфонів – у налаштуванні безпеки) та зберігати всю інформацію у хмарних сховищах. Також, коли залишаєте ноутбук без нагляду – обов'язково блокуйте екран (для Windows – кнопки Win+L, для MacBook – закрити кришку).

По-четверте, для захисту пристроїв від вірусів і шпигунських програм важливо: слідкувати за тим, щоб операційна система вчасно оновлювалась до останньої версії; використовувати виключно ліцензійні програми, у першу чергу це стосується антивірусу; бути уважним до повідомлень в електронній пошті та месенджерах [2].

Тобто, цифрова безпека журналіста є дуже важливою в професійній діяльності, оскільки є гарантією безпеки життя та здоров'я як самого журналіста, так і його джерела. Вищезазначені рекомендації показують, що їх дотримання є не складним процесом і доступним для непрофесійних програмістів.

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. Експерти Ради Європи провели для українських журналістів другий тренінг з цифрової безпеки. URL: <https://mkip.gov.ua/news/7819.html>