УДК 001:168

Олександр Александров,
Володимир Оскрого

♦

ІНФОРМАЦІЙНА БЕЗПЕКА: КРОСМЕДІЙНІСТЬ ТА ІНТЕРНЕТ-РЕАЛІЇ ПОТОЧНОГО МОМЕНТУ В УКРАЇНІ

У роботі аналізується висвітлення подій періоду «Майдан 2013–2014» в інтернет-просторі України на прикладі кількох відомих інтернет-порталів. Досліджується застосування кросмедійних технологій з урахуванням можливостей сучасної комунікаційної інфраструктури в Україні в аспекті інформаційної безпеки. Розглядається використання певних соціально-комунікаційних технологій, що застосовуються під час «інформаційної війни«, яка зараз триває в Україні.

Ключові слова: *інформаційна безпека України, кросмедійність, інтернет-реалії України.*

В работе анализируется освещение событий периода «Майдан 2013–2014» в интернет-пространстве Украины на примере нескольких известных интернет-порталов. Нас интересует применение кроссмедийных технологий с учётом возможностей современной коммуникационной инфраструктуры в Украине с точки зрения информационной безопастности. Мы рассмотрим использование определённых социально-коммуникационных технологий, которые будут полезными во время «информационной войны», которая сейчас ведётся в Украине.

Ключевые слова: *информационная безопасность Украины, кроссмедийность, интернет-реалии Украины.*

We consider the coverage of the period «Maydan 2013–2014«in the Internet space of Ukraine in several well-known Internet portals. We are interested in the use of cross media technologies and capacities of modern communications infrastructure in Ukraine in terms of information security. We consider the use of certain social and communication technologies that will be useful during the «information war«that is waged in Ukraine.

Key words: *information security of Ukraine, cross media technologies, Internet realities of Ukraine.*

У роботі аналізується висвітлення подій періоду «Майдан 2013–2014» в інтернет-просторі України на прикладі кількох відомих інтернет-порталів.

Нас цікавить застосування кросмедійних технологій з урахуванням можливостей сучасної комунікаційної інфраструктури в Україні з погляду інформаційної безпеки.

Розглянемо використання певних соціально-комунікаційних технологій, які будуть корисними під час «інформаційної війни«, що зараз точиться в Україні.

2014 рік в Україні був позначений не тільки трагічними подіями на сході й на півдні країни: загибель громадян, територіальні втрати, особливо Кримського півострову, так звана «антитерористична операція» — АТО, падіння економіки тощо. Зараз в нашій Батьківщині, крім військових дій (АТО), набирає обертів «інформаційна війна» з північним сусідом. Не слід забувати й про те, що сучасна Україна ще знаходиться на етапі переходу від суспільства індустріального до суспільства інформаційного.

Отже, слід особливо дбати про забезпечення як нашої інформаційної безпеки, так і про власне перемогу в інформаційній війні. На нашу думку, між цими речами існує певний зв'язок.

Не будемо розглядати величезний комплекс заходів, спрямованих на вдосконалення інформаційної безпеки, який має забезпечувати держава, — від відповідного законодавчого забезпечення аж до впровадження потрібних апаратних і програмних рішень. Зупинимось лише на «людському чиннику«.

Йдеться про так звану «соціальну інженерію«. Нагадаємо, що соціальна інженерія — метод несанкціонованого доступу до інформаційних ресурсів користувача, який використовує особливості людської психології. «Человеческая природа такова, что людям гораздо проще идти по пути наименьшего сопротивления — легче обойти кирпичный забор, нежели его сломать. Киберпреступники не являются исключением. Мошенники в сети, как правило, пытаются получить доступ к конфиденциальной информации путем обмана пользователя, а не взлома всей системы. Они используют склонность человека доверять, чтобы взломать его и получить доступ к информации. Мошенникам намного легче склонить кого-то выдать свой пароль, чем взломать его (если пароль хорошо защищен)» [2].

Ключові слова тут «найменший спротив» та «схильність людини довіряти«. Саме живі люди, а не технології є найслабшою ланкою в системі, що реалізує інформаційну безпеку. Для отримання потрібної інформації використовуються різноманітні маніпулятивні шахрайські схеми, що не обмежуються лише прийомами, пов'язаними з інформаційними технологіями або комп'ютерами. Вони сягають від виманювання, наприклад, паролю під час телефонного дзвінка й до застосування найвишуканіших технік нейролінгвістичного програмування (НЛП).

Спочатку НЛП було створено виключно з медичною метою. Зараз воно вважається «мутованою«формою гіпнозу, яка використовується соцінженерами як інструмент маніпуляції жертвами і тиску на них з метою змусити виконати певні дії: повідомити свій пароль, розголосити конфіденційну інформацію, відмовитися від будь-якого заходу безпеки й таким чином прибрати перешкоди на шляху зловмисників [4].

Як зазначає С. Ложкін, старший антивірусний фахівець Kaspersky Lab, «соціальна інженерія — це дешево й ефективно. Саме через це існують нігерійські шахраї, листи від яких регулярно потрапляють до наших поштових скриньок. Людський чинник — найскладніший для змін» [2].

Інтернет-загрози достатньо різноманітні й можуть підстерігати користувача практично скрізь — при читанні пошти, спілкуванні в соціальних мережах, ознайомленні з новинами і просто онлайн-серфінгу.

Сьогодні застосування комплексного рішення для убезпечення всіх пристроїв — це необхідність. Крім цього, користувачеві потрібно завжди уважно ставитися до того, що він робить в Інтернеті: які сайти відвідує, які файли завантажує і що запускає на своєму персональному комп'ютері чи на іншому пристрої. Не треба довіряти повідомленням від незнайомих осіб чи установ, не треба переходити за надісланими посиланнями й відкривати надіслані файли.

Дуже важливо завжди знати, які нові загрози чатують на нас у мережі, враховуючи і загрози, пов'язані із соціальною інженерією, — це допоможе уникнути атак як онлайн, так і в реальному житті. Слід пам'ятати, що ніякі технології не зможуть нас захистити, якщо ми не знаємо, як їх коректно застосовувати й не усвідомлюємо, на що здатні зловмисники.

Отже, «людский чинник» можливо нейтралізувати значною мірою шляхом постійного відповідного інформування, ненав'язливого виховання користувачів. З таким завданням цілком можуть упоратися сучасні журналісти, які спроможні висвітлювати таку тематику. А якщо вони будуть застосовувати кросмедійні технології, то зможуть вагомо підвищити ефективність своїх матеріалів. Адже під час рекламних кампаній успішно використовується так зване «cross-media advertising» [6, 20].

Кросмедійні технології полегшують працю журналіста, підвищують його «коефіцієнт корисної дії«. Це вельми важливо в сучасних умовах — умовах «інформаційної війни«.

Так, згідно з одним із останніх всеросійських опитувань, проведених протягом 14–17 листопада 2014 року соціологами «Левада-центру», були отримані наступні результати.

По-перше, дві третини росіян переконані, що цілісність сусідньої держави, тобто України, не є чимось важливим, значущим, чимось таким, що варто брати до уваги. Лише 12 % відсотків вважають інакше.

По-друге, майже кожен четвертий з-поміж опитаних (23 %) вже готовий підтримати відкриту війну із сусідньою державою, тобто Україною, яку нещодавно вважали братньою [5].

Ігор Яковенко підкреслює: «...щоб довести свідомість росіян до такого химерного стану, знадобилися досить специфічні засоби. Дев'ять місяців поспіль, 24 години на добу, всі сім днів на тиждень, мізки громадян Росії безперервно промивалися концентрованим розчином ненависті та брехні» [5].

Цей «концентрований розчин«готувався на вигадках російських мас-медіа щодо звірств, які начебто чинилися нашими військовими та патріотами на сході України. Не будемо їх перераховувати — вони добре відомі користувачам Інтернету, соціальних мереж. Спробуємо висвітити методологію, за якою цей розчин готувався, продовжує готуватися.

У цьому допоможе Віталій Каценельсон, який ввечері 17 листопада 2014 року опублікував у своєму блозі цікаву статтю «Світ Путіна: Чому погіршиться відвертий обмін думками Росії із Заходом» [9].

Він вирішив на своєму прикладі з'ясувати, як впливає на пересічного мешканця США російська пропаганда. Протягом тижня Віталій знайомився з новинною інформацією виключно з російського теле-

бачення — Першого каналу Росії та газети «Правда«. Результат перевершив усі сподівання: «...я завжди вважав Інтернет непереборною демократичною силою, яка завжди допоможе правді прослизнути скрізь тріщинки навіть у найміцнішому мурі пропаганди. Я помилявся. Після перегляду російського телебачення ви вже не бажаєте читати західну пресу через те, що ви переконані, що вона бреше. І що більш важливо, російське телебачення настільки потужне, що ви навіть не бажаєте дивитись щось інше тому, що ви переконані, що отримали незаперечувані факти», — стверджує Каценельсон.

Механізм такого «дива» спирається на особливості функціонування людського мозку: «...пропаганда Росії працює, змушуючи вашу праву півкулю мозку (емоційне) переважати над лівою (логічне), одночасно засмічуючи ваші логічні фільтри... Факти — це не те, чим переймається російське телебачення. Як тільки емоційні образи та багато дезінформації наповнять праву півкулю мозку, вона перемагає ліву, яка капітулює та припиняє ставити під сумнів подану інформацію» [9].

При цьому російські медійники старанно слідують добре відомому маркетологам і фахівцям з реклами та PR правилу: «...для того, щоб споживач запам'ятав, засвоїв вашу комунікацію, він має чути її щонайменше шість разів на день».

Що можна протиставити такій інформаційній агресії? Тільки правду! Не можна подолати брехню брехнею. Потрібно також розуміти, що журналіст має постійно дбати про якість своєї роботи. Адже навіть так звані технічні огріхи в комунікаті значною мірою знижують його вплив на реципієнта і можуть привести до протилежного результату [4, 18–20].

Шкода, але українські онлайнові видання хибують на різноманітні помилки: від орфографічних, стилістичних тощо аж до порушень журналістської етики. Окремо слід згадати «відхилення» від загально вживаних правил «складання та верстки«Інтернет-видань. Здається, що такі незначні, майже суто технічні помилки, як проблеми автора з орфографією чи з верстkою, не мають великого значення. Проте слід зважати на те, що в умовах інформаційної війни в читача-опонента і, можливо, не тільки опонента починає переважати ставлення до публікації на кшталт «в чужом глазу соринку замечает, а в своём бревна не чувствует».

Протягом десяти місяців, починаючи з березня 2014 року, ми намагалися зайнятися «моніторингом» матеріалів онлайнових видань України. У першу чергу нас цікавили матеріали, у яких йшлося про події типу «Майдан 2013–2014» та пов'язані з ними. Як «точку входу» зазвичай використовували портал «Ukr.Net» [http://www.ukr.net/]. Нам вдалось переглянути 864 публікації, які відповідали нашій меті. Більше не вдалося — від розкладу занять та інших адміністративних завдань не втечеш... Більше третини матеріалів (39,8 %) викликали зауваження. Розподіл виявлених, на наш погляд, недоречностей виглядає так:

орфографічні помилки — 68,4 %

складання та верстка — 20,3 %

інші недоліки — 11,3 %.

Цікаво, що більшість орфографічних помилок (89 %) можна віднести до так званих «помилок друку». Тобто до помилок, на усунення яких авторові просто не вистачило часу (принцип «презумпції невинуватості» у дії). Хоча в епоху царювання інформаційних технологій у журналістиці це робиться майже миттю — при потребі виділяємо усе повідомлення та імпортуємо його до, наприклад, текстового процесора, використовуємо функцію перевірки граматики, виправляємо помилки та виконуємо процес зворотнього імпортування, якщо це потрібно.

До речі, серед помилок, які ми віднесли до класу «інші недоліки», більшість (81 %) теж могли бути усунені, якби автор уважно стежив за тим, що він робить. Наприклад, наводячи результати соціологічного опитування автор публікації двічі написав «определённо да», хоч другий раз мало бути «определённо нет» [5].

Аналогічні ляпи виникають і тоді, коли дописувачі використовують, наприклад, різноманітні інтернет-перекладачі і не дають собі ради відредагувати переклад під гаслами «Немає часу» або «Якнайшвидше опублікувати у Мережі».

Отже, використання кросмедійних технологій допоможе журналісту вивільнити час для більш ретельного редагування своїх дописів та уникнути не тільки більшості помилок, зокрема помилок «складання та верстки», але й «професійної деформації».

Нагадаємо, що ефективне застосування кросмедійних технологій спирається на достатньо розвинену інтернет-інфраструктуру. Розглянемо, як з цим складається в Україні. Будемо спиратися на офіційні

документи «Міжнародного Союзу Електрозв'язку» (ITU). Аналіз офіційних звітів ITU за 2013 та 2014 роки засвідчує, що, на жаль, Україна продовжувала «пасти задніх». Звісно, зростала кількість користувачів у мережі та кількість підключень, збільшувалась швидкість передачі даних в українському сегменті Інтернету. Успішно розвивається послуга широкосмугового доступу до Інтернету, продовжує зростати покриття бездротовим Інтернетом — як за стандартом «майже 3G» так і «Wi-Fi». Але обіцяного справжнього прориву не відбулося...

Причини цього слід шукати у вищих ешелонах влади. Ще й досі остаточно не врегульовано умови, на яких будуть розподілятися «справжні 3G» ліцензії. А на черзі денній вже «4G» і наступні стандарти. Досить непевною видається ситуація з IT-сектором України — на початку другої половини грудня з інтервалом у два дні з'явилися дві інтернет-публікації діаметрально протилежного спрямування [8; 9].

Особливе занепокоєння викликає перехід «Укртелекому» — основного оператора зв'язку країни з державної власності у приватну. Це підприємство — не тільки основа національного Інтернет-сегменту, це ще й наріжний камінь інформаційної безпеки держави.

Однак останні заходи керівництва країни дозволяють сподіватися на краще. Створене «Міністерство інформації» — установа, яка відразу викликала гострі суперечки в суспільстві. Проте в умовах інформаційної війни такий координуючий заклад видається далеко не зайвим. Розпочинається «мовлення» за межі України. Тут «мовлення» розуміється в широкому сенсі — не тільки ефірне радіо та телемовлення, враховуючи супутникове, але й Інтернет-комунікації. Особливо приємною новиною є поновлення роботи вітчизняних радіостанцій у діапазоні середніх хвиль.

Отже, комунікаційна інфраструктура держави продовжує розвиватися. Залишається відкритим питання підготовки кваліфікованих кадрів, спроможних забезпечити якісну журналістику.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. *Гавриш О.* Локомотив экономики: IT-сектор растет как на дрожжах, несмотря на кризис и войну [Електронний ресурс] / Новое время / О. Гавриш. — Режим доступа: http://nvua.net/publications/lokomotiv-ekonomiki-it-sektor-rastet-kak-na-drozhzhah-nesmotrya-na-krizis-i-voynu--25376.html

2. *Иванова А.* Социальная инженерия: Как не попасться на удочку киберпреступнику [Електронний ресурс] / А. Иванова // Украинский бизнес ресурс. — Режим доступа: http://ubr.ua/business-practice/own-business/socialnaia-injeneriia-kak-ne-popastsia-na-udochku-kiberprestupnika-319414
3. *Поздняков В.* Рядом с Нигерией и Пакистаном. Аналитики оценили упадок украинских IT [Електронний ресурс] / В. Поздняков // Николаевская областная интернет-газета Новости N. — Режим доступу: http://novosti-n.org/ukraine/read/78523.html
4. *Шейко В. М., Кушнаренко Н. М.* Організація та методика науково-дослідницької діяльності : підручник / В. М. Шейко, Н. М. Кушнаренко. — 3-тє вид., стер. — К.: Знання-Прес, 2003. — 295 с.
5. *Яковенко И.* Соловьев, Мамонтов, Зейналова, Симоньян — это не журналисты [Електронний ресурс] / И. Яковенко // Новый Регион. — Режим доступа:http://nr2.com.ua/column/Igor_Jakovenko/Solovev-Mamontov-Zeynalova-Simonyan-eto-ne-zhurnalisty-85639.html
6. ICT & the future of Media: Industry Transformation — Horizon scan. Networked Society Lab. Telefonaktiebolaget LM Ericsson. — 2014. — P. 33.
7. Measuring the Information Society: The ICT Development Index. International Telecommunication Union. — 2013. — P. 254.
8. Measuring the Information Society: The ICT Development Index. International Telecommunication Union. — 2014. — P. 270.
9. *Katsenelson V.* Putin's World: Why Russia's Showdown with the West Will Worsen [Електронний ресурс] / V. Katsenelson // Institutional Investor. — Режим доступа: http://www.institutionalinvestor.com/blogarticle/ 3400888/putins-world-why-russias-showdown-with-the-west-will-worsen/banking-and-capital-markets-emerging-markets.html

Одержана 23.06.2015