

§ 3. Технології маніпулювання і методики пошуку, відбору, верифікації даних у журналістиці

Найважливішими передумовами сучасних інформаційних воєн і надійним підґрунтям для їх проведення є, безперечно, посилення ролі інформації, розвиток технологій її поширення, відкритий характер комунікації, глобалізаційні процеси у світі.

Ми живемо в інформаційному суспільстві і щодня маємо справу з великим потоком інформації: шукаємо й отримуємо нові знання про навколишній світ, спілкуємося за допомогою сучасних засобів комунікації, читаємо новинні стрічки, які розповідають нам про актуальні події. Отримана інформація впливає на наше сприйняття навколишньої дійсності, змінює моделі нашої поведінки та спосіб життя. Кількість інформаційних каналів постійно збільшується за рахунок науково-технічного прогресу.

До традиційних засобів поширення інформації (друковані видання, радіо і телебачення) не так давно приєднався Інтернет, який доповнив їх блогами і соціальними мережами, забезпечуючи оперативність реакції на події та інтерактивність взаємодії.

Цілком закономірно, що Інтернет поступово стає лідером і посідає провідне місце серед популярних джерел інформації, адже пошук даних у мережі простий, зручний і займає набагато менше часу, ніж похід до бібліотеки, читання архівів газет або навіть перегляд телевізора. У зв'язку з постійним розвитком інформаційних комп'ютерних технологій, у суспільстві сформувалася позитивна громадська думка про корисність Інтернету, а стрімке розширення його технічних можливостей і аудиторії зумовило появу безлічі інформаційних сервісів і ресурсів. Пошук інформації через Інтернет став прерогативою не тільки звичайних користувачів, але й державних службовців, бізнесменів і комерційних організацій. Адже своєчасне отримання інформації здатне приносити чималий прибуток і відчутну користь. Комунікація з клієнтами і споживачами, доступна

реклама для потенційної цільової аудиторії – все це відкрило чимало можливостей як для споживачів, так і для розповсюджувачів інформації.

Як і кожен «організм», що швидко розвивається, Інтернет не зміг уникнути так званих проблем зростання, пов'язаних із неконтрольованою лавиною інформації і перегонами в спробах організації й управління інтернет-спільнотою. Про основні загрози для розвитку всемережжя заявив сер Тім Бернес-Лі у своєму відкритому листі, оприлюдненому 12 березня 2017 року, напередодні 28-річчя W3C. Глава World Wide Web Consortium і творець Інтернету вважає, що загрозовими є три чинники.

Перший. «Ми втратили контроль над нашими особистими даними. Дуже широкого поширення набула бізнес-модель, яка пропонує безкоштовний контент в обмін на персональні дані. Більшість інтернет-користувачів погоджується на такі умови. Але ми втрачаємо переваги, якими могли б скористатися, якби самі володіли власними даними. Тоді люди самі могли б вирішувати, коли, з ким і якою інформацією ділитися. Окрім цього, уряди співпрацюють або ж змушують компанії ділитися персональними даними. Це нерідко призводить до зловживань, втручання в особисте життя. А у випадку з репресивними режимами – до арештів і вбивств. Постійне стеження за всіма в Інтернеті – це вже занадто.

Другий. Дезінформація дуже легко поширюється в Інтернеті. Більшість людей для пошуку інформації використовує лише кілька соціальних мереж і новинних сайтів. Ці ресурси на основі алгоритмів, які вивчають наші особисті дані, відбирають, що саме нам показувати. Як наслідок – сайти показують нам те, на що ми швидше за все «клікнемо». Отже, різні фейкові новини або відверта дезінформація може поширюватися як лісова пожежа. І такі можливості зловмисники можуть використовувати в своїх фінансових або політичних цілях.

Третій. Політичній рекламі потрібні прозорість і зрозумілість. Той факт, що більшість користувачів отримують новини тільки від декількох платформ, а зростаюча складність алгоритмів спирається на масиви особистих даних, означає, що політична реклама стає все

більш індивідуальною. За деякими даними, під час виборів 2016 року в США в Facebook щодня демонструвалося 50 тис. варіацій політичної реклами. Є підозра, що подібні інструменти використовувалися недобросовісно, для того, щоб маніпулювати виборцями» [14].

Це не вичерпний перелік ризиків, з якими стикаються користувачі Інтернету. Серед усіх фахівці виділяють найбільш явні і групують їх за природою і механізмами впливу. Так, у рекомендаціях Фонду Розвитку Інтернету щодо користування глобальною мережею, що укладені за результатами досліджень 2010-2011 років за методологією міжнародного дослідницького проекту Єврокомісії «EU Kids Online II», зазначено п'ять основних груп ризиків:

- 1) *тематичні*. Вони зумовлені різними матеріалами (текстами, зображеннями, аудіо- і відеофайлами, посиланнями на сторонні ресурси), що містять протизаконну, неетичну і шкідливу інформацію;
 - 2) *комунікаційні*. Пов'язані зі спілкуванням і міжособистісними взаєминами інтернет-користувачів. Прикладами таких ризиків можуть бути кібербулінг, незаконні контакти (наприклад, грумінг), знайомства в мережі і зустрічі з інтернет-знайомими та ін.;
 - 3) *електронні*. Йдеться про втрати персональної інформації або атаки шкідливих програм. Шкідливі програми – різне програмне забезпечення (віруси, черв'яки, «троянські коні», шпигунські програми, боти тощо), яке може завдати шкоди комп'ютеру та порушити конфіденційність зберігання інформації в ньому;
 - 4) *споживчі*. Є результатом зловживання в Інтернеті правами споживача. Вони містять: ризик придбання товару низької якості, підробок, контрафактної та фальсифікованої продукції, втрату грошових коштів без придбання товару або послуги, розкрадання персональної інформації з метою кібершахрайства та ін.;
 - 5) *інтернет-залежність*, тобто нав'язливе бажання увійти в Інтернет, перебуваючи офлайн, і нездатність вийти з Інтернету, коли особа перебуває онлайн. За своїми проявами вона схожа на
-

вже відомі форми адиктивної поведінки (наприклад, унаслідок вживання алкоголю або наркотиків), але належить до типу нехімічних залежностей, тобто не призводить безпосередньо до руйнування організму [3].

Усі вказані ризики і методи впливу на споживачів інформації становлять загрозу для інформаційної безпеки суспільства.

Загроза інформаційній безпеці (англ. information security treat) – сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам особистості, суспільства і держави в інформаційній сфері. Основні загрози інформаційній безпеці можна розділити на три групи:

- 1) загрози впливу неякісної інформації (недостовірної, фальшивої, дезінформації) на особистість, суспільство, державу;
- 2) загрози несанкціонованого і неправомірного впливу сторонніх осіб на інформацію й інформаційні ресурси (на виробництво інформації, інформаційні ресурси, на системи їхнього формування і використання);
- 3) загрози інформаційним правам і свободам особистості (праву на виробництво, розповсюдження, пошук, одержання, передавання і використання інформації; праву на інтелектуальну власність на інформацію і речову власність на документовану інформацію; праву на особисту таємницю; праву на захист честі й гідності тощо).

Це спонукає до втручання в інформаційний простір органів державної влади для захисту інформаційної безпеки, що в свою чергу теж становить загрозу обмеження й утиску прав і свобод особистості: інформація є важливою і невід'ємною складовою успішної життєдіяльності людини і суспільства загалом за умови обачливого використання і захисту особистих даних, а їх втрата становить небезпеку; недостовірні й навмисне перекручені інформації має маніпулятивний характер і становить основну загрозу для людини і суспільства, змушуючи вживати певні дії щодо обмеження певних свобод.

Маніпуляції інформацією як інструмент управління масами і формування поведінкової моделі особистості. Автор цитати «Хто

володіє інформацією, той володіє світом» навряд чи свого часу усвідомлював уповні, наскільки він має рацію, наскільки світ керований інформацією, наскільки легко підкорювати цілі народи за допомогою інформації.

Управління поведінкою людини може бути структурним, як в армії, коли керівник віддає накази і керує підлеглими. У такій структурі інформаційні процеси протікають по вертикалі й вирішуються завдання, поставлені зверху.

Однак управління може бути й безструктурним. У цьому випадку навколо об'єкта впливу формується таке інформаційне оточення, яка буде стимулювати його діяти так, як потрібно замовнику. Найпростішим прикладом такого управління є реклама. У ній немає безпосередніх вказівок купувати певні речі, вона діє по-іншому: створює привабливий образ товару й намагається сформувати в споживача реклами нову потребу, відповіддю на яку і буде придбання товару. Прямого наказу і організаційної структури в рекламі немає, а людина здійснює купівлю нав'язаного їй товару.

Проте рекламувати чи безструктурним методом просувати в суспільство можна не тільки предмети, а й моделі поведінки, погляди на життя, життєві орієнтири, ідеї, цінності. Цілеспрямоване і системне просування певних ідей безструктурним способом – це явище, що відоме загалу як «пропаганда», якою займаються всі без винятку засоби масової інформації.

Пропаганда (лат. *propaganda*, дослівно – «яка підлягає поширенню (віра)»), від лат. *propago* – «поширюю») – це форма комунікації, спрямована на поширення в суспільстві світогляду, теорії, твердження, фактів, аргументів, чуток та інших відомостей для впливу на суспільну думку на користь певної спільної справи чи громадської позиції. Пропаганда може класифікуватися відповідно до джерела та природи повідомлення, мати певне забарвлення та спрямування залежно від джерел інформації та мети.

В умовах інформаційних воєн найбільш важливими аспектами пропаганди є питання створення недостовірної інформації та управління нею. Щоб протидіяти негативній пропаганді і маніпулюванню, потрібно розуміти, як протікають процеси

безструктурного управління в суспільстві, знати методи опрацювання інформації для пошуку і відбору достовірних даних та методи протидії негативним формам інформаційного впливу на суспільство.

Технологія пропаганди. Під час Міжнародного симпозіуму «Революція, війна та їх наслідки», що відбувся 16 та 17 березня 2018 року у Варшаві, державний секретар Міністерства інформаційної політики України Артем Біденко нагадав про вже відому пропагандистську «4D»-стратегію Кремля: dismissing, distorting, distracting, dismaying (заперечення, спотворення, дезорієнтація, залякування). Він також озвучив учасникам симпозіуму ще одну формулу російської дезінформаційної кампанії – «4F»-стратегію, яка мітить: fake news, fake media, fake experts, fake events (фейкові новини, медіа, фальшиві експерти і події) [19].

Суть «4D-стратегії» полягає у використанні особливостей психології комунікації в соціальних групах. У первісному вигляді стратегія була викладена співробітником Центрального інституту європейської політики Беном Німмо (Ben Nimmo) у публікації на ресурсі інституту й передрукована багатьма іншими сайтами у перекладах. Так, зокрема, на Stopfake.org, де послідовно і детально були розглянуті елементи цієї стратегії [22].

Відхилення звинувачення – перша ланка стратегії. Такий підхід Росії до негативних звітів або коментарів полягає в тому, щоб спростувати їх або шляхом заперечення тверджень на місцях (у середовищі споживачів інформації), або шляхом обмовляння того, хто їх озвучує (джерела інформації), поставивши під сумнів його авторитет і значущість самої інформації. Як приклад Бен Німмо наводить послідовне заперечення Росією збройної анексії українського півострова Криму з використанням своєї армії з 22 лютого 2014 року: *«Росія не брала участь у конфлікті. Росія підтримувала кримських повстанців. Росія спланувала все»*. Тільки одне з цих тверджень може бути правдою! Те, що Путін зробив всі ці три заяви в сліпучому сяйві перед камерами, показує, до якої міри дійшли російські інформаційні засоби, маніпулюючи обманом [22].

Спотворення інформації полягає в тому, що зміст інформації може змінюватися в процесі її передавання різними каналами від

джерела до споживача. Ступінь спотворення прямо пропорційний числу каналів і ланок передачі, через які проходить повідомлення: чим більше учасників отримує доступ до тієї чи іншої інформації і передає її іншим людям, тим сильніше відрізняється остаточний варіант від початкового. Це найбільш поширене явище в сучасних засобах масової інформації, воно зумовлене цілою низкою причин, що тісно пов'язані між собою, починаючи від зниження якості інформаційного продукту через зменшення фінансування при скороченні термінів підготовки новинного контенту в умовах жорсткої конкуренції виробників і закінчуючи посиленням цензури з боку державних органів.

Серед найважливіших причин спотворення інформації можна виділити такі: 1) проблеми перекладу і полісемія створюють можливість різотлумачення одного й того самого повідомлення; 2) відмінності в рівні освіти, інтелектуальному розвитку, професіоналізмі; 3) неповнота інформації через обмеження доступу до неї або навмисна подача не в повному обсязі, що призводить до домислення і доповнення неперевіреними фактами та припущеннями; 4) недостатній рівень кваліфікації співробітника, що представляє інформацію; 5) емоційне напруження; 6) упередження щодо осіб або явищ, про яких ідеться в повідомленні.

Комплексність причин спотворення інформації можна продемонструвати на прикладі ставлення росіян до загибелі своїх співвітчизників у складі незаконного ПВК «Вагнера» в Сирії. «Заборона розголошення військових втрат у мирний час», тенденційне висвітлення новин про події в Сирії, тотальне насадження через соцмережі та засоби масової інформації ідеї «великої країни в кільці ворогів» призвели в результаті до того, що понад 54% опитаних росіян вважають допустимим спотворення інформації в державних інтересах, понад 71% респондентів схвалили цензуру [13] і не обурюються з приводу відсутності достовірної інформації про численні втрати співвітчизників у конфлікті на території чужої країни.

Дезорієнтація одержувача інформації – відповідь на питання іншим, причому логічно некоретним питанням або ж надання

надмірної кількості інформації, що не стосується справи, істинної або помилкової, з метою відволікти увагу від суті питання, що розглядається. Прикладом цього елемента стратегії може служити інформаційний фонтан версій знищення голландського Boeing МН17 з підтвердженнями сенсаційним фактажем з незнаних джерел, інтерв'ю з випадковими очевидцями та всілякими оцінками й коментарями цивільних і військових експертів [2]. Але при цьому російська делегація в Радбезі ООН блокує будь-які пропозиції щодо організації кримінального суду над особами, причетними до знищення цивільного літака, всіляко затягуючи завершення розслідування судом і покарання винних за злочин [17].

Залякування – залякування супротивника загрозою провалу його планів, поширення тривоги серед прихильників опонента, використання внутрішніх протиріч і опозиції всередині країни – об'єкта агресії.

Протягом останніх років залякування як метод міждержавного шантажу набуло просто-таки масштабів епідемії. Це легко відстежити навіть за медійними заголовками: «Глава Пентагону звинуватив Китай у залякуванні та примусі» (йдеться про розміщення Китаєм систем озброєнь на штучних островах у Південно-Китайському морі), «Китай закликає США припинити економічне залякування», «Навіщо Росія залякує світ бойовими літаками?», «Росія постійно погрожує, залякує та нападає на сусідні держави», «Росія і сепаратисти повинні припинити залякувати Україну», «Росія вбачає у ядерній зброї гарантію безпеки і спосіб залякування сусідів», «Росія залякує Ізраїль через закон щодо України», «США звинуватили РФ у залякуванні спостерігачів ОБСЄ», «Трамп: США та їхніх союзників неможливо залякати» тощо.

«4F»-тактика дезінформації. Дезорієнтація і фальсифікація є різновидами дезінформації, які дають змогу ввести людину в оману. **Дезінформацією** (або дезінформуванням) називається один із способів маніпулювання інформацією. Це введення кого-небудь в оману шляхом надання неповної або непотрібної інформації або спотворення частини інформації чи контексту.

Мета такого впливу завжди одна – опонент повинен учинити так, як це необхідно маніпулятору. Вчинок об'єкта, на якого спрямована дезінформація, може полягати в ухваленні потрібного маніпулятору рішення або у відмові від прийняття рішення, що не вигідне для маніпулятора. Але в будь-якому випадку кінцева мета – це дія, яку буде зроблено.

Відповідно до цього широко використовуються «4F-тактики» дезінформації.

Фейкові новини (фейк, фальшиві новини) – це інформаційна містифікація, навмисне поширення неправди або напівправди в соціальних медіа і традиційних засобах масової інформації з метою введення особи в оману для отримання фінансової або політичної вигоди. Відбувається створення підроблених новин, часто з використанням помітних заголовків, або повністю сфабрикованих історій для збільшення читацької аудиторії й цитованості.

Основна причина використання таких методів у звичайних обставинах – прибуток від замовника матеріалу або ж від накрутки кліків на ресурс з подальшим прибутком від розміщення рекламних матеріалів. Прибуток формується аналогічно до принципів клікбейтінга і є доходом від реклами, який генерується незалежно від достовірності опублікованих матеріалів за рахунок доступу до Ad-revenue (програми обліку переглядів реклами). Можливості анонімного хостингу сайтів, на яких публікуються анонімні автори або автори під псевдонімами, ускладнюють законне переслідування таких джерел за дезінформацію або наклеп.

Під час виборчих перегонів використання фейкових новин набуває зазвичай широкого розмаху й має воістину драматичний супровід політичних дебатів і поствиборчих розслідувань. Як приклад можна навести публікацію з розслідування фейкових новин, що продукувалися 2016 року в м. Велесі (Македонія) перед виборами президента Трампа в США: «У середині 2016 року редактор веб-ресурсу Buzzfeed Крейг Силверман помітив дивний потік придуманих історій, які надходили з маленького східноєвропейського містечка (Велес). Він з колегами почали журналістське розслідування. І незадовго до виборів у США було ідентифіковано щонайменше

140 новинних сайтів, які генерували брехливі новини. Невідомо, чи цікавила молодих людей у Велесі американська політика. Але за рекламу в Facebook вони отримували гроші» [21]. BuzzFeed довів, що фейкові новини в період президентської кампанії в США збирали більше кліків, ніж новини від The New York Times, The Washington Post та CNN.

У межах інформаційної війни фейкові новини використовуються як своєрідна «зброя», за допомогою якої ворогуючі сторони намагаються здобути перевагу. Згадаймо, 17 липня 2014 року на сході Донецької області був збитий Боїнг 777, загинули 298 осіб. Міжнародна слідча група встановила, що літак збили з доставленого з Росії зенітно-ракетного комплексу «Бук». Було ініційовано передання справи до міжнародного трибуналу. 7 грудня 2017 року «канал Міноборони Росії “Звезда” подав інтерв’ю з начебто колишнім офіцером ЗСУ Юрієм Батуріним. Чоловік сказав, що був начальником командного пункту військової частини А-1215 і... українські військові розповіли йому, як до катастрофи вони перевезли “Бук“ у селище Зарощенське, звідки... був здійснений пуск ракети по літаку “Малайзійських авіаліній”... Російські ЗМІ після цього вийшли із заголовками: “Боїнг над Донбасом все-таки збив український Бук”, “Екс-офіцер ЗСУ розповів, хто насправді винен у катастрофі Боїнга під Донецьком” та низкою подібних... У Генеральному штабі Збройних сил України... наголосили, що слова Батуріна не відповідають дійсності... Зарощенське не перебувало під контролем військових України. Російські ЗМІ вже не вперше поширюють дезінформацію про збиття літака рейсу МН17» [11] з метою вкотре виправдатися і уникнути міжнародного трибуналу за військовий злочин.

Загалом, один із ризиків фейкових новин полягає в «розширенні меж того, у що ми віримо». Ця фраза з The Guardian стала популярною в багатьох країнах: очевидно, люди повсюдно усвідомлюють, наскільки небезпечним є стирання «кордонів» між світами вимислу і реальності.

Фейкові медіаресурси – інформаційні ресурси, які створені з метою поширення недостовірної інформації певної тематики. Їхніми

характерними особливостями, як правило, є реєстрація і розміщення хостингу поза межами регіону, на який вони нібито орієнтовані; зазначення нетипових для регіону контактних даних; нетипові мовні вислови і чужорідні поведінкові шаблони у викладі матеріалу; наявність множинних ресурсів, що повністю подібні за оформленням, тематикою і контентом; контент, що не створюється, а копіюється з новинних агрегаторів; низька популярність серед населення регіону.

Прикладом існування таких медіаресурсів може слугувати недавній випадок із виявленням в Україні та США схеми керування із РФ новинних порталів для просування фейкових новин. Ось яким був перебіг розслідування: розробником всіх виявлених фейкових сайтів була вказана компанія з нетиповою для США назвою 1gorod.com. Привертало також увагу, що слово «gogod» – транслітерація. «Повний список сайтів, – зазначається в розслідуванні, – з однаковим шаблоном, принципом роботи і під керівництвом 1gorod.com... такий: Newsnyork.com (New York News), Newsinca.com (California News), Newsinkansas.com (Kansas News), Xerson.net (Новости Херсона), v-kieve.net (Новости Киева), novosti.lugansk.ua (Новости Луганска), novosti.donetsk.ua (Новости Донецка)» [1]. Система геолокації підтвердила, що спрямоване розслідувачами звернення в компанію прочитали власники e-mail в Москві та Єкатеринбурзі. Враховуючи те, що публікації сайтів неоригінальні й неправдиві, місце реєстрації видумане, зроблено висновок: мережа фейкових сайтів придумана з метою поширення неправдивої інформації [1].

Фейкові експерти – вигадані або несправжні авторитетні фахівці з певних галузей людської діяльності, думка яких покликана засвідчити значущість певної інформації, чуток, що не підтверджені вказівкою на офіційне джерело і викликають сумніви. Розвиток інформаційних технологій значно спростив процес фальсифікації офіційних документів, що підтверджують особу, а соціальні мережі, що дають змогу створювати «історії життя і коло спілкування» для загального ознайомлення та поверхневої перевірки, пришвидшили процес «легалізації» фейковий експертів.

Яскравим прикладом існування таких експертів і складності їх виявлення є розслідування діяльності фейкового експерта Пентагону

з питань Росії Девіда Джуберга. У період з 2015–2017 років на його думки і висловлювання на підтримку України і засудження агресії РФ часто посилалися в публікаціях соціальних мереж і навіть у матеріалах засобів масової інформації. Насправді це видуманий американським фінансистом Деном К. Рапопортом і його друзями персонаж, із такою самою вигаданою біографією, підставними фото, підробленими посвідченнями [12].

Фейкові події – це створення і нав'язування громадськості нової інтерпретації подій минулого або часткова підміна послідовності подій. В основі останнього процесу лежить таке поняття, як «конформізм пам'яті». Так називають властивість спогадів про минулі події спотворюватися під впливом чужої думки. Коли людина виявляє, що більшість людей з її оточення описує якийсь випадок, який вона теж пам'ятає, інакше, то вона схильна з ними погодитися. Психолог Аянна Томас з Університету Чарльза Тафтса в Массачусетсі експериментальним шляхом підтвердила вплив думки більшості або стереотипів, що існують в суспільстві, на появу помилкових спогадів у людей [20].

Цьому, зокрема, сприяє діяльність різних тематичних груп в соціальних мережах, де під впливом кола спілкування закладається стереотип ставлення до ключових питань сьогодення методом спотворення спогадів і зміни думки про події минулого. Найбільш показовим прикладом результату такої діяльності в масштабах соціуму може бути дія нарративу про «історичну перевагу» однієї нації над іншою аж до заперечення права на її існування (достатньо тільки поглянути на багатовікову історію взаємин Росії і України крізь призму нинішніх подій).

Алгоритм впливу інформації на соціум. Процес впливу інформації на соціум відбувається за таким алгоритмом:

- 1) Виділення в соціальних мережах й акцентування уваги на тих дописах (постах) або картинках (у випадку Instagram, Facebook тощо), які являють собою конфліктогенну інформацію.
 - 2) Виявлення і конкретизація фокус-групи / цільової аудиторії. Розписування матриці станів і векторів зсуву / трансформації активності груп. Одночасно з цими діями виконується
-
-

конкретизація тематичних пулів інформації, оцінка структури джерел верифікації / достовірності, сегментація модифікаторів за ступенем резонансу для правильної послідовності «розкачки».

- 3) Відпрацьовування шаблонів поведінкових норм. Будується перелік очікуваних результатів, відбирається перелік резонанс-модифікаторів, створюється мережа джерел верифікації, потім визначається мережа вузлів контролю резонансу для фокус-груп.
- 4) Об'єднання інформації в потік з дотриманням черговості подання. Інформація подається в тому руслі, в якому її зручно розкрутити в суспільстві.
- 5) Знаходження або створення приводу (провокації), що викликає яскраве суспільне невдоволення.
- 6) Запуск пулів інформації формує попередні шаблони поведінки. Запуск спускових пулів інформації для трансформації фокус-груп. Проходження інформації по вузлах контролюють і за потреби підключають модифікаторів корекції.
- 7) Далі можливе виведення людей на вулиці через соціальні мережі.
- 8) Запуск модифікаторів якісної трансформації шаблонів. Контроль і корекція вектора формування вогнищ активності.

Керуючи такими потоками відповідно підготовленої інформації, можна керувати певним сегментом суспільства, наприклад, радикально налаштованими групами чи об'єднаннями громадян з протестними настроями, які в стані емоційного збудження легко й некритично сприймають таку інформацію і спрямовують свою енергію в потрібне суб'єкту впливу місце в потрібний час, виконуючи, по суті, військове завдання, але не знаючи, що ними керують і хто це робить.

Як бачимо, інформація в сучасному суспільстві стала важливим економічним, політичним і соціальним ресурсом, а іноді «вибуховим пристроєм» в інформаційних війнах і засоби масової інформації є засобами формування та управління громадською свідомістю. Тому суть діяльності особи в таких умовах не в тому, щоб уникати будь-яких засобів комунікації, а щоб знати про вплив на людину

інформації і вміти виявляти реальні цілі, на досягнення яких працює певний медіаконтент.

Інформація. Види та властивості інформації

Щоб уміти перевіряти інформацію з мережі Інтернет, потрібно розуміти суть природи інформації та застосовуваних інформаційних технологій.

Насамперед спробуємо окреслити сутність поняття «інформація». Загальноприйнятого визначення інформації не існує. Термін використовується переважно на інтуїтивному рівні і має чимало визначень, кожне з яких залежить від сфери функціонування.

Цікаве трактування цього питання здійснене в роботі Л. Данильчук, де інформація досліджується в контексті наявності взаємозалежної пари об'єктів – джерела і споживача інформації. Інформація розглядається як складова інформаційної безпеки особистості – здатності особистості забезпечувати з певною вірогідністю достатні та захищені інформаційні потоки для підтримки своєї життєдіяльності, стійкого функціонування та розвитку; уміння протистояти інформаційним загрозам і небезпекам, негативним інформаційним діям на індивідуальну і суспільну свідомість і психіку [4].

У міжнародних і українських законодавчих актах та стандартах даються такі визначення поняттю інформація:

- 1) будь-які відомості та / або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді (Закон України «Про інформацію»);
- 2) знання про предмети, факти, ідеї і т. д., якими можуть обмінюватися люди в рамках конкретного контексту (ISO / IEC 10746-2: 1996);
- 3) знання щодо фактів, подій, речей, ідей і понять, які в певному контексті мають конкретний зміст (ISO / IEC 2382 до: 2015);
- 4) відомості, що сприймаються людиною (або) спеціальними пристроями як віддзеркалення фактів матеріального або духовного світу в процесі комунікації [9].

Серед інших визначень інформації, зокрема, такі:

- 1) інформація – це сукупність відомостей (даних), які сприймають із навколишнього середовища (вхідна інформація), видають у навколишнє середовище (вихідна інформація) або зберігають всередині певної системи [8];
- 2) інформація – це відомості про осіб, предмети, факти, події та процеси, незалежно від форми їх представлення [10];
- 3) «інформація являє собою сукупність відомостей про всілякі об'єкти, явища, процеси <...>, інформація є вибір одного варіанта (або декількох) із багатьох можливих і рівноправних» [6].

Отже, інформація – це продукт взаємодії даних та методів, який розглядається в контексті цієї взаємодії.

Інформація існує у вигляді документів, креслень, рисунків, текстів, звукових чи світлових сигналів, електричних та нервових імпульсів тощо. Саме слово «інформатика» походить від латинського *information*, що означає виклад, роз'яснення факту, події.

Найбільш важливими *властивостями інформації* є: достовірність; актуальність; оперативність; ідентичність; об'єктивність; повнота; адекватність; доступність; точність; цінність.

За призначенням інформацію поділяють на:

- 1) *масову*, що містить загальновідомі відомості і оперує набором понять, зрозумілим більшій частині соціуму;
- 2) *спеціальну*, що містить специфічний набір понять. Під час її використання відбувається передача відомостей, які можуть бути незрозумілі основній масі соціуму, але необхідні й зрозумілі в межах вузької соціальної групи, де використовується ця інформація;
- 3) *секретну*, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці країни [16], призначена вузькому колу осіб;

4) *особисту*, яка містить набір відомостей про особистість, що визначає її соціальний стан і типи соціальних взаємодій всередині певної спільноти.

Основні види інформації розрізняють за формами її представлення, кодування та збереження. Це графічна, звукова, текстова, числова, відеоінформація.

Дані є складовою частиною інформації і являють собою формально зареєстровані відомості. Під час інформаційних процесів дані перетворюються з одного виду в інший за допомогою певних методів. Опрацювання даних містить множину різних операцій. Основними операціями є:

- 1) збір даних – накопичення інформації з метою забезпечення достатньої її повноти для прийняття рішення;
- 2) формалізація даних – приведення даних, що надходять із різних джерел до однакової форми;
- 3) фільтрація даних – усунення зайвих даних, які не потрібні для прийняття рішень;
- 4) сортування даних – впорядкування даних за певною ознакою з метою зручності використання;
- 5) архівація даних – збереження даних у зручній та доступній формі;
- 6) захист даних – комплекс дій, що скеровані на запобігання втрат, відтворення та модифікації даних;
- 7) транспортування даних – прийом та передавання (поширення, розповсюдження) даних між віддаленими користувачами, учасниками інформаційного процесу. В інформатиці джерело даних прийнято називати сервером, а споживача – клієнтом;
- 8) перетворення даних – переведення даних з однієї форми або структури в іншу або зміна типу носія.

Поширення інформації може відбуватися у двох формах – **фактичного твердження** чи **оцінного судження**. Оцінними судженнями (за винятком наклепу) є висловлювання, які не містять фактичних даних, наприклад критика, оцінка дій, а також висловлювання, що не можуть бути витлумачені як такі, що містять

фактичні дані, зокрема з огляду на характер використання мовностилістичних засобів.

Комп'ютерне опрацювання інформації є лише одним із багатьох методів і виконується в чисельному вигляді. Уся символна, звукова, графічна, відеоінформація перетворюється в числа і є невід'ємною складовою будь-якої інформаційної системи.

Інформаційна система – взаємозв'язана сукупність персоналу, даних, обладнання, засобів пошуку, зберігання, опрацювання та видачі інформації, використовувана для забезпечення інформаційних потреб користувачів. Основний технічний засіб опрацювання інформації – комп'ютер, оснащений спеціалізованими програмними засобами.

Інформаційні технології, ІТ – сукупність методів, виробничих процесів і програмно-технічних засобів, інтегрованих з метою збирання, опрацювання, зберігання, розповсюдження, надання і використання інформації в інтересах її користувачів. Використовується також загальніший, вищий за ієрархією, термін – інформаційно-комунікаційні технології (Information and Communication Technologies, ICT)

Це технології, що забезпечують та підтримують інформаційні процеси, тобто процеси пошуку, збирання, передавання, збереження, накопичення, тиражування інформації та процедури доступу до неї.

Види сучасних інформаційних технологій: інформаційна технологія опрацювання даних; інформаційна технологія керування; інформаційна технологія підтримки прийняття рішень; інформаційна технологія експертних систем.

Термін «інформаційні технології» в його сучасному витлумаченні вперше з'явився в статті 1958 року, опублікованій у журналі «Harvard Business Review». Її автори – Гарольд Дж. Лівітт і Томас Л. Віслер – зазначили, що «у новій технології ще немає єдиної усталеної назви. Ми будемо називати це інформаційними технологіями (ІТ)». Їхнє визначення складається з трьох категорій: методів опрацювання, застосування статистичних і математичних методів для прийняття рішень та моделювання мислення вищого порядку за допомогою комп'ютерних програм.

Основні риси сучасних ІТ: структурованість стандартів цифрового обміну даними алгоритмів; широке використання комп'ютерного збереження і надання інформації в необхідному вигляді; передача інформації за допомогою цифрових технологій на практично безмежні відстані.

Основними засобами ІТ є: технічні засоби; комунікаційні засоби; організаційно-методичне забезпечення; стандартизація.

Однією з найважливіших функцій інформаційних технологій є поширення та пошук інформації. При цьому поширення інформації означає використання програмно-технічних засобів передачі даних і необхідних для цього інформаційних технологій [15].

До програмно-технічних засобів передачі даних належать засоби зв'язку (телекомунікації) і програмно-технічні комп'ютерні пристрої, системи та комплекси. Засоби зв'язку – обладнання приймання / передавання, пристрої та середовище поширення даних. Пристрої поширення даних забезпечують їхнє передавання дротовими й бездротовими лініями та каналами зв'язку. Середовище поширення – це певна сукупність пристроїв передавання даних і телекомунікацій, що дають змогу користувачам використовувати її для взаємообміну інформацією. Таким середовищем є Інтернет, що являє собою єдиний інформаційний простір і засіб комунікації.

Інтернет – це величезна (глобальна) міжнародна транспортна інформаційна магістраль, що дає змогу здійснювати обмін різноманітними даними практично з будь-якої точки планети. Інтернет водночас є й величезним сховищем розподіленої інформації різних форматів і видів. Він об'єднує безліч централізованих інформаційних систем і окремих серверів, що взаємодіють між собою завдяки використанню єдиних принципів і правил. До таких правил, або стандартів, відносяться мережеві протоколи взаємодії, а також правила адресації в Інтернеті. Користувачі Інтернету, сервери, сайти, інформаційні системи, портали тощо, що містяться в мережі, мають унікальні адреси, що називаються URL-адресами (Uniform Resource Locator – універсальний механізм вказівки місцезнаходження ресурсів або об'єктів мережі; уніфікований покажчик ресурсів).

URL-адреса складається з трьох частин і описує транспортний протокол, який використовується під час пересилання даних (http, ftp), доменне ім'я сервера в мережі Інтернету і визначає шлях до конкретного (шуканого) файлу.

Крім такої адресації, існують і цифрові IP-адреси (raw IP address), що формуються на основі системи доменних імен (Domain Name System, DNS) для перетворення умовних адрес в абсолютне значення унікального номеру. Вони складаються з чотирьох груп 3-розрядних чисел, відокремлених один від одного крапками.

Технології пошуку інформації. Інформаційний пошук – це виконання певних логічних і технічних операцій, необхідних для знаходження інформаційних матеріалів (документів, відомостей про них, фактів, даних і знань), які найбільш повно відповідають запиту (релевантність) та інформаційним потребам (пертинентність) користувача.

Надійний і водночас найшвидший вид пошуку інформації в Інтернеті – *пошук за адресами URL*. Багато з них наводяться в друкованих виданнях, спеціальних довідниках, звучать в ефірі популярних радіостанцій і з екранів телевізора.

В Інтернеті зосереджена величезна кількість документів. Щоб полегшити пошук потрібної інформації, створюються спеціальні пошукові машини.

Пошукові машини – це автоматичні системи, опитувальні сервери, підключені до глобальної мережі, що зберігають у своїй базі інформацію про наявні на серверах дані. За сформульованим певним чином запитом пошукові машини надають інформацію про те, де можна отримати необхідні дані. Як правило, пошукові машини складаються з трьох частин: робота, індексу і програми опрацювання запиту.

Робот (Spider, Robot або Bot) – це програма, яка відвідує веб-сторінки і зчитує (повністю або частково) їхній вміст. Роботи пошукових систем розрізняються індивідуальною схемою аналізу вмісту веб-сторінки.

Індекс пошукової системи – це сховище пошукових образів, відвіданих роботами сторінок. Пошуковий образ документа (зокрема і

веб-сторінки) – це опис змісту документа спеціальною інформаційно-пошуковою мовою. Цей опис містить коди виняткових слів документа, що відображають його зміст та суть. Індeksi в кожній пошуковій системі розрізняються за обсягом і способом організації інформації, що зберігається. Бази даних провідних пошукових машин зберігають відомості про десятки мільйонів документів, а обсяги їхнього індексу становлять сотні гігабайт. Індeksi періодично оновлюються і доповнюються, тому результати роботи однієї пошукової машини за одним і тим самим запитом можуть відрізнятись, якщо пошук проводився в різний час.

Програма опрацювання запиту – це програма, яка відповідно до запиту користувача «переглядає» індекс на предмет наявності потрібної інформації і повертає посилання на знайдені документи. Безліч посилань на виході системи розподіляється програмою в порядку зменшення релевантності, тобто починаючи від посилань, що найбільшою мірою відповідають запиту, і завершуючи тими, що мають найменшу релевантність.

Пошукові машини розрізняються за охопленням інформаційних ресурсів: 1) пошукові машини загальної тематики, що мають базу даних з усіх галузей знань і характеризуються великим індексом і обсягом накопичуваної інформації; 2) пошукові машини спеціального призначення, що переглядають тільки сайти певної тематики, наприклад музичні або музейні.

Основними характеристиками пошукових машин є: обсяг документів в індексі; частота оновлення інформації; інформаційний простір, який охоплює роботу пошукової машини, і різноманітність типів документів, про які збирається інформація; швидкість опрацювання запиту; критерій визначення релевантності (відповідності знайденого документа пошуковому запиту); можливість деталізації та уточнення запиту.

Пошук за рубрикаторм пошукової системи. Пошукові каталоги є систематизованою колекцією (добіркою) посилань на інші ресурси Інтернету. Посилання організовані як тематичний рубрикаторм, що являє собою ієрархічну структуру, переміщуючись якою, можна знайти потрібну інформацію.

Пошук за ключовими словами. Більшість пошукових машин мають можливість пошуку за ключовими словами. Це один із найпоширеніших видів пошуку. Для такого пошуку необхідно ввести в спеціальному вікні слово або кілька слів, які потрібно шукати, і пошукова система знайде у своїй базі та покаже документи, що містять ці слова. Таких документів може виявитися безліч, тож можна виконати пошук у вибірці або уточнити запит за допомогою додаткових умов.

Наведемо десять простих правил формулювання запиту в пошуковій системі:

- 1) ключові слова в запиті потрібно писати малими літерами; це забезпечить пошук всіх ключових слів, а не тільки тих, що починаються з великої літери;
- 2) під час пошуку враховуються всі форми слова за правилами мови пошуку, незалежно від форми слова в запиті (наприклад, певної часової форми чи форми множини);
- 3) для пошуку стійкого словосполучення потрібно взяти слова в лапки (наприклад, «особисті дані»);
- 4) для пошуку точної словоформи перед словом потрібно поставити знак оклику (наприклад, «! особисті дані»);
- 5) для пошуку всередині одного речення слова в запиті поділяють пропуском або знаком &: «особисті дані» або «особисті&дані»; кілька набраних у запиті слів, розділених проміжками, означають, що всі вони повинні входити в одну пропозицію шуканого документа;
- 6) якщо ви хочете, щоб були відібрані тільки ті документи, в яких трапляється кожне слово, вказане в запиті, поставте перед кожним з них знак плюс «+». Якщо ви, навпаки, хочете виключити деякі слова з результату пошуку, поставте перед цим словом мінус «-». Знаки «+» і «-» треба писати через пробіл від попереднього і разом з наступним словом. Наприклад, за запитом «особисті -дані» будуть знайдені документи, в яких є слово «особисті» і немає слова «дані»;

- 7) під час пошуку синонімів або близьких за змістом понять між словами можна поставити вертикальну риску «|». (особисті | дані);
- 8) замість одного слова в запиті можна підставити цілий вислів; для цього його треба взяти в дужки (особисті | дані) + (знаменні | дати);
- 9) знак «~» (тильда) дає змогу знайти документи з пропозицією, яка містить перше слово, але не містить другого;
- 10) якщо оператор зазначений один раз (наприклад, & або ~), то пошук відбувається в межах пропозиції; подвійний оператор (&&, -) задає пошук у межах усього документа.

Достовірність інформації. Перш ніж шукати інформацію, потрібно розібратися, яка інформація вважається достовірною, а яка недостовірною, і навчитися розрізняти їх.

Недостовірною вважається інформація, що містить відомості про події та явища, яких не існувало взагалі або які існували, але відомості про них не відповідають дійсності, вони неповні або перекручені.

Достовірна інформація – відомості, що відповідають дійсності, факти, наявність яких за необхідності можна підтвердити юридично коректними процедурами із залученням свідків, використанням документів, експертних висновків тощо. Достовірними також вважаються відомості, що публікуються з обов'язковим посиланням на джерело та автора.

Джерела інформації також можуть бути *достовірні* і *недостовірні*, *компетентні* і *некомпетентні*. Ними можуть бути: фізичні особи, що з огляду на своє службове положення і повноваження володіють відомостями, якими цікавляться засоби масової інформації; реальне середовище (природне, урбаністичне і предметно-речове, в якому живе людина); віртуальне інформаційне середовище; документи, які можна перевірити юридично; друковані видання, що мають вихідні дані (енциклопедія, підручник, стаття в друкованому журналі тощо); сайти в мережі інтернет (Інтернет-ЗМІ, Інтернет-портал, Інтернет-сторінка і т.д.).

Нижче в порядку зменшення ступеня достовірності наведені джерела, згруповані за критерієм значущості [7]:

- 1) ресурси офіційних державних, наукових, галузевих та освітніх установ, реквізити яких містять правильну назву верхнього доменного імені, контактні данні відповідальних посадових осіб, інформацію про авторів та посилання на інші видання такого самого рівня; більшість контенту на цих ресурсах – це документи, представлені в електронній та оцифрованій формі;
- 2) сайти офіційних засобів масової інформації державного та регіонального рівнів, новинних агрегаторів, незалежних засобів масової інформації з позначенням реєстраційних даних та контактних даних відповідальних осіб;
- 3) корпоративні сайти;
- 4) особисті сайти та сторінки;
- 5) безіменні сайти.

Наступним критерієм оцінювання достовірності інформації є **авторитет автора** матеріалу. Важливі джерела інформації – представники офіційних органів влади, адже державні установи зобов'язані звітувати про свою діяльність, забезпечувати громадян точною, правдивою інформацією.

Слід **розрізняти фактичні твердження та оціночні судження** й враховувати обґрунтованість оціночного судження. Поширення недостовірної інформації карається законодавством більшості країн. Так, в Україні відповідальність за це передбачена ч. 1 ст. 277 ЦК України. Водночас згідно зі ст. 47 Закону України «Про інформацію» ніхто не може бути притягнутий до відповідальності за висловлення оціночних суджень і оціночні судження не підлягають спростуванню та доведенню їх правдивості, на відміну від фактичних тверджень (документованих або публічно оголошених відомостей про події та явища, що відбуваються у суспільстві, державі й навколишньому природному середовищі) [18].

Європейський суд з прав людини виокремив три критерії, на яких може ґрунтуватись суб'єктивна оцінка: 1) факти, що вважаються загальновідомими; 2) підтвердження висловлювання яким-небудь

джерелом; 3) посилання на оприлюднені результати незалежного дослідження [5].

Методика перевірки інформації. Розглянемо рекомендовані фахівцями способи перевірки даних з отриманої інформації за допомогою перехресного пошуку відповідності в Інтернеті.

Перевірка фактичного матеріалу через джерела.

Факт вигадати майже неможливо, бо його достовірність строго встановлена та підтверджена джерелом, а часто й не одним. Перевірка точності фактів і статистичних даних покаже, на які дані спирається сайт. Наявність посилань на авторитетні джерела, на зразок агентств збору статистики або наукових інститутів, підвищують достовірність даних. Якщо ця інформація не є точною або не відповідає дійсності, то й інший матеріал також не заслуговує на довіру.

Особливу увагу слід приділяти ретельній перевірці фактажу при роботі зі соціальними мережами як джерелами інформації: потрібно пересвідчитися в достовірності акаунта, з'ясувати місцезнаходження автора повідомлення, перевірити дату повідомлення, передивитися цитування статусів і постів в інших засобах масової інформації (рис. 3.1).

Пошук альтернативних джерел інформації.

Порівняння – один з найефективніших способів пошуку істини. Рідко одна і та сама недостовірною інформація публікується на декількох сайтах відразу. Тому якщо одні й ті ж дані трапляються в Інтернеті на абсолютно різних ресурсах і в різних формах подання, то їм можна довіряти. При цьому варто приділити увагу авторитетності первісного джерела інформації. На жаль, не рідкісними є випадки, коли всі сайти посилаються на одне і те саме недостовірне джерело.

У разі потреби перевірити джерела інформації стосовно регіональної належності, реєстрації та розташування можна скористатися спеціалізованими онлайн-сервісами. Такі ресурси (check-host.net, speed-tester.info, 2ip.ua тощо) за доменним ім'ям сайту виконують пошук і нададуть вичерпну інформацію про місце розташування сервера, дані про провайдера та хостера, дату реєстрації та реєстратора ресурсу. Крім цього, можна скористатися

додатковими сервісами для перевірки автора матеріалу за даними геолокації акаунта, за нікнеймом або за IP-адресою.

Встановлення використання матеріалу іншими джерелами.

Передрук і копіювання даних з одного сайту іншими є хорошим знаком, оскільки це означає, що цьому джерелу довіряють. Чим більше посилань на вихідний матеріал знайдемо в Інтернеті, тим вище його авторитет в очах інших ресурсів. Безсумнівно, це говорить на користь наведеної інформації.

З'ясування рейтингу і авторитету джерела.

Найдієвіший спосіб переконатися в правдивості отриманої інформації – це ознайомитися з репутацією ресурсу, на якому вона розміщена. Відомі ресурси зазвичай заслуговують довіри, оскільки відповідально ставляться до свого рейтингу і не стануть розмінювати його на сумнівні сенсації. Дізнатися про популярність сайту можна за допомогою спеціальних рейтингових систем, що містяться в переліку сервісів пошукових систем. Додатково можна ознайомитися з відгуками про нього. Позитивним є наявність у ресурсу свідоцтва про реєстрацію засобу масової інформації. Крім того, перевірені дані публікують офіційні сайти, які є першоджерелами.

Отримання інформації про автора матеріалу.

Для того, щоб зрозуміти, чи варто довіряти певній статті, потрібно пошукати інформацію про статус і компетентність її автора, ознайомитися з іншими його працями, коментарями й відгуками читачів. Якщо автор статті має хороший журналістський досвід, почесну посаду або науковий ступінь, шанси на правдивість його доказів зростають. Крім цього, в Інтернеті можуть бути його блоги, сторінки в соціальних мережах та інша інформація, яка допоможе сформулювати думку про автора. Окрему категорію складають матеріали, передруковані з реальних джерел, але доступні в Інтернеті, наприклад, підручники та енциклопедичні дані. Водночас потрібно обережно ставитися до таких ресурсів, як Вікіпедія. Інформація, опублікована в ній, цілком може виявитися недостовірною, оскільки доступ до редагування статей має кожен охочий. Це може бути як досвідчений професор, так і звичайний школяр. Вікіпедія хороша для розширення кругозору, однак посылатися на неї в серйозній роботі вельми небезпечно. Те саме можна сказати і про блоги. Часто ніхто,

окрім автора блогу, не може підтвердити достовірність опублікованої інформації. Тому використовувати блогерські дані потрібно обережно, перевіряючи їх особливо ретельно.

У випадку аналізу наукової інформації і наукових джерел доцільно користуватися системами індексів наукового цитування (національна система – Український індекс наукового цитування, <http://uincit.urau.ua>) та звертати увагу на імпаکت-фактор українських і зарубіжних фахових журналів (у базах даних SCOPUS, Web of Science, THOMPSON ISI, Journal Citation Reports Science Edition, Journal Citation Reports Social Science Edition та ін.).

Вдосконалення алгоритму формування пошукового запиту.

Грамотний підхід до формування пошукових запитів значно пришвидшує процес пошуку інформації. Не завжди точно відома назва сайтів, на яких можна отримати потрібні дані, тому доцільно використовувати популярні пошукові сервіси, зокрема такі, як Google. Далі багато залежить від пошукової процедури і формулювання запиту. Будь-яка пошукова система шукає у своїй базі даних із мільярда сторінок ті, що відповідають заданим параметрам, і використовує для цього власні програми пошуку та індексації. Пошукові системи зберігають попередньо опрацьовані сторінки у файлах бази даних у проіндексованому вигляді, щоб сторінку можна було знайти за ключовими словами після запиту користувача. Варто враховувати, що в різних пошукових систем відрізняються алгоритми опрацювання та індексації інформації. Тому для більш результативного пошуку є сенс шукати інформацію одночасно в різних пошукових системах, з урахуванням регіону та мовних особливостей, враховуючи принцип таргетування за цілим переліком можливих критеріїв.

Переходимо до висновків. Керуючись правилами елементарної логіки, підготовлений користувач зможе відрізнити правду від брехні. Однак навіть найдосвідченіша людина може виявитися ошуканою. Засилля гарно оформлених сайтів шахраїв і жовтої преси здатне ввести в оману кого завгодно. Щоб не потрапити в пастку, варто дотримуватися низки правил.

1. Обов'язково потрібно перевіряти інформацію і її джерела. Важливо перевіряти всі важливі дані, знайдені в Інтернеті, оскільки

наслідки використання недостовірної інформації можуть бути вельми негативними. Слід перевіряти достовірність даних і першоджерела, вивчати синтаксичний план функціонування інформації, логіку її будови та структури.

2. Потрібно критично сприймати й оцінювати інформацію, зважаючи на аргументацію, науковість і коректність фактів. Варто виробити власну методику перевірки інформації за критерієм логічного збігу відомостей під час порівняння даних з декількох джерел, а також взяти за правило не користуватись неперевіреними даними.

3. Необхідно вибудувати власну рейтингову систему джерел інформації за ступенем довіри (на основі власного досвіду, дослідження їхньої достовірності). Насамперед на довіру заслуговують офіційні сайти державних і наукових установ, інформаційні агентства та їхні прес-релізи. Потрібно пам'ятати, що офіційні державні та регіональні онлайн-ЗМІ несуть відповідальність за опубліковані дані.

4. Важливо мати навички грамотного і чіткого формулювання пошукових запитів та вміння працювати з пошуковими системами. Потрібно увляти собі те, що шукаємо, адже це допоможе правильно сформулювати пошуковий запит і заощадить багато часу і зусиль, збільшить шанси знайти саме те, що потрібно. Слід пам'ятати про відмінності пошукових алгоритмів у різних пошукових систем та про існування так званої «маски» користувача, де зберігається інформація про його зацікавленість певними сферами, таргетування за регіональним принципом на основі опрацювання його попередніх запитів.

Завдання і запитання до параграфа

1. Які основні групи інформаційних ризиків вам відомі? Наведіть приклади їх виявів у мережі Інтернет?
 2. Поясніть, що таке загроза інформаційній безпеці й назвіть основні види загроз.
 3. Поясніть комплексну дію складових «4D»-стратегії. У чому полягає складність протидії цій стратегії?
-
-

4. Поясніть комплексну дію складових «4F»- тактики. У чому полягає складність протидії цій тактиці?
5. Дайте визначення поняттю *інформація* та назвіть основні її властивості.
6. Дайте визначення поняттю *інформаційна технологія* та назвіть її основні види.
7. Що таке інформаційний пошук? Якими методами він здійснюється?
8. Що таке інформаційно-пошукові системи та як їх класифікують?
9. Які основні правила формування запиту в пошуковій системі? Наведіть приклади застосування в запиті спеціальних символів.
10. Що таке достовірна інформація? Назвіть три основні її ознаки.
11. Вкажіть, якою має бути послідовність дій для підтвердження достовірності інформації.
12. Назвіть джерела інформації за статусом її надійності.
13. Проаналізуйте на достовірність самостійно підібране повідомлення новинної агенції, звертаючи увагу на першоджерела, аргументацію, фактаж, підкріплення інформації висновками фахових експертів, та відтворіть схему створення медіаповідомлення (відстежте першоджерела, авторство та авторитетність експертної оцінки).
14. Проаналізуйте будь-яку новинну агенцію за такими критеріями: репутація, заангажованість, компетентність, достовірність. Порівняйте власні висновки з рейтингом пошукових сервісів та висновками фахових експертів.

Список використаної та рекомендованої літератури

1. Бондаренко А. Фейковые украинские и американские сайты с лживыми новостями об Украине [Електронний ресурс] / А. Бондаренко // Fakeoff.org. – 03.09.2015. – Режим доступу: <http://fakeoff.org/politics/iz-rf-upravlyayut-setyu-feykovykh-ukrainskimi-smi> (дата звернення: 01.05.2018).
2. Бугоркова О. Катастрофа МН17: как менялись версии российских СМИ [Електронний ресурс] / Ольга Бугоркова // BBC. News. – 28.09.2016. – Режим доступу: <https://www.bbc.com/russian/features-37496581> (дата звернення: 04.04.2018).

3. Глобальная сеть: правила пользования [Электронный ресурс] / Фонд Развития Интернета. – Режим доступа: <http://docplayer.ru/25883581-Globalnaya-set-pravila-polzovaniya.html> (дата звернення: 01.04.2018).
4. Данильчук Л. Сутність дефініції «інформація» / Лариса Данильчук // Педагогіка і психологія професійної освіти. – Львів, 2012. – № 5. – С. 18-26.
5. ЄСПЛ назвав три критерії обґрунтованості оціночного судження [Електронний ресурс] // Закон і бізнес. – 28.03.2013. – Режим доступу : <http://zib.com.ua/ua/pda/15222.html> (дата звернення: 04.04.2018).
6. Згуровський М. З. Вступ до комп'ютерних інформаційних технологій : навч. посібник / М. З. Згуровський, І. І. Коваленко, В. М. Міхайленко. – Київ : Вид-во Європ. ун-ту, 2003. – 256 с.
7. Зубец В. В. О качестве сетевой информации [Электронный ресурс] / В. В. Зубец, И. В. Ильина // Вестник Тамбовского университета. – 2016. – Вып. 12. – С. 168-172. – Режим доступа : <https://cyberleninka.ru/article/v/o-kachestve-setevoj-informatsii> (дата звернення: 09.04.2018).
8. Інформатика: Комп'ютерна техніка. Комп'ютерні технології : підруч. для студентів вищих навчальних закладів / за заг. ред. О. І. Пушкаря. – Київ : Видавничий центр «Академія», 2002. – 704 с.
9. Інформація та документація. Словник термінів (ISO 5127:2001, IDT) : ДСТУ ISO 5127:2007. – Київ : Держспоживстандарт України, 2010. – 237 с.
10. Кадемія М. Ю. Інформаційно-комунікаційні технології навчання: термінологічний словник / М. Ю. Кадемія. – Львів : Вид-во «СПОЛОМ», 2009. – 260 с.
11. Канал «Звезда» поширив ще один фейк про МН17? // Радіо Свобода. – 17 грудня 2017. – Режим доступу : <https://www.radiosvoboda.org/a/28910403.html> (дата звернення: 18.02.2018)
12. Кузьменко А. Загадочная история Девида Джуберга, фейкового эксперта Пентагона по России [Электронный ресурс] / А. Кузьменко // Stopfake.org. – 03.04.2018. – Режим доступа: <https://www.stopfake.org/zagadochnaya-istoriya-devida-dzhuberga-fejkovogo-eksperta-pentagona-po-rossii> (дата звернення: 10.04.2018).
13. О средствах массовой информации. ФОМ попросил россиян оценить работу СМИ [Электронный ресурс]. – Режим доступа : <http://fom.ru/SMI-i-internet/11427> (дата звернення: 10.04.2018).
14. Оліярник М. Творець інтернету розповів про основні загрози для розвитку всесвітньої павутини [Електронний ресурс] / Микола Оліярник // Новое время. Бизнес. –13.03.2017. – Режим доступа : <https://biz.nv.ua/ukr/publications/tvoretz-internetu-rozpoviv-pro-osnovni-zagrozi-dlja-rozvitku-vsesvitnoji-pavutini-797191.html> (дата звернення: 05.04.2018).

15. Павлиш В. А. Основи інформаційних технологій і систем : навч. посіб. / В. А. Павлиш, Л. К. Гліненко ; М-во освіти і науки України ; Нац. ун-т «Львів. Політехніка». – Л. : Вид-во Львів. політехніки, 2013. – 500 с.
16. Про державну таємницю : Закон України [Електронний ресурс] // Верховна Рада України : офіційний веб-портал. – Режим доступу : <http://zakon3.rada.gov.ua/laws/show/3855-12> (дата звернення: 06.04.2018).
17. Проект резолюции ООН о трибунале по Boeing MH17 был отклонен [Електронний ресурс] // Ведомости. – 29.07.2015. – Режим доступу: <https://www.vedomosti.ru/politics/articles/2015/07/29/602720-proekt-rezolyutsii-oon-o-tribunale-po-boeing-mh17-bil-otklonen> (дата звернення: 01.04.2018).
18. Рішення колегії суддів Судової палати у цивільних справах Верховного Суду України [Електронний ресурс] // Верховний Суд України : офіційний веб-сайт. – Режим доступу : <http://www.scourt.gov.ua/clients/vs.nsf/0/C5D24368703DC8B9C225735B00482BE2?OpenDocument> (дата звернення: 01.04.2018).
19. У Варшаві держсекретар МІП озвучив формулу російської дезінформаційної кампанії – «4 F» // Детектор медіа. – 19.03.2018. – Режим доступу : <http://detector.media/infospace/article/135750/2018-03-19-u-varshavi-derzhsektar-mip-ozvuchiv-formulu-rosiiskoi-dezinformatsiinoi-kampanii-4-f> (дата звернення: 12.04.2018).
20. Ученые раскрыли тайну ложных воспоминаний [Електронний ресурс] // РБК –Україна. – 08.11.2011. – Режим доступу: <https://www.rbc.ua/ukr/digests/pochemu-my-pomnim-to-chego-ne-bylo-08112011164000> (дата звернення: 08.04.2018).
21. Уэндлинг М. История «фейковых новостей» [Електронний ресурс] / Майк Уэндлинг // BBC Trending. – 23.01.2018. – Режим доступу : <https://www.bbc.com/ukrainian/features-russian-42794529> (дата звернення: 07.04.2018).
22. Nimmo B. Anatomy of an info-war: How Russia's propaganda machine works, and how to counter it = Анатомія інформаційної війни: як працює пропагандистська машина Росії і як протистояти їй [Електронний ресурс] / В. Nimmo. – Режим доступу: <https://www.stopfake.org/en/anatomy-of-an-info-war-how-russia-s-propaganda-machine-works-and-how-to-counter-it> (дата звернення: 01.04.2018).

Автор параграфа:
асист. каф. журналістики
НПУ імені М.П. Драгоманова
ОЛЕКСАНДР КЛИМЕНКО


ІЛЮСТРАЦІЇ

<https://www.bravica.net/ru/net-geo.html?cmd=npu.edu.ua>

ИНФОРМАЦИЯ ДЛЯ NPU.EDU.UA

Имя хоста: npu.edu.ua - [Whois](#) • [Трассировка](#) • [Пинг](#)

IP адрес: 213.169.81.98

Страна:  Украина

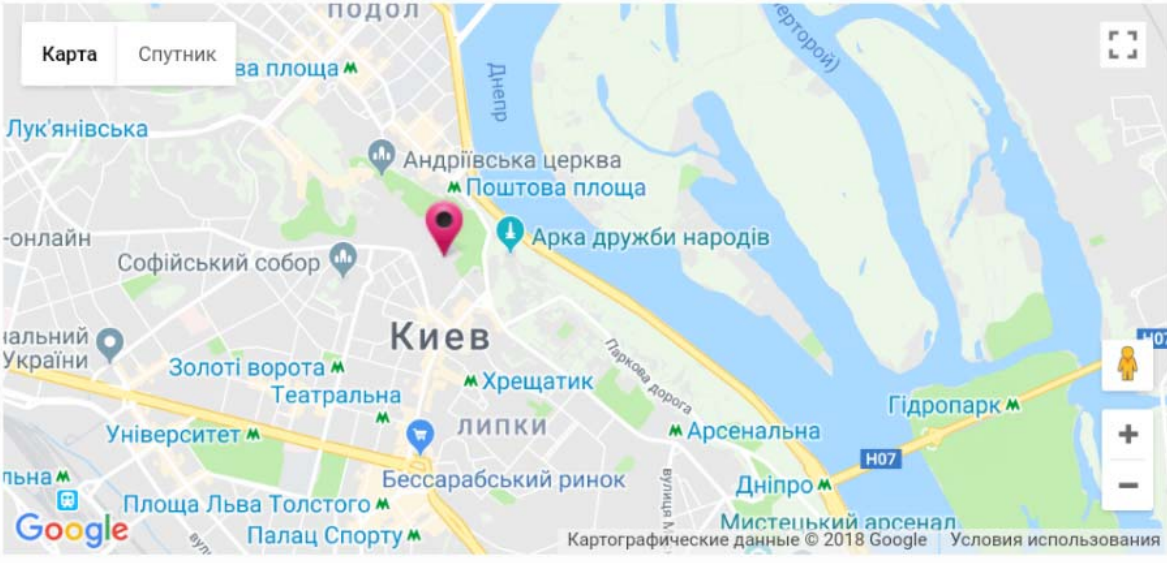
Код страны: UA

Регион: Киев

Город: Киев

Координаты: долгота 50.45466°, широта 30.5238°

Местное время: 19:49, 17.04.2018, временная зона: Europe/Kiev



Карта Спутник

Google

Картографические данные © 2018 Google Условия использования

Рисунок 3.1. Перевірка достовірності джерела інформації

ГІБРИДНА ВІЙНА І ЖУРНАЛІСТИКА

ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

ДЕЗІНФОРМАЦІЯ
МАНІПУЛЮВАННЯ
НАВІЮВАННЯ
ФЕЙКИ



НАЦІОНАЛЬНИЙ ПЕДАГОГІЧНИЙ УНІВЕРСИТЕТ
імені М. П. ДРАГОМАНОВА

ГІБРИДНА ВІЙНА І ЖУРНАЛІСТИКА

ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Навчальний посібник

Київ
Вид-во НПУ імені М. П. Драгоманова
2018

УДК 070:355.01-025.26(07)

Г 46

*Рекомендовано Вченою радою
Національного педагогічного університету імені М. П. Драгоманова
(протокол № 14 від 26 червня 2018)*

*За загальною редакцією
доктора філософських наук, професора кафедри журналістики
НПУ ім. М. П. Драгоманова, академіка НА вищої освіти України
В. О. Жадька*

Рецензенти: *Іван Васильович Крупський*, доктор історичних наук, професор, завідувач кафедри теорії і практики журналістики Львівського національного університету імені І. Франка;
Ірина Миколаївна Жиленкова, доктор історичних наук, професор кафедри історії та етнополітики Національного педагогічного університету імені М. П. Драгоманова.

Авторський колектив:

В. О. Жадько, О. І. Клименко, П. П. Куляс, О. Т. Марків, Ю. С. Полтавець,
О. І. Харитоненко, О. В. Харчук, С. В. Шевчук.

Ілюстрація на обкладинці:

Ф. В. Сергеев

Г 46 Гібридна війна і журналістика. Проблеми інформаційної безпеки : навчальний посібник / за заг. ред. В. О. Жадька ; ред.-упор. : О. І. Харитоненко, Ю. С. Полтавець. – Київ : Вид-во НПУ імені М. П. Драгоманова, 2018. – 356 с.

ISBN 978-966-931-181-8

Підготовлений викладачами кафедри журналістики НПУ імені М. П. Драгоманова посібник присвячено питанням інформаційної безпеки, діяльності журналіста в умовах гібридної війни, проблемам медіаосвіти. У книзі чотири розділи, що висвітлюють суть та складові сучасних гібридних протистоянь, їхній інформаційний, інформаційно-психологічний, семантичний, технологічний та силовий аспекти. Видання доповнене термінологічним словником. Посібник призначений для студентів спеціальності «Журналістика», а також для всіх, хто прагне навчитися критично оцінювати й аналізувати медіаповідомлення та інформацію загалом.

ISBN 978-966-931-181-8

УДК 070:355.01-025.26(07)

© Авторський колектив, 2018

© Сергеев Ф. В., обкладинка, 2018

© Вид-во НПУ імені М. П. Драгоманова, 2018

ЗМІСТ

ПЕРЕДМОВА 5

ВСТУП

Гібридна війна в сучасному світі.

Що про неї повинен знати журналіст і редактор? 12

Розділ 1

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНА АГРЕСІЯ

- § 1. Визначення, види, актуальні напрямки дослідження інформаційних війн..... 28
- § 2. Інформаційні війни в історії та сучасності: характерні ознаки новітніх протистоянь 64
- § 3. Технології маніпулювання і методики пошуку, відбору, верифікації даних у журналістиці..... 96
- § 4. Фактчекінг у роботі сучасного журналіста – дієвий спосіб протистояння інформаційним загрозам 126

Розділ 2

СМИСЛОВІ ВІЙНИ В МЕЖАХ ГІБРИДНИХ ПРОТИСТОЯНЬ

- § 5. Інформаційні та смислові війни: наукові підходи до розмежування понять..... 142
- § 6. «Зброя» смислової війни. Основні інструменти для зміни системи цінностей..... 161
- § 7. Тактика смислових війн і спроби протидії 190
- § 8. Класична журналістика в умовах гібридних воєн: конфлікт теорії і сучасних комунікативних практик..... 202

Розділ 3

ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИЙ, ТЕХНОЛОГІЧНИЙ І СИЛОВИЙ ВИМІРИ ГІБРИДНИХ ЕКСПАНСІЙ

- § 9. Інформаційно-психологічні операції: поняття, види, способи використання в умовах гібридної війни..... 229
- § 10. Інформаційно-технологічні атаки і способи захисту кіберпростору: новітні тактики габридних війн..... 246
- § 11. Особливості роботи журналіста в зонах військових конфліктів..... 264

РОЗДІЛ 4

МЕДІАОСВІТА ЯК ФУНДАМЕНТАЛЬНА СКЛАДОВА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

§ 12. Роль медіаграмотності в професійному та особистому становленні людини інформаційної епохи	272
§ 13. Формування в майбутніх журналістів культури роботи з інформацією в умовах гібридної війни	290
§ 14. Світові та вітчизняні тенденції розвитку медіаосвіти	305
СЛОВНИК ТЕРМІНІВ	316

Навчальне видання

ГІБРИДНА ВІЙНА І ЖУРНАЛІСТИКА

ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Навчальний посібник

За загальною редакцією

*доктора філософських наук, професора кафедри журналістики
НПУ ім. М. П. Драгоманова, академіка НА вищої освіти України*

В. О. Жадька

Авторський колектив:

Жадько Віктор Олексійович, док. філос. н., проф., зав. каф. журналістики НПУ імені М. П. Драгоманова (§ 2 «Інформаційні війни в історії та сучасності: характерні ознаки новітніх протистоянь»)

Клименко Олександр Іванович, ас. каф. журналістики (§ 3 «Технології маніпулювання і методики пошуку, відбору, верифікації даних у журналістиці»)

Куляс Павло Петрович, канд. іст. н., доц. каф. журналістики (вступ «Гібридні війни в сучасному світі. Що про них повинен знати журналіст і редактор?»)

Марків Олександра Тимофіївна, канд. педагог. н., доц. каф. журналістики (§ 9 «Інформаційні й психологічні операції: поняття, види, способи використання в умовах гібридної війни»; § 12 «Роль медіаграмотності в професійному та особистісному становленні людини інформаційної епохи»; § 13 «Формування в майбутніх журналістів культури роботи з інформацією в умовах гібридної війни»)

Полтавець Юлія Сергіївна, канд. філол. н., ст. викл. каф. журналістики (§ 4 «Фактчекінг у роботі сучасного журналіста – дієвий спосіб протистояння інформаційним загрозам»; § 10 «Інформаційно-технологічні атаки і способи захисту кіберпростору: новітні тактики гібридних війн»)

Харитоненко Олена Іванівна, канд. філол. н., доцент каф. журналістики (§ 1 «Визначення, види, актуальні напрямки дослідження інформаційних війн» – у співавторстві; розділ 2 «Смислові війни в межах гібридних протистоянь»)

Харчук Олена Василівна, канд. філол. н., доцент каф. журналістики (§ 1 «Визначення, види, актуальні напрямки дослідження інформаційних війн» – у співавторстві)

Шевчук Світлана Вікторівна, ас. каф. журналістики (§ 11 «Особливості роботи журналіста в зонах військових конфліктів»; § 14 «Світові та вітчизняні тенденції розвитку медіаосвіти»)

Технічний редактор – Т. С. Меркулова

Макетування – Т. М. Ветраченко

Обкладинка – Ф. В. Сергеев



Підписано до друку 26 червня 2018 р.
Формат 60x84/16. Папір офісний. Гарнітура Times New Roman.
Ум. др. арк. 22,25. Об.-вид. арк. 17,75.
Наклад 300 прим. Зам. № 397
Віддруковано з оригіналів

Видавництво Національного педагогічного університету
імені М. П. Драгоманова. 01601, м. Київ-30, вул. Пирогова, 9.
Свідоцтво про реєстрацію ДК № 1101 від 29.10.2002 (044) 234-75-87
Віддруковано в друкарні Національного педагогічного університету
імені М. П. Драгоманова (044) 239-30-26