

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ
Науково-дослідна лабораторія з проблемних питань
кримінального аналізу
Кафедра адміністративної діяльності поліції

АНАЛІЗ, ВИЯВЛЕННЯ ТА УБЕЗПЕЧЕННЯ ВІД
НЕПРАВДИВИХ ПОВІДОМЛЕНЬ, ЯК СКЛАДОВОЇ
ЧАСТИНИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ
Методичні рекомендації

Одеса
2022

УДК 351.746.1(072)(477)

Рекомендовано до друку Науково-методичною радою
Одеського державного університету внутрішніх справ
Протокол від «22» грудня 2022 р. № 5.

Автори-упорядники:

Дмитро АФОНІН кандидат юридичних наук, завідувач науково-дослідної лабораторії з проблемних питань кримінального аналізу Одеського державного університету внутрішніх справ

Карен ІСМАЙЛОВ кандидат юридичних наук, доцент, старший науковий співробітник науково-дослідної лабораторії з проблемних питань кримінального аналізу Одеського державного університету внутрішніх справ

Дмитро ЛІСНІЧЕНКО кандидат юридичних наук, старший науковий співробітник науково-дослідної лабораторії з проблемних питань кримінального аналізу Одеського державного університету внутрішніх справ

Алла ПИШНА кандидат юридичних наук, доцент, завідувач кафедри адміністративної діяльності поліції факультету підготовки фахівців для підрозділів превентивної діяльності Одеського державного університету внутрішніх справ

Олена КОВАЛЬОВА кандидат юридичних наук, старший науковий співробітник, професор кафедри адміністративної діяльності поліції факультету підготовки фахівців для підрозділів превентивної діяльності Одеського державного університету внутрішніх справ

Ан64 Аналіз, виявлення та забезпечення від неправдивих повідомлень, як складової частини інформаційної безпеки держави : методичні рекомендації / Д. Афонін, Д. Ісмаїлов, Д. Лісніченко, Д. Пишна, О. Ковальова. – Одеса : ОДУВС, 2023. – 40 с.

ЗМІСТ

Вступ	4
I. Інформаційна безпека як складова національної безпеки України.	7
II. Види маніпуляцій з інформацією.	12
III. Інструменти виявлення неправдивих повідомлень.	27
IV. Відповідальна поведінка у соціальних мережах під час війни.	32
Використана література	43

ВСТУП

Забезпечення інформаційної безпеки України є однією з найважливіших функцій держави. Сьогодні безпека роботи з інформацією, як ніколи, є актуальною. Ми живемо в час, коли медіапростір стрімко змінюється. Сьогодні під словом «медіа» мають на увазі все – від друкованих видань до цифрової інформації. Медіа охоплюють телерадіомовлення, пресу та онлайн-контент (соціальні мережі, подкасти, блоги та онлайн-статті), тобто всі види масової комунікації. Змінилася й наша роль у медіа – зі слухачів і читачів ми перетворилися на авторів та поширювачів інформації. Інформація стала такою доступною, а її об'єми – такими великими, що не дивно, що іноді ми можемо загубитися в ній. Ще більше ускладнює ситуацію те, що деяка інформація може бути викривлена, маніпулятивна або й зовсім неправдива. Великі об'єми інформації можуть перетворити наш вибір на виснажливе завдання «у що та кому вірити».

Підвищення рівня медіаграмотності суспільства та протидія дезінформації є одними із стратегічних цілей України. Одним із завдань, спрямованих на досягнення зазначеної цілі є підготовка та проведення просвітницької кампанії з медіаграмотності, що включатиме такі компоненти, як розвиток критичного мислення, навички перевірки фактів і визначення маніпуляційних технік, ознайомлення з найпоширенішими порушеннями прав людини із застосуванням інтернет-технологій тощо. Особливої актуальності це питання набуває в умовах воєнного стану. Слід усвідомити, що маніпуляції з інформацією – це зброя, а інформаційний простір – це один із фронтів ведення війни. Деструктивна пропаганда, поширення дезінформації як ззовні, так і всередині України застосовуються державою-агресором з метою підризу стійкості суспільства та інформаційної дестабілізації держави. Українське суспільство повинне бути захищене від деструктивного впливу маніпулятивної інформації.

Інформаційна безпека та кібербезпека, – складові частини національної безпеки України. В Україні створені спеціальні органи влади, до функцій яких відноситься їх забезпечення. Однак дотримання правил інформаційної та кібербезпеки на сьогодні актуальні для кожної людини. Медіаосвіта не розвивається так швидко, як технології, які ми використовуємо щодня. На жаль, поки що система освіти не може дати нам знань, які б допомогли орієнтуватись у сучасній складній інформації. Замислитесь, як часто ви перевіряєте свою стрічку у Facebook та обговорюєте новини з друзями? Ми отримуємо регулярні оновлення та сповіщення звідусіль – месенджери, електронна пошта, медіа. «Бути в курсі» – модно, тож ми намагаємось охопити якомога більше інформації. Однак інформація може бути оманливою та перевантажувати наш мозок. Як ранкова кава бадьорить нас, так критичне мислення допомагає нам бути зосередженими та пильними. Кава стала щоденним ритуалом для багатьох із нас. Таким самим ритуалом повинна стати й медіаграмотність. Нам потрібні навички аналізу, оцінки та створення інформації, адже саме вони є основою медіаграмотності.

Тому останнім часом прийнято вести мову про кібергігієну як окрему сферу знань та навиків людини, в тому числі спрямованих на розвиток медіаграмотності суспільства, зокрема убезпечення від неправдивих повідомлень. У світі існує достатньо велика кількість тлумачень слова «кібергігієна». Вони, як правило, відображають найбільш значущі аспекти цього терміна, важливі для конкретної галузі знань. Більш спрощена інтерпретація цього терміну дозволяє представити кібергігієну як дотримання правил безпечної поведінки у кіберсфері. Навики кібергігієни можна віднести до сучасних soft-skills («м'яких навиків»), важливих для кожної людини, незалежно від її сфери зайнятості.

Такий підхід дає змогу значно посилити систему колективної безпеки суспільства та держави в цілому. Кібергігієна повинна дотримуватись так само, як особиста гігієна. Порушення правил кібергігієни може призвести для згубних наслідків не лише для окремої людини. Досить часто від дій зловмисників страждає і роботодавець. Навіть великі держави можуть зазнати величезної шкоди від необачного ставлення до вимог безпеки однієї людини. Часто порушники використовують окрему особу як лаз для проникнення на об'єкти критичної інфраструктури, викрадення чутливих державних даних, створення умов для скоординованих повномасштабних атак. Розповсюдженим видом інформаційних атак є маніпуляції з інформацією в медіа. Для того, щоб мінімізувати ризик успішної реалізації таких атак, як раз і потрібна кібергігієна. Уміння фільтрувати та критично оцінювати інформацію — життєво необхідна навичка у сучасному світі. Недотримання вимог кібергігієни здатне завдати значної матеріальної та моральної шкоди. А крім того, суттєво вплинути на Вашу особисту репутацію. По суті, кібергігієна – це рутинний процес. Найкращий варіант, якщо Ви зробите кібергігієну своєю повсякденною звичкою. При цьому вона не потребує суттєвих витрат коштів і часу. Згодом ви звикнете до виконання відповідних процедур і відчуете їх корисність як в особистих, так і в службових справах. Дотримуватися правил кібергігієни та інформаційної безпеки – це не тільки корисно, але й розумно, комфортно і відповідально.

Кібергігієна межує як з інформаційною, так і з кібербезпекою. Вона є інструментом забезпечення виконання завдань та елементом кожної з них. Проте ці поняття не є тотожними. Якщо кібербезпека пов'язана з об'єктивним оцінюванням дій, спрямованих на підтримку безпеки та дотримання захисту від кібератак, то кібергігієна асоціюється зі знаннями про безпеку в Інтернеті та правилами покращення кібербезпеки. Також кібергігієна передбачає дотримання правил поведінки, що стосуються інформаційної безпеки.

Однак, кібергігієна не має нормативно-правової регламентації та її поняття не закріплене в сучасних нормативно-правових актах. Тому, враховуючи, що дані методичні рекомендації присвячені саме убезпеченню від неправдивих повідомлень, а дане питання на нормативно-правовому рівні

є складовою інформаційної безпеки, ми будемо вести мову саме про інформаційну безпеку.

Дані методичні рекомендації пояснюють як орієнтуватися в інформації довкола, як розпізнавати різні види маніпуляцій з інформацією, які інструменти виявлення неправдивих повідомлень можна використовувати та як поводитись у соціальних мережах під час війни.

I. ІНФОРМАЦІЙНА БЕЗПЕКА ЯК СКЛАДОВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ.

У національних нормативно-правових актах на сьогодні відсутнє безпосереднє згадування такої категорії як кібергігієна. Водночас найбільш дотичними термінами у досліджуваному контексті є «інформаційна безпека» та «кібербезпека». Інформаційна безпека та кібербезпека держави є складовою частиною її національної безпеки. В Україні питанню забезпечення національної безпеки традиційно приділяють велику увагу. Здійснивши екскурс в історію, можна побачити, що від самого початку становлення України як незалежної держави методично ухвалювалися нормативно-правові акти, які містили безпосередні вказівки для того чи іншого напрямку забезпечення національної безпеки.

У зв'язку з появою нових системних загроз національній безпеці 21 червня 2018 р. було ухвалено новий Закон України «Про національну безпеку України», який відобразив сучасні безпекові реалії та стратегічні напрямки розвитку сектору безпеки України. Відповідно до п. 9 ч. 1 ст. 1 цього Закону, **національна безпека** – це захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу й інших національних інтересів України від реальних і потенційних загроз.

За вказаними напрямками безпеки здійснюється планування. Документи, що містять довгострокові плани, отримали назву стратегії. Відповідно, в законі описуються в загальному вигляді стратегії національної безпеки, воєнної безпеки, громадської безпеки та цивільного захисту України тощо.

Згідно зі статтею 17 Конституції України, забезпечення інформаційної безпеки є однією з найважливіших функцій держави, справою всього Українського народу. Комплексний характер актуальних загроз національній безпеці в інформаційній сфері потребує визначення інноваційних підходів до формування системи захисту і розвитку інформаційного простору в умовах глобалізації та вільного обігу інформації.

В 2021 році Указами Президента України були введені в дію рішення РНБО України про затвердження Стратегії кібербезпеки України (Указ Президента України від 26 серпня 2021 року № 447/2021) та Стратегії інформаційної безпеки України (Указ Президента України від 28 грудня 2021 року № 447/2021).

Відповідно до Стратегії кібербезпеки України цифрові навички, кіберобізнаність щодо сучасних кіберзагроз та протидії ним мають стати невід'ємними елементами освіти кожного громадянина України.

Відповідно до Стратегії інформаційної безпеки **інформаційна безпека України** – складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом.

Суб'єктами забезпечення інформаційної безпеки як складової національної безпеки України є:

- громадяни України та їх об'єднання;
- Верховна Рада України, яка, серед іншого, ухвалює закони у сфері інформаційної безпеки, визначаючи тим самим державну політику в цій сфері;
- Президент України, який забезпечує послідовне проведення державної інформаційної політики, інформаційний суверенітет та інформаційну безпеку України;
- Кабінет Міністрів України, який забезпечує формування та реалізацію інформаційної політики держави, забезпечує інформаційний суверенітет, фінансування програм, пов'язаних з інформаційною безпекою, спрямовує і координує роботу міністерств, інших органів виконавчої влади у цій сфері;
- Рада національної безпеки і оборони України, яку очолює Президент України, координує діяльність органів виконавчої влади щодо забезпечення національної безпеки в інформаційній сфері, зокрема з використанням спроможностей Центру протидії дезінформації;
- інші органи виконавчої влади, які у взаємодії з органами місцевого самоврядування, Центром протидії дезінформації та інститутами громадянського суспільства забезпечують реалізацію Стратегії згідно з планом заходів, який затверджується Кабінетом Міністрів України;
- засоби масової інформації та інші суб'єкти, які здійснюють інформаційну діяльність;
- наукові установи та навчальні заклади, які забезпечують науково-аналітичне та експертне супроводження процесу формування та реалізації державної інформаційної політики та, серед іншого, проводять наукові дослідження та здійснюють підготовку фахівців з інформаційної безпеки.

В Стратегії інформаційної безпеки виокремлені глобальні та національні виклики та загрози.

До глобальних викликів та загроз віднесені:

-  збільшення кількості глобальних дезінформаційних кампаній;
-  інформаційна політика Російської Федерації – загроза не лише для України, але й для інших демократичних держав;
-  соціальні мережі як суб'єкти впливу в інформаційному просторі;
-  недостатній рівень медіаграмотності (медіакультури) в умовах стрімкого розвитку цифрових технологій.

До національних викликів та загроз віднесені:

-  інформаційний вплив Російської Федерації як держави-агресора на населення України;
-  інформаційне домінування Російської Федерації як держави-агресора на тимчасово окупованих територіях України;
-  обмежені можливості реагувати на дезінформаційні кампанії;
-  несформованість системи стратегічних комунікацій;
-  недосконалість регулювання відносин у сфері інформаційної діяльності та захисту професійної діяльності журналістів;
-  спроби маніпуляції свідомістю громадян України щодо європейської та євроатлантичної інтеграції України;
-  доступ до інформації на місцевому рівні;
-  недостатній рівень інформаційної культури та медіаграмотності в суспільстві для протидії маніпулятивним та інформаційним впливам.

Отже, недостатній рівень інформаційної культури та медіаграмотності в суспільстві для протидії маніпулятивним та інформаційним впливам визначається одним із національних викликів. Відсутність належного рівня інформаційної культури та медіаграмотності в суспільстві в умовах стрімкого розвитку цифрових технологій створює підґрунтя для маніпулювання громадською думкою, проведення стрімких деструктивних інформаційних операцій, що зумовлює існування потенційних та реальних загроз інформаційній безпеці України.

При цьому **однією із стратегічних цілей** визнано **підвищення рівня медіакультури та медіаграмотності суспільства.**

Щодня ми споживаємо величезні обсяги інформації. Телебачення, соціальні мережі, газети, реклама – інформаційні повідомлення ми отримуємо звідусіль. Не слід недооцінювати їх вплив на нашу життєдіяльність, зокрема на пізнання, впевненість, ставлення, настрої, поведінку, фізіологічний вплив тощо.

Вплив на пізнання включає в себе вплив на збір, обробку та зберігання інформації. Медіа надають нам дані, які наш мозок перетворює у знання. Повідомлення з різних медіа можуть групуватися, об'єднуватися, видозмінюватися й набувати цілком іншого змісту. Уявіть, що на якомусь телеканалі повідомили, що поліцейським відтепер потрібно щомісяця проходити медогляд. Ви почули цю інформацію один раз. Можливо, запам'ятали, а може – ні. Згодом те саме ви почули по радіо в автобусі та прочитали в газеті – і ця інформація перетворилася у вашій голові в знання. Тобто ви тепер знаєте, що вам потрібно проходити медогляд щомісяця. І не важливо, правда це чи ні¹.

Вплив на впевненість/віру включає в себе вплив на формування стереотипів і уявлень про щось чи когось. Медіа дають нам змогу побачити й дізнатися значно більше, ніж ми можемо самі. Вони формують наші уявлення про речі, яких ми ніколи не бачили, але точно знаємо, що вони є, бо про них повідомили ЗМІ. Чи знали ви, що чим менша навчальна група – тим кращі результати навчання? Про це говорять на форумах у фейсбуці та в національних телеефірах. Це очевидно, і це знають всі. Але насправді така впевненість, підкріплена медіа, – міф. Навпаки: менші класи часто забирають фінансування, яке було б доцільніше витратити на інші потреби. Наприклад, на вищу заробітну плату для викладачів. Згідно з дослідженням PISA, найуспішніші освітні системи зазвичай надають пріоритет якості викладання, а не розміру класів. Але почувши цей міф по телевізору, ми починаємо йому вірити.

Вплив на ставлення, в тому числі вплив на стандарти оцінювання чогось або когось. Медіа змушують нас підсвідомо наділяти історії та інформацію суб'єктивною оцінкою. І забарвленням цієї оцінки можна маніпулювати. Уявіть: ви чуєте історію 45-річної викладачки з Одещини, яка 20 років викладає у закладі освіти майже безкоштовно – їй регулярно затримує зарплату керівник. Які почуття у вас виникли? Вам шкода викладачку, а не порядність керівника викликає осуд та злість? А якщо трохи змінити цю новину, приміром, так: «Викладачка 20 років викладає у закладі освіти. Нерідко в закладі освіти затримують зарплату, бо керівник спрямовує кошти з зарплатного фонду на оплату таксі для студентів з інвалідністю. Завдяки цьому вони можуть комфортно доїжджати до закладу освіти». Як змінилися ваші емоції? Усе ще прикро за викладачку, але керівник вже не є винуватцем цієї історії? Чи правильно він вчиняє? Це автори новини залишають на розсуд вам. Отже, уточнення можуть цілком змінити зміст новини. Саме через вплив на ставлення медіа найчастіше нами маніпулюють.

Вплив на настрої дещо перегукується із впливом на ставлення. Але якщо за допомогою ставлення ми наділяємо інформацію певною оцінкою, то вплив на настрої сприяє формуванню емоцій у нас самих. Та медіа не лише

¹ Тут і далі в цьому розділі адаптовано приклади, наведені в онлайн курсі «Години медіаграмотності».

провокують нас на емоції, а й можуть допомогти впоратися зі стресом. Уявіть, що ви переглянули сюжет про ремонт якогось закладу освіти коштом державної субвенції. Керівниця каже: «Тепер кожен заклад освіти може так сплатити за ремонт». Надихає, правда ж? Або ви почули, що зарплати викладачам з великих міст скоротять у 1,5 рази. Погодьтеся, це вже не так весело. Різні новини викликають у нас найрізноманітніші емоції. Почасти ми спеціально шукаємо хороші новини, аби відпочити після роботи чи стресового дня.

Фізіологічний вплив. Медіа та інформація в них можуть впливати на тиск, кровообіг, потовиділення. Тож новини безпосередньо впливають на наше здоров'я. Новини про війну викликать у нас страх, а отже – пришвидшене серцебиття, сильніше потовиділення. А от допис у твіттері про підвищення зарплати поліцейським точно покращить настрій.

Вплив на поведінку та на наші повсякденні дії. Медіа можуть мотивувати до дії або бездіяльності. Згадайте допис Мустафи Найєма у фейсбуці в ніч на 21 листопада 2013 року. Тоді, зокрема і через заклик журналіста, десятки людей вийшли на майдан Незалежності.

Враховуючи значний вплив медіа на нашу життєдіяльність інформаційна безпека безумовно є складовою національної безпеки. Її забезпечення залежить від кожного та кожної з нас. Саме від нас залежить перемога на інформаційному фронті та перемога України у війні з країною-агресором в цілому.

II. ВИДИ МАНІПУЛЯЦІЙ З ІНФОРМАЦІЄЮ.

Чи замислювалися ви, що певний контент має на меті інформувати вас, а інший – намагається переконати?

Інформація містить факти, мета яких – ознайомити нас з певними темами. Автори інформаційного матеріалу мають використовувати лише факти і не додавати до них власних думок і оцінок. Вони мають давати інформацію об'єктивно. Наприклад, репортаж про президентські вибори, який містить їх офіційні результати – це інформаційний матеріал. Якщо з будь-якого питання виникає дискусія, інформаційний матеріал мусить висвітлювати аргументи всіх сторін. Так споживачі матеріалу зможуть зробити власні висновки.

Мета пропаганди та суджень – вплинути на аудиторію та переконати її у чомусь. Головним чином такий контент спирається на емоції та уяву, а тому його автори зазвичай використовують лише ті факти та посилання, які підтримують їхні точки зору. Тобто стаття про вибори президента, в якій підтримується той чи інший кандидат, створена для того, щоб переконати нас.

Чому маніпуляції з інформацією переважно спираються на емоції? Справа в тому, що **емоції заважають критичному мисленню, яке є запобіжником сприйняття неправдивих повідомлень за «чисту монету».** Як не піддатися впливу емоцій? Розвивати свої навички кібергігієни, в тому числі навички медіаграмотності. **Коли ми отримуємо ту чи іншу інформацію перш за все слід для себе визначитись, ця інформація є фактом чи судженням.**

Як відрізнити факт від судження?

Судження – це чиєсь переконання або чиясь точка зору. Докази можуть підтримувати судження, але ви ніколи не зможете довести правдиве це судження чи хибне. Наприклад, твердження про те, що Україна є найкращою країною для відпочинку є судженням.

Факт можна підтвердити або спростувати. Можна довести його правдивість або неправдивість за допомогою доказів: певних статистичних показників, результатів досліджень. При цьому важливо, щоб було вказано джерело походження фактів. Слід враховувати, що констатація фактів також може бути хибною. Наприклад, факт, що населення США становить 1 більйон – це неправда. Він містить інформацію, яку ми можемо перевірити і переконатися, що це неправда.

Судження містять факти та власні думки авторів. Однак ці факти використані не для того, щоб проінформувати нас. Автори вживають їх, щоб підтвердити власні судження. Таким чином вони намагаються переконати нас у чомусь. Судження мають бути відокремлені від новин і автори мають

вказувати, що це їх власна думка. Інформування не повинно містити власних думок авторів, адже його головна мета – повідомляти. Проте новини можуть містити судження інших людей. Наприклад, журналіст може написати: «Це жахлива політика» – сказав експерт Роман Василенко». Роман Василенко висловлює власну думку, однак те, що він зробив таку заяву – це факт. Тому новина, яка містить власну думку Романа залишається новиною.

Деякі видання не розуміють різницю між фактами та судженнями, тому споживачі новин мають самі розуміти, що саме вони читають чи дивляться, аби мати змогу оцінювати інформацію.

Однак судження – це не завжди погано. Вони можуть допомогти нам сформуванню власну точку зору і подумати про різні підходи до проблеми. Важливо розуміти різницю між судженнями і новинами. Адже якщо ми зможемо розпізнати інформацію, мета якої переконати нас, ми зможемо захиститися від маніпуляцій.

При аналізі правдивості інформації слід також аналізувати джерело її висвітлення.

Багато з нас звикли починати свій день з чашки кави та стрічки новин. Але чи задумувалися ви, хто вирішує, що саме ми читатимемо вранці? І як відбувається відбір новин?

Медіа відрізняються за формою власності та способом фінансування. Чому важливо знати, кому належать або хто фінансує медіа, які ти дивишся, читаєш чи слухаєш? Приватні медіа існують у всьому світі. Щоб інтереси власників не заважали об'єктивному висвітленню подій, необхідна чітка редакційна політика. За даними на 2019 рік 10 із 11 українських каналів прямо чи опосередковано пов'язані з політичними діями. Найбільш актуальну інформацію про власників телеканалів та радіо можна перевірити на їх сайтах, інформацію щодо власності газет та інформантств – у Єдиному державному реєстрі юридичних осіб та фізичних осіб - підприємців. Ще один тип традиційних медіа – суспільне мовлення. І хоча його зазвичай фінансує держава, редакційна свобода – основний фактор, який відрізняє суспільне мовлення від інших державних медіа.

Довкола нас щодня відбувається набагато більше подій, ніж медіа можуть висвітлити. Тому інформацію потрібно відфільтровувати, щоб глядачі та читачі отримували лише актуальні новини. Існує багато складних факторів, що впливають на те, які новини ми отримуємо та які з них запам'ятаємо. Якщо ми знаємо про них, ми краще розуміємо, що ми бачимо і чому. Одним із них є рішення редакції, на яке впливає багато факторів: чого хочуть читачі або слухачі; що медіа має право висвітлювати; про що вже говорили раніше; про що наразі говорять інші медіа тощо.

Стандарти журналістики ґрунтуються на наступних засадах:

- надійність джерела інформації
- баланс думок і поглядів
- повнота фактів та інформації
- відокремлення фактів від суджень
- достовірність матеріалу

Головною метою всіх новин у медіа має бути інформування. Підготовка всіх журналістських матеріалів має містити етап фактчекінгу (англ. *fact checking* – *перевірка фактів*), щоб перевірити правдивість інформації.

Згідно з Кодексом етики Спільноти професійних журналістів, один з головних принципів журналістики – перевірка інформації з використанням декількох джерел. Однак журналісти не завжди дотримуються цього правила. Через необхідність швидко опублікувати матеріал, брак досвіду чи розуміння, автори нехтують ретельною перевіркою. Іноді журналісти створюють і поширюють неправдиву інформацію навмисно, а іноді – через брак професійної компетентності чи незнання Кодексу Етики.

Однак, історії, які ми читаємо, дивимося і слухаємо – це не лише результат вибору редакторів. Ми всі відповідальні за новини, які споживаємо. Слід враховувати, що вебсайти та соціальні медіа використовують алгоритми. З огляду на нашу попередню історію пошуку, «подобається» та «поділитися», ці алгоритми пропонують нам те, що, на їхню думку, нас цікавить. У такий спосіб ми потрапляємо в інформаційну бульбашку, тобто отримуємо лише ту інформацію, яка підтримує наші погляди.

Сьогодні за один день ми отримуємо більше інформації, ніж люди в 15 столітті отримували впродовж життя. Наприклад, лише століття тому людина за все життя могла прочитати лише 50 книг. Згідно з дослідженням Мартіна Гілберта у 1986 році людина за день отримувала об'єм інформації, який можна було помістити у 40 газет. У 2007, завдяки Інтернету та легкому доступу до телебачення, кількість інформації значно збільшилася: інформація, яку людина отримувала щодня, помістилася б у 174 газети.

Як і будь-яка глобальна система, медіасередовище – забруднене. У нашій інформаційній екосистемі є безліч неякісної, неправдивої інформації, яка погіршує нашу здатність конструктивно спілкуватися одне з одним, дестабілізує та поляризує суспільство. Іноді мета неправдивого контенту – підвищити відвідуваність вебсайту, розпочати дискусію чи спровокувати конфлікт у коментарях. Такі коментарі використовують для формування громадської думки в соціальних мережах, тобто ставлення людей до певної

події, особи чи країни. Деяка інформація в медіа може бути створена, щоб зашкодити, ввести в оману або просто задля розваги. Доцільно навчитись розрізняти типи маніпулятивного контенту в своєму медіапросторі.

Здатність визначати та аналізувати неправдиву чи неточну інформацію – в важлива навичка у XXI столітті. Існують багато різних видів маніпуляцій з інформацією. Зробимо короткий огляд найбільш розповсюджених з них.

Дезінформація.

Цей тип неправдивої інформації створюють спеціально, щоб завдати шкоди особі, соціальній групі, організації чи країні.

Якщо люди поширюють неправдиву інформацію, вони часто вірять у те, що поширюють. Дезінформацію ж створюють і поширюють навмисно, щоб ввести в оману інших. Часто трапляється, що неправдива інформація з наміром зашкодити перетворюється на інформацію без такого наміру. Наприклад, якщо політик стратегічно поширює неправдиву інформацію у формі статей, фото, мемів – це неправдива інформація з наміром зашкодити.

Більшість дезінформації ґрунтується на методі напівправди, коли брехню поєднують з правдою, щоб неправдива інформація здавалася більш достовірною. Цей тип неправдивої інформації часто цитує «очевидців» та різні «дослідження», які можуть бути повністю сфабриковані. Іноді дезінформацію ретельно розробляють спеціалісти та політтехнологи, щоб схилити громадську думку на користь чогось чи когось або посіяти сумнів чи суперечки.

Деякі люди створюють дезінформацію, щоб певне пояснення чи інформація здавалися сумнівними, коли насправді це не так. Наприклад, згадайте літак компанії Malaysia Airlines на рейсі МН17, який збили у 2014 році. Російські медіа запропонували безліч неправдивих гіпотез, щоб пояснити катастрофу: літак збила українська ракета «Бук» або український винищувач; українці думали, що МН17 – особистий літак путіна і спробували вбити його; це був літак на радіокеруванні, на борту якого були вже мертві пасажери; катастрофу спричинили місцеві сепаратисти, які використовували зенітні ракети. Головна мета – не примусити людей повірити в одну з цих суперечливих гіпотез, а викликати сумніви щодо того, що дійсно могло статися, та відвернути їхню увагу від доказів, що літак збила ракета російських військових.

Центр протидії дезінформації Ради національної безпеки і оборони України періодично публікує дайджести з прикладами дезінформації, яка поширюється мережею та з поясненням мети такою дезінформації.

Цензура.

«Кожен запис було знищено або підроблено, кожну книжку – переписано, кожну картину – перемальовано, кожну статую та будівлю – переіменовано, кожну дату – змінено. І цей процес триває день за днем, хвилина за хвилиною. Історія зупинилася. Нічого не існує, крім безкінечного тепер, у якому Партія завжди має рацію». Так описує Міністерство правди Джордж Орвелл у своєму романі-антиутопії «1984». Незважаючи на назву, це Міністерство не має нічого спільного з правдою. Воно переписує минуле, коли потрібно пристосувати його до існуючої доктрини партії. А також змінює записи, якщо передбачення Великого Брата, верховного правителя, та його уряду не здійснюються. Так Великий Брат завжди має рацію. Це – версія світу без свободи преси Джорджа Орвелла.

З 2002 року міжнародна організація «Репортери без кордонів» (Reporters Without Borders (RSF)) щорічно публікує рейтинг – «Індекс свободи преси». Для цього рейтингу організація використовує власну оцінку рівня свободи преси у різних країнах, яка ґрунтується на даних за рік. У 2021 році до рейтинга ввійшли 180 країн. Серед країн з найвищим індексом свободи преси – Норвегія, Фінляндія та Швеція. Тут журналісти зазнають значно менше політичного тиску та цензури, ніж в інших країнах. Крім того, право власності на медіа регулює закон. Україна посіла 97 місце у цьому рейтингу.

Найнижчі місця у рейтингу посідають Туркменістан, Північна Корея, Еритрея та Китай. У цих країнах існують окремі закони, які забороняють поширювати ідеї та критикувати уряд. Наприклад, багато вебсайтів, зокрема Google, Facebook, Instagram та YouTube, заблоковані у континентальному Китаї. Усі вони підлягають під політику Інтернет-цензури, головна мета якої – попередити колективні дії, наприклад, протести та розповсюдженню порнографії, а також критиці уряду, політики та спірних національних питань.

Клікбейт.

Заголовок – найважливіший елемент будь-якої статті чи відео. Його головна мета – привернути увагу аудиторії та спонукати її прочитати чи проглянути матеріал. Саме тому журналісти та редактори часто використовують у своїх заголовках елементи драми та сенсації, наголошуючи на аспектах новин, які, на їхню думку, зацікавлять цільову аудиторію. Заголовок може також містити зображення, щоб підсилити емоційний вплив. Нашестя, обурення, сенсація дня, терміново – усі ці слова привертають увагу читачів та змушують їх переходити за посиланням. Це називається **клікбейт** (англ. *clickbait*, від *click* «клацання» та *bait* «наживка»).

Сатиричне онлайн-видання *The Science Post* опублікувало статтю з назвою «Дослідження: 70% користувачів Facebook читають лише заголовки наукових статей перед тим, як коментувати». Перший абзац статті написаний

англійською. Однак другий абзац – це стандартний текст *lorem ipsum* – варіант умовного беззмістовного тексту, який використовують графічні дизайнери у своїх макетах. Статтю поширили понад 194 400 користувачів².

Сатирична стаття привернула увагу багатьох науковців, оскільки вона допомогла дослідити поведінку тих, хто читає новини в соціальних мережах. Науковці з багатьох дослідницьких центрів США проаналізували 2,8 мільйонів ретвітів та з'ясували, що 59% ставлять «подобається» та поширюють посилання, навіть якщо самі не переходили за ним.

Скоріш за все, ви не раз помічали рекламні банери, з заголовками типу:

- *«Ти схуднеш на 10 кг за тиждень, якщо перед сном випиватимеш...»*
- *«Ванга передбачила, що до 2020 року з планети зникнуть всі...»*
- *«Ви не повірите, але це ...»*
- *«Те, що відбулося далі, ШОКУЄ вас ...».*

Такі заголовки спокушають аудиторію клікати на посилання і переходити на сайти, де відповідей на ці запитання точно не знайти. Перейшовши за посиланням, ви потрапите на якийсь сумнівний сайт, а інформація, яка вас зацікавила, виявиться або пустушкою, або цілковитим маренням. При створенні таких ось приманок, зазвичай використовують теми пов'язані з відомими особистостями. Так само добре працюють картинки провокаційного характеру та мають відношення до актуального інформаційного приводу.

Часто статті з такими заголовками містять ще й зображення, які суперечать змісту або заголовку. Їхня мета – збентежити читачів ще більше, щоб вони перейшли за посиланням. Але навіщо все це вигадали? Онлайн-медіа отримують значну частину свого прибутку з реклами. Що більше користувачів вони мають на своїх вебсторінках, то більше рекламодавців хочуть розміщувати там свої оголошення. У такий спосіб прибуток власників медіа збільшується.

Фейк.

Фейк – це:

-  подання фактів у спотвореному вигляді або свідомо неправдивої інформації;
-  сфабрикована інформація, що не відповідає дійсності;
-  повідомлення про щось, що ніколи не відбувалось.

Зазвичай фейки складаються з частково правдивих фактів або замасковані під реальну новину.

² Дані наведені станом на квітень 2022 року.

Ознаки, які можуть вказувати на фейк наведені у таблиці нижче.

Джерела	Експерти
➤ відсутність джерел інформації ➤ анонімні джерела ➤ інформацію взято із неперифікованих акаунтів у соцмережах ➤ покликання на підозрілі або маловідомі джерела	➤ представники структур, яких насправді не існує ➤ експерти без вказування інституцій, які представляють ➤ анонімні експерти («вчені вважають...») ➤ політично заангажовані експерти
Емоції	Подання інформації
➤ думку чи оцінку подано як факт ➤ заголовок занадто емоційний або не відповідає новині ➤ журналісти вживають слова, що викликають позитивні / негативні емоції ➤ навішування ярликів, поширення стереотипів	➤ соціологічні дані без вказання вибірки, замовника, географії тощо ➤ однобоке подання фактів, оцінок і коментарів, узагальнення ➤ викривлене подання новини: реальні факти подають з неправдою ➤ неправдиві фото чи відео подають як підтвердження інформації

Фейки бувають невинними. Їх створюють заради популярності та підписників. Часом таким займаються онлайн-ЗМІ: заради більшої кількості кліків, а отже, грошей від реклами.

Приклади:

- 1) У соцмережах просять поширити інформацію про перемогу на конкурсі чи змаганнях;
- 2) У маленькому українському містечку побачили нереально багато веселок.

Пам'ятайте: може виявитися, що сторінка, на яку ви підписалися завдяки фейку, почала просувати якогось політика або товар. Ви завжди можете від неї відписатися.

Іноколи фейки пов'язані з життям (чи смертю) відомих людей. Як от, смерть акторів.

Фейки здатні змінювати життя цілих країн, можуть призвести до справжньої ворожнечі та людських смертей.

Як фейкові новини можуть змінювати минуле та спогади?

У 2010 році журналісти видання Slate вигадали п'ять подій з історії США, а потім запитали своїх читачів, чи пам'ятають вони ці події. Виявилось, що в середньому майже 27% читачів сказали, що пригадують одну з фейкових історій і вважають її справжньою.

Як швидко поширюються фейки? І які поширюються найкраще?

Фейки поширюються у **шість разів** швидше за правду. Про це йшлося в дослідженні, опублікованому в березні 2018 року в журналі Science. Дослідники взяли масив даних правдивих та фейкових повідомлень у Твіттері за період з 2006 по 2017 рік. А це – більше 100 000 історій, які були поширені 4,5 млн разів. Виявилось, що фейкові історії більше подобаються користувачам та краще поширюються. В результаті виявилося, що фейк може стати віральним і без допомоги ботів. Головний висновок цього дослідження невтішний: **правда не може конкурувати з фейковими новинами**. Люди також схильні активніше поширювати інформацію, що містить емоцію злості. До такого висновку дійшли дослідники китайського аналогу Твіттеру – соцмережі Weibo. Вони виявили, що погане люблять поширювати більше, ніж хороше.

Ще один тип маніпуляції з інформацією – несправжні, або **фейкові, фото**. Існує 3 види маніпуляцій з фото:

-  справжнє фото місця чи людини, яке використовують як зображення зовсім іншого місця чи особи, або для маніпуляції з підписом до фото;
-  підроблені фото, змінені у графічних редакторах (наприклад, Photoshop), щоб додати або прибрати певні елементи;
-  обрізані фотографії, які показують лише частину зображення без контексту.

Справжнє фото місця чи людини, яке використовують як зображення зовсім іншого місця чи особи, або для маніпуляції з підписом до фото.

Іноді фотографії можуть бути неправильно підписані, щоб посилити емоційний вплив на читачів. Наприклад, ось це фото – оригінальне, але підпис – не що інше, як маніпуляція. Адже він створює враження, що українського солдата врятував від кулі його телефон. Під час обговорення цього фото користувачі навіть хотіли зібрати гроші на новий телефон для солдата.

Фото із жахливими кадрами, де люди прячуться від атаки країни-агресора під мостом Ірпеня, деякі блогери видавали за свідчення зриву гуманітарного коридору в Маріуполі.

Фото, яке поширювалось соціальними мережами України під час пандемії COVID-19. Перевірка фото за допомогою спеціального інструменту

Google для пошуку зображень, свідчить, що дівчина на зображенні публікації не є українкою, вона є відомою порноакторкою.

Тобто автори фейкової публікації використали фото сторонньої людини із мережі, при цьому обрали молоду дівчину для того, щоб більше вплинути на емоції читачів.

Під час російсько-української війни у соцмережах поширювалось фото та відео врятованих сиріт. Ці матеріали супроводжувались закликом «швидко всиновити» та про готовність влади України передавати дітей-сиріт у «добрі руки. Центр протидії дезінформації при РНБО України спростував цей фейк та пояснив, що він розрахований зробити з тих, хто готовий взяти дитину, у кращому разі – жертву шахраїв, у гіршому – порушників українського законодавства. Адже торгівля, передання або одержання дитини підпадають під дію ст.146 Кримінального кодексу України і караються позбавленням волі на строк від 5 до 12 років.

Підроблені фото, змінені у графічних редакторах (наприклад, Photoshop), щоб додати або прибрати певні елементи.

На фото, яке набуло популярності в мережі – український солдат, який обіймає дівчину біля потяга. Фото мало підпис «Боець АТО проводить свою дівчину до Москви».

За допомогою зворотного пошуку зображень можна знайти те саме фото, проте знак на потязі інший – «Харків – Ужгород».

Ще один сервіс для пошуку зображень TinEye знаходить це ж фото на форумі ще у 2016 році. Коли журналістам вдалося відшукати юнака з фотографії, він був обурений такою маніпуляцією. Він сказав, що фото зробили, коли він їхав з Харкова у Тернопіль. Колишнього бійця АТО допоміг ідентифікувати волонтер.

Як з'ясувалося, це колаж, створений у Photoshop. Фотографії, які використали для цього, можна легко знайти за допомогою зворотного пошуку зображень.

В 2014 році сотні російських, а згодом і українських видань, поширили інформацію про жертв на окупованих територіях України, яку підтвердили за допомогою фото з фільму «Брестська фортеця», події якого відбуваються під час Другої світової війни.

Намагаючись виправдати свій військовий напад на Україну, країна-агресор вдається до продукування фейків про ніби то наявну інформацію, що Україна готувалась до військового взяття Криму. На підтвердження цього були навіть створені фейкові фото медалі «За взяття Криму» та посвідчення до неї.

Однак критичний аналіз представленого на фото посвідчення дозволяє спростувати даний фейк. По-перше, Президент України видає не накази, а

укази. По-друге, українською мовою ініціали Президента України не В.А., а В.О. – Володимир Олександрович.

Обрізані фотографії, які показують лише частину зображення без контексту.

Іноді фотографії, змінені у такий спосіб, вважають фейком. Адже суть того, що вони зображають, може бути повністю змінена.

Згідно з AFP Factcheck, «десятки тисяч людей поділилися твітом з двома фото з антиурядових протестів «жовтих жилетів» у Парижі 2018 року, з підписом "Перспектива має значення».

Це порівняння демонструє, як кутом, з якого зроблене фото, і композицією фотографії можуть маніпулювати в медіа, щоб додати драматизму незначній події. Однак два фото з прикладу – теж маніпуляція. Їх зробили в різний час та в різних місцях.

Якщо у вас виникли сумніви щодо правдивості відео, зверніть увагу на його **якість**. Підозріле відео може мати різні формати: десь кадр ширше, десь навпаки – квадрат. Варто звернути увагу й на **озвучку**. Адже текст, який супроводжує відео, може суттєво впливати на наше сприйняття.

Також важливо дізнатися, хто **автор каналу**, на якому опубліковане відео. Краще не довіряти відео, якщо канал виглядає підозріло. Наприклад, немає аватарки конкретної людини або організації, опису каналу, посилань на офіційний сайт чи інші соціальні медіа.

Якщо ви натрапили на популярне відео, але сумніваєтеся, що воно справжнє, **зверніть увагу на коментарі**. Цілком можливо, що хтось вже його спростував. Також можна пошукати ролик за ключовими словами і побачити, чи є інші варіанти відео.

Пам'ятайте, що будь-яке відео – це набір світлин. Отже, можна робити скріншоти й перевіряти їх як фото.

У липні 2017 року дослідники університету Вашингтону навчилися створювати відео, у яких Барак Обама відкривав рот так, щоб відповідати вхідній звуковій доріжці. Тобто на відео Обама міг говорити будь-який запрограмований текст. Така технологія дозволяє штучному інтелекту вчитися на основі існуючих відео. А потім – замінювати практично будь-яке обличчя у відео на потрібне. Ці фальшиві відеоролики називаються **deepfakes** (глибокі фейки) та є потужним інструментом дезінформації.

Пропаганда.

Пропаганда – це упереджена чи оманлива інформація, спрямована на поширення певної точки зору та зміну моделей поведінки. Пропаганда

небезпечна не лише масовим поширенням неправдивої інформації, а й спрямованістю на спонукання її споживачів до певних дій.

Пропаганда є інструментом інформаційного впливу. В його потужності переконались українці, які під час російсько-української війни намагались донести до своїх родичів та знайомих, які проживають в РФ, правду про події в Україні.

Для поширення пропаганди застосовуються державні інструменти: державні органи, державні медіа, спецслужби, «зливні бачки», боти, тролі, групи у соцмережах тощо. Вплив пропаганди особливо посилюється при наявності цензури в країні, оскільки в такому разі відсутні альтернативні джерела інформації.

Характерні риси пропаганди:

-  частий повтор
-  створення великої кількості майданчиків, які повторюють тези
-  у деталях ці тези можуть відрізнятися, але суть повідомлень одна й та сама.

Психологиня Елізабет Лофтус з Каліфорнійського університету ще з дев'яностих досліджує формування фальшивої пам'яті. Вона – одна з авторів концепту **«ефекту хибної інформації»**. Цей ефект з'являється, коли людина намагається щось пригадати. Спогади стають менш точними, конкретні епізоди спотворюються, тому що з'являється інформація після події, пост-фактум. Вона змінює наше сприйняття минулого, і, як наслідок, – самі спогади. Це явище вказує на сугестивність та помилку атрибуції пам'яті:

- **сугестія** – це навіювання або піддатливість. Тобто, нашу пам'ять можуть трансформувати інші люди та соціальні очікування, коли ми несвідомо підлаштовуємось під вимоги та звички суспільства.
- **помилка атрибуції пам'яті** – це наша здатність пам'ятати саму інформацію, але помилятися щодо джерела її походження.

Мета пропагандистів – отримати від нас потрібну поведінку. При чому людина, яка стала жертвою маніпуляції, вважає, що діє за власним бажанням і за власним вибором.

Експертна думка.

Медіа можуть використовувати думки несправжніх експертів, іноді навмисно, а іноді – випадково.

Висловлювання, оцінки та прогнози експертів з сумнівною репутацією завжди слід перевіряти в Інтернеті. Пошук експерта чи організації може показати, що про них майже немає інформації онлайн. Так звані «експерти» можуть не бути представниками респектабельних установ чи аналітичних

центрів. Навпаки, вони можуть співпрацювати з організаціями, які належать політикам або політичним угрупованням. Висловлювання таких експертів потрібно сприймати скептично, оскільки може виявитися, що вони не є експертами взагалі, а їхні прогнози чи оцінки – сфабриковані.

30 вересня 2014 року «Российская Газета» опублікувала інтерв'ю з удаваним латвійським політиком на ім'я Ейнарс Граудіньш. Його відрекомендували як латвійського правозахисника, який разом з групою експертів Організації з безпеки та співробітництва в Європі (ОБСЄ) відвідував місця масових поховань в Україні. Він заявив, що 400 тіл знайшли похованими поблизу Донецька. Тим часом RIA Novosti та Vesti.ru представили Ейнарса Граудіньша експертом ОБСЄ. ОБСЄ виступила з заявою, що такого експерта в моніторинговій місії в Україні не було.

Тому, якщо маєте можливість, перевіряйте експертів в Інтернеті. Ось на що варто звертати увагу:

- ✚ освіта та кар'єра. Пошукайте його онлайн або просто погугліть, чим займався експерт раніше, скільки працює в сфері. Також варто поцікавитися освітою експерта.

- ✚ місце роботи. Навіть якщо на Фейсбук-сторінці експерта вказаний дослідницький центр, не факт, що такий заклад дійсно існує. Або що в цьому аналітичному центрі працює ще хтось крім самого експерта. Погугліть! Досить часто експертами називають тих, хто працює у великих компаніях, а не дослідницьких центрах. Вчитель може виступити експертом з питань освіти. Або лікар може прокоментувати медичну реформу. Потрібно розуміти, що думка лікаря або вчителя у таких випадках може бути досить суб'єктивною. Це варто враховувати.

- ✚ власники дослідницьких організацій. Прозорість структури власності та фінансування дуже важливі. Більшість дослідницьких центрів в Україні отримують фінансування з чотирьох джерел: грантові кошти, державні замовлення, замовлення аналітики від бізнесу, благодійні внески населення.

- ✚ наукові дослідження або статті. Справжні експерти досить часто працюють у дослідницьких центрах, мають наукові ступені, вчені звання та пишуть дослідницькі роботи. Якщо експерта цитують у західних наукових роботах або його роботи публікують у великих наукових журналах, його роботи можна знайти на сайті Google Scholar.

- ✚ коло експертних тем. Що кращий експерт, то вужче коло тем він або вона коментують. Експерти, які цінують свою репутацію, завжди відмовляються коментувати тему, яку вони не знають або знають поверхово.

- ✚ крос-чек. Якщо ви погано знаєте тематику, яку коментує експерт, перевірити буде важко. Але спробуйте знайти у його промовах або колонках

те, про що ви знаєте або чули. Або інформацію, яку можете перевірити в гуглі. Така точкова перевірка може показати, наскільки гарно експерт працює з даними та знає фактаж. Іноді корисно перевірити терміни, числа або висновки, які використовує експерт.

✚ Риторика та категоричність. Хороші експерти завжди обережно роблять висновки, намагаються представити всі можливі точки зору та взяти до уваги всі можливі фактори. Експерти працюють зі складними даними. Ймовірніше, вони назвуть багато різних факторів, які впливали на певний показник або явище. Але точно не скажуть щось просте та категоричне. Тому що гарний експерт – обережний у висновках і розуміє, що несе відповідальність за свої слова, адже вони можуть вплинути на життя багатьох людей.

Прихована реклама / Джинса

Медіа повинні дотримуватися балансу між своїми комерційними інтересами та дотриманням стандартів журналістики. Іноді ці поняття змішуються, правила – порушуються і, як результат, аудиторія отримує джинсу – рекламу, замасковану під журналістський матеріал.

Прихована реклама, або джинса, спотворює відображення важливих соціальних явищ та подій. Ми отримуємо неточну та маніпулятивну інформацію, за публікацію якої редактори отримали гроші, але презентували її як новину, а не рекламу. Наприклад, фармацевтична компанія може заплатити виданню за публікацію матеріалу, у якому йдеться про неймовірну користь їхнього нового вітамінного комплексу.

Важливо фільтрувати, що ми бачимо і чуємо, та вміти відрізнити якісну журналістику від маніпулятивного контенту.

Як розпізнати приховану рекламу?

✚ опублікований матеріал не містить жодної прив'язки до місця і часу. Запитайте себе: «Чому цей матеріал опублікували саме зараз?»

✚ використання соціологічних досліджень сумнівних організацій, результати яких зазвичай дуже відрізняються від інших соціологічних досліджень.

✚ псевдоаналітичні матеріали маловідомих авторів, яких позиціонують як «політологів», і які дають «експертну» оцінку певної події з позиції, яка вигідна одному з політичних угруповань. Це може бути ознакою прихованої реклами, але не завжди.

✚ один зі стандартів журналістики – дотримання балансу думок. Тому надмірно позитивний або гостро негативний матеріал може бути ознакою прихованої реклами.

✚ деякі журналісти можуть співпрацювати з політиками чи політичними партіями. Тому багато новин містять їхні коментарі, хоча вони не є експертами. Або ж у новинах можуть згадувати про «своїх» кандидатів, навіть якщо події ніяк їх не стосуються.

✚ матеріали без автора: доволі часто журналісти не хочуть залишати своє ім'я під джиною, тож багато матеріалів публікують без підпису або під псевдонімом. Якщо матеріал здається підозрілим, спробуйте знайти інші публікації цього автора на вебсторінці або в газеті. Ви можете скопіювати та вставити абзаци з цього матеріалу в пошуковик та перевірити, чи фігурує він ще десь.

Маніпуляція фактами / маніпуляція джерелом.

Уявіть ситуацію, коли одна людина стверджує, що йде дощ, а інша – заперечує це. Кому б ви повірили? Звісно, ви б просто подивилися у вікно та перевірили, хто має рацію. Це називається перевіркою джерела – ми звертаємося до першоджерела інформації, до первинних документів або до людей, які були присутні під час події.

Першоджерелами можуть бути:

- ✚ офіційні пресрелізи урядових та судових органів, місцевих органів влади та міжнародних організацій;
- ✚ офіційні листи, звернення та запити на інформацію;
- ✚ повідомлення з місця подій (без редагування та коментування);
- ✚ офіційні вебсторінки організацій;
- ✚ люди, особисто причетні до події, зокрема свідки.

Якщо ви не можете визначити першоджерело, слід обережно ставитися до запропонованої інформації. Саме журналісти та редактори несуть відповідальність за достовірність інформації в матеріалах, які вони публікують або транслюють. Іноді вони нехтують правилом перевіряти інформацію за допомогою щонайменше двох джерел. Це відбувається з різних причин. Наприклад, через необхідність опублікувати матеріал якомога швидше, недостатню фахову підготовку чи розуміння, або навіть просто через недоступність джерел. Часто журналісти посилаються на інші медіа щодо інформації, яка стосується певної історії. Професійні і чесні медіа для посилення на ці первинні джерела використовують фрази на зразок «як повідомляє Reuters» або «згідно з Укрінформ». Онлайн-медіа зазвичай додають посилення на джерело, щоб читачі мали змогу звернутися до нього. Зауважте, що іноді необхідно шукати далі, адже джерело інформації, на яке посилаються, могло отримати інформацію з іншого джерела. Продовжуйте пошуки, доки не знайдете оригінальне першоджерело.

Коли стається щось надзвичайне, ймовірно, що багато медіа повідомлять про це. Журналісти використають свідчення очевидців та матеріали «з перших рук» (наприклад, відео з телефонів). Якщо ви читаете про подію, яка справді здається дивовижною, але через декілька годин пошуків не можете знайти кадри з місця подій чи інші докази, сприймайте цю інформацію скептично та не поширюйте її.

Іноді медіа оприлюднюють інформацію з посиланнями на анонімні джерела. Це може статися через різні, цілком обґрунтовані причини. Найчастіше, через особисту безпеку. Або внаслідок того, що деякі особи не мають права публічно говорити на певні теми. Але навіть якщо ці причини виправдані, інформацію з анонімного джерела неможливо перевірити. У такому разі подумайте, чи має причина замовчування джерела сенс у контексті запропонованої інформації.

На що ще слід звернути увагу під час перевірки видання:

-  чи є контактні дані видання на вебсторінці або посилання на активні соціальні мережі;
-  як довго це видання існує;
-  звідки видання отримує фінансування;
-  чи є ім'я автора під статтею або відео;
-  чи є на вебсторінці інші статті цього автора³.

³ Більше інформації про інструменти перевірки джерела інформації міститься у наступному розділі.

III. ІНСТРУМЕНТИ ВИЯВЛЕННЯ НЕПРАВДИВИХ ПОВІДОМЛЕНЬ.

Для перевірки повідомлень та інших матеріалів на предмет їх актуальності та достовірності можуть бути використані різні аналітичні методи. Для полегшення цього процесу також варто застосовувати і низку технічних рішень.

➤ Перевірка джерела інформації, власника медіа, фото.

В Україні однією з потужних фактчекерських організацій є проект **StopFake**. Його команда викриває фейки РФ й поширює спростування тринадцятьма мовами.

Перевірку інформації в онлайні можна почати із сервісу **ICANN**, який допомагає з пошуком реєстраційних даних, за допомогою яких можна зрозуміти, хто створив сайт, коли й коли його планували закрити.

Для перевірки фото можна використовувати наступні сервіси:

 **RevEye Reverse Image Search** (встановити у браузері Chrome) – допоможе шукати фотографію в різних пошуковиках;

 **TinEye** – дозволяє побачити зміни у фотографії та дізнатися, коли зображення опублікували вперше;

 **Fotoforensics** – підійде для аналізу зображень та покаже, які частини фото однорідні, а які значно відрізняються, отже, найімовірніше, були відредаговані. Тобто, ви зможете побачити об'єкти, що додали або домалювали до основного фото.

 **ImgOps** – допоможе розібратися з метаданими фото.

 **Deepfake detection** – це інструмент, який дозволяє виявляти підробку у різних мультимедійних файлах. Для використання цього продукту достатньо перейти за вказаним посиланням **<https://platform.sensity.ai/deepfake-detection#>**, авторизуватися. Після цього стають доступними функції завантаження мультимедійного документа для перевірки.

Зображення можуть не мати ознак маніпуляцій, проте використовуватися у неправдивих повідомленнях у різних контекстах.

 **Who stole my pictures** – для того, щоб знайти першоджерело відповідних малюнків. Завантажити описане розширення можна за адресами:

- для браузера «Chrome» (<https://chrome.google.com/webstore/detail/whostole-my-pictures/mcdbnfhkikiofkkicppioekloflmaibd>);
- для браузера «Firefox» (<https://addons.mozilla.org/ru/firefox/addon/who-stolemy-pictures/>).

 **Пошук Google** (<https://images.google.com>) – дозволяє знайти схожі зображення. Так, наприклад, за допомогою даного сервісу знайдений оригінал фото, з якого був зроблений фейк про Королеву Великобританії, вдягнену в українську вишиванку. Пам'ятайте, що результати пошуку розташовуються не в хронологічному порядку, тому для пошуку оригіналу фото слід знайти найдавнішу дату.

AnalogExif (<https://sourceforge.net/projects/analogexif>) – утіліта, яка дозволяє перевірити метадані (дата, координати місця створення тощо) фото.

 **FactCheck** (<https://www.factcheck.org/>) – проект Центру публічної політики Анненберга Університету Пенсільванії, який прагне знизити рівень обману та плутанини в політиці та спростовує неправдиві повідомлення в медіа.

 **Проект «По той бік новин»** - спростовує побутові та щоденні фейки та маніпуляції.

 **Проект «Тексти»** – база псевдосоціологічних служб та прихованих піарників.

 **Webmii** (<https://webmii.com/>) – пошук згадок та посилань на особу в інтернеті, допомагає визначити несправжні облікові записи.

 **Bigmir** – сайт, який дозволяє перевірити рейтинг видання.

 **Exifdata** – показані мета-дані фотографій: дата та час зйомки, витримка, фокусна відстань, роздільна здатність, камера, на яку зробили фото, інші технічні параметри. Професійний фотограф зможе зрозуміти як саме робили світлинку.

 **<https://texty.org.ua/d/2018/mnews/>** – українське незалежне медіа «Тексти» провело дослідження і підготувало рейтинг суперечливих засобів масової інформації.

 **Чат-бот «ПЕРЕВІРКА»** – бот для перевірки сумнівної інформації та новин від українських журналістів.

 **Нотаєнота** – аналізує та спростовує або підтверджує розповсюджену у медіа інформацію, яка викликає суспільний резонанс.

 **Як не стати овочем** – волонтерський просвітницький проект з інформаційної гігієни.

 **EU vs Disinfo:** онлайн ресурс з базою дезінформації та її аналітикою

Базові навички фактчеку та критичного мислення.

1. Джерело інформації. Дізнайтеся, звідки пішла інформація. Визначте, яке видання першим про це написало. Якщо перед вами сумнівна новина або стаття, спробуйте **перевірити інформацію** у великих інформаційних агенціях або виданнях. Якщо ж ідеться про новину, написану на основі анонімних джерел, перевірити цю інформацію буде важко. Тому краще її не поширювати, доки інформація не підтвердиться з офіційних джерел.

Фейкові новини часто розповсюджують маленькі інтернет-ресурси, за якими стоїть невідомо хто. Якщо ви натрапили на новину з невідомого сайту і готові в неї повірити, почніть з назви та адреси ресурсу. Якщо назва схожа на назву відомого видання, можливо, це медіа створене саме для його дискредитації. А також – щоб ввести в оману людей, які не уважно читають. Адже коли назва та дизайн схожі, можна й не помітити, що це інший ресурс.

З точки зору якості контенту, краще, якщо медіа працює багато років, а не кілька місяців. Цю інформацію можна знайти під час перевірки домену. Втім, бувають нові медіа, яким можна довіряти. У цьому випадку важливу роль відіграють редактори та журналісти видання. Якщо вони давно працюють на цьому ринку і мають гарну репутацію, то найімовірніше, будуть відповідально ставитися і до якості нового медіа.

Важливо звернути увагу на інформацію про сайт, чи є розділ «Про нас» і скільки там інформації. Краще, якщо там є відомості про засновників, тих, хто працює на сайті, теми видання.

Наприклад, публікації на сайті видання UaReview виглядають досить правдивими. Проте наприкінці інтернет-сторінки можна знайти інформацію «Про сайт», де зазначено, що UaReview – сатиричне онлайн-видання, що публікує вигадані новини українською. Тобто саме видання позиціонує себе як таке, що публікує неправдиві повідомлення.

Однак деякі видання, не дотримуючись правил перевірки інформації, роблять перепости їх публікації. Так, ми можемо побачити, що саме публікація UaReview є першоджерелом, оскільки новина публікована 23.06.2021, а публікація у іншому виданні – 24.06.2021.

Ось чому важливо шукати та аналізувати першоджерело інформації.

2. Емоційна мова та лексика. Це правило стосується заголовку, тексту новини або посту. Якщо лексика емоційна, викликає обурення або, навпаки, позитив – **дуже ймовірно, що перед вами неправдива інформація**. Відповідно до стандартів журналістики, **заголовки та статті мають бути нейтральними** та подавати сухі факти. Що більше емоцій викликає

заголовок або текст, то більша ймовірність, що вам намагаються нав'язати недостовірну інформацію. Думки в журналістських матеріалах можуть давати тільки експерти. Журналіст може висловити власну думку лише в авторській колонці, але не в статті, навіть якщо вона аналітична. Завдання журналіста — показати факти та ситуацію з усіх можливих сторін, дозволити читачу самостійно зробити висновки.

Приклади емоційних фраз: сумновідомий, одіозний, так званий, погано пахне, викликає сумніви. А ще – фрази, виділені капслоком: ШОК! СЕНСАЦІЯ! НАЙБІЛЬША ПРАВДА, ВАШЕ ЖИТТЯ ЗМІНІТЬСЯ, КОЛИ ВИ ДІЗНАЄТЕСЬ ЦЕ!

Зверніть увагу на словосполучення: «експерти вважають», «джерело в Адміністрації Президента», «чиновник в Міністерстві фінансів», «депутат, який брав участь в обговоренні», тощо. Якщо журналіст спілкувався з експертами або представниками влади, то обов'язково наведе їхні цитати та імена.

Під час фактчекінгу вимикати емоції, постійно ставити додаткові запитання до теми, не шкодувати часу й використовувати всі засоби та інструменти для перевірки одного факту.

3. Дата публікації. Часто під виглядом новини нам подають «старини» – новини, які були актуальними багато років тому. І можливо навіть в іншій країні. Доволі часто це відбувається, коли фото до публікації містить слова «Сьогодні», «Терміново» і т.д., тому слід звертати увагу на дату публікації, а не лише на текст.

4. Відповідність дійсності, критичне мислення.

Два основних правила інформаційної гігієни:

- 1) не «лайкайте», якщо не прочитали матеріал;
- 2) не поширюйте сумнівну інформацію.

Якщо ви впевнені, що сайту можна довіряти, за матеріалом стоїть конкретна людина, а написана інформація пройшла хоча б базовий фактчек, можна поділитися нею з друзями та колегами. Якщо ви помилились, варто визнати помилку, заявити про неї і написати правду.

При пошуку та перевірці інформації варто користуватись ключовими словами, часовими рамками та операторами.

Заходи протидії неправдивим повідомленням:

Державні ініціативи:

➤ **Центр протидії інформації при РНБО України⁴** створений Указом Президента для виявлення і нейтралізації дезінформації та інформаційного тероризму, окрім неопублічної діяльності, веде сторінки у соціальних мережах для інформування українців про небезпечні маніпуляції ворога.

➤ **Центр стратегічних комунікацій та інформаційної безпеки** при Міністерстві культури та інформаційної політики⁵ створений у березні 2021 року для протидії зовнішнім загрозам, об'єднанні зусиль держави та громадських організацій у боротьбі з дезінформацією, оперативному реагуванні на фейки, а також на промоцію українських наративів.

➤ **Курси для держслужбовців з кібергігієни, цифрової грамотності**, розпочаті за підтримки ОБСЄ в 2020 році

Соцмережі та кампанії.

У разі масового надходження скарг на публікацію, соціальні мережі можуть блокувати публікацію або додавати до публікації повідомлення про неправдивість інформації.

Кожна особа може вжити заходів для боротьби з неправдивими повідомленнями:

- підвищити власну медіаграмотність;
- мислити критично та бути пильними;
- віддавати перевагу авторитетним та офіційним джерелам;
- перевіряти факти, які зустрічаємо в соціальних мережах, перш ніж повірити їм; звертати увагу на дату, автора та справжність фото;
- взяти на себе зобов'язання прочитати весь текст, а не лише заголовки, перш ніж поширювати публікацію;
- вказати іншим на ресурси перевірки фактів, коли бачимо, що неправдива інформація поширюється.

Озброєні обізнаністю особи можуть зробити все можливе, щоб розпізнати неправдиві повідомлення і працювати над тим, щоб зупинити їх поширення. Пам'ятайте, що маніпуляції – всюди. Завжди піддавайте сумніву сенсаційні заголовки і неймовірні фото. Не дозволяйте їм обманути себе. Будьте пильними.

Міністерство внутрішніх справ України розробили 10 порад як не стати жертвою дезінформації.

⁴ <https://cpd.gov.ua/>

⁵ <https://spravdi.gov.ua/>

IV. ВІДПОВІДАЛЬНА ПОВЕДІНКА У СОЦІАЛЬНИХ МЕРЕЖАХ ПІД ЧАС ВІЙНИ.

Ми проводимо в соціальних медіа багато часу: ділимося своїми думками та подіями з життя, спілкуємося з друзями, читаємо новини. Соціальні мережі стають «сірим» джерелом інформації, де будь-хто та будь-коли може поширювати будь-який контент. Соціальні мережі та месенджери люди сприймають як дружні канали інформації, до яких є велика довіра. Спілкування відбувається лише «зі своїми», тому ореол довіри поширюється на всю соціальну мережу. Проте чи дійсно всі «свої»? росія вторглася в Україну задовго до 24 лютого. Скажена пропагандистська машина роками отруювала український інформпростір потужними вкидами, чутками та ретельно спланованими маніпуляціями. Інформаційні диверсанти рф тисячами додавалися до українців у друзі в соцмережах, дезінформували та сварили нас між собою у коментарях. Сьогодні Facebook, Instagram, Twitter та Telegram генерують основну частину інформації про події в Україні та світі. А під час війни важливо ретельно ставитись до формування об'єктивної картини дня.

 **Міністерство культури та інформаційної політики підготувало три простих поради щодо поведінки у соціальних мережах, які зменшать кількість неякісної інформації у вашій стрічці та допоможуть зберегти мільйони нервових клітин.**

До порад поведінки у соціальних мережах також можна додати наступні:

- не поширюйте неперевірену інформацію;
- не виконуйте нічиїх вказівок та порад, окрім тих, що опубліковані на офіційних сторінках військового керівництва держави чи органів державної влади, або тих, які лунають в ефері офіційних каналів сповіщення;
- не вступайте у соціальних мережах у жодні конфлікти чи кампанії цькування, ініційовані невідомими вам людьми;
- не вигадуйте і не поширюйте патріотичних фейків «для підтримання бойового духу»;
- не відкривайте сумнівних листів та повідомлень від невідомих вам відправників;
- не залишайте своїх персональних даних на невідомих ресурсах.

Які дописи у соціальних мережах та месенджерах будуть шкідливими під час воєнного стану?

 *Фото/відео та координати чи опис подій, де щойно вибухнув снаряд чи був обстріл.* Таким чином можна скорегувати дії окупанта. Війна гібридна і способи її ведення тяж – не варто поширювати будь-яку інформацію в мережу, якщо в цьому немає термінової необхідності. Слід дочекатися коментарів офіційної влади.

 *Інформацію про рух колон української техніки, яку ви бачите особисто, а також інформацію про це з неперевіраних джерел із дописом не фотографувати та не поширювати таке.* Таким чином ви можете дійсно поширити час і локацію руху наших військ або поширити фейк, який піднімає тривогу та паніку серед населення. Як відомо, в нас на сьогодні два ворога – ворожі війська та паніка.

 *Номери рахунків невідомих/неперевіраних людей, які буцімто збирають кошти для військових або людей, які постраждали внаслідок війни.* Якщо ви впевнені в повідомленні про збір коштів, знаєте організацію або людину особисто – можна поширювати. Якщо повідомлення скопіювали в малознайомої людини, немає вказаного імені чи конкретних речей, на які проводять збір – це можуть бути шахраї.

 *Інформацію про невідомих людей, яких назвали мародерами або диверсантами.* Це може бути фейком, який налякає мешканців вказаних вами територій. Звертайте увагу на опис таких повідомлень – зазвичай він виглядає підозріло (дуже багато зброї в машині, одне й те саме авто вказують в багатьох повідомленнях про різних людей, немає чіткого опису ситуації тощо). Довіряти можна тільки повідомленням із офіційних джерел, опублікованих на офіційних сторінках органів влади або особистих сторінках представників органів влади.

 *Гнівні пости про поведінку біженців та внутрішньо переміщених осіб з інших територій.* Центр протидії дезінформації при РНБО України та проект «По той бік новин» вже спростував поширену інформацію про негідну поведінку переміщених осіб в місцях переміщення. Повідомлення можуть бути зібраними, кожне може стосуватись одиничного випадку в різних локаціях, проте через чутки вони збираються в одне ціле і в цілому шкодять репутації всіх переміщених осіб.

 *Інформацію про зброю та матеріально технічне обладнання, яке ми отримуємо від партнерів.* Це чутлива інформація, яку збирає супротивник.

Основні принципи публікацій під час війни:

- не звинувачувати своїх: зараз ворог відомий, він у всіх спільний, між собою після війни розберемося;
- не сіяти паніку, страх та зневіру;

- не засмічувати стрічку видимістю допомоги, бо люди мають бачити пости про справжню актуальну потребу в допомозі;
- перевіряти інформацію, так як будь-яку неправдиву інформацію може запускати ворог.

Особливо слід бути обережними щодо поширюваної інформації представникам органів влади, оскільки інформація від них з більшою вірогідністю сприймається як достовірна. На даному відео: <https://www.youtube.com/watch?v=9Qoets8dLRo&t=64s>⁶ ви можете переглянути, чому держслужбовцям та всім представникам органів влади слід бути дуже пильними щодо інформації, яку вони поширюють.

Які дописи будуть корисними під час воєнного стану?

 *Поширювати інформацію про полонених / загиблих військових рф.* Росіяни у інформаційній ізоляції через введену в країні-агресорі цензуру та багаторічну пропаганду – хтось не вірить у війну через цензуровані медіа, хтось не розуміє причини санкцій через ті ж причини. Потрібно показувати їм, де насправді їх солдати, показувати злочини їхньої влади, які стали причиною санкцій.

 *Поширювати інформацію про рух ворожої техніки та військових.* Ми не хочемо, аби постраждали ЗСУ. Тож допомага українським захисникам для корегування вогню по ворожим локаціям та своєчасного захисту власних позицій буде доречною. СБУ закликала українців повідомляти про ворожі війська і техніку в офіційний **чат-бот @stop_russian_war_bot**.

 *Поширювати відеодокази злочинів окупантів на міжнародну аудиторію.* Тиск на Європу та НАТО може допомогти у вирішенні критично важливих питань для України, як от закриття повітряного простору. Нарізки відео палаючих будинків, фото постраждалих серед цивільного населення, неадекватної поведінки російських військових із міжнародними тегамі поширювати можна і треба.

 *Поширювати повідомлення від української влади про зафіксовані фейки.* Багато неправдивої інформації вже вдалось нейтралізувати – це теж завдяки активності та сповіщенню відповідних структур. Важливо поширювати інформацію про фейки лише від офіційних джерел.

 *Блокувати роботу пропагандистських сторінок/каналів/ЗМІ – закликати до цього інших.* Якщо ви знайшли ворожий канал, який поширює

⁶ Відео створене в рамках проекту "Посилення спроможностей українських державних органів у сфері кібергігієни та кібербезпеки", що реалізується Кординатором проектів ОБСЄ за підтримки урядів Німеччини та Сполученого Королівства й у співпраці з Національним агентством України з питань державної служби та Українською школою урядування.

фейки, інформацію про рух української техніки чи побачили повідомлення із закликом блокувати такі ресурси – надсилайте скарги. Інформаційна війна займає важливе місце у протистоянні України та росії – допомагайте владі.

 *Поширювати повідомлення від офіційних джерел/представників влади із актуальними оновленнями.* Часто люди не можуть знайти офіційні канали або не знають, що вони є – допомагайте своїм співгромадянам перевіреною інформацією.

Основні принципи інформаційної гігієни під час війни:

➤ *Уникайте повторюваної інформації.* Часте повторення інформації записує її у нашу підсвідомість та змушує повірити в неї. Якщо в публікації одна й та сама думка повторюється багато разів різними словами – варто насторожитись. Це ознаки пропаганди.

➤ *Знижуйте інформаційне навантаження.* Контролюйте кількість та якість інформації, яку ви споживаєте. Старайтеся дізнаватись лише необхідне та корисне для вас, але ретельно та повноцінно. Не читайте все, що репостять у соціальних мережах ваші друзі. Читайте не лише заголовки. Заголовки мають коротко переповідати суть новин, але насправді часто не відповідають змісту публікації. Періодично влаштовуйте собі інтернет-детокс. Так само потрібно мати на увазі, що чим меншою буде кількість інформації, яку Ви хочете вберегти, тим менше Вам потрібно буде вживати дій для її убезпечення. Тому під час продукування фотознімків, написання повідомлень в мережі, спілкування телефоном з незнайомими та навіть знайомими людьми подумайте, чи дійсно це є необхідним і наскільки шкідливим може бути використання відповідної інформації проти вас.

➤ *Вивчайте різні точки зору на одну проблему.* Не довіряйте першій новині та першій думці. Краще – знайдіть не менше 3-х (бажано авторитетних та/або офіційних) джерел інформації, написаних різними людьми.

➤ *Насторожуйтесь, коли починаються емоції.* Звертайте особливу увагу, коли починається загострення уваги на поодиноких випадках замість масового огляду явища. Особливо, коли воно шокує. Насторожуйтесь, коли бачите емоційні висновки та особисті думки авторів новин.

➤ *Шукайте, кому вигідно, щоб ви дізнались новину та повірили в неї.* Чого хочуть домогтися певними повідомленнями та закликами? Хто виграє, якщо ви будете робити так, як пропонують або натякають? Під час комунікації в соціальних мережах спрацьовує такий ефект у мислені, ніби це відправили лише мені чи якійсь обмеженій групі людей. Тоді людина починає думати, що ця інформація має велику цінність, тому що вона більш унікальна та персоналізована. Відповідно, вірить цьому. Крім того, у месенджерах намає бар'єру публічної стрічки новин, як в соцмережах. Люди впевненіше пересилають будь-які повідомлення знайомим, не боячись осуду коментарями. Слід пам'ятати, що те, що звучить у месенджері як гіпотеза,

проходить через сарафанне радіо і сприймається вже як реальна загроза. Тому слід критично мислити та аналізувати всю інформацію, яка надходить через соціальні мережі та месенджери.

Крім того, слід з пересторогою ставитись до тих джерел інформації, в яких зустрічаються **російські нарративи** на кшталт⁷:

Адаптація нарративу росії про «Україну як неспроможну державу».

РФ використовує плітки на кшталт історій «про розпилювання гуманітарки» та корупційні схеми. Сюди ж належать спекуляції на темі мобілізації. Варто не поширювати повідомлення у стилі «сусідка сестри моєї дружини розказала, як її сина схопили посеред вулиці і відправили на війну».

«Краще мир на будь-яких умовах, ніж активні бойові дії».

Такий меседж фіксується у групі кремлівських телеграм-каналів із самого початку вторгнення. Проте зі зростанням кількості постраждалих серед цивільного населення дедалі частіше пропагандисти намагаються схилити українців до того, що Україні нібито не потрібні Крим чи Донбас, «якщо стільки людей гине».

Розчарування в НАТО, ЄС та міжнародних партнерах України.

Насправді світова спільнота нам дуже допомагає. Кількість грошей, зброї, гуманітарної допомоги тощо, яку передають українцям, безпрецедентно велика, а наші громадяни отримують притулок і допомогу закордоном.

Мовне питання.

Мовне питання штучне й роздмухане російською пропагандою. «Проте це той коник, з якого росія не буде злазити, навіть якщо він здох» – пише «Детектор медіа». Зараз його використання може мати неочікуваний і негативний ефект. До прикладу, мем про «паляницю» в українських російськомовних групах у соцмережах намагаються зробити токсичним. Ботоподібні профілі підбурюють російськомовних почуватися «гіршими українцями».

Внутрішньополітичні чвари та негаразди.

Очікувано, що кожна політична сила чи людина з політичними амбіціями буде формувати навколо себе спільноту. Дуже часто таку спільноту формують шляхом відколювання її від загального масиву. Країна-агресор дуже вправно вміла підживлювати чвари наших політиків. Свідченням є безперервна робота анонімних телеграм-каналів із їхніми «інсайтами».

⁷ Використано матеріали тренерки Національної тренерської мережі ГО «Ла Страда-Україна» Марини Матвійчук.

Окрему увагу слід звернути на **вид месенджера, який ви використовуєте**. Доцільно поступово відмовлятися від найменш захищеного месенджера *Viber*, хоча у багатьох з нас саме в даному месенджері є багато батьківських чатів, чатів будинку тощо.

Під час війни особливою популярними серед українців стали канали *Telegram*. Однак слід пам'ятати, що в **Telegram різниця в імені навіть в одну літеру означає іншу групу**. Одна різна літера або слово в Username означає абсолютно інший чат/бот/людину. Наприклад, ви шукаєте @stop_russian_war_bot, і результати пошуку мають різні комбінації: stop_war, stop_warbot, stop_rusian_war_bot, stop_russian_warbot. Це все абсолютно відмінні канали, ніж той що ви шукаєте "@stop_russian_war_bot". Обов'язково звіряйте Username профілю.

Також в Telegram немає перевірки групи та організаторів. Зважуйте, хто вам повідомив про чат та які є докази, що цей чат організували справжні українські захисники. Найбезпечніше переходити за прямими посиланнями з перевірених державних сторінок.

Найбільш захищеним на сьогодні в Україні вважається месенджер *Signal*, на спілкування яким українці поступово переходять під час війни.

Важливо не забувати про **захист власних акаунтів у соціальних мережах**:



Використовуйте надійний пароль для захисту акаунта.

Причиною більшості атак залишається використання слабких паролів (ще й досі найпопулярніша комбінація серед користувачів 123456) та застосування однакового ключа для входу до різних облікових записів.



Використовуйте двофакторну аутентифікацію для додаткового захисту акаунта.

Двофакторна аутентифікація (2FA) – це найпростіший спосіб створення додаткового рівня для захисту акаунтів у соціальних мережах. Як правило, програми двофакторної аутентифікації для підтвердження особистості користувача використовують SMS-коди, повідомлення на електронну пошту та біометричні дані, такі як відбитки пальців або сканування обличчя.



Налаштування приватності та безпеки.

Ці налаштування дозволяють блокувати користувачів, сторінки або події; ви можете дозволити певним користувачам бачити вашу сторінку, контактувати з вами або читати інформацію, яку ви розміщуєте на сторінці. Тримайте друзів близько, а ворогів на безпечній дистанції, тобто зробіть обмеження у налаштуваннях профайлу.

Більше про правила безпеки акаунтів та особливості налаштування захисту акаунтів у соціальних мережах можна дізнатись, ознайомившись на платформі Дія.Освіта⁸ з **онлайн серіалом з основ кібергігієни для держслужбовців**, створеним в рамках проекту «Посилення спроможностей українських державних органів у сфері кібергігієни та кібербезпеки», що реалізується Координатором проектів ОБСЄ в Україні за підтримки Міністерства закордонних справ і міжнародного розвитку Великобританії та Федерального міністерства закордонних справ Німеччини.

Технології змінюють світ, те, як ми спілкуємось та сприймаємо навколишнє середовище. Контролюйте свої технічні пристрої, щоб вони не контролювали вас.

Проектом «По той бік новин» розроблено алгоритм побудови фейків з месенджерів.

На наступному прикладі одного із типових фекових повідомлень у месенджері можна побачити застосування цього алгоритму.

Наступний приклад фейкового повідомлення отримували мешканці багатьох міст України. Зверніть увагу на погану орфографію та написання міста російською мовою, в той час як саме повідомлення написано українською. Також в повідомленні відсутні контакти станції переливання крові.

Багато людей, прочитавши його, пішли до місцевих станцій переливання крові, тим самим практично паралізувавши їх роботу.

Розглядаючи відповідальну поведінку у соціальних мережах, слід окремо зосередити увагу на **Facebook та Instagram**. У 2021 році їх аудиторія в сукупності становила майже 28 мільйонів унікальних користувачів з України. Ці соціальні мережі можуть впливати на «серця та думки» понад 63% населення України. Але хто вирішує, що ви бачите у своїй стрічці новин у Facebook? Як часто вам трапляються різні погляди? Facebook, якому належить Instagram, та Google, якому належить YouTube, досить добре вміють показувати вам те, що ви хочете, і приховувати ідеї, які вам не подобаються або з якими ви не погоджуєтесь.

Усе, що суперечить вашим поглядам, відфільтровують, і ви опиняєтесь в **«інформаційній бульбашці»** – явище, яке обмежує доступ людини до повного спектру новин та іншої інформації в Інтернеті шляхом алгоритмічного визначення пріоритетів вмісту, який відповідає демографічному профілю користувача та онлайн-історії, або виключаючи вміст, який йому не відповідає. Термін запропонував інтернет-активіст Елі Парайзер. Він навіть написав книжку про цей феномен «Інформаційна бульбашка: що приховує від вас Інтернет».

⁸ <https://osvita.dia.gov.ua/courses/cyber-hygiene>.

Як працює інформаційна бульбашка?

Уявімо, що у вас є два друга на Фейсбук. Один підтримує вакцинацію, інший – ні. Якщо ви «за» вакцинацію, то будете більше «лайкати» та коментувати лише одного друга. Тоді повідомлення того, хто не підтримує вакцинацію, автоматично зникнуть з вашої новинної стрічки. Так ви опинитесь у середовищі людей, з думкою яких погоджуєтесь. Це і є **ефект інформаційної бульбашки** [filter bubble] – обмежений інформаційний простір, де світ сприймається однобоко та відповідно до наших уявлень.

Інформаційні бульбашки створюються завдяки феномену **«помилки підтвердження»** (confirmation bias) – це схильність людини знаходити серед всієї інформації саме ту, що буде підтверджувати її думку та позицію.

Інформаційні бульбашки – чудове середовище для поширення неправдивих повідомлень. Якщо фейк потрапив у вашу бульбашку, інформаційний простір буде розривати від неправдивої інформації. І, тому, найімовірніше, ви в неї повірите. Бути всередині інформаційної бульбашки означає бути в інтелектуальній ізоляції, що здається дивним, якщо говорити про Інтернет. Вебсторінки можуть застосовувати алгоритми, які відстежують, що ви шукаєте, на що натискаєте, що вам «подобається» або «не подобається», що ви коментуєте і де перебуваєте. Ці алгоритми аналізують усю цю особисту інформацію і за допомогою шаблонів вирішують, що саме ви хочете бачити. Це означає, що пошукові результати, посилення, реклама та дописи у Facebook можуть бути результатом вашої попередньої поведінки онлайн. Наприклад, якщо ви шукали в Google інформацію про зміну клімату, ваша стрічка новин може наповнитися дописами, статтями та відеороликами екологічних організацій.

Без фільтрів ви могли б загубитися в усій інформації, що доступна онлайн. Але, з іншого боку, ви не отримуєте важливу інформацію, яку алгоритми, після аналізу вашої поведінки та інтересів, вважають нецікавою для вас. Соціальні медіа та пошукові системи можуть ізолювати вас від інформації, яка суперечить вашим переконанням. Вони можуть обмежити вас від різноманіття ідей та поглядів на події, тренди та проблеми, які існують у світі. Через інформаційні бульбашки ви можете думати, що весь світ вважає так, як ви. Але це не так. Ви просто ізольовані від інших поглядів, оскільки вони перебувають поза вашою інформаційною бульбашкою. Згодом це може призвести до ще більшої політичної поляризації суспільства, а також до того, що люди поділятимуть ще більш екстремістські погляди.

Що ви можете зробити, аби звільнитися від інформаційної бульбашки?

Пам'ятайте, що інформацію, яку ви бачите, визначають ваші вподобання. Запитуйте себе: чому люди можуть мати інші погляди? Як вони підтримують свої переконання? Цілеспрямовано шукайте альтернативну інформацію з різних джерел.

Перевіряйте джерела інформації. Дуже легко забути про думки інших, якщо ви бачите інформацію, з якою погоджуєтеся. Особливо якщо її поширили ваші друзі у Facebook або люди, яких ви поважаєте.

Пам'ятайте, що за безкоштовні додатки та популярні у Facebook тести типу «Ким ти був у минулому житті» користувачі часто розраховуються персональною інформацією. А компанії-розробники можуть навіть продавати її третім особам. Тож перед тим, як дізнатися, який з факультетів Хогвартсу радо прийняв би тебе на навчання, або подивитися на себе з новою зачіскою чи обличчям, рекомендуємо спочатку дізнатися, які дані про тебе отримує додаток, та чи не має він дозволу розміщувати пости чи писати повідомлення від твого імені.

Згадайте, а чи було з вами таке: «Щойно з друзями ви обговорювали, як круто було б поїхати в подорож Європою. І ось вся твоя стрічка у Facebook вже заповнена туристичною рекламою – авіаперельоти, бронювання готелів та статті про місця, які потрібно відвідати». За тобою стежать? Наразі не існує ані доказів, ані спростувань того, що Facebook може нас підслуховувати. Однак існують чіткі алгоритми роботи соцмереж. Алгоритми соцмереж щодня обробляють тонни користувацької інформації та поведінкові шаблони – що та коли ти лайкаєш, де буваєш, чим цікавишся та на кого підписаний/-на. Крім того, соцмережі розпізнають текстовий і графічний контент, наприклад, фотографії, якими ти ділишся з друзями. Ця інформація допомагає не лише аналізувати користувача, а й прогнозувати його поведінку в мережі.

Facebook також аналізує пошукові запити та активність на інших сайтах, пов'язаних з соцмережею, як от Booking.com чи AirBnB, де ви, можливо, вже шукали інформацію та авторизовувалися через FB. З одного боку, алгоритми можуть здатися корисними і здебільшого нешкідливими для звичайного користувача. Але не слід забувати, що завдяки алгоритмам до твоєї стрічки може потрапити не лише корисна та цікава інформація, а й пропаганда та фейки.

Алгоритми соцмереж відслідковують, з ким ти спілкуєшся найчастіше та показують тобі оновлення від цих людей. Це – своєрідна інформаційна бульбашка. Алгоритми соцмереж аналізують не тільки твою поведінку та інтереси, а й твоїх друзів, аналізують ваші спільні фото та геотеги. Це дозволяє дуже чітко категоризувати інформацію та групувати користувачів, щоб показувати їм ту інформацію, яка буде для них найбільш цікавою. Цю інформацію соцмережі можуть продавати для різних, в тому числі ворожих цілей.

Щоб трохи навести лад у власному Facebook, ви можете налаштувати рекламні вподобання свого профілю⁹.

Пам'ятайте! Насправді, ми відіграємо важливу роль у медіапросторі, адже саме ми поширюємо інформацію в соціальних мережах та усно. **Щоразу коли ми пасивно сприймаємо і поширюємо контент без належної перевірки, ми примножуємо шум та збентеження, які вже існують у**

⁹ https://www.facebook.com/ads/preferences/?entry_product=ad_settings_screen.

перенасиченому інформаційному середовищі. Тож ми несемо таку саму відповідальність за перевірку інформації, яку поширюємо, як і її автори.

Як розпізнати бота або троля.

Сьогодні соціальні медіа схожі на криве дзеркало. Завдяки ілюзіям, які вони створюють, ми можемо вважати когось популярним або навіть лідером думки. «Лайки» та «репости», на які полюють користувачі, стали інструментом для поширення маніпулятивних новин, нападів на людей чи організацій. Зазвичай у цьому задіяні боти і тролі.

Боти, скорочено від «роботи» — анонімні, штучно створені користувачі, які прикидаються справжніми людьми. Насправді ж, ними керують ті, хто не хочуть розголошувати свої справжні імена та наміри. Однак не всі боти обов'язково погані. Наприклад, деякі з них поширюють поезію чи мотивуючі цитати. Але зазвичай ботів використовують, щоб поширювати певні повідомлення та дописи.

Окрім ботів, також існують тролі. На відміну від запрограмованих ботів, тролі – це справжні люди. Їхня головна мета – викликати певні емоції, розпочинати та підтримувати дискусії онлайн.

Тролями можуть бути:

- люди, які отримують плату за розпалювання та підтримку дискусій;
- прихильники ідеології, які роблять це безкоштовно та керуються власними мотивами;
- звичайні люди, адже ми всі іноді беремо участь в обговореннях у коментарях, захищаємо власну думку та навмисно провокуємо наших опонентів.

Як правило, боти здатні лише до примітивних діалогів, а тролі можуть використовувати складні аргументи та докази. Щоб виявити ботів серед ваших друзів чи підписників, ви можете використати спеціальне програмне забезпечення: Botometer¹⁰ (перевіряє, чи керує обліковим записом бот).

Будьте обережні з людьми, з якими дружите або за якими стежите в соціальних мережах, але з якими не знайомі в реальному житті. Якщо ви бачите, як хтось розпалює дискусію в коментарях, краще лишайтесь осторонь. Адже ви можете мати справу з ботом або з професійним тролем.

Українські збройні сили героїчно протистоять російським окупантам на військовому фронті. Наше з вами завдання – тримати удар на інформаційному. З гарячим серцем і холодною головою.

¹⁰ <https://botometer.osome.iu.edu/>

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Про національну безпеку України: Закон України від 21 червня 2018 року № 2469-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2469-19#Text>.
2. Конституція України. URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text>.
3. Стратегія кібербезпеки України: введено в дію Указом Президента України від 26 серпня 2021 року № 447/2021. URL: <https://www.president.gov.ua/documents/4472021-40013>.
4. Стратегія інформаційної безпеки: введено в дію Указом Президента України від 28 грудня 2021 року № 685/2021. URL: <https://www.president.gov.ua/documents/6852021-41069>.
5. Методичний посібник для тренерів з питань кібергігієни у рамках спеціальної професійної (сертифікатної) програми підвищення кваліфікації: Практикум. – Київ: ВАІТЕ, 2021. – 106 с.
6. Години медіаграмотності: онлайн курс. URL: <https://study.ed-era.com/uk/courses/course/824>.
7. Lynn Hasher, Thomas Toppino. Frequency and the conference of referential validity. *Journal of Verbal Learning and Verbal Behavior*. Volume 16. Issue 1. 1977. P. 107 – 112.
8. Very Verified: онлайн-курс з медіаграмотності. URL: <https://verified.ed-era.com/ua>.
9. Кодекс етики спільноти професійних журналістів. URL: <https://www.spj.org/pdf/spj-code-of-ethics.pdf>.
10. Hilbert, M., & López, P. (2011). The World's Technological Capacity to Store, Communicate, and Compute Information. *Science*, 332(6025), 60 – 65.
11. Why “Misinformation” Was Dictionary.com’s 2018 Word Of The Year. URL: https://www.dictionary.com/e/word-of-the-year-2018/?itm_source=parsely-api.
12. Reporters Without Borders (RSF). URL: <https://rsf.org/en/ukraine>.
13. 2021 Word Press Freedom Index. URL: <https://rsf.org/en/ranking>.
14. SP Team. Study: 70% of Facebook users only read the headline of science stories before commenting. *The Science Post*. URL: <http://thesciencepost.com/study-70-of-facebook-commenters-only-read-the-headline/>.
15. Онлайн-курс «Фактчек: довіряй-перевіряй». URL: <https://courses.ed-era.com/courses/course-v1:VOXU-EdEra+FactCheck101+2018/courseware/e8d96cead34b47229890e1ef67b0080e/5b5f423f425d4aba8528403747c073e7/>.

16. Телесюжет про розп'ятого хлопчика. Вікіпедія. URL: https://uk.wikipedia.org/wiki/%D0%A2%D0%B5%D0%BB%D0%B5%D1%81%D1%8E%D0%B6%D0%B5%D1%82_%D0%BF%D1%80%D0%BE_%D1%80%D0%BE%D0%B7%D1%96%D0%BF%27%D1%8F%D1%82%D0%BE%D0%B3%D0%BE_%D1%85%D0%BB%D0%BE%D0%BF%D1%87%D0%B8%D0%BA%D0%B0.
17. Де за дня. У Росії переможцем виборів в Україні оголосили Яроша. URL: <https://www.radiosvoboda.org/a/25399262.html>.
18. Війна Росії проти України: спростовуємо 30 фейків окупантів. URL: https://24tv.ua/viyna-rosiyi-proti-ukrayini-sprostovuyemo-feyki-okupantiv-onovlyuyetsya_n1889316.
19. William Saletan. The Ministry of Truth. A mass experiment in altering political memories. Slate. 2010. URL: <https://slate.com/technology/2010/05/slate-conducted-a-mass-experiment-in-altering-political-memories-were-you-fooled.html>.
20. Фотофейк: Первая жертва вакцинации умерла в Чернигове. URL: <https://www.stopfake.org/ru/fotofejk-pervaya-zhertva-vaktsinatsii-umerla-v-chernigove/>.
21. Військовий викрив гучний фотофейк: я повертався з АТО додому. URL: <https://www.radiosvoboda.org/a/29412450.html>.
22. No, an elephant was not photographed carrying a lion cub in its trunk. URL: <https://factcheck.afp.com/no-elephant-was-not-photographed-carrying-lion-cub-its-trunk>.
23. Кадр из кинофильма «Брестская крепость» представляется как фото с Донбасса. URL: <https://www.stopfake.org/ru/kadr-iz-kinofilma-breetskaya-krepost-predstavlyaetsya-kak-foto-s-donbassa/>.
24. No, photos from 'yellow vest' protests were not framed by journalists to look more severe. URL: <https://factcheck.afp.com/no-photos-yellow-vest-protests-were-not-framed-journalists-look-more-severe>.
25. Таинственный эксперт. URL: <https://www.svoboda.org/a/26615443.html>.
26. Neigel A. R., Claypoole V. L., Waldfogle G. E., Acharya S., Hancock G. M. Holistic Cyber Hygiene Education: Accounting for the Human Factors. *Computers & Security*. 2020. Vol. 92. 101731 (DOI: 10.1016/j.cose.2020.101731).
27. Інформаційна гігієна для держслужбовців. URL: <https://www.youtube.com/watch?v=9Qoets8dLRo&t=64s>.
28. Презентація тренерки Національної тренерської мережі ГО «Ла Страда-Україна» Марини Матвійчук, продемонстрована під час вебінару «Відповідальна поведінка в соціальних мережах та месенджерах під час війни» 30 березня 2022 року.

Науково-методичне видання

АФОНІН Дмитро
ІСМАЙЛОВ Карен
ЛІСНІЧЕНКО Дмитро
ПИШНА Алла
КОВАЛЬОВА Олена А

**АНАЛІЗ, ВИЯВЛЕННЯ ТА УБЕЗПЕЧЕННЯ ВІД
НЕПРАВДИВИХ ПОВІДОМЛЕНЬ, ЯК СКЛАДОВОЇ
ЧАСТИНИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ**

Методичні рекомендації

Підп. до друку 22.12.2022. Формат 60x84/16.
Друк цифровий. Папір офсетний. Гарнітура Times.
Ум.-друк. арк. 2,56. Обл.-вид. арк. 2,3.
Наклад 30 прим.
Надруковано з готового оригінал-макета
Редакційно-видавничий відділ
Одеського державного університету внутрішніх справ
м. Одеса, вул. Успенська, 1,
Свідоцтво суб'єкта видавничої справи ДП № 3507 від