

Убезпечення від неправдивих повідомлень

План лекції

Вступ

1. Види маніпуляцій
 2. Пропаганда
 3. Заходи протидії
- Висновки

Рекомендована література

Основна

1. Даник Ю.Г., Грищук Р.В. Основи кібернетичної безпеки: монографія. Житомир: ЖНАЕУ, 2016. 636 с.
2. Манжай О.В., Манжай І.А. Правові засади захисту інформації: підручник / вид. друге, переробл. та доповн. Харків: Промарт, 2020. 162 с. з іл. URL: <https://univd.edu.ua/science-issue/issue/4315>.
3. Методичний посібник для тренерів з питань кібергігієни у рамках спеціальної професійної (сертифікованої) програми підвищення кваліфікації: практикум / О.В. Манжай, В.В. Носов. К.: ВАІТЕ, 2021. 106 с.
4. Робочий зошит для учасників тренінгу з питань кібергігієни. Загальна короткострокова програма підвищення кваліфікації / О.М. Барановський, В.В. Гузій, Д.І. Майорников, О.В. Манжай, В.В. Носов. К.: ВАІТЕ, 2021. 262 с.

Допоміжна

5. Простворення Центру протидії дезінформації: Рішення Ради національної безпеки і оборони України від 11.03.2021, введено в дію Указом Президента України від 19.03.2021 № 106/2021. URL: <https://zakon.rada.gov.ua/laws/show/106/2021#Text>.
6. Стратегія інформаційної безпеки, затверджена Указом Президента України від 28.12.2021 № 685/2021. URL: <https://zakon.rada.gov.ua/laws/show/685/2021#Text>.

Інформаційні ресурси в Інтернеті

7. Освітній серіал «Основи кібергігієни». URL: <https://osvita.diia.gov.ua/courses/cyber-hygiene>.

Текст лекції

Вступ

Ви, напевно, неодноразово чули фразу про те, що той, хто володіє інформацією, володіє світом. Сьогодні ця теза є актуальною як ніколи. Технології неправдивих повідомлень для впливу на маси почали активно використовувати у XX столітті (рис. 1).



Рис. 1. Видалення з фото учасника першого загону космонавтів Григорія Нелюбова

Але якщо раніше для цього залучалися професійні команди, то сьогодні, із появою різних комп'ютерних технологій та мережі Інтернет, буквально кожен більш-менш обізнаний користувач може створювати фейкові повідомлення та поширювати їх. Згадайте, наприклад, як за допомогою фоторедакторів ви або ваші знайомі редагували зроблені фотознімки. Із появою штучного інтелекту проблема лише поглибилась. Зараз за допомогою відповідних програм досить легко зробити не тільки неправдиве фото (рис. 2, 3), а й відео (рис. 4), яке буде виглядати як справжнє (github.com/iperov/DeepFaceLive, kaiber.ai) та навіть аудіо (fakeyou.com, [@clonevoicebot](https://clonevoicebot.com)). Серед іншого, почастишали випадки створення порнографічного контенту за допомогою штучного інтелекту з використанням фото певних осіб з метою їх подальшого шантажу або порнопомсти (bleepingcomputer.com/news/security/sextortionists-are-making-ai-nudes-from-your-social-media-images/). Так, наприклад, для оголення осіб на фото може бути застосований Telegram-бот [@BodyScannerBot](https://t.me/BodyScannerBot).

У згаданому контексті однією з небезпечних тенденцій є генерування контенту, який містить зображення насильства, зокрема над дітьми, з використанням

систем штучного інтелекту. Зокрема, окремі користувачі використовують для генерування подібних зображень продукт stablediffusionweb.com. Так, на теперішній час в мережі Даркнет можна знайти тисячі зображень, які містять сцени сексуального насильства над дітьми та оголених дітей, і це, насправді, є ще одним викликом для правоохоронної системи.

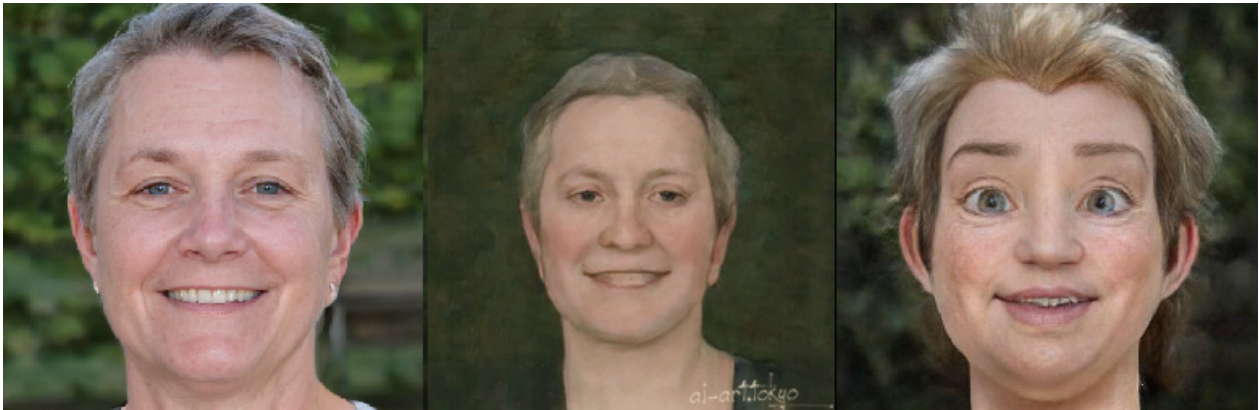


Рис. 2. Зображення, створені за допомогою штучного інтелекту, зліва направо: зображення неіснуючої людини, створене за допомогою сервісу thispersondoesnotexist.com; портрет, створений на основі першого фото за допомогою сервісу ai-art.tokyo; мультяшний персонаж на основі першого фото, створений за допомогою одного з ботів Telegram



Рис. 3. Зображення, створені за допомогою штучного інтелекту, зліва направо: зображення неіснуючої людини, створене за допомогою сервісу thispersondoesnotexist.com; зміна зачіски за ключовими словами «Trump's hair», на обличчі з першого фото за допомогою сервісу anything-ai.com

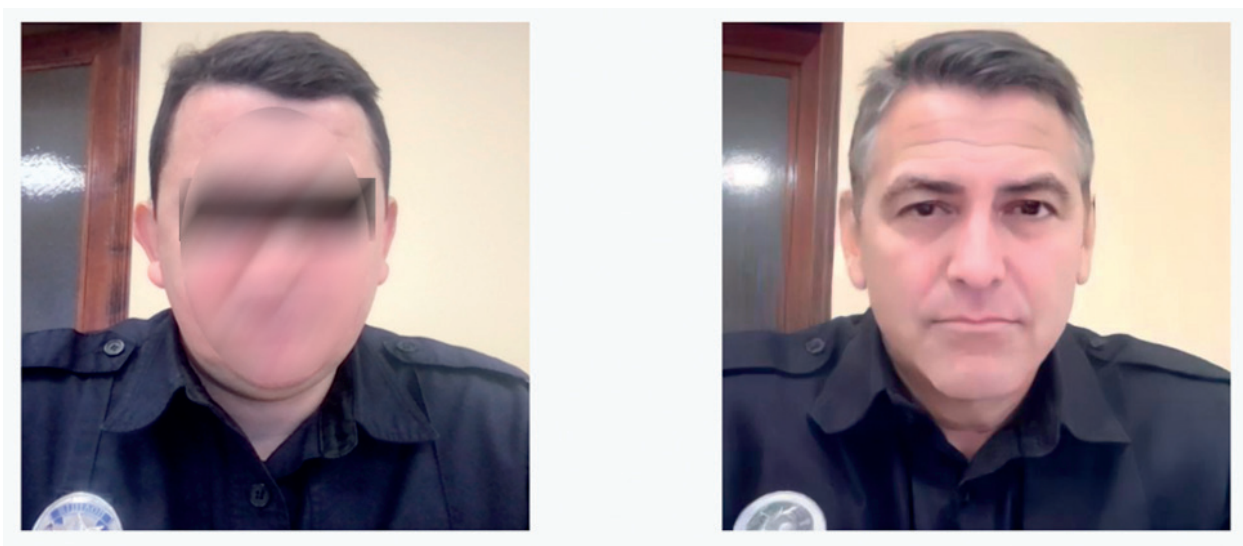


Рис. 4. Діпфейк відео, яке створюється в режимі реального часу за допомогою інструменту fal.ai/camera

Серед інших інструментів, за допомогою яких можна генерувати різноманітний контент, можна згадати Telegram @DeepPaintBot – для покращення якості фото, @qq_2d_ai_bot – для перетворення фото на аніме, @videotoanimebot – для анімації фото у різних стилях, сервіс www.deepswap.ai – для заміни обличчя тощо.

Як не заблукати в мережі, відрізнити правду від вимислу? Саме цим питанням присвячено цю тему.

1. Види маніпуляцій

Перенесення переважної кількості інформаційних потоків у мережу Інтернет, з одного боку, значно полегшило доступ користувачам до різних відомостей і знань, а з іншого – створило велику кількість можливостей для маніпуляції з боку правопорушників. Такі маніпуляції можуть бути спрямовані на окремих осіб, групи, створювати передумови для формування «потрібної» громадської думки.

Маніпуляції можуть бути *свідомими* або *несвідомими*, проте вони все одно здатні вплинути на прийняття рішень як звичайними користувачами, так і керівним складом державних органів.

Одним із найбільш поширених прикладів подібних відомостей є інформаційні сторінки, що містять інформацію з минулого, але позиціонуються як новина дня.

01 листопада 2020 року в мережі Інтернет було розміщено новину про те, що доларові депозити завдають їхнім власникам збитки, у той час як гривневі є більш прибутковими³. Проте, якщо уважно проаналізувати зміст повідомлення, стає зрозуміло, що це – новина 2013 року, і на день публікації вона може бути зовсім неактуальною.

Неправдиві ресурси часто називають фейками. Наприклад, ресурс fakeinfo.net (рис. 5) дозволяє створити фейки за різними напрямками. Так само для створення неіснуючих об'єктів може бути використано сервіс thisxdoesnotexist.com (рис. 6).

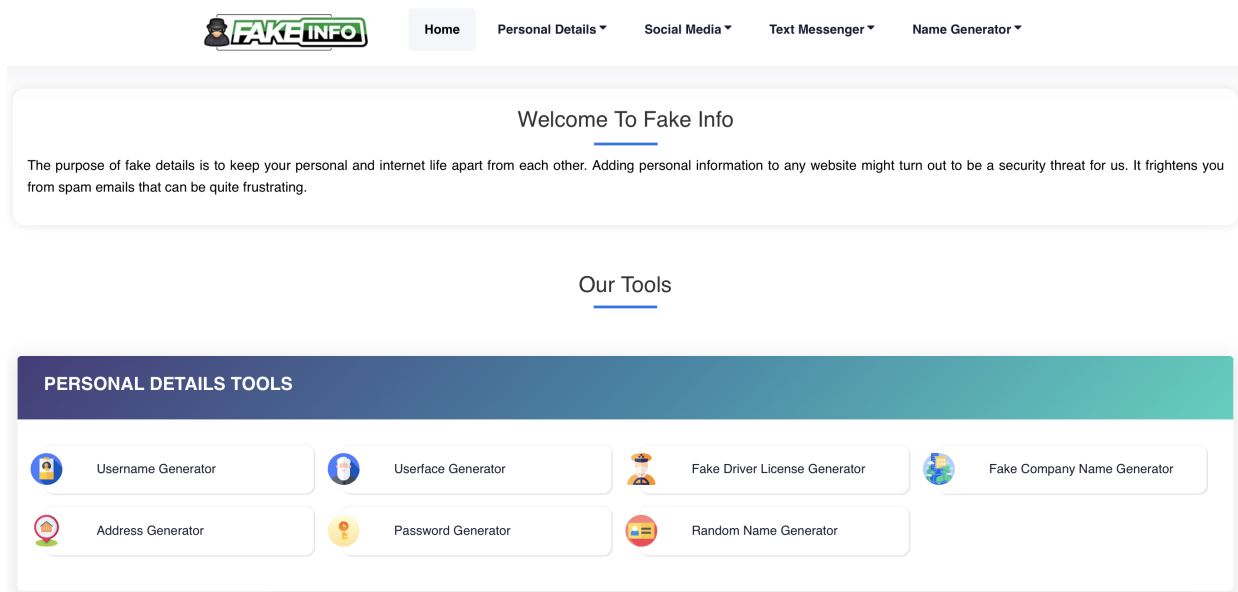


Рис. 5. Зовнішній вигляд ресурсу для генерування фейків

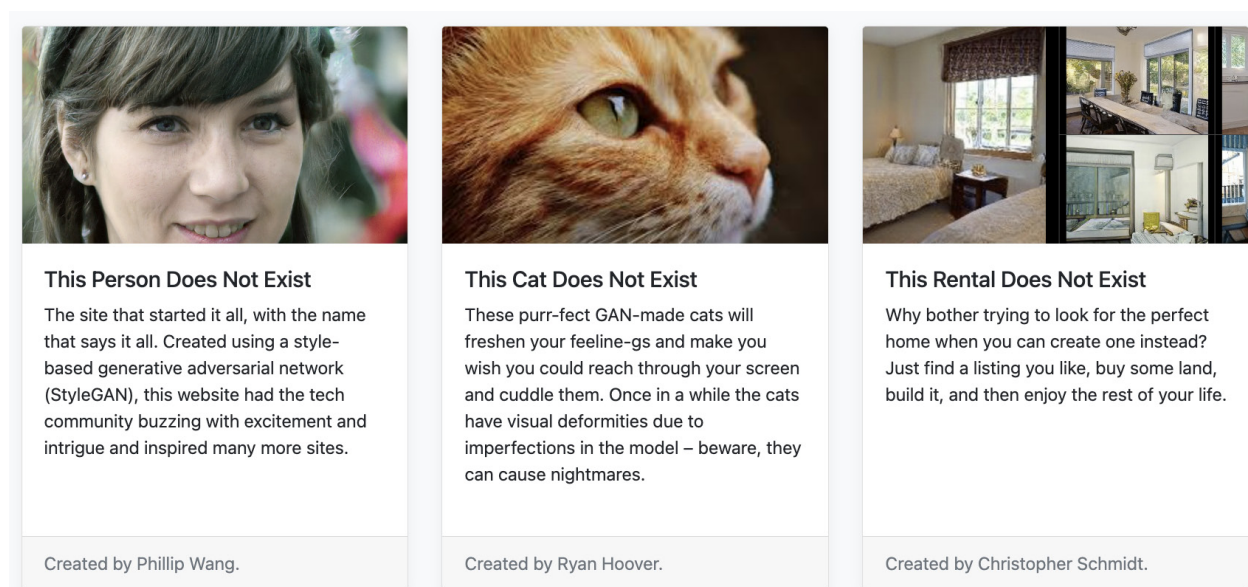


Рис. 6. Зовнішній вигляд ресурсу для генерування неіснуючих об'єктів

³ Долларовые депозиты приносят их держателям одни убытки, в то время как вклады в гривне дают более значительную доходность. URL: <https://web.archive.org/web/20201106213245/https://telegraf.com.ua/biznes/finansyi/amp-656615-depozityi-v-grivne-vyigodnee-chem-v-dollarah.html>.

Фейк може бути візуальним, для чого використовуються графічні та відеоредактори. У межах інформаційного впливу під час доведення до відома інформації використовується певний набір характеристик: видовищність, порушення звичної моделі світу, примушуюча пропаганда, «наклеювання ярликів», «тролінг» (активна участь у багатьох дискусіях під вигаданими іменами), копіпастинг. Типові ознаки троля: емоційні меседжі, чіткі тези із закликами, одноманітний профіль у мережі, незначна кількість віртуальних друзів, відсутність власних постів, створена нещодавно сторінка⁴.

У мережі Інтернет найбільш частими каналами для поширення фейків є веб-сайти новин, соціальні мережі, блоги, розсилки електронною поштою.

У жовтні 2020 року в мережі Інтернет низка ЗМІ поширила повідомлення про те, що президент Туреччини не визнає Крим російським, оскільки вважає, що півострів належить його країні. Ця інформація з'явилася на фоні просування Міністерством закордонних справ України ідеї створення «Кримської платформи», покликаної вирішити питання деокупації Криму.

У відповідних матеріалах ЗМІ посилалися на турецьке видання «Haberler», в одній з новин якого була стаття із розділом «Ердоган бажає, щоб Крим віддали Туреччині». У цьому розділі видання посилається на фрагмент статті з газети «Московський комсомолец», у якій її автор зробив припущення про позицію президента Туреччини. Таким чином, в результаті маніпуляції припущення, яке пройшло через низку «фільтрів», у підсумку було подано як факт. Згодом інформацію було спростовано⁵, але не всі звернули на це увагу.

Фейки можуть бути орієнтовані на конкретну національну аудиторію, а можуть бути й інтернаціональними.

У мережі Інтернет можна знайти фейк про те, що в німецькому виданні Fuldaer Zeitung було викладено інтерв'ю з ветераном Другої світової війни Людвігом Піллером (Ludwig Piller) з ФРН, у якому він нібито зауважив (рис. 5), що найкращими роками його сімейного життя був полон у росіян. Якщо спробувати знайти першоджерело цієї новини по ключових словах або на сайті fuldaerzeitung.de, то позитивного результату досягнути не вдасться, тому що це – спотворена інформація. Людвіг Піллер дійсно був у полоні, але не в СРСР, а у Франції (<https://www.faz.net/aktuell/gesellschaft/menschen/hochzeit-im-zweiten-weltkrieg-das-paar-heiratete-vor-80-jahren-16376299.html>), і не п'ять років, а рік

⁴ Іванцова А. Інтернет-тролі на службі в олігархів та політиків. URL: <https://www.radiosvoboda.org/a/27042051.html>.

⁵ «Надо вернуть Турции»: РосСМИ распространили фейк о позиции Эрдогана по Крыму. URL: <https://bykvu.com/ru/bukvy/treba-povernuti-turechchini-roszmi-rozpovsjudili-fejk-shhodo-pozicii-erdogana-po-krimu/>.

(<https://www.donaukurier.de/archiv/ludwig-der-flieger-2385405>).

Незважаючи на неправдивість цього повідомлення, вказана інформація з 2020 року продовжує жити своїм життям та нерідко з'являтися в німецькомовних облікових записах в соціальних мережах, наприклад (рис. 7), <https://web.archive.org/web/20230814120415/https://www.facebook.com/photo/?fbid=183523304070831>.



Рис. 7. Фейкове фото

Кілька років тому О. Юркова на підставі сучасного практичного досвіду представила низку способів створення недостовірних новин⁶. Серед них:

1. Маніпуляції з медіаданими:

- ▶ редагування;
- ▶ подання справжніх медіаданих в іншому контексті, зміна часу і місця їх створення;
- ▶ створення повністю недостовірного медіаконтенту.

2. Маніпулювання новинами:

- ▶ викривлення сенсу заголовків новин;
- ▶ подання окремої думки як факту;
- ▶ викривлення фактів;
- ▶ подання повністю недостовірної інформації як факту;
- ▶ ігнорування важливих деталей, які змінюють контекст.

⁶ Yurkova O. Six Fake News Techniques and Simple Tools to Vet Them. URL: <https://gijn.org/six-fake-news-techniques-and-simple-tools-to-vet-them/>.

3. Маніпулювання експертними оцінками:

- ▶ використання думок псевдоекспертів (несправжніх експертів, експертів в інших сферах тощо) та аналітичних центрів;
- ▶ перекручування заяв експертів або приписування видуманих заяв справжнім експертам;
- ▶ викривлення перекладу.

4. Маніпулювання повідомленнями:

- ▶ використання повідомлень маргінальних суб'єктів;
- ▶ перекручування реальних повідомлень з авторитетних джерел;
- ▶ посилення на неіснуючі повідомлення з авторитетних джерел.

5. Маніпуляції з результатами досліджень:

- ▶ використання слабкої або несправжньої методології;
- ▶ неправильна інтерпретація результатів;
- ▶ неправильні порівняння.

У цій самій праці було розкрито методи та інструменти викриття подібного виду підробок.

Однією з основних ознак інформаційної атаки є різкий дисбаланс позитивних і негативних повідомлень у доборі матеріалів, відсутність коректного обговорення різних точок зору, коли витісняється раціональна складова, а обговорення відбувається на рівні емоцій та особистих звинувачень⁷.

Емоційна складова є характерною рисою інформаційно-психологічного впливу. Коли людина лякається, в неї перестають працювати аналітичні центри. Психовіруси розраховані на те, щоб викликати в людини паніку та страх шляхом спекуляції на базових потребах. Наприклад, панічні новини про те, що все «жахливо подорожчає», вводять особу в стан паніки, вона перестає нормально аналізувати дійсність. Коли людину «зомбують», регулярно підкидаючи їй певні ідеї, вони приживаються як негласні аксіоми. Така людина буде вкрай важко сприймати будь-які нові ідеї, якщо вони входять у конфлікт з укоріненими старими⁸.

У серпні-вересні 2008 року один з українських банків зазнав прицільної інформаційної атаки⁹, у тому числі із застосуванням повідомлень у мережі Інтернет. Ця атака тривала кілька тижнів та була спрямована на те, щоб спровокувати паніку серед вкладників, які б масово почали виводити з банку свої кошти. Такі зловмисні дії досягли запланованої мети. За короткий період часу тисячі вкладників забрали з банку кілька мільярдів доларів. У результаті Національний банк України був вимушений здійснити

⁷ Пода Т.А. Інформаційна війна як стратегія формування політичної свідомості (соціально-філософський аналіз). *Вісник Національного авіаційного університету*. Сер.: Філософія. Культурологія. 2014. № 1. С. 69.

⁸ Ющенко А.Г. Україна обязана выиграть информационную войну. *Україна третє тисячоліття*. 2014. № 3. С. 22.

⁹ Жертва рейдерів. Хроніка атаки на «Промінвестбанк». URL: <https://minfin.com.ua/2008/10/17/pib/>.

рефінансування цього банку на суму 5 млрд. грн. Генеральною прокуратурою України було порушено кримінальну справу за доведення установи до банкрутства за ознаками злочину, передбаченого ч. 3 ст. 15, ст. 219 Кримінального кодексу України. Описана ситуація в подальшому сприяла посиленню фінансової кризи в усій державі.

2. Пропаганда

Одним з інструментів інформаційного впливу є пропаганда. Часто застосовуваними методами пропаганди є:

- ▶ *«гнилий оселедець»*. Використовується проти конкретної особи або групи осіб, стосовно яких висувуються неправдиві звинувачення, які мають бути якомога скандальнішими (розбещення дітей, убивство з корисливих мотивів тощо). Метою є виклик широкого обговорення несправедливості, неправдивості обвинувачення. Поступово згадування об'єкта у зв'язку зі скандалом наростає та немовби в'їдається в його одяг, залишаючи за ним шлейф «гнилого оселедця». Таким чином, під час згадування імені об'єкта він постійно асоціюється з брудним скандалом;
- ▶ *«перегорнута піраміда»* є прийомом створення текстів, коли пріоритетність інформації зменшується від початку тексту до його закінчення. Цим досягається приковування уваги до гучного початку матеріалу. Об'єкт впливу може не дочитувати матеріал до кінця, проте основний посил залишиться в його пам'яті;
- ▶ *«велика брехня»*. Полягає в тому, що аудиторії впевнено пропонується скомпонована та добре продумана велика брехня, здатна викликати емоційну травму. Це – така глобальна та страшна брехня, коли практично неможливо повірити, що можна брехати про таке (наприклад, інформація про розіп'ятого хлопчика);
- ▶ *«40 на 60»*. Полягає в донесенні інформації, в якій 60 % інформації дається на користь супротивника, а інші 40 % – на користь суб'єкта інформаційного впливу. Перша частина інформації спрямована на заслужування довіри супротивника, друга – на донесення дезінформації;
- ▶ *«абсолютна очевидність»* спрямована на створення у групи людей ефекту приєднання. Інформація, яку планується впровадити в маси, не доказується, а позиціонується як очевидний факт, що підтримується більшістю людей. Незважаючи на свою простоту, цей метод є дуже ефективним, оскільки людська психіка автоматично реагує на думку більшості, намагаючись долучитися до неї. Більшість має бути переважаючою, а її підтримка – абсолютною та безперечною, адже в іншому випадку ефект приєднання буде відсутнім.

Пропаганда може бути очевидною та неочевидною, орієнтованою на різні вікові категорії. Так, наприклад, пропаганда ксенофобії може бути спрямована навіть на дітей для того, щоб привчити їх до думки про те, що принижувати інші національності є нормою.

У російському мультфільмі «Овощи» із серії «Синій трактор» (https://www.youtube.com/watch?v=a_Zc4PFtxVg) овоч баклажан асоційовано з особою, одягненою в національний костюм мешканців Кавказу, яка має відповідний акцент (рис. 8).

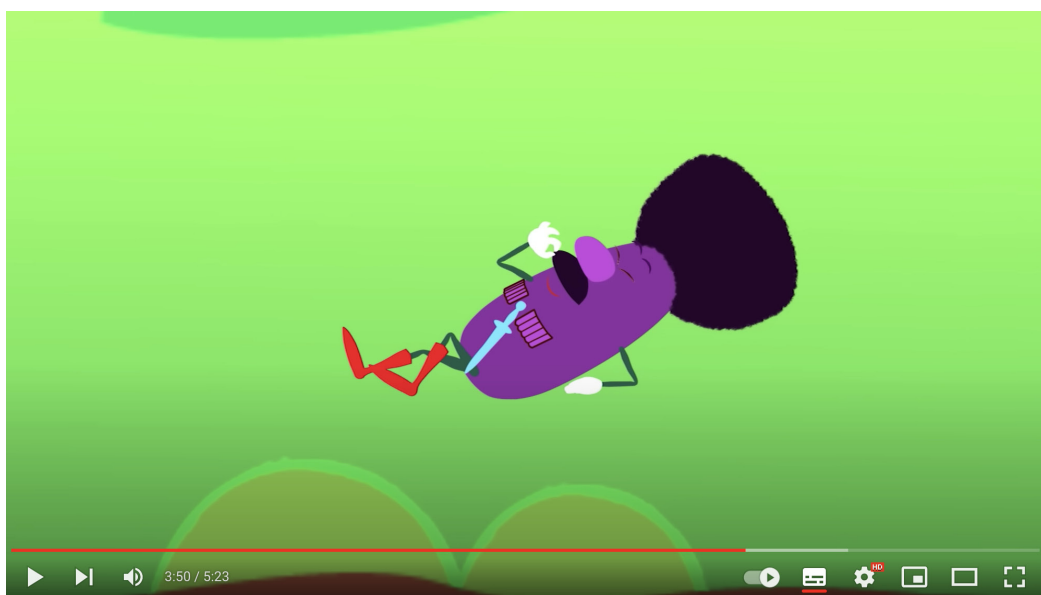


Рис. 8. Фрагмент мультфільму «Овощи»

У той же час, здійснивши пошук в мережі Інтернет за ключовими словами російською мовою «кого называют баклажаном», можна побачити, що на жаргоні відповідним терміном російськомовні можуть називати темношкірих осіб, що, до речі, продемонстровано в фільмі «Жмурки».

Інформаційні ресурси з доброю репутацією подекуди самі можуть ставати інструментом маніпуляції. Особливо це актуально для тих ресурсів, які не проводять ретельний аналіз наданих їм даних на достовірність. Так, через спеціально створений ресурс запускається недостовірна інформація, яку без перевірки публікують інші засоби масової інформації та інформаційні ресурси всередині країни. ЗМІ іншої держави, зацікавленої у проведенні інформаційної операції, викривають представлену інформацію як недостовірну, тим самим формуючи суспільну думку як у своїй державі, так і в країні, про яку йдеться у недостовірній інформації, – і саме це стає метою проведення інформаційної операції.

Як зазначив у своєму Телеграм-каналі журналіст Андрій Цаплієнко (<https://t.me/Tsaplienko/35018>), напередодні саміту НАТО у 2023 році російські пропагандисти створили відео-фейк щодо втоми США від Президента України Володимира Зеленського. Начебто, на перехресті 5-ої авеню та 57-ої вулиці Нью-Йорку вивісили плакат «Немає Зеленського, немає війни», на підтвердження чого додали відеофайл.. Насправді це відео було змонтовано з оригіналу, який можна знайти за адресою <https://m.youtube.com/watch?t=66&v=yhkbg8p2Gts&feature=youtu.be>

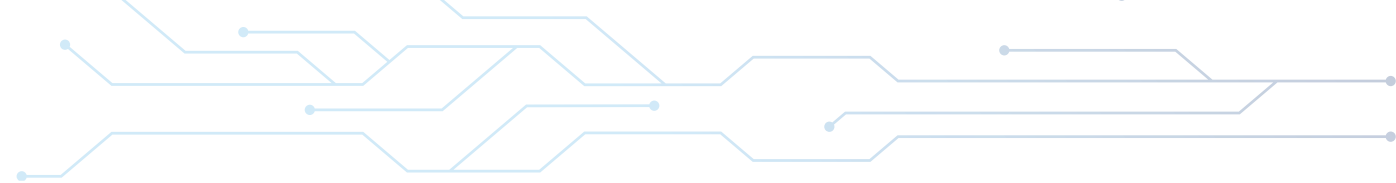
Фейковий варіант відео перепостили всі агенти російського впливу в Америці. Тож можна зробити висновок, що інформаційна спецоперація була розрахована на американців.

У іншому своєму дописі Андрій Цаплієнко викриває інший приклад пропаганди, орієнтованої на громадян США з метою зменшити підтримку України (<https://t.me/Tsaplienko/38326>).

Так, на опублікованому Fox News (<https://www.foxnews.com/politics/cartoons-slideshow#bf7f54c7-7bf7-5bb1-aa2a-ed0f82aff5b>) малюнку (рис. 9) зображено посил, який можна інтерпретувати таким чином, що ледачий, брудний хіппі незрозумілої орієнтації, який підтримує Україну, «хейтить» звичайного роботящого хлопця із зоряно-смугастим прапором на футболці: «Цей прапор мене ображає». Тобто, якщо вимагаєш підтримувати Україну, значить, ти брудний ледачий нероба із заплутаною орієнтацією. Є й більш маніпулятивна деталь. На синьо-жовтому прапорці написано «Підтримуй війну в Україні». Нібито це сама Україна її розпочала. І асоціальний тип, який сидить на плечах у добропорядного платника податків, насправді виступає за продовження війни, а не за її припинення.



Рис. 9. Малюнок з ознаками пропаганди



Розквіт пропаганди в країні нерідко межує з «епідемією» такого явища, як «стукацтво». У гіпертрофованому вигляді це можна було спостерігати за часів СРСР періоду правління Йосипа Сталіна. Сьогодні те саме починає простежуватися на російській території. Так, одним з ентузіастів у січні 2023 року було розроблено жартівливий застосунок «Мой Донос». До травня 2023 року через застосунок надійшло вже більше 5 тис. доносів, 20% з яких містили докладний опис «правопорушень» та особисті дані правопорушників¹⁰.

Під час війни пропаганда набуває особливого розквіту. Бельгійська дослідниця Анна Морелі узагальнила напрацювання Понсоби та вивела 10 основних принципів воєнної пропаганди:

1. «Ми не хочемо війни».
2. «У цій війні винні лише наші противники».
3. «Наш ворог – це втілення зла та самого диявола».
4. «Ми б'ємося за благородну мету, а не за власні інтереси».
5. «Ворог навмисно проявляє жорстокість, інциденти з нашого боку вимушені або випадкові».
6. «Ворог використовує заборонену зброю».
7. «У нас незначні втрати, в той час як втрати ворога – величезні».
8. «Визнані артисти та інтелектуали нас підтримують».
9. «Наша мета – священна».
10. «Кожен, хто ставить нашу пропаганду під сумнів, – зрадник».

У 2022 році А. Романюк у статті «10 принципів воєнної російської пропаганди на прикладі Херсона» (censor.net/ua/b3346432) достатньо докладно описала на прикладі українського міста, як працюють ці 10 принципів.

3. Заходи протидії

Існує низка способів протидії неправдивим повідомленням. Умовно їх можна розділити на логічні, технічні та комбіновані. Найбільш простими та дієвими логічними способами є такі:

- ▶ критичне осмислення будь-якої інформації;
- ▶ під час сприйняття інформації потрібно намагатися більше керуватися розумом, аніж емоціями;
- ▶ звертати увагу на репутацію інформаційних ресурсів;
- ▶ перевіряти інформацію з кількох джерел;
- ▶ намагатися переглядати першоджерело відповідного інформаційного повідомлення.

Для логічного опрацювання мультимедійних даних може стати в нагоді ресурс, який акумулює інформацію про різноманітні предмети та особливості країн, – geohints.com.

¹⁰ Андрусак А. «Такий молодий, а вже проти Путіна»: росіяни написали понад 5000 доносів на жартівливому сервісі. URL: <https://focus.ua/uk/world/584979-takij-molodij-vzhe-proti-putina-rosiyani-napisali-ponad-5000-donosiv-na-zhartivlivomu-servisi>.

Як приклад технічних інструментів викриття неправдивих фотоповідомлень можна навести плагіни «Who stole my pictures» (рис. 10) та «Fake news debunker by InVID & WeVerify», що їх легко знайти в мережі Інтернет та встановити у відповідному браузері.

Яркая иллюстрация, как в Украине защищают от коронавируса врачей и чиновников



Размещено: 16.04.2020



Наибольшее количество зарегистрированных случаев COVID-19 среди медиков в Черновицкой области - 126 медицинских работников. Сегодняшние данные Минздрава.

Что с обеспечением средствами индивидуальной защиты в Черновицкой области? Официальные данные Кабмина показывают обеспеченность на уровне 62,33%, то есть чуть больше половины от потребности.

Что сказать властям, которые переживают за больницы, могли закупить маски? Пожелания можно подкреплять стабильным обеспечением.

Защиты. Слева - врачи, справа - чиновники,

чиновников Украины.

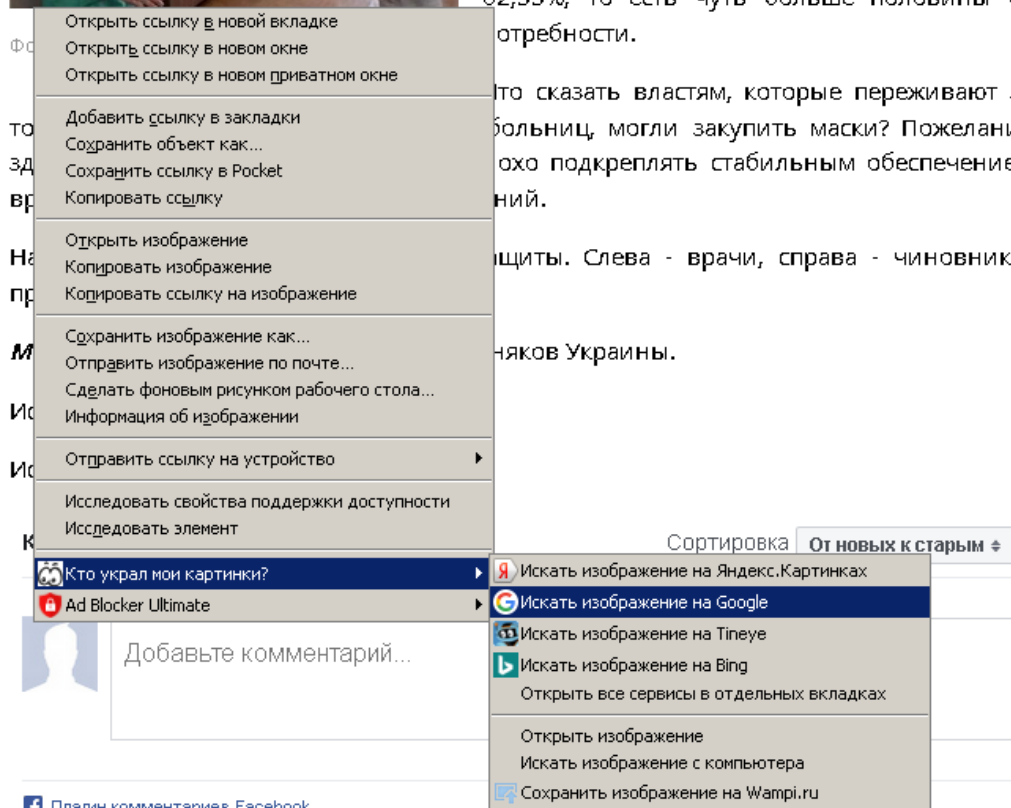


Рис. 10. Використання інструменту

Коментуючи новину на рис. 10, потрібно відзначити, що вона була спрямована на маніпулювання громадською думкою (<http://archive.is/tUogM>). У ній коментується фотографія, яка нібито зроблена в українській лікарні, у той час як насправді зображення запозичено із новини про відвідування лікарні губернатором Псковської області в Російській Федерації.

Для пошуку зображень в мережі Інтернет також згодиться і простий реверс-пошук за зображенням у пошуковій системі (рис. 11).

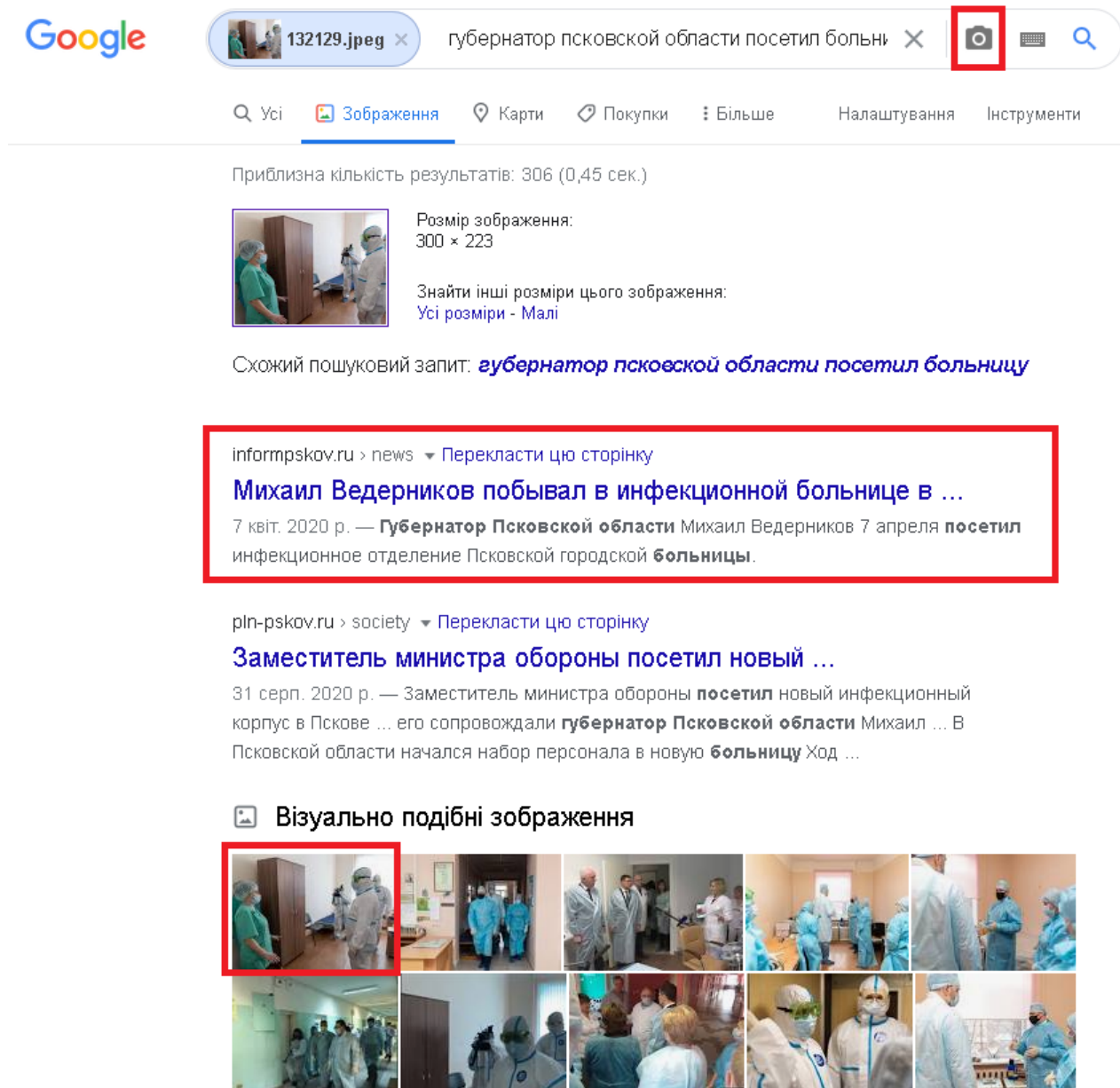


Рис. 11. Використання зворотного пошуку за зображенням у пошуковій системі Google здійснюється шляхом натискання на зображення фотокамери на сторінці пошукової системи пошуку зображень «Who stole my pictures»

Крім наведених інструментів, для виявлення редагування зображень та аналізу додаткових даних можна використовувати такі сервіси, як www.imageforensic.org, 29a.ch/photo-forensics та fotoforensics.com. Наприклад, вид аналізу Error Level Analysis, або ELA дозволяє виявити накладені зображення, оскільки вони різняться за рівнем шуму – яскравістю точок (рис. 12).

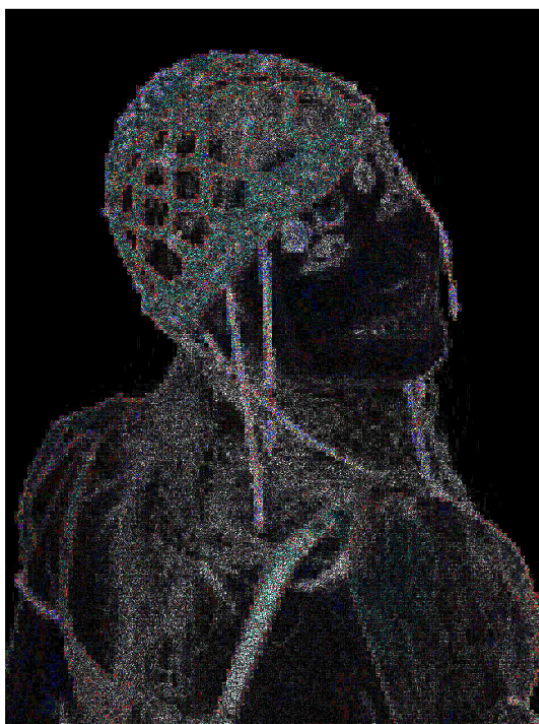


Рис. 12. На рисунку видно, що рівень шуму для білого фону різко відрізняється від загального, і це свідчить про те, що білий фон було створено окремо від основного фото (fotoforensics.com/tutorial-ela.php)

Для аналізу відеофайлів, розміщених на сервісі YouTube, може бути використаний сервіс citizenevidence.amnestyusa.org (рис. 13).



Youtube DataViewer

Теперь то уж точно! Украина СПАСЕНА!!!

Оригинал видеозаписи по адресу <http://www.youtube.com/watch?v=dvZD-2ww1ww> от 19.07.2014г. Читай подробнее досье на Порошенко и других украинских политиков на сайте <http://whoswho.com.ua/>

Video ID: sTzK4MgKfoU
Upload Date (YYYY/MM/DD): 2014-09-01
Upload Time (UTC): 12:03:18 ([convert to local time](#))

Thumbnails:



[reverse image search](#)

Рис. 13 <https://ebird.org/>. Аналіз фейкового відео, в якому опис не відповідає відеоряду

Як додаткові інструменти для аналізу метаданих відео у YouTube можна також запропонувати сервіси:

- ▶ youtube-lookup.vercel.app;
- ▶ mattw.io/youtube-metadata.

У листопаді 2020 року блогер А. Шарій випустив відеоролік, у якому продемонстрував фотографію Президента України з лікарями та вказав, що під час хвороби Президент, нехтуючи масковим режимом, фотографується з лікарями без маски (рис. 14).



Рис. 14. Фрагмент відеоблога А. Шарія

подальшого зворотного пошуку в пошуковій системі легко встановити, що знімок було зроблено у 2016 році в Ізраїлі, про що йдеться, наприклад, у знайденій новині (рис. 15) за адресою <http://www.bagnet.org/news/pressreliz/353826/pervyy-meditsinskiy-tsentr-tel-aviva-gorod-zdorovya-v-gorode-mechty>.

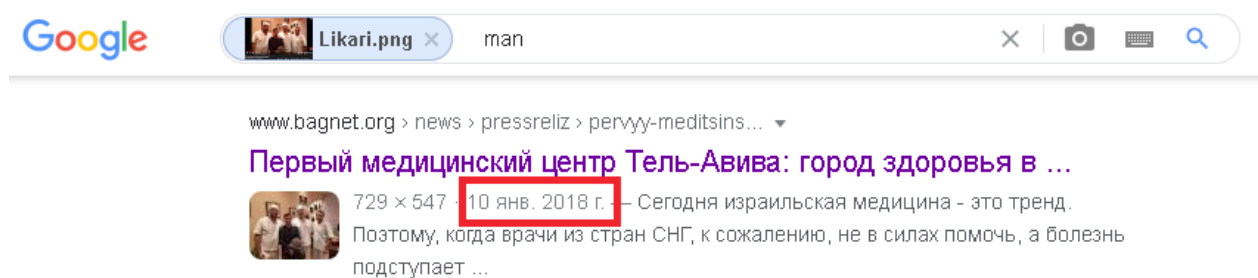


Рис. 15. Результати зворотного пошуку

Наразі після публічного викриття А. Шарій перемонтував своє відео та видалив частину з описаним фото. Натомість видалений фрагмент можна переглянути за посиланням: https://censor.net/ru/photo_news/3230988/propagandist_shariyi_vydal_feyik_o_tom_chno_bolnoyi_koronavirusom_zelenskiyi_fotografiruetsya_s_vrachami¹¹.

Нерідко для того, щоб зрозуміти політику наповнення того або іншого інформаційного ресурсу, потрібно проаналізувати сайт, через який доноситься інформація. З цією метою вельми корисним вбачається застосовувати ресурс github.com/jonkeegan/behind-this-website, який містить чекліст для визначення особи, яка стоїть за тим або іншим сайтом. Технічні особливості виявлення сайтів з дезінформацією можна знайти за адресами:

- ▶ A Look at Misinformation & Disinformation and How to Fight It: Part 1 (maltego.com/blog/infographic-misinformation-and-disinformation/);
- ▶ Investigating Misinformation & Disinformation: Part 2 (maltego.com/blog/investigating-misinformation-and-disinformation-campaigns/).

Коли йдеться про комбіновані способи виявлення фейків, тут поєднуються обидва раніше наведених підходи. І це, насправді, найбільш ефективний інструмент протидії інформаційним загрозам.

27 березня 2014 року в мережі Інтернет за адресою: <https://www.youtube.com/watch?v=LTBpSGnD09I> було розміщено аудіозапис із назвою «Телефонный разговор бойцов СОКОЛА. Следующая цель СБУ – ЯРОШ (18+) без цензури», в якому нібито два працівники спецпідрозділу міліції України обговорюють наказ свого керівництва про злочинну ліквідацію під час затримання одного відомого громадського і політичного діяча. Аналіз мови діалогу дозволяє зазначити, що один із співрозмовників має характерний російський говір, в який він зрідка вставляє українські слова, хоча для так званого українського суржику навпаки є притаманною вставка російських слів в українську мову. Аналіз сигналу запису в звуковому редакторі дозволив виявити факт того, що аудіосигнал нібито перехоплення телефонної розмови складається із двох незалежних сигналів для кожного співрозмовника. Тобто запис учасників діалогу здійснювався із двох відокремлених незалежних мікрофонів, а потім два моносигнали було об'єднано у стереосигнал діалогу, що суперечить факту запису мовного сигналу із монофонічного телефонного каналу зв'язку. На рис. 16 показано перші 3 секунди аудіозапису, де звучить дійсна стереофонічна музична заставка, й в кожному каналі існують корельовані сигнали, а на рис. 17 показаний наступний фрагмент некорельованих моносигналів, що об'єднанні у стереосигнал нібито перехоплення із монофонічного телефонного каналу зв'язку.

¹¹ Пропагандист Шарій выдал фейк о том, что больной коронавирусом Зеленский фотографируется с врачами, прикрепив фото 4-летней давности. ВИДЕО+ФОТО. URL: https://censor.net/ru/photo_news/3230988/propagandist_shariyi_vydal_feyik_o_tom_chno_bolnoyi_koronavirusom_zelenskiyi_fotografiruetsya_s_vrachami.

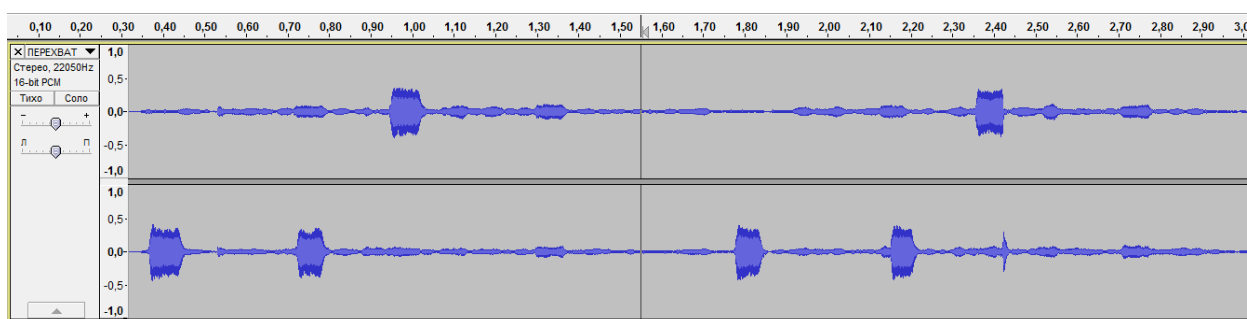


Рис. 16. Перші 3 секунди аудіозапису, де звучить дійсна стереофонічна музична заставка, і в кожному каналі існують корельовані сигнали

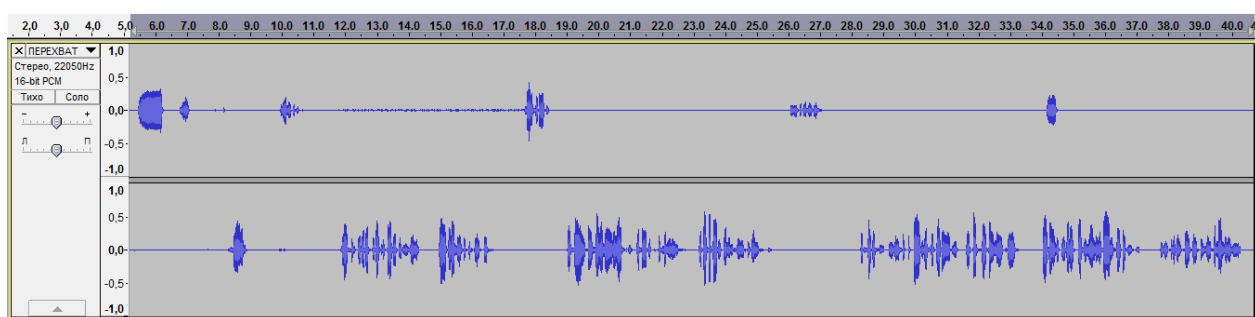


Рис. 17. Фрагмент аудіозапису некорельованих моносигналів, що об'єднані у стереосигнал нібито перехоплення із монофонічного телефонного каналу зв'язку¹²

Велику кількість інструментів розпізнавання фейків наведено на сайтах stopfake.org, snopes.com, factcheck.org, truthorfiction.com.

Для перевірки новинного контенту на предмет його висвітлення засобами масової інформації різної спрямованості досить корисним буде ресурс ground.news. За його допомогою можна оцінити подачу різного новинного матеріалу з точки зору лівих, центристських та правих засобів масової інформації (рис. 18).

У цього проекту також є розширення та функція Blindspot, яка допомагає вивчити новини, що не потрапили у тренди.

¹² Носов В.В., Манжай О.В. Окремі аспекти протидії інформаційній війні в Україні. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2015. № 1(29). С. 26–29.

Russia attacked civilian building in Zaporizhzhia -officials

Left

Center

Right



- A Russian missile struck a hotel in Zaporizhzhia, [Ukraine](#), killing one person and injuring 16 others. The Iskander missile hit the city at 7:20 p.m.
- The damaged hotel, Reikartz Hotel, was frequently used by United Nations personnel and NGOs, according to Denise Brown, the humanitarian coordinator for Ukraine.
- The Zaporizhzhia nuclear plant, which is controlled by the Russian military, lost connection to its main external power line and switched to a reserve line. The reserve line has less power capacity and poses a risk to the plant's equipment.

Insights by Ground AI ⓘ

GROUND
News

Published 3 days ago · [Ukraine](#)



News Articles

All

Left

Center

Right

More Filters



TVA Nouvelles

Lean Left

Mixed Factuality



A child killed by a Russian strike in western Ukraine

An eight-year-old child was killed by a Russian missile in the Ivano-Frankivsk region on Friday.

3 days ago

[Read Full Article](#)

Рис. 18. Результат роботи сервісу ground.news

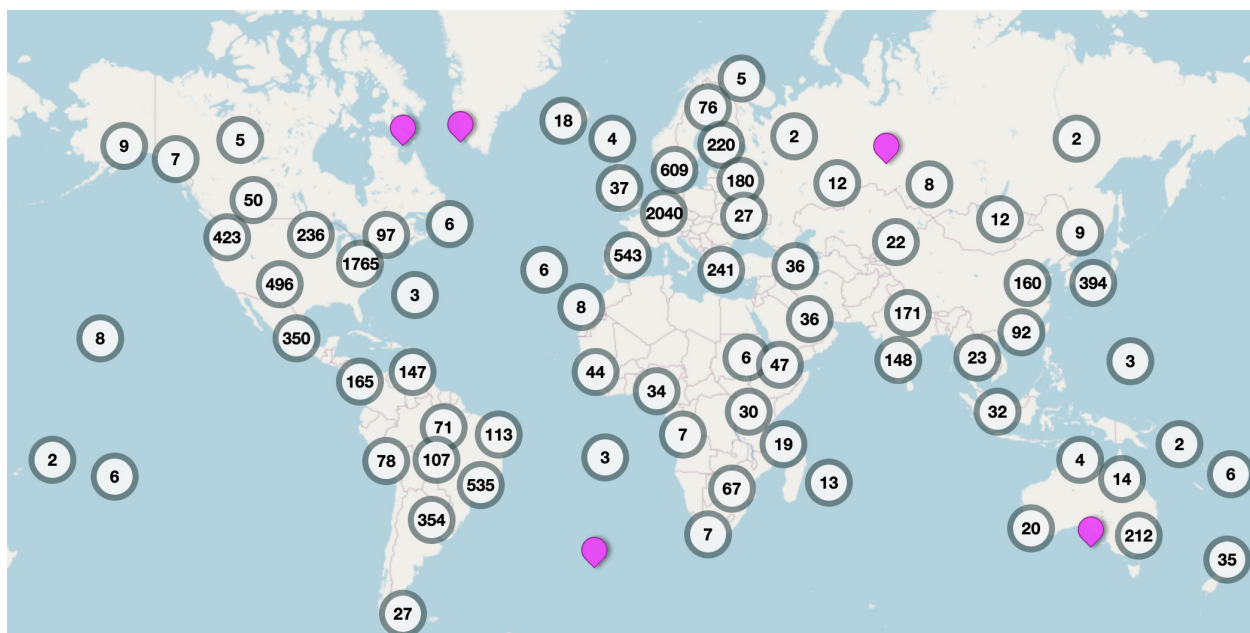


Рис. 19. Ресурс Newspaper Map (newspapermap.com)

Також Google має у своєму арсеналі інструментарій Fact Check Tools (toolbox.google.com/factcheck), за допомогою якого можна перевіряти окремі відомості на достовірність (рис. 20).

Україна

More results in other languages

Language filter

Ukrainian



Claim by notes_veterans:

"Просто YouTube Music опублікував ТОП виконавців для прослуховування в Україні. Жодного виконавця українською"

Голос Америки rating: Неправда

Націоналістичні канали в Росії підтасовують дані YouTube, щоб стверджувати, що українці буцімто не слухають українських музикантів

6 days ago

Музикант

YouTube

Україна

Голос Америки

Fact Check Explorer

Україна

Language filter

Ukrainian



Claim by Пост у Фейсбучі:

На фото – український паспорт Олени Зеленської

Demagog rating: Фейк

Ізраїльський паспорт Олени Зеленської? Це фальшивка

Jun 27, 2023

Олена Зеленська

Паспорт

Україна

Demagog

Рис. 19. Fact Check Tools

Також Google має у своєму арсеналі інструментарій Fact Check Tools (toolbox.google.com/factcheck), за допомогою якого можна перевіряти окремі відомості на достовірність (рис. 20).

Висновки

Найбільш складним і часовитратним, проте достатньо ефективним методом протидії неправдивим повідомленням, на нашу думку, є підвищення аналітичних здібностей суспільства, навчання методам критичного аналізу повідомлень, убезпечення від інформаційних диверсій. Усе наведене дає підстави говорити про необхідність активізації в нашій країні зусиль з розбудови ефективної структури інформаційного протиборства.