

3. Taddeo, M., & Floridi, L. (2023) The ethics of artificial intelligence in cybersecurity: A social-technical perspective. *Journal of Cybersecurity*, 9(1), 1–15. <https://doi.org/10.1093/cybsec/tyad004>

4. Ruzickova, M., Dzhalladova, I., Kaminsky, O., Bartash, O., & Pavlov, A. (2023). AI and LLM models to analyze and identify cybersecurity incidents. CEUR Workshop Proceedings, 3746, 115–123. <https://ceur-ws.org/Vol-3746/paper11.pdf>

Калганова В.І.,
старший викладач,
Барташ О.В.,
асистент,
КНЕУ імені Вадима Гетьмана

ІНФОРМАЦІЙНА ЕТИКА ЯК ІНСТРУМЕНТ ПРОТИДІЇ КОРУПЦІЇ В СОЦІАЛЬНИХ МЕРЕЖАХ

У сучасному цифровому середовищі соціальні мережі стали потужним каналом не тільки для комунікації, а й для поширення маніпуляцій, фейкових новин і корупційних схем. Ці платформи використовуються для впливу на громадську думку, мобілізації електорату, дестабілізації ситуації, фінансових зловживань. Тому зростає потреба у формуванні інформаційної культури з акцентом на етичні норми поведінки в цифровому просторі. Інформаційна етика, як складова інформаційної культури, виступає одним із найважливіших чинників стримування подібних загроз [5].

Інформаційна етика — це система моральних принципів, що регулює процес створення, поширення та споживання інформації в Інтернеті. Її ключовими складовими є достовірність, відповідальність, приватність, прозорість намірів та поважне спілкування [5]. Дотримання цих принципів знижує ризик участі в інформаційних маніпуляціях та сприяє прозорості цифрового простору.

Окреме значення має протидія фейковим новинам, які, за даними дослідження МІТ, поширюються у Twitter на 70% швидше, ніж достовірна інформація [2]. Їх часто супроводжують емоційні заголовки, навмисне

спотворені факти та цільове використання ботів. Такі технології активно використовуються для прикриття корупційних дій, просування політичних інтересів або фінансових афер.

Технології штучного інтелекту та машинного навчання вже сьогодні допомагають виявляти фейки, але їхня ефективність значною мірою залежить від етичної поведінки користувачів [2]. Саме тому розвиток інформаційної етики повинен супроводжувати технологічний прогрес.

Інформаційна етика також пов'язана з правовою культурою. Користувач, який усвідомлює свої інформаційні права та відповідальність, здатен не лише захистити себе, а й виявляти порушення, ініціювати розслідування і долучатися до формування здорового інформаційного простору.

Феномен цифрової корупції охоплює низку проявів: від дезінформації та замовних кампаній до прихованої реклами, шахрайських зборів коштів та маніпулювання громадською думкою. Ці процеси активно впроваджуються через ботоферми, тролів, фейкові акаунти та таргетовану рекламу. З огляду на низький рівень цифрової грамотності серед частини населення, такі загрози набувають системного характеру та впливають на національну безпеку [4].

Інформаційна етика — це сукупність норм і правил, що регулюють поведінку користувачів у цифровому середовищі. Вона базується на принципах:

- достовірності (перевірка джерел, недопущення поширення фейків),
- відповідальності (усвідомлення наслідків цифрових дій),
- прозорості (відкрите зазначення намірів, партнерства, реклами),
- поваги до приватності (збереження конфіденційності),
- етичного діалогу (уникнення хейту та тролінгу).

Дотримання цих принципів формує безпечне інформаційне середовище, у якому мінімізується ризик цифрової корупції.

Окрему загрозу становлять фейкові новини. Дослідження МІТ доводять, що неправдива інформація поширюється швидше, ніж достовірна, особливо в емоційно забарвленому контексті. Цей феномен використовується у політичних

та фінансових цілях — з метою відволікання уваги, очорнення опонентів або просування шахрайських схем.

У контексті боротьби з корупцією в соціальних мережах особливу роль відіграє медіаосвіта.

Медіаосвіта та критичне мислення — це фундаментальні інструменти, що формують здатність людини розпізнавати маніпуляції та фейки. В Україні вже діють освітні ініціативи, що сприяють розвитку медіаграмотності:

- шкільні проєкти («Вивчай та розрізняй» за підтримки IREX),
- курси у вишах (журналістика, цифрова безпека),
- платформи онлайн-освіти (Prometheus, EdEra, Filter) [6].

Медіаосвіта має інтегрувати в собі етичні компоненти — навчання усвідомленому використанню інформації, повазі до прав інших, відповідальності за власні цифрові дії. Вона формує критичне мислення, здатність перевіряти факти, розрізняти джерела та уникати поширення маніпулятивного контенту.

Крім того, етична комунікація у публічному просторі має стати нормою для журналістів, блогерів, політиків. Відмова від прихованої реклами, маніпулятивних наративів, хейту та дезінформації — основа для формування довіри в суспільстві [4]. Технологічні рішення для боротьби з дезінформацією та цифровою корупцією наведено в таблиці 1.

Таблиця 1.

Аналіз технологічних рішень для боротьби з дезінформацією та цифровою корупцією

Категорія дій	Інструменти	Функції
Розпізнавання фейків	ШІ-моделі, аналіз NLP	Автоматизований аналіз контенту на правдивість
Фактчекінг	StopFake, VoxCheck, Bellingcat	Перевірка достовірності тверджень та новин
Аналіз бот-активності	Botometer, Hoaxy	Виявлення неавтентичної активності в мережі
Контент-фільтрація та маркування у соцмережах	Meta, Google, TikTok	Позначення потенційно шкідливого чи маніпулятивного контенту

Держава і громадянське суспільство мають діяти у взаємодії. З боку держави необхідне:

- законодавче врегулювання цифрової поведінки (регламентація політичної реклами, прозорість сторінок, боротьба з фейковими акаунтами);
- підтримка освітніх проєктів;
- розвиток цифрової інфраструктури ("Дія.Освіта", "Дія.Центр").

Також, технології штучного інтелекту пропонують інструменти для урядів (зверху вниз) і, що ще важливіше, для громадян (знизу вгору) для перевірки уряду (посадовців). Ці відносно нові форми використання ШІ для боротьби з корупцією поки отримали мало емпіричної уваги. Тому детальніше окреслюємо унікальні можливості та недоліки штучного інтелекту у підходах «зверху вниз» та «знизу вгору» (див. таблицю 2).

Таблиця 2.

Огляд потенціалу та проблем використання ШІ для боротьби з корупцією

Інструменти на базі штучного інтелекту для боротьби з корупцією	Підхід згори вниз (Top-Down)	Підхід знизу вгору (Bottom-Up)
Учасники (Актори)	Кримінальні слідчі, прокурори, інспектори з дотримання норм, аудитори	Журналісти, блогери, активісти громадянського суспільства, пересічні громадяни
Вхідні дані	Засекречені та відкриті урядові дані, краудсорсингові дані, (соціальні) медіа	Відкриті урядові дані, витоки даних, краудсорсингові дані, (соціальні) медіа
Алгоритмічний підхід	Орієнтованість на мінімізацію хибнонегативних результатів	Орієнтованість на мінімізацію хибнопозитивних результатів
Інституційна реалізація	Усунення людини з процесу, щоб уникнути пастки корупції	Участь людини у процесі для забезпечення легітимності
Приклади	MARA, Kalsada	Botivist, Dozorro

Участь з боку громадськості також здійснюється через незалежний моніторинг діяльності посадовців та медіа (YouControl, Bihus.Info); адвокація змін у політиці протидії дезінформації; участь у просвітницьких кампаніях. Таке

партнерство створює підґрунтя для сталого розвитку інформаційної етики на національному рівні [3].

Таким чином, інформаційна етика не є факультативом — вона є базисом цифрової гігієни, надійною основою для протидії корупції та засобом збереження інформаційної безпеки держави. Її формування потребує комплексного підходу: від освітніх програм до нормативно-правового регулювання та просування відповідального ставлення до цифрового контенту.

Висновки. Інформаційна етика є не просто набором правил, а ключовою складовою цифрової безпеки та демократичного розвитку. Її формування потребує системної просвіти, ефективного регулювання та індивідуальної відповідальності кожного користувача.

У боротьбі з цифровими формами корупції інформаційна етика виконує кілька важливих функцій:

- знижує ефективність фейків і маніпуляцій;
- підвищує рівень критичного мислення;
- зміцнює довіру до достовірних джерел;
- формує культуру поваги й відповідального спілкування в інформаційному просторі.

Формування інформаційної етики — це довготривалий процес, який вимагає участі всіх соціальних інститутів: школи, ЗМІ, держави, бізнесу та громадянськості. Саме завдяки такій співпраці можливо створити прозоре, відповідальне й безпечне цифрове середовище.

Список використаних джерел

1. Shao, C., Ciampaglia, G. L., Flammini, A., & Menczer, F. (2016). *Hoaxy: A Platform for Tracking Online Misinformation*. arXiv:1603.01511.
2. Shu, K., Sliva, A., Wang, S., Tang, J., & Liu, H. (2017). *Fake News Detection on Social Media: A Data Mining Perspective*. arXiv:1708.01967.
3. UNESCO (2021). *Media and Information Literacy Curriculum for Educators and Learners*.

4. Wardle, C., & Derakhshan, H. (2017). *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*. Council of Europe.
5. Оксамитна С.О. (2020). *Інформаційна етика в умовах цифровізації суспільства*. Вісник КНУКіМ. Серія: Соціальні комунікації, №2.
6. Куліш А.М. (2022). *Медіаграмотність як засіб запобігання дезінформації в Україні*. Наукові записки Інституту журналістики, №4.

Калюх В.О.,
здобувачка вищої освіти (першого) бакалаврського рівня,
Потапенко С.Д.,
кандидат економічних наук, доцент,
Київський національний економічний університет імені Вадима Гетьмана

АНАЛІТИКА БЕЗПЕКИ В ЗАДАЧАХ БІЗНЕСУ ТА ЕКОНОМІКИ

У сучасному світі дані стали стратегічним ресурсом, який визначає конкурентоспроможність компаній та ефективність державного управління. Достовірність даних та надійність методів їх обробки відіграють важливу роль в ефективному вирішенні задач бізнесу та економіки. Аналітика безпеки відіграє ключову роль у прийнятті якісних управлінських рішень, допомагаючи перетворювати масиви інформації у реальні дії та стратегії.

Аналітика безпеки у бізнесі — це процес збору, обробки та аналізу внутрішньої інформації компанії для оптимізації її діяльності, підвищення прибутків, скорочення витрат, формування ефективної політики інформаційної безпеки. Економічна аналітика охоплює макрорівень: аналіз державного бюджету, ВВП, інфляції, рівня безробіття, внутрішніх та зовнішніх загроз розвитку держави.

Існує чотири основні підходи до забезпечення аналітики безпеки: описова (пояснює що сталося), діагностична (пояснює чому це сталося), прогностична (оцінює ймовірність майбутніх подій) та прескриптивна (надає конкретні рекомендації щодо дій з метою усунення загроз та небезпек).