HEINRICH BÖLL STIFTUNG
КИЇВ
Україна

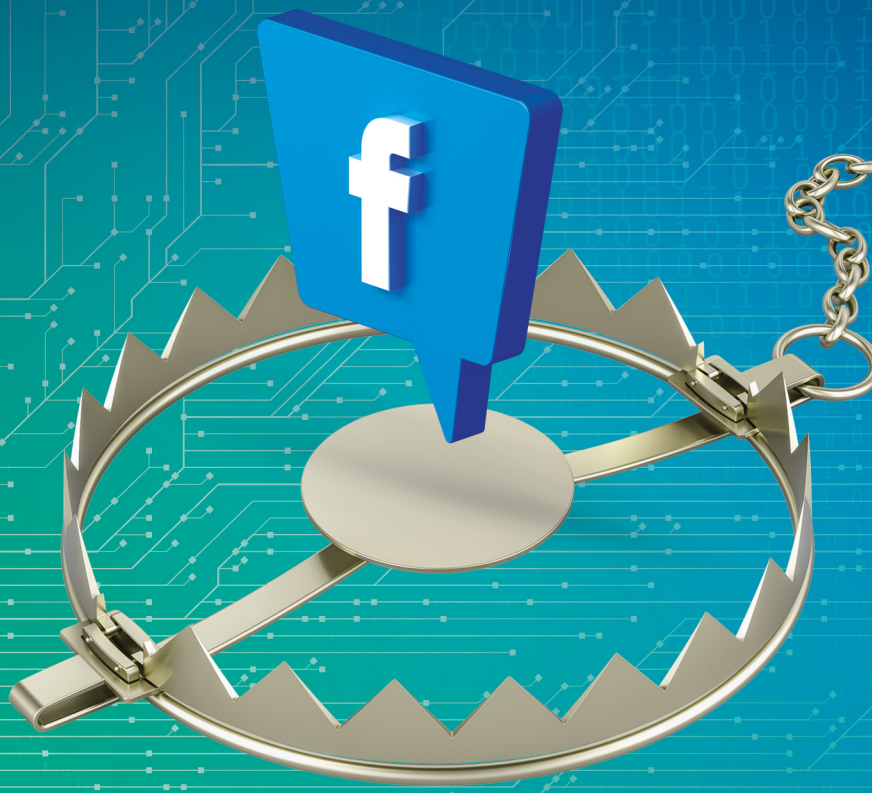
ЦЕНТР ДЕМОКРАТІЇ ТА
ВЕРХОВЕНСТВА ПРАВА

НЕБЕЗПЕКА У СТРІЧЦІ FACEBOOK:

клікбейт і таргетована реклама як знаряддя маніпуляцій та шахрайства

Павло Бурдяк

аналітик напряму «Незалежні медіа» Центру демократії та верховенства права



2025

Дослідження проведено за фінансової підтримки Фонду ім. Гайнріха Бьолля, Бюро Київ — Україна. Думки, висновки та рекомендації належать авторам цього дослідження і не обов'язково відображають погляди Фонду ім. Гайнріха Бьолля, Бюро Київ — Україна та уряду Німеччини.

Зміст

Вступ

У контексті повномасштабної війни проти України питання цифрової та інформаційної безпеки набуває дедалі більшого значення. Соціальні мережі, зокрема платформи Meta (особливо Facebook), відіграють ключову роль у поширенні критично важливої інформації, формуванні громадської думки та взаємодії громадян. Та водночас вони стають інструментом для поширення небезпечного контенту, маніпуляцій і шахрайства, спрямованого як на фінансову, так і на інформаційну експлуатацію користувачів.

Це дослідження зосереджується на двох ключових проблемах, характерних для українського сегменту Facebook. По-перше, воно аналізує **клікбейтні сторінки як один із основних інструментів поширення маніпулятивного та шахрайського контенту**. Під поняттям «клікбейт» ми розуміємо маніпулятивну практику формулювання заголовків або візуального оформлення публікацій, які через провокативність, сенсаційність чи емоційність стимулюють користувачів взаємодіяти з контентом переходити за відповідними посиланнями. Як наслідок, користувачі стають потенційними жертвами інформаційних або шахрайських маніпуляцій.

Другим аспектом дослідження є **поширення шахрайських схем та дезінформації за допомогою рекламних інструментів платформи Facebook**. Зловмисники активно використовують алгоритми таргетованої реклами для охоплення значних аудиторій, поширюючи інформацію про нібито соціальні виплати, фіктивні фінансові послуги, псевдомедичні препарати, шахрайство з орендою акаунтів і рахунків тощо. Така реклама ефективно експлуатує вразливі соціальні групи та суспільні настрої, які посилилися під час війни.

На основі конкретних прикладів, отриманих у результаті моніторингу та аналізу українського інформаційного середовища Facebook, дослідження окреслює специфіку зазначених схем, визначає ключові ризики, які виникають для користувачів, а також пропонує практичні рекомендації користувачам, як запобігти цим загрозам. Також окремо надаються рекомендації для компанії Meta, як удосконалити політику модерації та підвищити загальний рівень безпеки на платформі.

Таким чином, **метою цього дослідження** є комплексний аналіз механізмів поширення маніпулятивного клікбейту та шахрайської реклами на платформі Facebook, оцінка їхніх ризиків для українських користувачів, а також вироблення рекомендацій для підвищення стійкості українського сегменту Facebook до подібних загроз.

Методологія дослідження

Для вивчення шкідливих сторінок в українському сегменті Facebook, що використовують клікбейт, шахрайські схеми та фішинг, у цьому дослідженні застосовуються кілька взаємопов'язаних методів збору та аналізу інформації, які охоплюють емпіричну й теоретичну складові. Такий комплексних підхід дозволяє всебічно дослідити специфіку діяльності шкідливих (клікбейтних та шахрайських) сторінок, визначити їхню приховану мету та розробити рекомендації для користувачів Facebook і загалом платформи Meta.

1. Збір первинних та вторинних даних. На початковому етапі здійснювався збір шкідливих сторінок і конкретних кейсів фішингу та шахрайства. Для цього автори дослідження вдалися до таких активностей:

- **моніторинг та документування**. Дослідники промоніторили та задокументували діяльність клікбейтних і шахрайських сторінок на Facebook через пошук за ключовими словами та бібліотеку реклами Meta (Ad Library). Також слід виокремити взаємодію зі шкідливими (клікбейтними та шахрайськими) сторінками, внаслідок якої алгоритми Facebook пропонували ще більше схожих сторінок;

- **збір кейсів від Центру демократії та верховенства права (ЦЕДЕМ)**. Аналіз даних із конкретних кейсів, які були виявлені й передані до Meta Центром демократії та верховенства права;

- **аналіз відкритих джерел.** Вивчалися наявні публічні джерела, звіти, дослідження та аналітичні матеріали, що документують діяльність подібних сторінок у Facebook: як в Україні, так і в інших країнах;

- **створення бази даних із кейсами.** У межах дослідження було створено таблицю, яка містить детальну інформацію про шкідливі сторінки: дати створення, історія змін назви сторінки, тип поширюваного контенту, місцезнаходження адміністраторів і типові поведінкові патерни.

2. Експеримент — взаємодія зі шкідливими сторінками. Для визначення алгоритмічних особливостей платформи було створено спеціальний окремий профіль на Facebook, який взаємодіяв зі шкідливими клікбейтними сторінками. Експеримент мав на меті перевірити, чи пропонує Facebook користувачам схожий контент після такої взаємодії і наскільки швидко та інтенсивно це відбувалося.

3. Контент-аналіз. Класифікація шкідливих сторінок за типами контенту (клікбейт, шахрайство), аналіз тематичних і стилістичних особливостей постів.

4. Кейс-стаді. Проведено поглиблене дослідження окремих репрезентативних кейсів шкідливих сторінок, щоб показати процес їхнього розвитку, переходу від нейтрального контенту до поширення шахрайства, дезінформації та контенту низької якості.

5. Метод індукції. На основі аналізу конкретної вибірки шкідливих сторінок дослідники сформували узагальнені висновки щодо закономірностей їх створення, розвитку, способів залучення аудиторії та прихованих цілей.

6. Аналіз політик Meta. Оцінено ефективність політик платформи Meta в боротьбі зі шкідливим контентом. Увагу приділено маркуванню контенту, створеному за допомогою штучного інтелекту, реакції на клікбейт та фішинг, а також протидії шахрайським схемам. А також ролі й місцю фактчекерів у цих процесах.

7. Розробка рекомендацій для користувачів Facebook. На основі результатів дослідження були сформовані зрозумілі й практичні рекомендації для користувачів Facebook. Рекомендації включають поради, як розпізнати шкідливий контент, розуміти їхні загрози, уникати взаємодії з клікбейтними та шахрайськими сторінками, розпізнавати фішингові повідомлення й сайти.

8. Розробка рекомендацій для Meta. На підставі отриманих даних та аналітичних висновків сформульовано конкретні, практичні рекомендації для платформи Meta, як посилити захист користувачів від шкідливого контенту, покращити маркування контенту, створеного за допомогою штучного інтелекту, а також як вдосконалити загальну систему реагування на шкідливі та шахрайські сторінки.

Тож комплексний підхід, який поєднує різноманітні методи дослідження — від збору даних до багаторівневого аналізу, — дозволив глибоко проаналізувати феномен шкідливих сторінок у сегменті українського Facebook. Завдяки цьому дослідження пропонує ефективні та практичні рекомендації і для компанії Meta щодо покращення її політик і механізмів захисту, і для користувачів щодо підвищення цифрової грамотності й безпеки в онлайн-просторі. Дослідження покликане сприяти формуванню безпечнішого інформаційного середовища в українському сегменті Facebook.

1. Клікбейтні сторінки у Facebook: від емоцій до маніпуляцій

У цифрову добу, коли платформи соціальних мереж стали основним джерелом споживання новин та інформації, здатність відрізнити достовірне від маніпулятивного набуває вирішального значення. Одним із найбільш поширених і водночас недооцінених інструментів впливу на аудиторію є клікбейтні сторінки у Facebook.

Клікбейтні сторінки у Facebook — це сторінки, які систематично публікують емоційно насичений, візуально привабливий та маніпулятивний контент, щоб спонукати користувачів до активної взаємодії (лайків, коментарів, поширень) і таким чином нарощувати охоплення. Їхня мета — не інформувати, а сформувати аудиторію, серед якої згодом можна просувати приховану адженду — політичні меседжі, дезінформацію тощо.

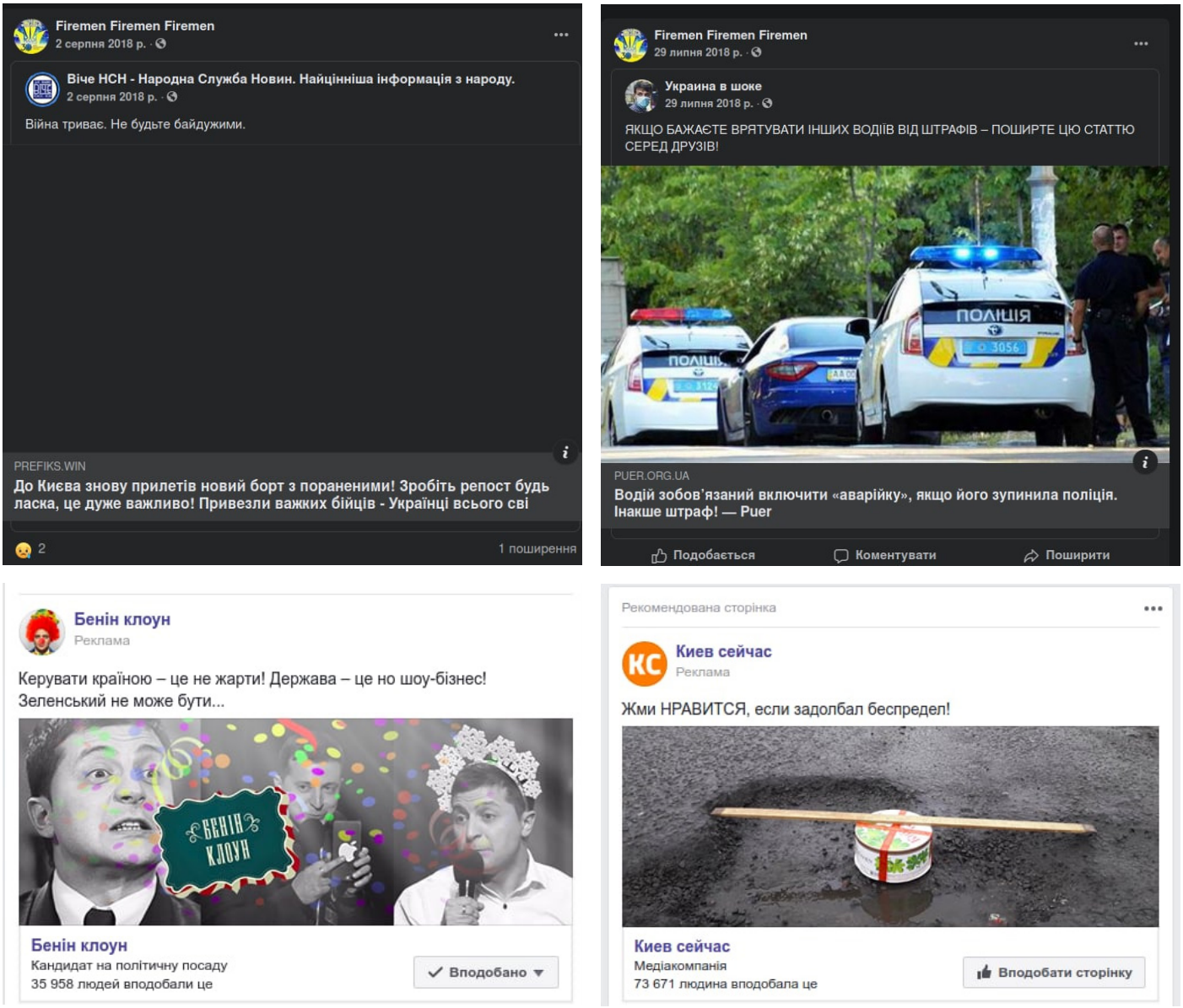
На перший погляд, клікбейтні пости можуть здаватися щирими та безневинними: вони зворушують, апелюють до патріотичних почуттів або релігійних переконань, іноді навіть надихають. Але за фасадом «лайкни, якщо підтримуєш» приховується продумана стратегія маніпуляції. Усе частіше такі сторінки використовуються для досягнення політичних, пропагандистських чи маніпулятивних цілей, і це особливо помітно у воєнний час, коли емоційна вразливість суспільства зростає.

У цьому розділі ми розглянемо, як виникають і функціонують клікбейтні сторінки, які саме тактики вони використовують для залучення уваги, яку приховану мету переслідують, а також які технічні та алгоритмічні чинники у Facebook дозволяють таким сторінкам досягати широкого охоплення. Окрему увагу буде приділено візуальному обману за допомогою зображень, створених штучним інтелектом, а також порадам як для звичайних користувачів, так і для самої платформи щодо протидії згаданим загрозам.

1.1. Походження проблеми

Клікбейтні сторінки — не нове явище в українському сегменті Facebook. Ще до повномасштабного вторгнення Росії у 2022 році на платформі траплялися сторінки, які збирали аудиторію за допомогою емоційних зображень, сентиментальних текстів і маніпулятивних закликів до взаємодії з контентом. Наприклад, у період 2018–2021 років часто поширювалися дописи з драматичними повідомленнями про війну, «невідкладними» порадами та «сенсаційними» попередженнями, рекламні оголошення з примітивними емоційними тригерами, а також політичний клікбейт, що експлуатував усталені образи та стереотипи.

Спільною рисою цих прикладів клікбейту було прагнення викликати сильну емоційну реакцію та стимулювати швидку взаємодію — репости, лайки або переходи за посиланнями.



Джерело: скриншоти ЦЕДЕМ

Проте після 2022 року масштаб і вплив цього явища суттєво зросли. На це є кілька причин. По-перше, повномасштабна війна створила новий емоційно насичений контекст, у якому особливо легко викликати реакцію користувачів — пости про захисників, обстріли, втрати й молитви за Україну стали потужним інструментом залучення користувачів. По-друге, зростання доступності інструментів штучного інтелекту дало змогу швидко й масово генерувати зображення, що виглядають емоційно зворушливо та водночас викликають довіру — навіть якщо вони цілком вигадані. По-третє, соціальні мережі стали основним джерелом новин для більшості українців. Зокрема, Facebook для споживання інформації використовують 44,6% українців. Поєднання цих трьох факторів зробили соцмережі, такі як Facebook, особливо привабливим полем для зловживань із боку клікбейтних сторінок, що експлуатують емоції українських користувачів у часи війни.

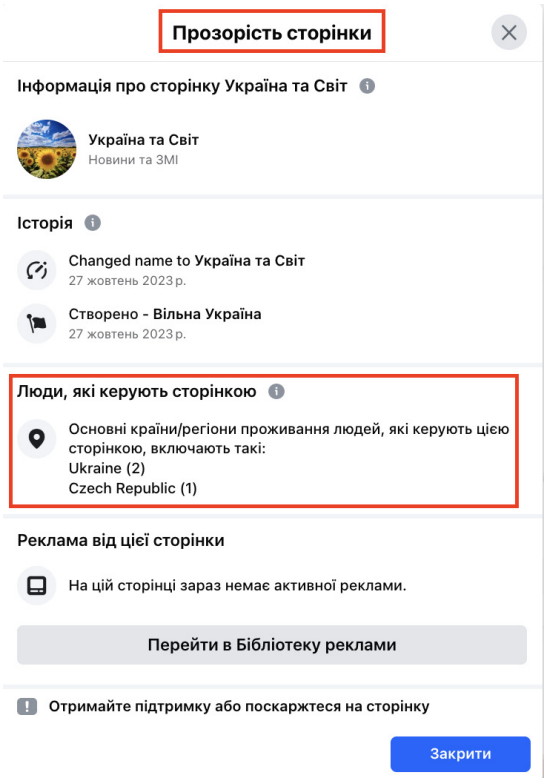
1.2. Ознаки клікбейтних сторінок

Нова хвиля клікбейтних сторінок спостерігалася в 2022–2024 роках. Загалом ці сторінки можна визначити за такими **типовими ознаками:**

1. Назви сторінок, які або викликають емоції, або мають незрозуміле звучання. Назви клікбейтних сторінок можуть мати найрізноманітніше звучання: від українських патріотичних або нейтральних назв до сторінок з іменами, характерними для азійського регіону, або вигаданими фразами, які не несуть особливого сенсу. Приклади включають:

- українські або патріотичні назви: «Українська реальність», «Наша улюблена Україна», «Слава Українському народу»;
- азійські, англійські та інші іноземні слова, імена або випадкові фрази: «Garen Atariха», «Niat Sae», «Gossip here»;
- слова українською або російською, які не мають жодного відношення до контенту сторінки: «Ключ», «Море Внутри», «Я знаю»;
- мімікрування під новинні видання зі словами «новини», «news», «Україна», «світ»: «Україна та Світ», «Ukrainian News»;
- релігійні елементи (українською чи російською): «Православна щоденна молитва», «Молитвы НА Каждый ДЕНЬ».

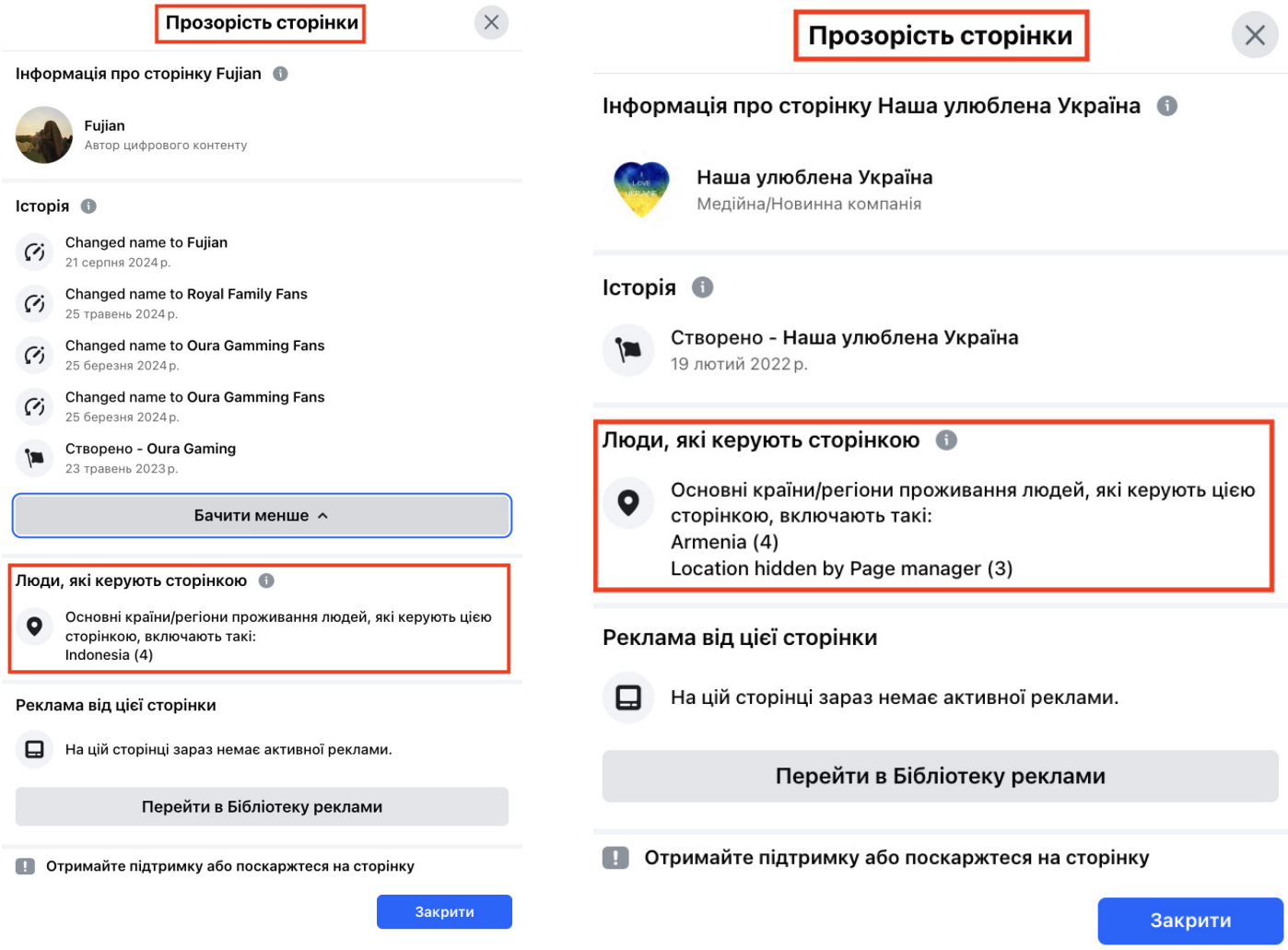
2. Керування сторінкою з-за кордону. Багато клікбейтних сторінок, згідно з аналізом технічної інформації, мають адміністраторів або географічне походження з-за меж України. Якщо до повномасштабного вторгнення більшість таких сторінок модерувалися з Вірменії, то сьогодні поруч із Вірменією стрімко зросла кількість сторінок, що походять з Індонезії. Цю інформацію можна знайти у вкладці «Прозорість сторінки».



Джерело: скриншоти ЦЕДЕМ

Трапляються й сторінки, які модеруються з України — або з України та інших країн, якщо модераторів багато. Хоча незрозуміло, чи сторінки, позначені як такі, що «керуються з України», охоплюють виключно підконтрольну Україні територію, чи також тимчасово окуповані території.

Втім іноді дані про країну адміністрування приховані або не відображаються. Натомість міститься напис «Location hidden by Page



Джерело: скриншоти ЦЕДЕМ

manager» («Місцезнаходження приховано адміністратором сторінки»). Через цю функцію досліджувати походження сторінки значно складніше.

3. Аватар сторінки. Залежно від назви і «легенди» сторінки підбирається відповідне візуальне оформлення. Умовно можна виокремити п'ять основних типів аватарів відповідно до виду сторінки:

- патріотичні сторінки зазвичай мають аватари з українською символікою, як-от із прапором чи тризубом. На обкладинках використовуються зображення українських військових, патріотичні підписи тощо. Такий візуал має одразу викликати довіру, співпереживання та ідентифікацію з українським контекстом;

- зображення осіб азійської або європейської зовнішності як аватар сторінок, названих відповідними іменами. Обкладинки — абстрактні або генеративні візуали, пейзажі, випадкові зображення предметів або «гарні картинки» без суттєвого смислового навантаження;

- випадкові зображення у сторінок із неавтентичними назвами. Сторінки з випадковими назвами (наприклад, «Море Внутри», «Я знаю») використовують аватари без чіткої ідентичності: це можуть бути фрагменти зображень, умовні портрети, частини предметів або фони. Обкладинки подібно до аватарів — випадкові, нерелевантні, іноді з дивною композицією. Усе це створює ефект присутності, але без суттєвого смислового наповнення;

- аватари та обкладинки сторінок, які імітують новинні ресурси, стилізують під логотипи відомих медіа. Вони можуть використовувати шрифти, кольори або композиції, які нагадують візуальний стиль справжніх медіа. Це робиться, щоби ввести користувача в оману — створити враження, що сторінка є частиною легітимного інформаційного ресурсу. Навіть якщо користувач не помічає стилізацію, схожість на логотипи знайомих брендів підсвідомо може викликати довіру та підвищувати ймовірність взаємодії з контентом;

- сторінки з релігійними назвами мають аватари з іконами, хрестами, зображеннями релігійних персонажів або інших релігійних символів. Обкладинки оформлені в тому ж стилі: сцени молитви, храмів, ікони, цитати зі святого письма. Такий візуал апелює до духовних почуттів і спонукає до «благочестивої» взаємодії.

4. Маніпулятивні дописи

Ще одна типова ознака клікбейтних сторінок — публікації, які грають на емоціях, але часто не містять правдивої інформації. Їхня головна мета — не інформувати, а викликати реакцію: змусити поставити лайк, написати коментар або поширити пост.

Часто це зворушливі звернення «від імені» військових, дітей, самотніх або літніх людей, у яких «день народження, але ніхто не привітав», «зроблені власноруч вироби, які ніхто не похвалив» тощо. Поширеними є й псевдоновини, оформлені як термінові, на кшталт «Обстріл у столиці! Подробиці шокують!», але без жодних джерел чи дат.

Такі дописи майже завжди супроводжуються візуально привабливими, але згенерованими штучним інтелектом зображеннями, які створюють ілюзію справжності.

Усе це — спроба створити враження щирого, «людяного» контенту, який викликає довіру і не виглядає як маніпуляція. Але саме за допомогою таких постів сторінки швидко набирають охоплення і впливають на користувачів.

Більшість цих тактик і прихованих цілей детально розглядатимемо в наступних розділах дослідження.

1.3. Тактики залучення уваги

Щоб отримати якомога більше охоплення, клікбейтні сторінки у Facebook використовують набір повторюваних тактик, спрямованих на емоційне залучення

користувачів. Їхня мета — не поінформувати людину, а викликати емоцію, яка спонукає до взаємодії, як-от поставити лайк, залишити коментар або поділитися постом. Усе це підвищує шанси потрапити до стрічок інших користувачів, адже саме така взаємодія є «паливом» для алгоритмів платформи.

Завдяки продуманому поєднанню емоційних сюжетів, візуального оформлення, закликів до дії та технічних «трюків» клікбейтні сторінки досягають значного успіху в охопленні аудиторії — навіть якщо не несуть жодної достовірної інформації.

Нижче описано п'ять основних тактик, якими найчастіше послуговуються клікбейтні сторінки в українському сегменті Facebook.

1.3.1. Використання емоційних сюжетів

Найчастіша і найефективніша тактика — це опублікувати пости з емоційно забарвленим зверненням. Їхній зміст може бути різним, але мета одна: зворушити, викликати емоцію, спонукати відреагувати. Типові сюжети можна умовно поділити на кілька груп:

- **Про військових.** Ці звернення використовують образи українських військових, щоб викликати почуття гордості, вдячності й емпатії. Часто додають зображення військових із втраченими кінцівками чи протезами. Типові пости мають такі підписи:
  - «Ми їдемо на фронт. Скільки людей сподіваються, що ми повернемося живими?»
  - «Перш ніж піти, подаруйте трохи любові українському солдату»
  - «Був важкий бій. Підтримайте, будь ласка, бо зараз дуже морально важко!»
  - «Дуже прикро, що ця фотографія [українських військових] набере менше ніж якась оголена співачка»
  - «Чарівна жінка — українська військова»

- **Релігійні звернення.** Тут маніпуляція відбувається через поєднання патріотизму з релігійністю. Приклад типових постів:
  - «Нехай Бог відповість на наші молитви. Амінь»
  - «Якщо Бог коли-небудь допомагав вам у вашому житті, будь ласка, доторкніться до зображення і напишіть "Амінь"»
  - «Хто молитиметься за нас [військових], щоб ми всі повернулися додому живими?»
  - «Моліться за мене [військового]»

- **Повідомлення про день народження.** Ця техніка базується на співчутті до окремої людини, яка нібито переживає важливу подію, таку як день народження, наодинці та/або просить привітати її. Типові дописи включають такі:

- «Цікаво, скільки людей привітає мене і побажає щастя»
- «Сьогодні мій день народження, а в мене немає ні торта, ні квітів, і ніхто мене не привітає!»
- «99 людей просто пролистають, і лише одна людина напише: “З Днем народження”»
- «Я національний пілот. Сьогодні мій день народження, але ніхто мене не привітав!»

- **Повідомлення про сімейні події.** Ці публікації імітують новини про весілля, народження дітей, багатодітність, довге подружнє життя тощо. Вони покликані пробуджуватиу користувача не жаль чи співчуття, а теплу емоцію радості й бажання розділити «щастя» з іншими. Типові формулювання:
  - «Сьогодні ми одружилися. Просимо вам привітати й побажати щастя»
  - «Велика, але щаслива сім’я, Будь ласка, не йдіть, не даруючи їм трохи любові»
  - «Хай Бог береже ці родини військових»
  - «Після 10 років шлюбу у нас народилася трійня ..... Дякуємо всім, хто нас привітав, це наш найбільший скарб!»

- **Саморобки.** Ще один поширений прийом — пости, у яких повідомляється, що якась людина нібито сама створила щось символічне (малюнок, іграшку, саморобку), але не отримала жодного відгуку чи похвали. Наприклад:
  - «Ця 90-річна бабуся щодня пече хліб для нашого захисника, підбадьоріть її»
  - «Ручна робота, але, на жаль, ніхто її не цінує.»
  - «Ця дівчина виклала з каміння портрет своєї покійної мами, але ніхто не підтримує її!»
  - «Витрачено багато сил, але жодного відгуку»
  - «Це було створено повністю вручну. Дякуємо всім, хто знаходить час оцінити це»
  - «Мій батько це зробив. Шкода, що нікому не подобається твоя робота»

Усі ці сюжети об’єднує спільна риса: вони вигадані, але виглядають «дуже людяно». Користувачеві важко залишитися байдужим — і саме це робить тактику такою ефективною.

1.3.2. Прямі заклики до взаємодії з клікбейтними публікаціями

Іншою тактикою, яку використовують клікбейтні сторінки, є відверті, прямі заклики до користувача зробити щось: поставити лайк, залишити коментар або поширити пост. Це не просто прохання — у таких закликах часто присутній емоційний або моральний тиск, що робить відмову від дії ледь не «неприпустимою».

Такі заклики можуть бути відносно «м'якими»:

- «Я тебе захищаю. Будь ласка, побажайте мені удачі!»
- «99 пролистають і лише 1 напише "Повернувся живим"»

Водночас трапляються й наполегливіші та маніпулятивніші формулювання:

- «Постав сердечко, і я буду захищати твою сім'ю»
- «Ти ніколи не пожалкуєш, що оцінив(ла) це фото [зображення українського військового]»
- «Так, як ти ставишся до цього фото, так і складеться твій 2025 рік»
- «Якщо Бог багато разів рятував ваше життя, напишіть "Амінь"»
- «Я не розумію, чому люди соромляться ставити лайки під такими фотографіями»

Вплив подібних фраз глибший, ніж здається на перший погляд. Вони діють на трьох рівнях:

- спричиняють емоційний тиск — користувач починає відчувати, що «правильно» лайкнути чи прокоментувати щось, інакше він ніби проявляє черствість або зраду (особливо коли йдеться про військових, релігію, дітей);
- приносять алгоритмічну вигоду — кожен лайк, коментар чи репост «піднімає» пост у стрічках інших користувачів, адже система Facebook сприймає таку активність як ознаку популярності;
- відкривають пряму комунікацію — коментарі чи репости створюють поле для дискусій, втягують у взаємодію друзів користувача, запускають нові кола обговорень. Як наслідок, публікація отримує ще більший розголос і охоплення.

У результаті взаємодія відбувається, зокрема, через те, що користувача «підштовхнули» до неї. Ця тактика залучення взаємодії ефективна — особливо в умовах війни, коли люди підвищено чутливі до тем підтримки, віри чи патріотизму.

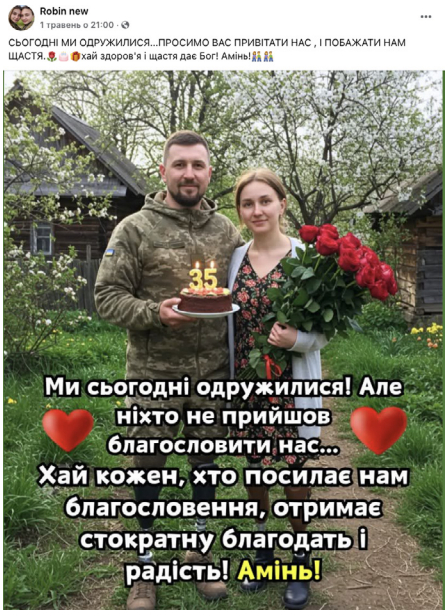
1.3.3. Використання згенерованих штучним інтелектом зображень

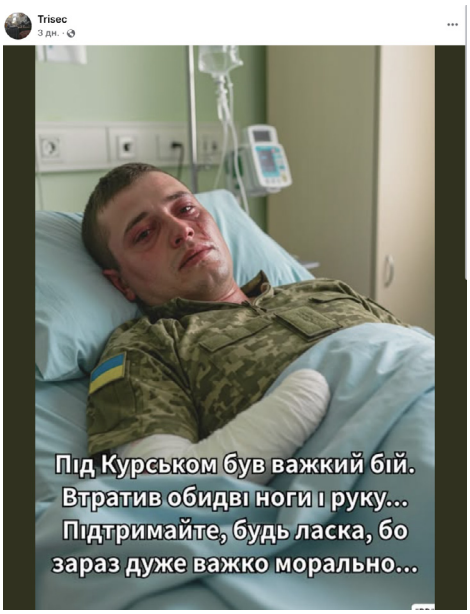
Зображення — одна з важливих складових типового клікбейтного посту. Візуальний елемент у таких публікаціях не просто ілюструє текст, а створює ілюзію правдивості. Якщо користувач бачить «фото» військового, родини чи бабусі з хлібом — його мозок автоматично сприймає це як доказ: «це справжня історія». Саме цим активно користуються адміністратори клікбейтних сторінок і саме так, судячи з коментарів під багатьма такими дописами, вдається ввести в оману численних користувачів.

Щоб виробляти потрібні зображення швидко, дешево і без значних зусиль, адміністратори клікбейтних сторінок усе частіше використовують інструменти генерації зображень за допомогою штучного інтелекту. Ці візуали створюються буквально за хвилини — і, що головне, вони виглядають емоційно переконливо, попри те, що не мають жодного стосунку до реальності.

Типові клікбейтні пости з використанням ШІ-зображень включають:

- «військового» із проникливим поглядом, іноді з ампутованими кінцівками або протезом, з українським прапором тощо:





Джерело: скриншоти ЦЕДЕМ

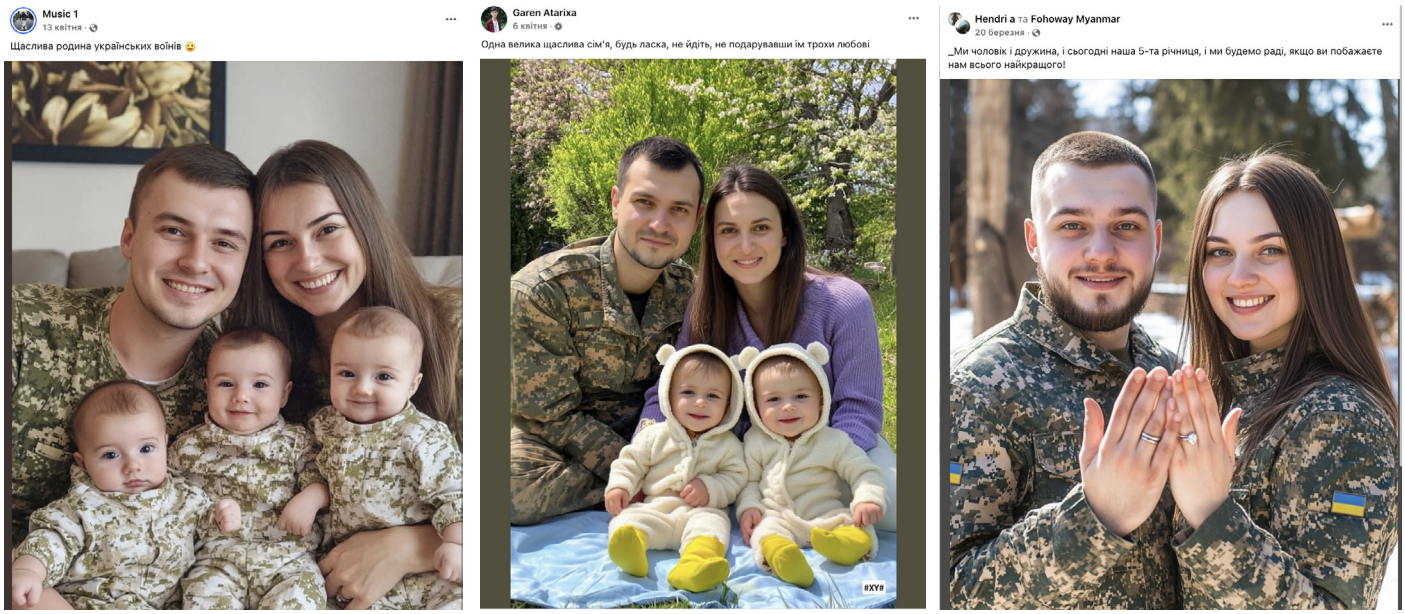
- стареньку, яка «щодня пече хліб для ЗСУ»:

Джерело: скриншоти ЦЕДЕМ

- малюнки, вироби чи портрети, які «зробила» дитина чи рідна людина:

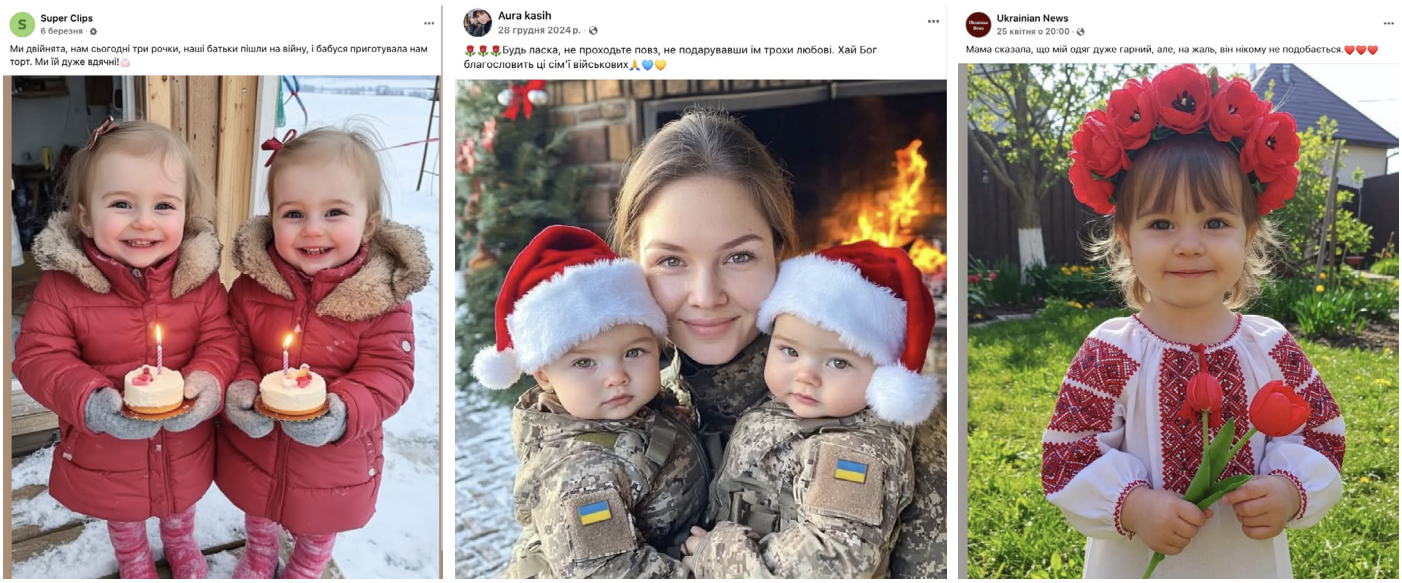
Джерело: скриншоти ЦЕДЕМ

- сімейну пару у формі (щойно одружились, народилися діти тощо):



Джерело: скриншоти ЦЕДЕМ

- дітей у вишиванках, формі, з патріотичною символікою чи написом:



Джерело: скриншоти ЦЕДЕМ

Ці зображення з'являються, як правило, із супровідним текстом, який подає певну сюжетну історію та апелює до емоцій. Разом комбінація цих елементів створює ефективну маніпулятивну конструкцію: вигаданий емоційний текст із закликом до взаємодії + реалістичне візуальне підтвердження = довіра і реакція пересічного користувача.

Чому клікбейтні сторінки використовують ШІ-зображення? Причин багато:

- у відкритому доступі є безкоштовні та дешеві ШІ-інструменти для генерації зображень. Це зручно й економно для адміністраторів клікбейтних сторінок, які можуть публікувати десятки постів щодня;
- це безпечніше, ніж брати чужі фото з інтернету. Власний ШІ-контент зменшує ризики, що зображення буде видалено за скаргами на авторські права, тому він стабільніше «триматиметься» у стрічці;
- потрібний візуал можна створювати дуже швидко й масово. Кілька кліків — і маємо «військового», «стареньку», «весілля» або «дитячий малюнок» на будь-який смак;
- візуали виглядають відносно переконливо. Якісні генератори ШІ здатні створювати зображення, що справляють враження щирості, болю, тепла або вдячності — саме те, що найкраще працює в емоційних постах.

Ризик у тому, що багато користувачів не вміють розпізнавати ШІ-зображення або й не здогадуються, що створювати штучні реалістичні зображення взагалі можливо. Тож вони щиро вірять, що клікбейтний пост — правдива історія, і взаємодіють із ним, посилюючи його охоплення. Рекомендації для користувачів щодо розпізнавання зображень, згенерованих ШІ, дивіться в розділі 1.6.

1.3.4. Поширення сенсаційних псевдоновин, які змушують реагувати

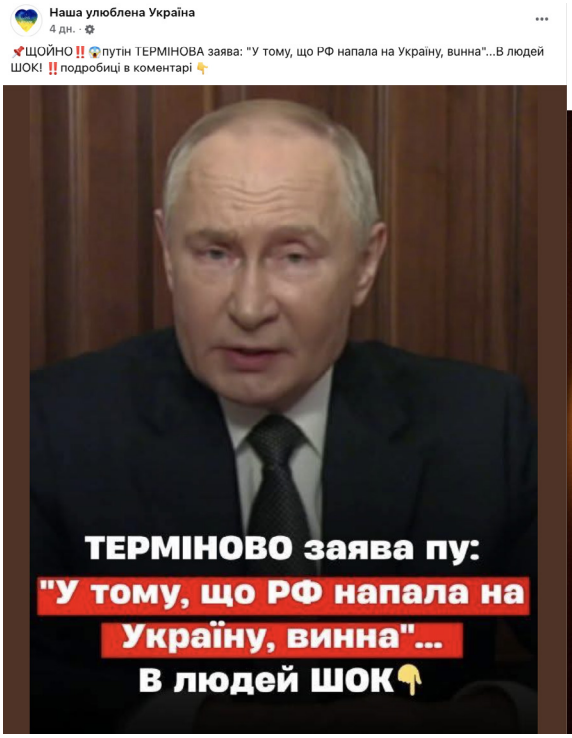
Ця тактика ґрунтується на простій, але ефективній ідеї: імітувати актуальне, сенсаційне чи панічне новинне повідомлення, щоби привернути максимум уваги і змусити користувача негайно зреагувати. Такі публікації зазвичай оформлені як термінові повідомлення, подаються у форматі «ексклюзиву» або «щойно сталося», але насправді або не мають під собою перевіреної інформації, або маніпулюють інфоприводами, щоб генерувати охоплення.

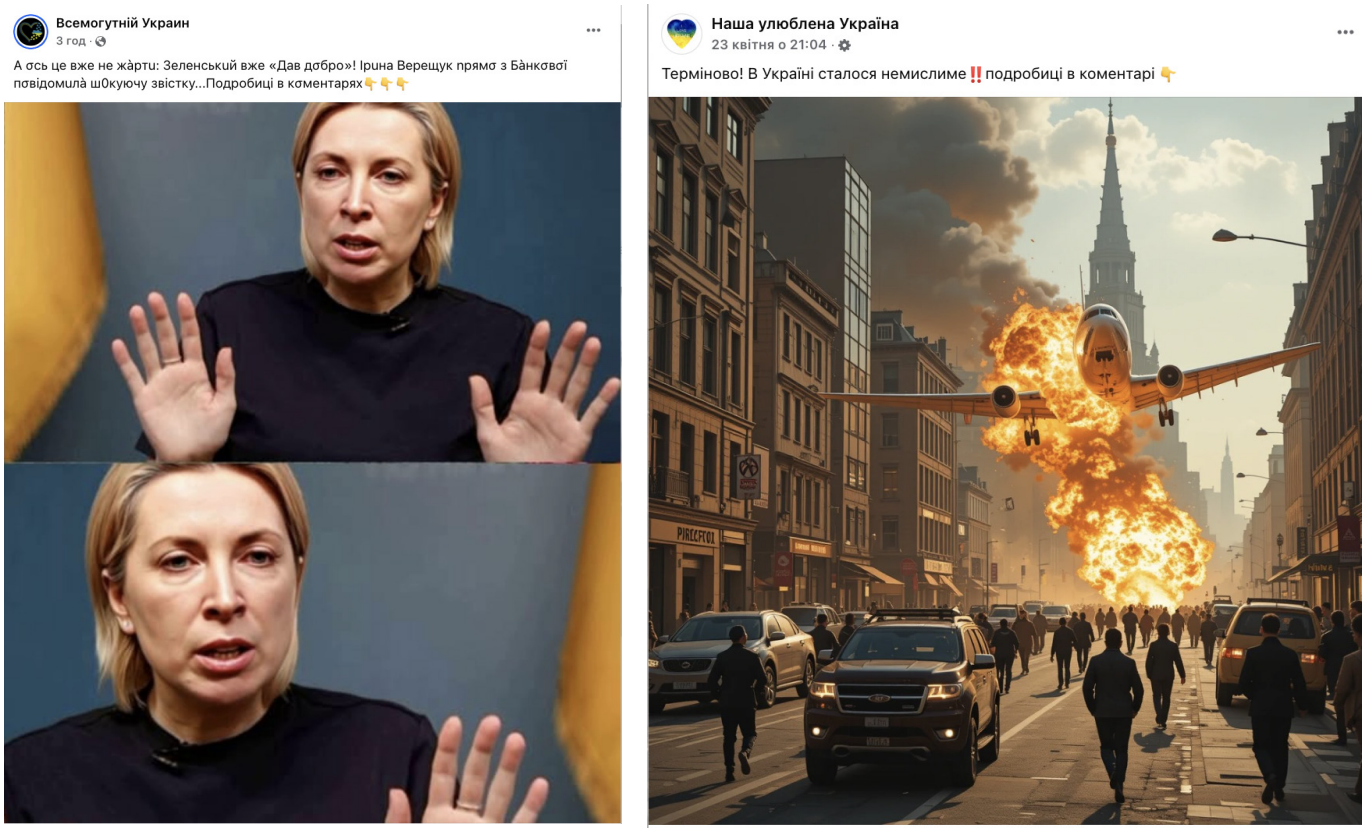
Як це виглядає?

Типові заголовки формулюються з максимально емоційним наголосом. У хід ідуть великі літери, знаки оклику, емодзі (‼️, ⚠️, 😱), слова на кшталт «Терміново», «Щойно», «Важливо», «Шок».

Ось кілька типових прикладів таких заголовків:

- *«📌ЩОЙНО‼️😱путін ТЕРМІНОВА заява: «У тому, що РФ напала на Україну, винна»...В людей ШОК! ‼️подробиці в коментарі»*
- *«В сам0му центрі Києва уб*или ....‼️подробиці в коментарі 👇»*
- *«А σсь це вже не жàрти: Зеленський вже “Дав дσбро”! Ірина Верещук прямσ з Бàнкσвσї пσвідомилà ш0куючу звістку...Подробиці в кσментарях 👇👇👇»*
- *«Терміново! В Україні сталося немислиме ‼️ подробиці в коментарі 👇 »*





Джерело: скриншоти ЦЕДЕМ

Заголовки й тексти таких постів навмисно спотворюють: часто замінюють літери на символи або іншомовні знаки. Таким чином клікбейтні сторінки намагаються обманути алгоритми Facebook. Адже політики платформи декларують, що Facebook обмежує видимість і поширення неякісного контенту, зокрема клікбейту і «приманок» для залучення. Відповідно, щоб їхні дописи не класифікували як клікбейт, автори часто спотворюють слова в заголовках / текстах, намагаючись таким чином обійти автоматичні фільтри.

До цих заголовків додаються супровідні зображення: портрети відомих політиків та «зірок», фотографії вибухів, руїн або трагічних сцен. Ці візуали можуть бути реальними, але вирваними з контексту, а іноді — взагалі згенерованими штучним інтелектом.

На перший погляд здається, що сталося щось справді серйозне. Хочеться дізнатися, що саме, — і ми натискаємо. А там — або нічого конкретного, або стара подія, або фото, вирване з контексту, або взагалі фейк.

У деяких випадках такі пости не містять посилання на «джерело інформації». Однак трапляються й більш витончені підходи. Наприклад, у тексті може з'явитися фраза на кшталт: «Посилання на термінову новину — в першому коментарі». Часто посилання в коментарях є, і вони можуть вести на сторонні «новинні» ресурси низької якості чи канали в Telegram. А іноді обіцяного посилання в коментарях просто немає.

Ще одна поширена практика — використання старих новин, які публікуються так, ніби йдеться про подію, що сталася «щойно». Жодної актуальної інформації в пості не буде, але емоційна реакція користувача вже є. Нерідко використовуються старі фотографії — з обстрілів 2022 року, стихійних лих або катастроф, — які подаються як «сьогоднішні».

Також трапляються пости з випадковими фотографіями людей із чорною стрічкою — ніби повідомлення про загибель, хоча такої людини може взагалі не існувати або ж вона може бути живою й ніяк не пов'язаною з війною.

Усе це створює враження сенсаційності без фактичного змісту, а в коментарях шириться паніка, співчуття чи обурення — навіть якщо подія неактуальна, гіперболізована або взагалі вигадана.

Ця тактика працює, бо вона грає на нашій природній реакції: переляк, цікавість і потреба знати «що сталося» прямо зараз. Ми не встигаємо критично осмислити — просто клацаємо, реагуємо, ділимося. Саме на це й розрахунок.

Щойно користувач натискає лайк, залишає коментар або поширює — алгоритми Facebook починають активніше просувати пост, показуючи його іншим людям. Таким чином, навіть повністю фейковий або беззмістовний пост може завіруситися.

У чому небезпека?

Подібний контент створює ілюзію новинності й терміновості, хоча насправді є лише емоційною приманкою, розрахованою на шокову реакцію. З одного боку, це обман уваги, марнування часу користувача. З іншого — це джерело дезінформації, паніки, розгубленості чи навіть політичних маніпуляцій.

Це особливо критично в умовах війни, адже війна і постійна небезпека формують підвищений рівень тривожності в суспільстві. Люди живуть у стані очікування загроз. Саме в такому стані вони найвразливіші до сенсаційних вкидів. Один фейковий заголовок про обстріл Києва, смерть відомого бійця чи падіння літака — і в коментарях уже здіймається хвиля емоцій.

Це дестабілізує інформаційне середовище, знижує довіру до реальних новин і посилює відчуття безнадії.

Ці пости не покликані розповісти новину. Їхнє завдання — змусити вас відреагувати миттєво: клацнути, лайкнути, поділитися. Хтось лайкнув, бо пережив. Хтось — бо не дочитав. А інший — бо повірив. Саме це і є метою — реакція без перевірки. Маніпуляція замість новини.

1.3.5. Використання нерелевантних популярних хештегів

Ще одна поширена тактика, яку використовують клікбейтні сторінки у Facebook, — додавання до публікацій великої кількості хештегів, незалежно від того, чи мають

вони стосунок до змісту посту. Сюди також належить «паразитування» на популярних хештегах заради збільшення охоплення.

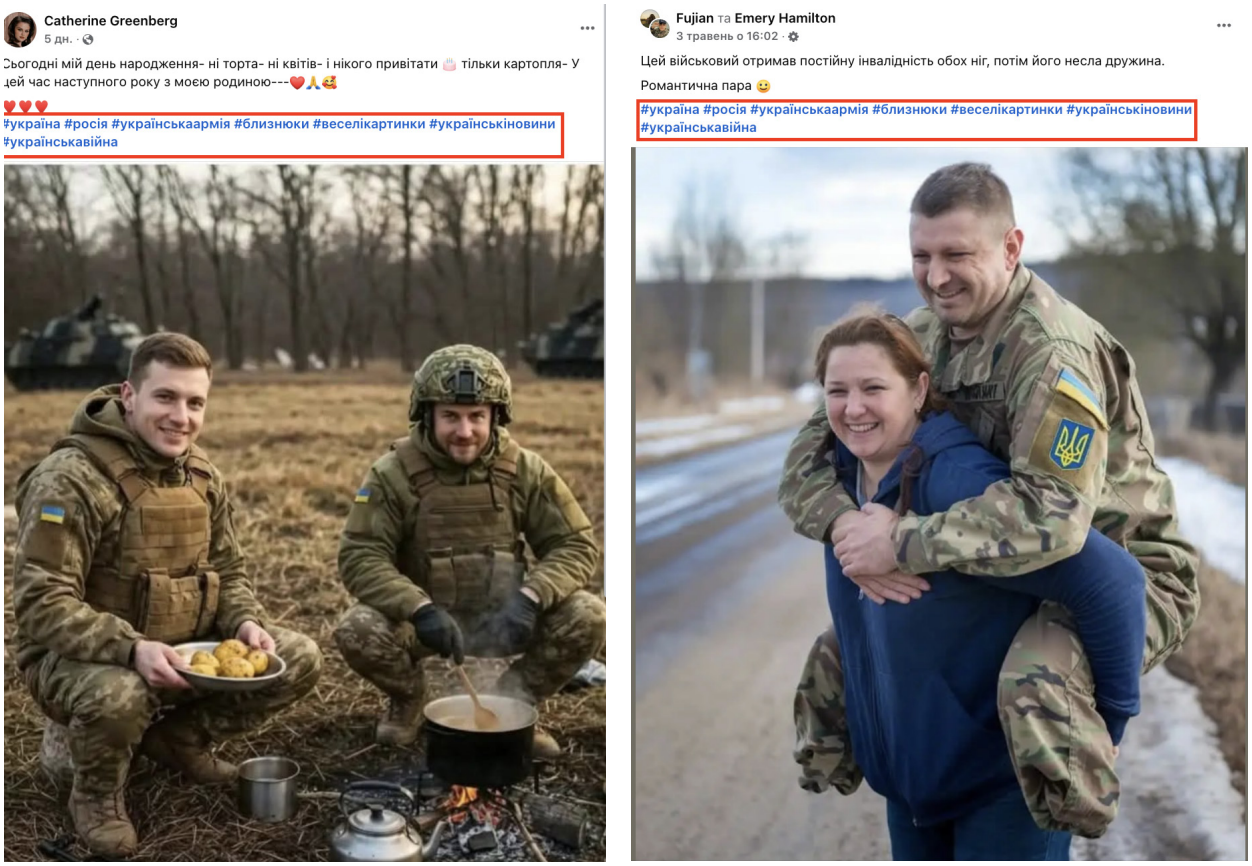
У теорії хештеги мають допомагати орієнтуватися в тематиці публікацій та категоризувати контент. На практиці ж у клікбейтних постах вони перетворюються на інструмент залучення додаткової аудиторії та маніпуляції алгоритмами.

Це працює за принципом «зачепити будь-кого», навіть випадково. Людина може знайти пост через знайомий хештег, зупинитися, переглянути його — і цього достатньо, щоб алгоритми Facebook розцінили пост як «цікавий» і показали його іншим. Та залежно від аудиторії й мови публікації ця тактика реалізується по-різному.

Якщо говорити про **українськомовний сегмент Facebook**, у багатьох випадках адміністратори клікбейтних сторінок додають змішаний набір хештегів, частина з яких частково відповідає темі посту, а інша — є зовсім нерелевантною.

Один із найпоширеніших наборів хештегів виглядає так: **#україна #росія #українськаармія #близнюки #веселікартинки #українськіновини #українськавійна**

Цей самий набір може з'явитися як під постом про захисників зі втраченими кінцівками чи «українських військових», яких ніхто не привітав із днем народження, так і під дописом зовсім іншого характеру, як-от про саморобки від дідуся чи зображення дитини у вишиванці.



Джерело: скриншоти ЦЕДЕМ

Джерело: скриншоти ЦЕДЕМ

У таких випадках хештеги використовуються не для відображення теми, а для алгоритмічного «проштовхування» посту до ширшої аудиторії.

Особливо показовим є хештег *#веселікартинки*, який з'являється під постами будь-якого змісту — від трагедій до псевдоновин. Він функціонує виключно як інструмент для збільшення видимості у стрічках новин користувачів.

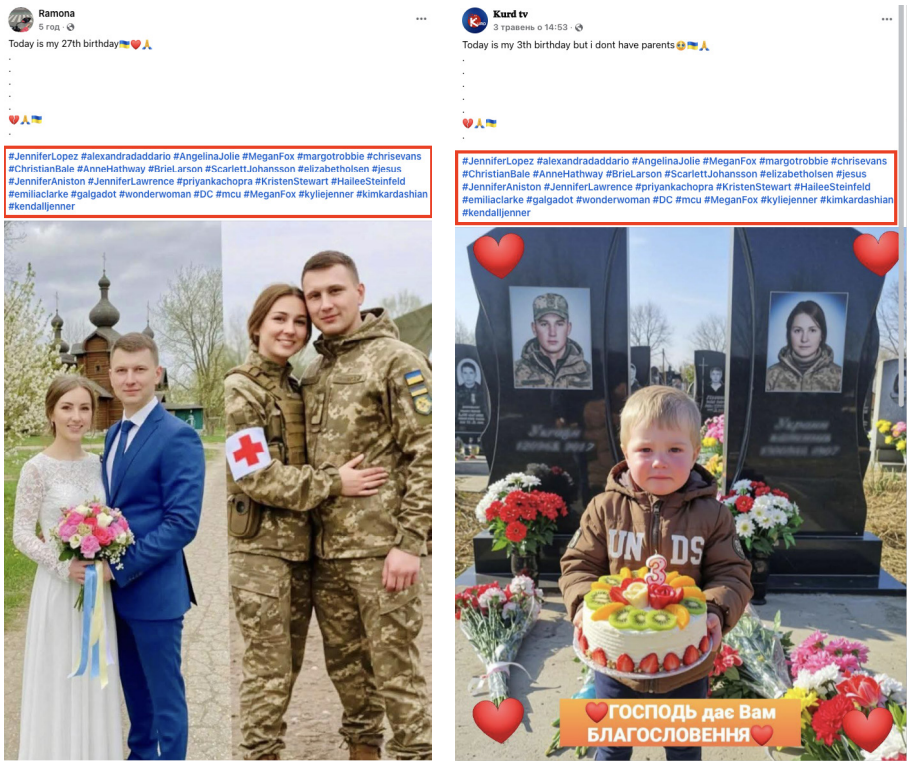
Якщо говорити про **хештеги для іноземної аудиторії**, клікбейтні сторінки, які публікують контент на українську тематику англійською мовою, використовують ще очевиднішу форму хештег-маніпуляції. Вони масово додають хештеги з іменами зірок шоубізнесу, фільмів, супергероїв, які абсолютно не мають стосунку до зображень чи тексту допису.

Типовий набір хештегів для англомовного сегменту виглядає приблизно так: ***#JenniferLopez #AngelinaJolie #MeganFox #margotrobbie #chrisevans #ChristianBale #BrieLarson #ScarlettJohansson #jesus #mcu #kyliejenner #kimkardashian #wonderwoman #DC #galgadot***

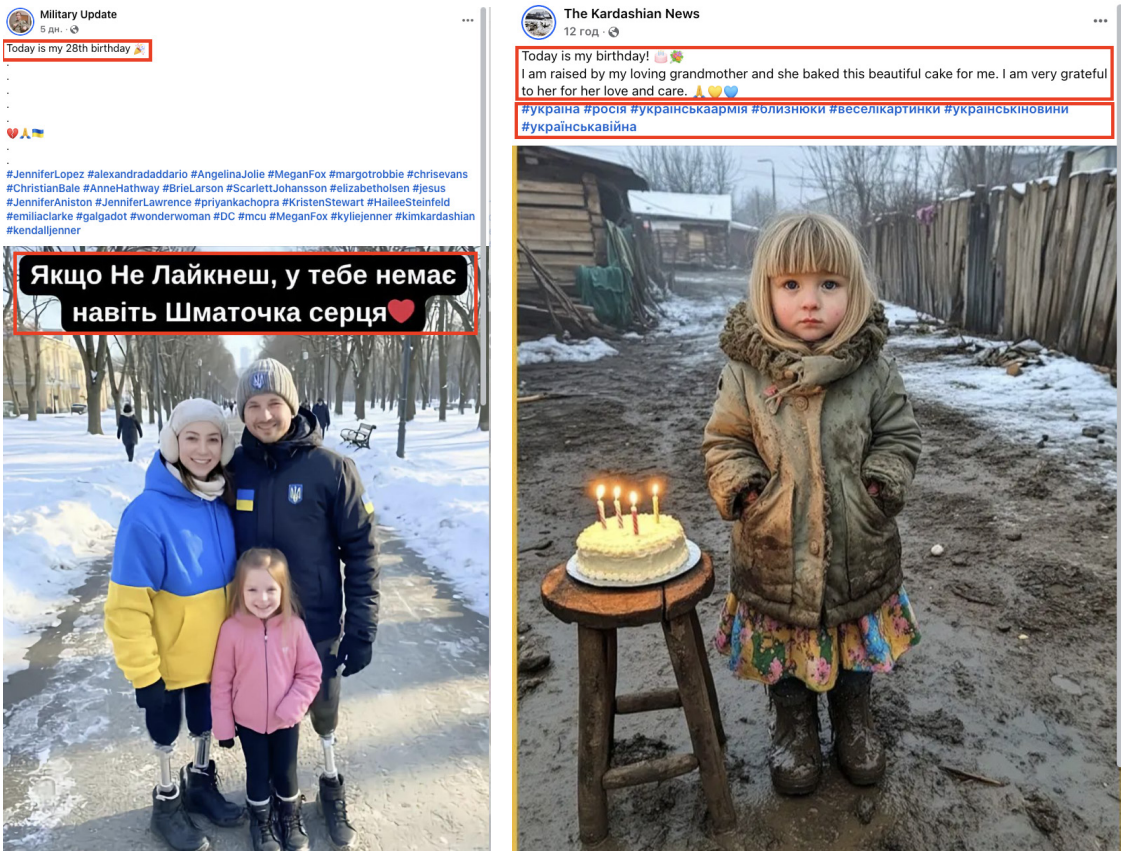
Такі хештеги можуть стояти і під постом із зображеннями українських військових, які наче святкують день народження чи одружуються, і під зображенням дитини, яка начебто втратила батьків.

Насправді ж ці клікбейтні пости не мають жодного зв'язку ані з кінематографом, ані з релігією, ані з відомими персонами. Але алгоритми Facebook можуть показати цей пост тим, хто цікавиться відповідними тегами, — або ж платформа просто може трактувати допис як «популярний» через перелік упізнаваних слів.

Іноді з'являються дивні поєднання, коли до тексту англійською додається [картинка](#) з написом українською чи українські [хештеги](#).

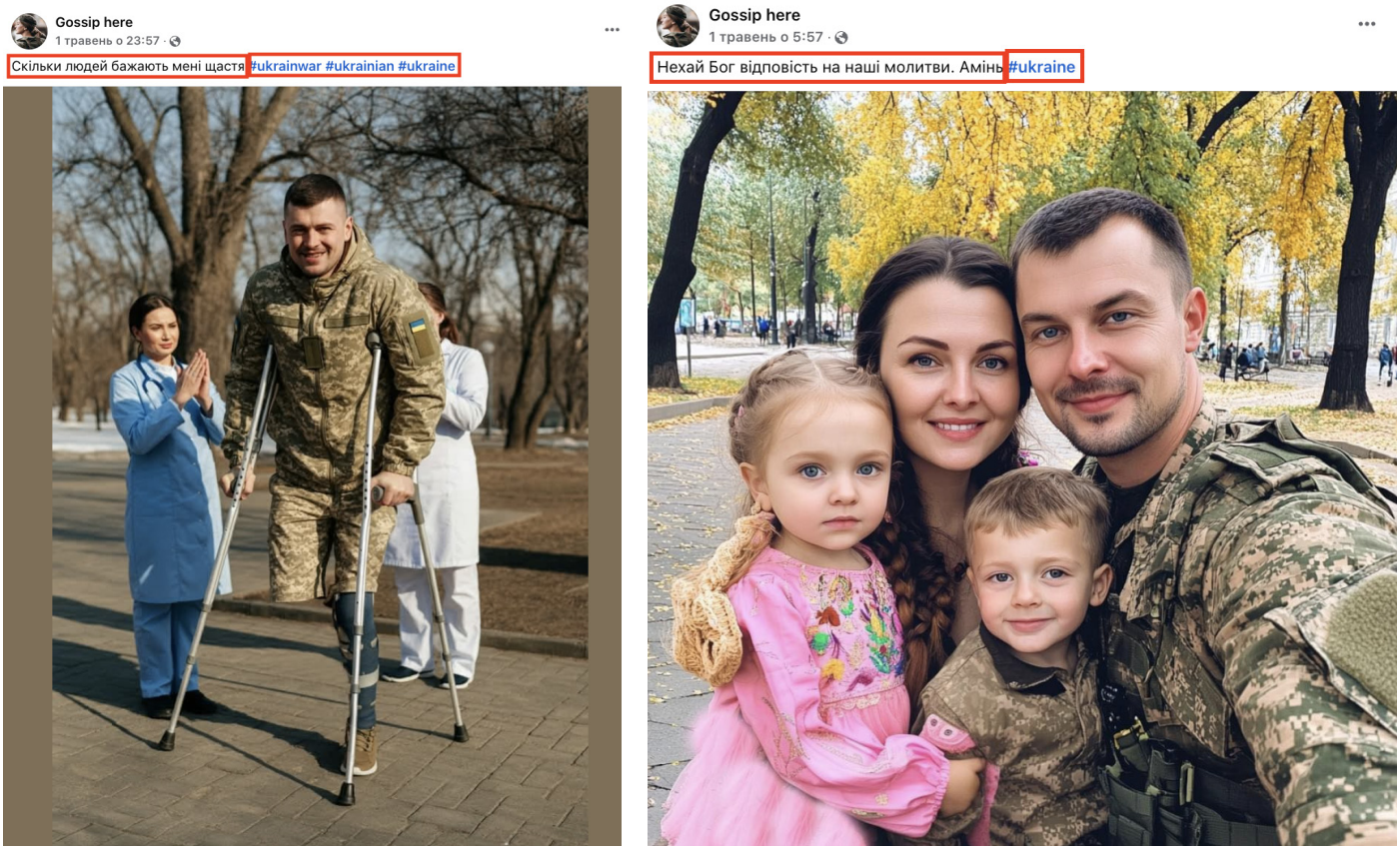


Джерело: скриншоти ЦЕДЕМ



Джерело: скриншоти ЦЕДЕМ

А може бути й навпаки — до українських дописів можуть додаватися тематичні хештеги англійською.



Джерело: скриншоти ЦЕДЕМ

Коли в одному пості поєднується текст англійською мовою та візуальний або хештеговий супровід українською, це може бути як випадковість, так і ознака тактичного підходу до «розширення охоплення» залежно від особливостей функціонування і модерації клікбейтної сторінки. Про що може йтися?

1. Намір охопити одночасно кілька аудиторій. Це може бути свідомий крок для того, щоби пост був помітний і для української аудиторії, і для англомовних користувачів з інших країн. Наприклад:

- текст англійською звертається до іноземної аудиторії: «Today is my 28th birthday»;
- а зображення містить фразу українською: «Якщо не лайкнеш, у тебе немає навіть шматочка серця»;
- хештеги — імена знаменитостей.

Такий пост може потрапити до стрічки українцям (завдяки зображенню) і водночас до іноземців, які цікавляться попкультурою (через мову та глобальні теги). Це подвійний удар по охопленню.

Або інший приклад:

- текст українською: «Скільки людей побажають мені щастя»;
- зображення українського військового з ампутованими кінцівками;
- хештеги — #Ukrainwar, #Ukraine, #Ukrainian.

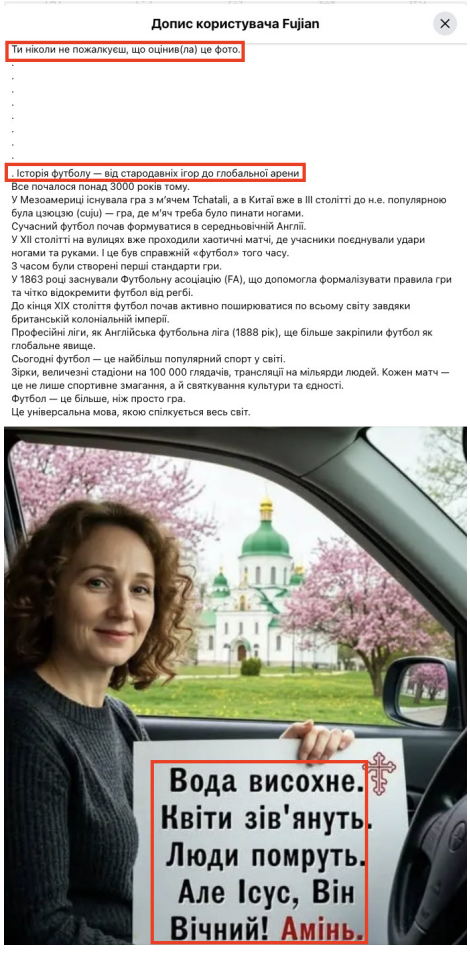
Такий пост можуть побачити як українці (завдяки тексту), так і іноземці, які цікавляться подіями в Україні (завдяки хештегам).

2. Автоматизація або шаблонність публікацій. У деяких випадках дивні комбінації мов і тем — результат не цілеспрямованої стратегії, а використання шаблонів або автоматичних систем публікації, які «міксують» елементи з різних джерел. Наприклад:

- текст і зображення створюються окремо, а потім об'єднуються без редагування;
- хештеги додаються автоматично до кожного посту, незалежно від мови.

Це може вказувати на відсутність реальної модерації або живого автора в деяких клікбейтних сторінок, а також на масове виробництво клікбейтного контенту.

3. Незнання або байдужість до мовної логіки. Іноді за сторінками стоять іноземні адміністратори, які можуть не розуміти ні української, ні англійської на достатньому рівні, щоб помітити або виправити змішування. У результаті пости виглядають дивно або нелогічно — але емоційно «працюють» і досягають цілі.



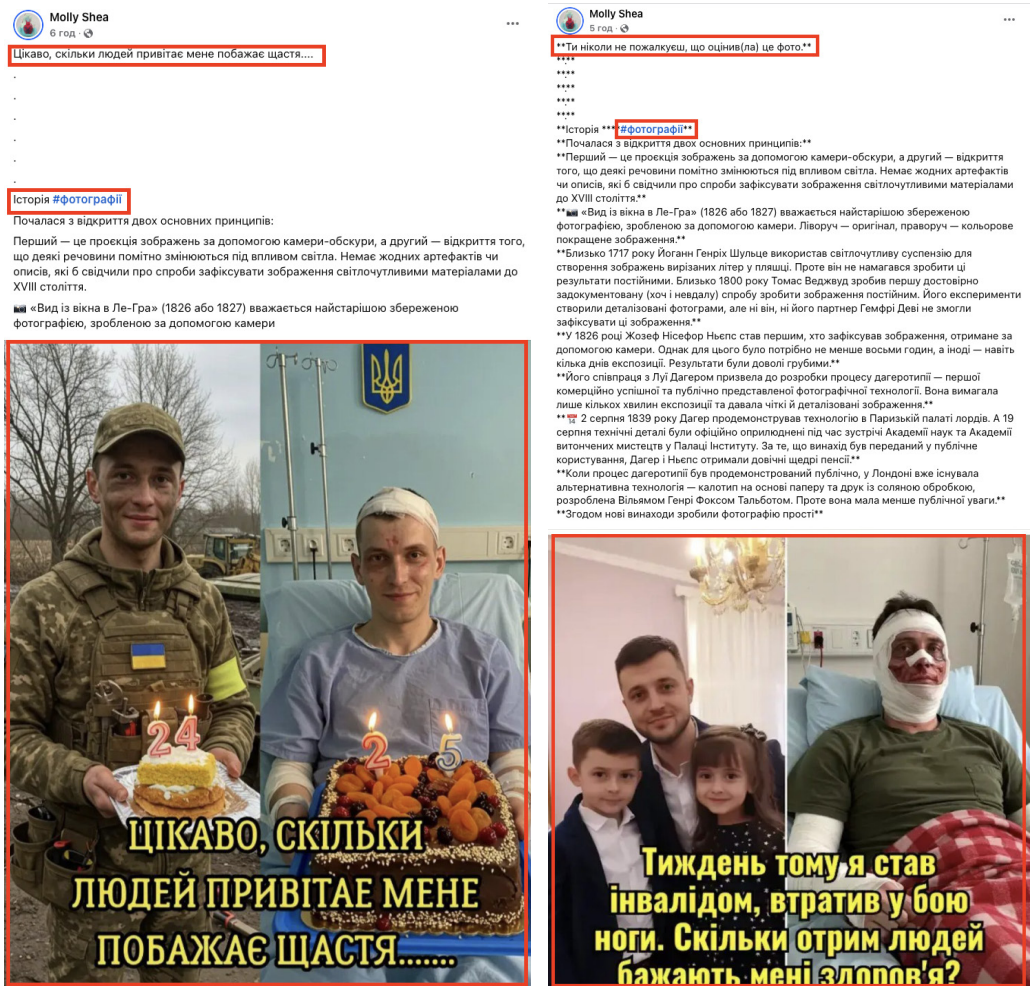
Загалом же клікбейтні публікації не намагаються бути послідовними чи змістовними — їхня мета лише в тому, щоб зачепити якомога більше людей, незалежно від мови, країни чи теми.

1.3.6. Додавання «тематичного хвоста»

Ще одна помітна тактика, до якої вдаються автори клікбейтних сторінок, — це додавання до публікації «тематичного хвоста». Йдеться про другий абзац або частину тексту, яка розміщується нижче основної, емоційної частини посту і жодним чином не пов'язана з його змістом.

Зовні така структура виглядає як пост, що складається з **двох частин**:

- **перша частина** — типовий емоційний або маніпулятивний текст із супровідним зображенням;
- **друга частина** — умовно нейтральна або пізнавальна інформація, стилізована під «факт дня» або «освітню довідку».



Джерело: скриншоти ЦЕДЕМ

Ці дві частини **не мають між собою жодного логічного зв'язку**, але разом створюють враження, ніби пост є більш об'ємним та багатошаровим. Така структура — не випадкова, ідеться про цілеспрямовану спробу змінити сприйняття посту.

Яку функцію виконує «тематичний хвіст»?

1. Потрапляння у стрічки людей, які шукають іншу інформацію. «Тематичний хвіст» нерідко підбирається так, щоб містити слова або теми, які активно шукають користувачі. Це може бути короткий абзац про футбол, історію, фотографію, кіно тощо — теми, які викликають стабільний інтерес і асоціюються з «нейтральним» або «освітнім» контентом.

У такому випадку алгоритми Facebook можуть «зчитати» ці слова як тематичний сигнал, який допомагає визначити, кому ще показати пост — окрім тих, хто зазвичай взаємодіє з клікбейтним контентом. У результаті публікація може потрапити до стрічки користувачів, які просто цікавляться футболом чи кіно.

Щоб підсилити цей ефект, до «тематики хвоста» часто додають відповідні хештеги, як-от *#фотографія*. Це допомагає створити додаткові шляхи для просування допи-

су, ще більше розширюючи охоплення, навіть якщо основний зміст посту і фотографія не мають жодного стосунку до «тематичного хвоста».

2. Ілюзія багатошаровості чи «універсальності» контенту. Коли користувач бачить у дописі і зворушливу історію, і якийсь нібито «пізнавальний факт», він може сприйняти пост як корисний чи навіть «випадково цікавий». Тому основна емоційна частина працює на емоцію, а другорядна — створює ілюзію змістовності для тих, хто загляне глибше. Це підвищує шанси на взаємодію: хтось відреагує на емоцію, хтось зацікавиться інформацією.

3. Маскування клікбейту під нешкідливий або корисний контент. Другий абзац також виконує роль «інформаційного прикриття». Додавання нейтральної інформації після емоційного звернення може бути спробою зробити пост менш однозначно маніпулятивним. Змішування емоційного заклику з беззмістовною інформацією створює враження, що пост не має єдиної спрямованості. Це може ускладнити модерацію або автоматичне визначення його як маніпулятивного. Пост перестає бути чітким сигналом — і стає інформаційним шумом.

На перший погляд такі пости можуть виглядати як «нешкідливі» або навіть «повчальні». Але їхня реальна мета залишається незмінною: викликати емоційну реакцію, зібрати взаємодії та посилити охоплення. «Тематичний хвіст» — це спосіб зробити клікбейтний пост менш очевидним: він зміщує фокус уваги й ускладнює сприйняття основного меседжу як маніпулятивного.

1.3.7. Редагування контенту після збору взаємодій

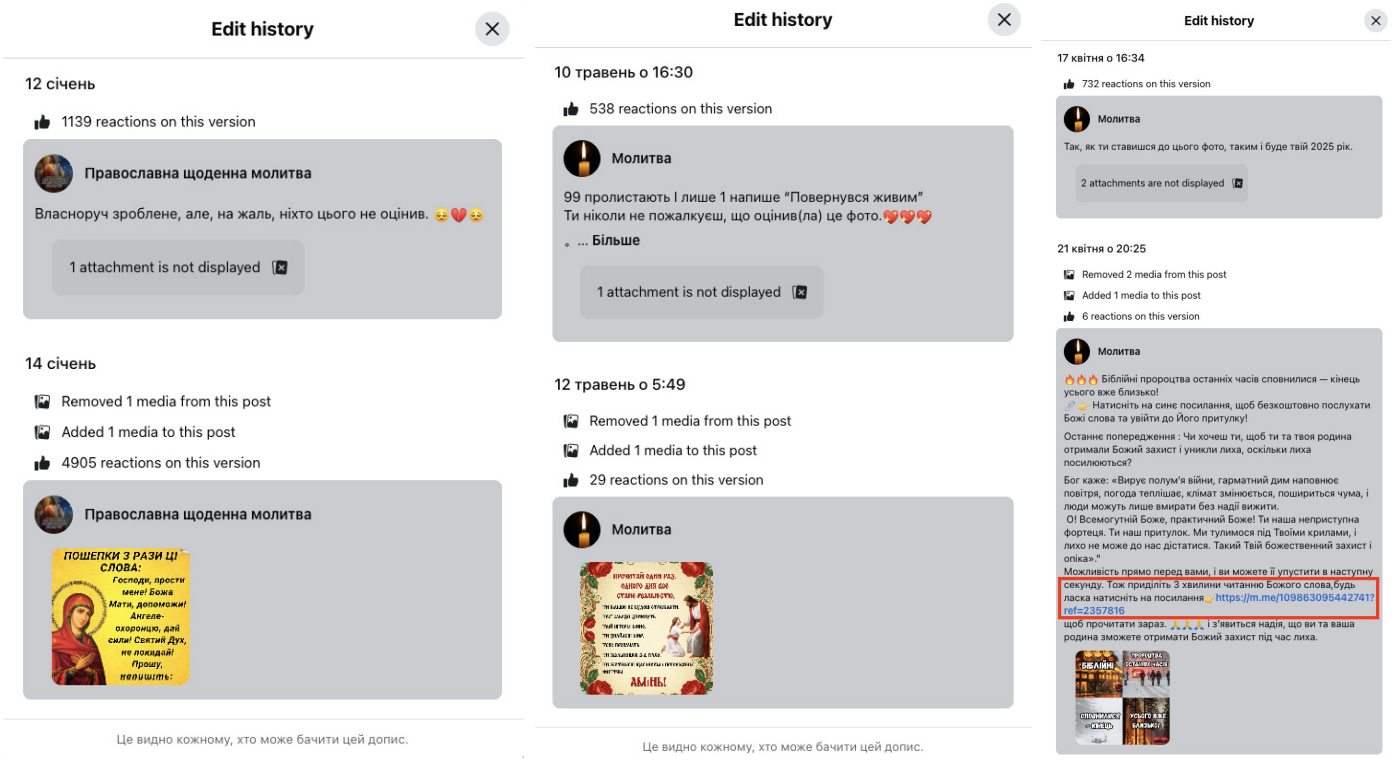
Ще одна малопомітна, але ефективна тактика, яку використовують клікбейтні сторінки, — це зміна змісту публікації після того, як вона вже набрала багато лайків, коментарів або поширень. Зовні все виглядає так, ніби це той самий пост, який ви лайкнули чи поширили, але насправді його зміст уже інший, іноді навіть кардинально.

Як це працює?

Перший варіант посту зазвичай виглядає емоційно, патріотично та з закликом до взаємодії. Наприклад, клікбейтні сторінки можуть використати вже знайомі нам сюжети на кшталт «Власноруч зроблене, але, на жаль, ніхто цього не оцінив», «99 пролистають І лише 1 напише “Повернувся живим” Ти ніколи не пожалкуєш, що оцінив(ла) це фото» чи «Так, як ти ставишся до цього фото, таким і буде твій 2025 рік».

Такий текст легко «заходить» аудиторії — його лайкають, коментують, поширюють. Алгоритми Facebook починають активно його показувати у стрічках інших користувачів.

А потім — через кілька годин або днів — власник сторінки редагує цей допис і замінює текст на зовсім інший (наприклад, релігійні заклики помолитися, написати «амінь» чи приєднатися до закритої групи в месенджері).



Джерело: скриншоти ЦЕДЕМ

На перший погляд, пост усе ще «з емоційною картинкою» і має «багато лайків»,а отже вартий довіри. Але насправді він просуває зовсім інший зміст, на який люди не підписувалися.

Як можна побачити на скриншотах вище, особливо активно до цієї тактики вдаються сторінки, які спочатку позиціонують себе як релігійні або духовні спільноти. Вони публікують загальні молитви, патріотичні цитати, слова підтримки для воїнів. Усе виглядає щиро і знайомо.

Але після того, як пости збирають десятки або сотні реакцій, сторінка поступово змінює зміст: популярні пости редагуються, до них додаються посилання на чати з представниками цих організацій, які переслідують власну адженду і часто пропагують так звану Церкву Всемогутнього Бога (також відому як Eastern Lightning) — не традиційну конфесію, а маргінальну секту, яка активно просуває себе через клікбейтні сторінки.

Ця тактика небезпечна, бо користувачі часто не помічають змін. Вони вже лайкнули чи поширили один пост — а тепер під ним інший текст, із яким вони не обов'язково погоджуються чи підтримують. Наприклад, пост, первинно присвячений дню народження військового чи молитві за Україну, тепер просуває релігійну секту, але при цьому зберігає всі лайки, коментарі й поширення.

Тож з погляду клікбейтних сторінок редагування постів — це спосіб перетворити масову емоційну реакцію на інструмент просування свого порядку денного. За-

мість одразу опублікувати заклик приєднатися до певної групи чи організації (що могло б відштовхнути аудиторію), сторінки «заробляють» довіру шляхом «паразитування» на тематиці патріотизму, віри чи загальнолюдських тем, а вже потім підмінюють зміст, зберігаючи набрані в оригінальній версії посту лайки, коментарі й поширення як візуальну «легітимізацію».

1.4. Прихована мета клікбейтних сторінок

Попри зовнішню «доброчесність» та емоційність, клікбейтні сторінки у Facebook створюються не з метою щирої підтримки чи інформування аудиторії. Їхнє головне завдання — накопичити охоплення й довіру, щоби згодом використати це у власних інтересах. Після того, як сторінка набирає достатньо підписників і взаємодій, її контентна стратегія змінюється — іноді поступово, іноді різко. Саме на цьому етапі стає помітною справжня мета таких сторінок.

1.4.1. Поширення російської пропаганди та дезінформації

Однією з головних прихованих цілей частини клікбейтних сторінок є **трансляція російської пропаганди або контенту, що підігрує російським інформаційним наративам**. Такі сторінки зазвичай діють поступово. Спершу вони публікують типовий емоційний контент: ШІ-згенеровані світлини українських захисників чи релігійних образів, фрази на кшталт «Підтримай ЗСУ» або «Шкода, що це фото не набере багато лайків» — і таким чином збирають довіру та лояльність аудиторії. А вже коли кількість підписників і реакцій досягає потрібного рівня, у стрічці з'являються дописи іншого характеру. Саме на тлі патріотичного або духовного контенту поступово починають з'являтися політично забарвлені повідомлення, які вкидають сумніви, поширюють дезінформацію або повторюють меседжі російських посадовців.

Цей перехід може бути майже непомітним:

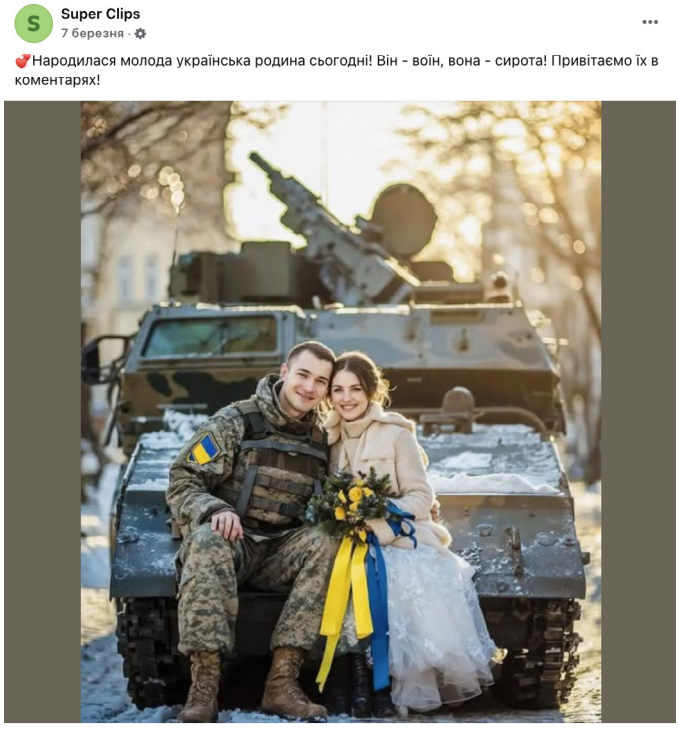
- поруч із клікбейтним контентом починає з'являтися політичний контент проукраїнської спрямованості;
- поступово починають з'являтися маніпулятивні та пропагандистські дописи з ознаками «зрадофільства» — коли на перший план виходять тези про «зраду», «корумповану владу», «даремні жертви», перекручені повідомлення про міжнародну підтримку України;
- а згодом — і відверта російська пропаганда: цитати російських посадовців, меседжі про «нацистів в Україні», заклики до миру на російських умовах тощо.

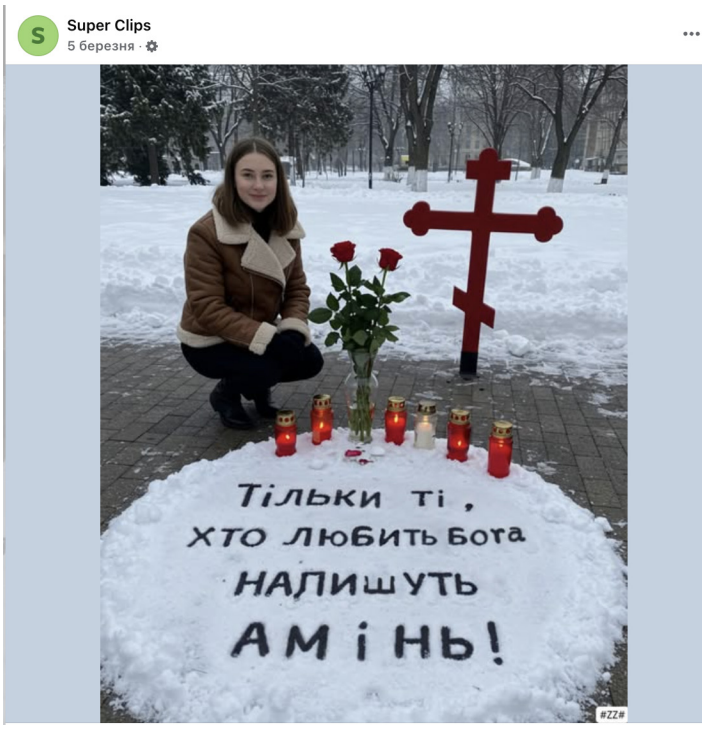
Показовим прикладом такої поведінки є сторінка Super Clips.

На перший погляд вона виглядає як типовий клікбейтний ресурс, який публікує відео і зображення військово-патріотичної та релігійної тематики. У стрічці можна побачити:

- знайомі нам клікбейтні дописи на військово-патріотичну та духовну тематику, як-от:

- Народилася молода українська родина сьогодні! Він - воїн, вона - сирота! Привітаємо їх в коментарях!
- Тільки ті, хто любить Бога, напишуть Амінь



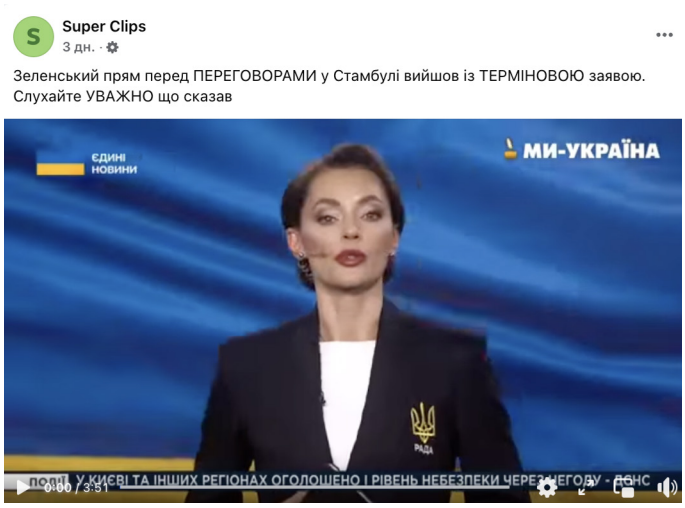


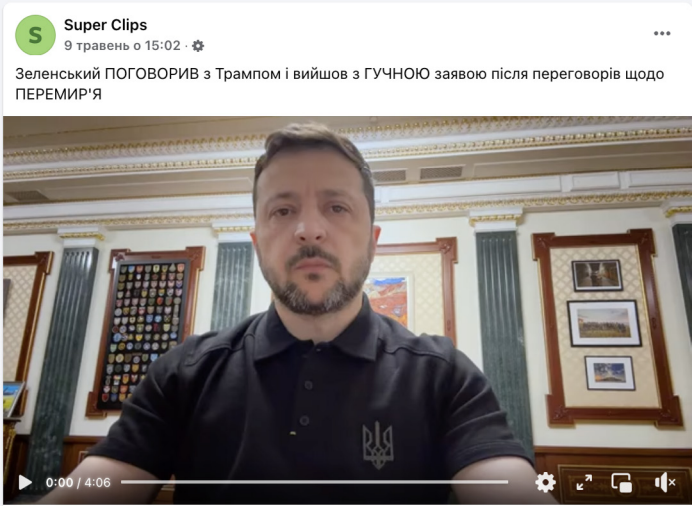
Джерело: скриншоти ЦЕДЕМ

- фрагменти проукраїнського контенту, наприклад, «Єдиних новин» та звернень президента Зеленського:

- Зеленський прям перед ПЕРЕГОВОРАМИ у Стамбулі вийшов із ТЕРМІНОВОЮ заявою. Слухайте УВАЖНО що сказав

Зеленський ПОГОВОРИВ з Трампом і вийшов з ГУЧНОЮ заявою після переговорів щодо ПЕРЕМИР'Я





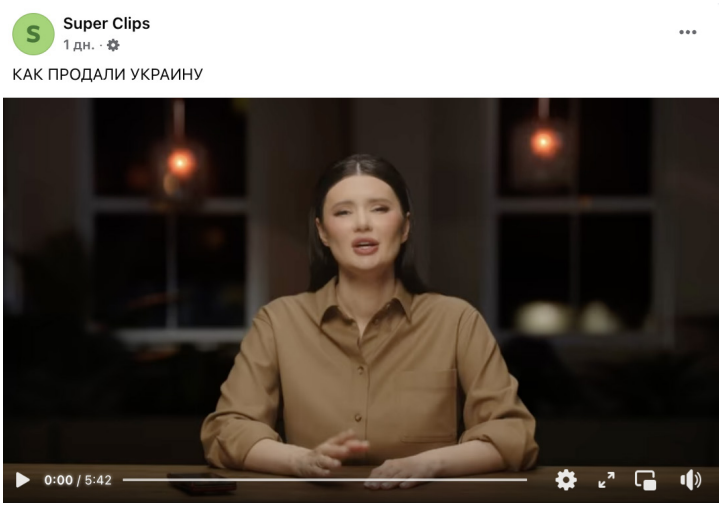
Джерело: скриншоти ЦЕДЕМ

Цей контент створює ілюзію щирої проукраїнської позиції, завдяки чому сторінка набирає підписників і реакції.

Однак із часом з'являються дописи іншого характеру. Наприклад:

- **пости з відверто зрадофільськими тезами**, які посилюють недовіру до влади та підживлюють уявлення, що «Україну продали», війна «нікому не потрібна» або «все дарма». Наприклад, поширюють відео проросійської ведучої Діани Панченко, в якому угода між Україною та США щодо доступу до українських корисних копалин подається як «зрада» і перетворення України на сировинний придаток;

▸ КАК ПРОДАЛИ УКРАИНУ



Джерело: скриншот ЦЕДЕМ

- використання прямих цитат російських посадовців або президента РФ, поданих без контексту або навіть із «нейтральним» чи проросійським тоном, наприклад:

▸ Значит вы за нацизм! Лавров обозначил неудобную правду для ЕС и назвал Зеленского _ЖАЛКИМ_

Джерело: скриншот ЦЕДЕМ

Сторінки на кшталт Super Clips використовують довіру, яку вони накопичили через емоційний та патріотичний контент, як стартову платформу для просування прихованої адженди. У підписників створюється відчуття, що це «наша» сторінка — і саме тому вони рідше перевіряють факти, менш критично оцінюють зміну тону публікацій і легше піддаються маніпуляціям.

1.4.2. Поширення радянської ностальгії

Ще один тип прихованої мети, яка виявляється після того, як клікбейтна сторінка набирає аудиторію, — це **поширення ідеалізованого образу радянського минулого**. Ця практика не є випадковою: апеляція до ностальгії — один із найстабільніших інструментів м'якої пропаганди, який активно використовується в пострадянському просторі.

Як це відбувається?

Сторінки починають діяти за знайомою схемою: публікують зворушливий або духовний контент — фотографії українських військових, релігійні цитати, історії про доброту або втрату. Аудиторія реагує: підписується, лайкає, поширює. Алгоритми платформи підсилюють охоплення.

Коли сторінка накопичує достатньо довіри, тон публікацій поступово змінюється. Типовий представник цієї категорії — сторінка Trisec. Серед емоційного військово-патріотичного та духовного контенту там з'являються пости на зразок:

- Як добре й щасливо жилося в СРСР
- У Радянському Союзі хліб був натуральним, без добавок — не те, що зараз

- Радянські мультфільми - улюблені
- Зірки радянської естради - сумуємо за ними
- Зберігання радянських «артефактів» як прояв ностальгії

Джерело: скриншоти ЦЕДЕМ

Такі пости зазвичай супроводжуються архівними зображеннями: радянські вітрини, усміхнені працівники на заводі, сільські пейзажі, діти в тогочасному одязі, радянські «артефакти» тощо. Все подано у стилістиці «теплої, доброї пам'яті».

У чому прихована мета?

Ностальгія — сильне почуття. І в умовах тривалої війни, економічної нестабільності, втрат і невизначеності вона стає психологічним притулком для частини аудиторії. Клікбейтні сторінки використовують це, щоби:

- створити позитивну асоціацію з радянським періодом;
- протиставити його сучасності, яку зображують як несправедливу, занадто складну або нестабільну;
- формувати підґрунтя для політичних меседжів, які згодом можуть підважувати українську незалежність або просувати «альтернативні погляди» на геополітичну ситуацію.

Людина, яка щойно поставила сердечко під постом про українського захисника, легко пролайкає і «ностальгійне» зображення з текстом «Пам'ятаєте, як у СРСР бабусі пекли хліб у печі? Смак дитинства...» І навіть не замислиться, що перед нею — не просто спогад, а інформаційний гачок, який поступово змиває контраст між окупаційною спадщиною і національною незалежністю.

Поширення радянської ностальгії через клікбейтні сторінки — це форма м'якої ідеологічної обробки, що подається через формат розваги, пам'яті або «невинного порівняння». Такий контент виглядає емоційно теплим, але працює на розмивання історичної пам'яті і зниження довіри до сучасних демократичних інституцій.

1.4.3. Перенаправлення трафіку в інші канали

У деяких випадках клікбейтні сторінки використовують Facebook не як основний майданчик для розміщення контенту, а лише як інструмент для «захоплення» аудиторії. Їхнє головне завдання — привернути увагу, викликати емоційну реакцію, зібрати підписників і взаємодії, а далі спрямувати людей на зовнішні канали, де контент публікується вже без жодних обмежень.

Куди ведуть аудиторію?

1. Групи в Telegram, WhatsApp або Messenger. Користувачам пропонують «долучитися до закритої групи», «отримувати ексклюзивну інформацію» або «молитися разом». Ці групи часто стають простором для поширення неперевірених повідомлень, чуток або координованих вкидів — у форматі, який важко відстежити чи модерувати.

2. Зовнішні сайти. Посилання ведуть на ресурси низької якості, створені спеціально для клікбейту або збору даних. Такі сайти можуть містити фейкові новини, нав'яз-

ливу рекламу, шкідливі скрипти чи підроблені петиції. Вони часто створюються на безкоштовних хостингах або мають масово скопійований контент без джерел.

3. Анонімні Telegram-канали. Тут часто розміщується відверта дезінформація, російська пропаганда, конспірологічні теорії або маніпулятивний контент політичного характеру. Оскільки Telegram менш контрольований, це ідеальне середовище для токсичного або сумнівного контенту, який би не пройшов модерацію у Facebook.

Навіщо це робиться?

Перенаправлення трафіку — це спроба вивести аудиторію з-під правил Facebook і водночас закріпити вплив на «підігрітих» користувачів, які вже емоційно залучені. За межами публічної платформи автори можуть:

- публікувати контент, що порушує політики Meta (шкідливі фейки, заклики до насильства, мову ворожнечі);
- закликати до фінансової підтримки, реєстрації, участі в організаціях тощо;
- формувати паралельну інформаційну реальність — із власними «новинами», «коментаторами» і «свідченнями».

1.4.4. Комерційна мета

Окрім ідеологічних цілей, певна частина таких сторінок може мати комерційну мотивацію. Деякі з них беруть участь у монетизаційних програмах Meta, наприклад, через бонуси за відео чи автоматичну рекламу. Існують також ознаки можливої комерціалізації, зокрема: розміщення посилань на онлайн-магазини сумнівної якості, участь у вірусних рекламних кампаніях або зміна назви й тематики сторінки, що може свідчити про її передачу іншому власнику. Хоча прямі підтвердження таких схем рідкісні, поведінкові патерни вказують на ймовірну фінансову мотивацію деяких авторів.

1.5. Між політикою і практикою Meta: чому клікбейт продовжує працювати у Facebook

Meta декларує зобов'язання боротися з дезінформацією, низькоякісним контентом і маніпулятивними практиками на своїх платформах, зокрема у Facebook. Водночас досвід аналізу українського сегменту показує, що значна частина клікбейтних сторінок продовжує функціонувати, зростати і навіть отримувати алгоритмічну підтримку. Це не обов'язково є наслідком недоброчесності чи байдужості з боку платформи — радше йдеться про прогалини в політиках, обмеження в діяльності алгоритмів і технічні виклики, які вимагають вдосконалення.

У цьому розділі ми розглядаємо п'ять ключових проблем, які ускладнюють виявлення та обмеження клікбейтного і дезінформаційного контенту. Вони можуть слугувати підставою для формування рекомендацій, спрямованих на покращення прозорості та ефективності політик Meta в українському контексті.

1.5.1. Можливість приховати країну адміністрування сторінки

Функціонал Meta дозволяє адміністраторам сторінок у деяких випадках не показувати країну, з якої здійснюється модерація. Це створює суттєві труднощі для дослідників, журналістів та громадських організацій, які намагаються встановити походження сторінок. У результаті частина клікбейтних сторінок має або неповну секцію «Прозорість сторінки», що унеможливлює просту перевірку географії їх адміністрування — зокрема, виявлення іноземного або сумнівного походження.

1.5.2. Непрозоре позначення сторінок із тимчасово окупованих територій

Окреме питання викликає відображення геолокації сторінок, які модеруються з тимчасово окупованих територій України, зокрема з Криму. Деякі повідомлення свідчать, що такі сторінки можуть позначатися як «українські» (що де-юре відповідає міжнародному праву), однак на практиці це створює непрозору ситуацію, особливо у випадках, коли сторінка має приховану проросійську або маніпулятивну адженду. Було б логічно запровадити спеціальне уточнення — наприклад, «Україна (тимчасово окупована територія)», — щоб користувачі могли точніше оцінити джерело контенту.

1.5.3. Неефективне маркування згенерованого ШІ-контенту

Meta публічно оголосила про намір впровадити політику маркування зображень, створених штучним інтелектом, зокрема в партнерстві з великими компаніями. Та на практиці значна частина ШІ-згенерованих візуалів на клікбейтних сторінках не має жодного маркування. Це ставить під сумнів ефективність відповідних алгоритмів і створює ілюзію, ніби зображення є реальними. У ситуації, коли контент «виглядає щиро», а користувачі сприймають фото як доказ, відсутність маркування значно підвищує ризик дезінформації.

Більше того, навіть позначки або логотипи «AI-generated» не завжди спрацьовують: частина аудиторії однаково активно лайкає та поширює такий контент, сприймаючи його як справжні фото чи відео.

1.5.4. Недостатнє застосування фактчекінгу до візуально маніпулятивного контенту

Meta співпрацює з незалежними фактчекерами, які мають можливість позначати неправдиві або частково неправдиві публікації. Проте ця політика орієнтована переважно на текстові або «інформаційні» пости, тоді як клікбейтні сторінки часто публікують візуально-емоційний контент із маніпулятивними підписами, який не містить формально неправдивого твердження, але вводить в оману.

Наприклад, пости на кшталт «У мене день народження» із ШІ-згенерованим фото військового подають вигадану історію як реальність. Хоча текст не містить фактів, які можна спростувати, загальна композиція посту створює хибне враження і має

дезінформаційний ефект. Питання залишається відкритим: чи повинна платформа реагувати на такі випадки через механізми фактчекінгу або інші модераційні практики?

1.5.5. Алгоритми, які підсилюють залучення до низькоякісного контенту

Згідно з офіційною позицією Meta, платформа має знижувати охоплення контенту низької якості, зокрема клікбейту. Проте на практиці все виглядає інакше.

За спостереженнями аналітиків Центру демократії та верховенства права, навіть пасивна взаємодія з клікбейтним контентом — наприклад, перегляд сторінки без підписки чи лайків — призводила до появи ще більшої кількості подібних сторінок у стрічці рекомендацій. Це вказує на те, що алгоритм Meta інтерпретує сам факт зацікавленості / перегляду як сигнал для посилення показів, попри заявлену політику боротьби з клікбейтом.

У цьому криється серйозна проблема: контент, що здається нешкідливим, насправді стає «воротами» до дезінформації або пропаганди, про що йшлося в попередньому підрозділі.

1.6. Поради користувачам

Попри складність алгоритмів і зовнішню правдоподібність клікбейтного контенту, користувачі мають інструменти для захисту від маніпуляцій. У більшості випадків для цього достатньо базових навичок критичного мислення та уважного ставлення до деталей. Нижче наведено низку простих порад, які допоможуть не стати частиною схеми клікбейтної взаємодії.

1. Ставити запитання перед реакцією

Перед тим як поставити лайк, поширити допис або написати коментар — зупиніться на кілька секунд і запитайте себе:

- Хто це опублікував?
- Чи є докази, що історія справжня?
- Чому мене прямо просять взаємодіяти?

Кожна взаємодія з постом — це сигнал для алгоритму. Навіть «добрий» коментар під сумнівним постом посилює його видимість.

2. Уникати взаємодії з надто емоційними закликами

Фрази на кшталт «Напиши “Амінь” у коментарях», «Пошир, якщо не байдужий», «Лайкни, якщо підтримуєш» мають на меті не об’єднати, а **змусити вас взаємодіяти — іноді несвідомо**. Якщо емоція занадто сильна, а інформація — розмита, це причина бути обережними.

3. Перевіряти сторінку, яка поширила пост

Зверніть увагу на такі ознаки:

- Коли створено сторінку?
- Чи видно країну адміністрування?
- Чи є контактна інформація?
- Чи змінювалася назва сторінки?
- Які інші публікації є на сторінці?

Сторінка, що позиціонує себе як «патріотична», але містить десятки однотипних постів без конкретики, може бути частиною клікбейтної мережі.

4. Вміти впізнавати зображення, згенеровані ШІ

Уникайте довіри до постів, де:

- обличчя або тіла виглядають неприродно — надто ідеальними, часто плачуть, синхронно радіють,
- фон містить дивні або нечіткі деталі,
- є незрозумілі написи або спотворений текст,
- загальна композиція надто «глянцева».

Згадані ознаки можуть вказувати на те, що зображення було згенеровано штучним інтелектом. Навіть якщо зображення виглядає реалістично — воно може бути вигаданим.

Можна також скористатися онлайн-інструментами перевірки (як-от **AI or Not**, **Illuminarty**, **Metadata2Go**), якщо є підозра, що це ШІ-зображення. Водночас результати перевірки цими інструментами не можна вважати стовідсотково достовірними: іноді система може помилково визначити автентичний контент як згенерований ШІ, а іноді — навпаки, не розпізнати штучно створене зображення. Тому завжди варто враховувати контекст та інші додаткові ознаки, вказані вище.

5. Підписатися на фактчекінгові ресурси

В Україні працює низка авторитетних ініціатив, які регулярно аналізують маніпулятивний контент та дезінформацію:

- VoxCheck
- StopFake
- Центр протидії дезінформації
- Центр стратегічних комунікацій та інформаційної безпеки

Стеження за ними дозволяє розпізнавати нові типи шахрайства, клікбейту й дезінформації і не потрапляти в типові пастки.

6. Не боятися скаржитися на сумнівний контент

Якщо ви бачите пост або сторінку, що викликає підозру, — не залишайтеся осторонь. Скарга на контент або сторінку — це легальний і швидкий спосіб привернути увагу модераторів платформи. Навіть якщо реакція не буде миттєвою або прийде відмова, що порушень не знайдено, — сигнал залишиться, і кожна така скарга має значення в системному аналізі ризиків.

1.7. Рекомендації для Meta

Попри те, що Meta вже робить кроки для протидії дезінформації та співпрацює з українськими партнерами, клікбейтні сторінки й далі залишаються проблемою. Вони продовжують збирати велику аудиторію, поширювати сумнівний контент і обходити правила платформи. У цьому розділі зібрано практичні пропозиції, які можуть допомогти Meta ефективніше виявляти, обмежувати й попереджати діяльність таких сторінок — особливо в умовах війни та високої емоційної вразливості користувачів.

1. Зробити прозорішою інформацію про адміністрування сторінок

Деякі сторінки приховують, з якої країни ними керують. Це ускладнює дослідження й аналіз. Було б корисно:

- зменшити можливість приховувати країну адміністрування хоча б для сторінок із великою аудиторією;
- чітко позначати сторінки, які модерує хтось із тимчасово окупованих територій України (наприклад, із Криму). Навіть якщо де-юре це Україна, така додаткова інформація допоможе краще розуміти, хто стоїть за контентом;
- полегшити доступ дослідників до даних прозорості сторінок — наприклад, удосконалити API або зробити статистику доступнішою.

2. Краще маркувати контент, створений ШІ

Meta вже заявила про намір маркувати контент, створений за допомогою штучного інтелекту. Але на практиці багато ШІ-згенерованих зображень, зокрема на клікбейтних сторінках, залишаються без позначок. Щоби змінити ситуацію, можна:

- покращити автоматичне розпізнавання таких зображень;
- обмежити використання та поширюваність ШІ-картинок у чутливих темах — наприклад, коли йдеться про війну, смерть, дітей — якщо немає пояснення, що це ілюстрація або ШІ-зображення;
- додати опцію поскаржитися на зображення чи відео як «імовірно, створене ШІ», щоб користувачі могли самі звертати увагу модераторів на підозрілий візуал.

3. Звернути більше уваги на маніпулятивні зображення

Meta вже співпрацює із фактчекерами, але переважно у випадках, коли є чітко сформульоване неправдиве твердження. Проблема в тому, що деякі пости не містять конкретної брехні, але все одно вводять в оману, як-от ШІ-зображення військового з підписом «сьогодні мій день народження», яке викликає співчуття, але не має нічого спільного з реальністю.

Можна було би:

- розробити спеціальну окрему політику щодо маніпулятивного візуального контенту;
- відповідно позначати і приділяти більше уваги сторінкам, які систематично використовують емоційні зображення, щоб викликати довіру, а згодом змінюють тематику на політичну чи пропагандистську.

4. Перевірити, як працюють алгоритми рекомендацій

Навіть пасивна взаємодія з клікбейтними сторінками (наприклад, просто перегляд їхніх постів) може призвести до того, що користувачеві починають рекомендувати ще більше подібного контенту. Це суперечить заявленій політиці Meta щодо обмеження охоплення контенту низької якості.

Meta могла би:

- провести додатковий аудит, як саме алгоритми реагують на клікбейт;
- зробити так, щоби сторінки, які часто використовують заклики «напиши в коментарях», «пошир», «постав лайк», не потрапляли в розділ «Рекомендоване».

5. Посилити співпрацю з українськими організаціями

Meta вже працює з українськими партнерами, такими як ЦЕДЕМ, StopFake, VoxCheck. Але ці зв'язки можна зробити ще ефективнішими. Наприклад:

- активніше комунікувати з партнерами, які досліджують шкідливі клікбейтні практики у Facebook та Instagram;
- дати можливість довіреним партнерам повідомляти про проблеми, які формально не порушують правила, але вказують на потенційний ризик — наприклад, сторінки з постійними емоційними «гачками», які можуть змінити тематику на пропаганду чи дезінформацію.

Ці дії допоможуть зменшити охоплення сумнівного контенту, посилити прозорість платформи і підвищити довіру користувачів — особливо в умовах війни, коли інформаційна та цифрова безпека є критично важливими для захисту як окремих людей, так і суспільства загалом.

1.8. Висновки до першого розділу

Клікбейтні сторінки в українському сегменті Facebook — це не просто прояв емоційного контенту. Це системне явище, яке використовує людську вразливість, алгоритмічну логіку платформи й технології на кшталт штучного інтелекту, щоб генерувати взаємодію та здобути довіру користувачів, зібрати охоплення і зрештою впливати на думки, поведінку або навіть безпеку користувачів.

На перший погляд подібні сторінки виглядають нешкідливими: вони публікують патріотичні зображення, просять про підтримку чи молитву. Але за цією емоційною «обгорткою» нерідко ховаються комерційні інтереси, проросійська пропаганда або спроби маніпулювати аудиторією. Особливо небезпечно, що такі сторінки, набравши аудиторію, змінюють тематику, редагують старі пости й використовують технології ШІ для створення зворушливих, але вигаданих історій.

Алгоритми Facebook часто не стримують поширення таких сторінок — навпаки, вони можуть рекомендувати їх іншим користувачам. Частина функціоналу платформи дозволяє приховати країну адміністрування або неефективно позначає контент, створений штучним інтелектом. Це створює прогалини, якими користуються маніпулятори.

У цьому розділі ми описали, як функціонують клікбейтні сторінки, які тактики вони використовують, яку небезпеку становлять, із якими труднощами стикається Meta в боротьбі з цими сторінками і як на це можуть реагувати самі користувачі. Ми також сформулювали конкретні пропозиції до Meta, які могли би зробити платформу безпечнішою для українських користувачів, особливо в умовах війни.

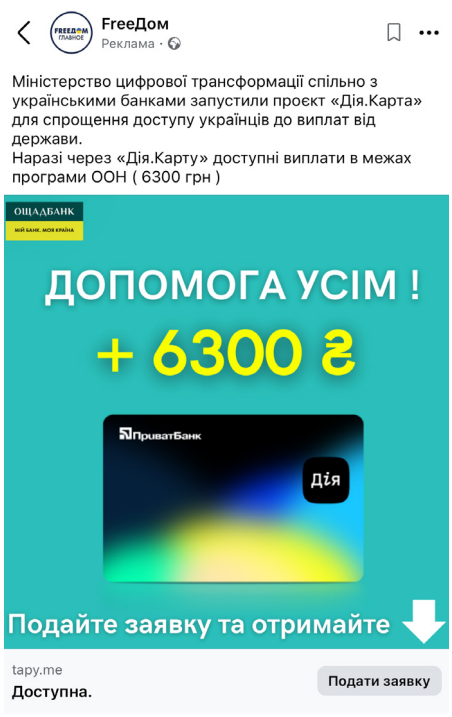
Клікбейт — це інструмент впливу, який має бути в центрі уваги дослідників, громадянського суспільства і самих платформ. Якщо клікбейтні сторінки вчасно не зупинити, вони продовжать маніпулювати і формувати спотворену картину дійсності для мільйонів користувачів.

2. Таргетована реклама як інструмент аферистів на платформах Meta

Платформи Meta, зокрема Facebook, давно стали звичним середовищем для спілкування, обміну новинами й пошуку корисної інформації. Та дедалі частіше між звичними дописами миготять яскраві рекламні зображення й відео з обіцянками «швидких грошових виплат» і «диво-рішень для покращення здоров'я». Такі оголошення вирізняються яскравим оформленням і простими обіцянками: достатньо лише натиснути, ввести дані — і отримати бажане. **Проте за зовнішньою привабливістю часто ховаються добре продумані шахрайські схеми, які на кожному наступному кроці втягують користувача в небезпечну пастку**. Нижче — шість популярних шахрайських схем, які поширюються за допомогою реклами на платформах Meta.

2.1. Фальшиві грошові виплати

На фоні війни та складної економічної ситуації мільйони українців потребують підтримки — і саме на цій вразливості спекулюють шахраї. У стрічках Facebook дедалі частіше з'являються оголошення з привабливими закликами: «Допомога кожному українцю вже сьогодні!», «Виплати від ООН», «Компенсація за комунальні послуги», «Фінансова допомога переселенцям». На екрані — герб України, обличчя президента, логотипи «Дії», Червоного Хреста, міжнародних організацій. Усе виглядає офіційно.



Джерело: скриншоти ЦЕДЕМ

Насправді ж це ширма для **фішингової атаки**.

Перейшовши за посиланням, користувач потрапляє на сайт-дублер, який імітує сторінку банку, «Дії» або відомої установи. Далі — вводить дані картки, логін, пароль до онлайн-банкінгу або навіть отримує справжній «дзвінок з банку», але дані було введено на шахрайському клоні. Тобто ви підтверджуєте вхід не собі, а шахраям. Результат — втрата персональних даних, а часто і всіх коштів із рахунку й навіть кредитних коштів.

Шахраї безжально експлуатують довіру та відчуття терміновості. Часто вони оновлюють свої кампанії відповідно до реальних програм підтримки — імітуючи «Дію», «Фонд гарантування вкладів» або виплати від міжнародних структур.

Схема незмінна вже роками — росте лише кількість подібних сторінок і різноманіття «програм». Варто зауважити, що зловмисники часто підлаштовуються під актуальні інфоприводи. Наприклад, якщо держава розпочинає «Зимову єПідтримку», шахраї теж будують схеми навколо цього. Те саме відбувається з іншими приводами.

2.1.1. Як працює схема

1. Шахрайське повідомлення. Користувач отримує рекламу в стрічку новин Facebook з інформацією про «компенсацію» — нібито грошова допомога від держави або міжнародної організації. Треба лише перейти за посиланням і отримати.

2. Фішинговий сайт. За вказаним посиланням відкривається сторінка, що візуально імітує сайт банку або урядовий портал. Дизайн, логотипи й навіть анімації створюють відчуття автентичності.

3. Збір конфіденційної інформації. Для «отримання виплати» користувача просять:

- ввести реквізити банківської картки;
- підтвердити вхід через SMS-пароль;
- повідомити PIN-код або тризначний CVV-код на звороті картки;
- пройти «опитування» і поділитися даними з друзями;
- сплатити «державне мито», «комісію», «верифікацію» тощо;
- увійти в клієнт-банк.

4. Крадіжка коштів

Отримавши дані, зловмисники:

- знімають гроші з рахунку;
- оформлюють онлайн-кредити;
- підписують користувача на платні сервіси;
- використовують його картку для шахрайських транзакцій — «дропів».

У чому небезпека?

- Повна втрата грошей з рахунку.
- Оформлення кредитів на ваше ім'я.
- Ризик зловживань вашими персональними даними.
- Можливість втрати соціальних чи банківських виплат.
- Психологічний стрес і зневіра у реальній допомозі.

2.1.2. Поради користувачам

1. Довіряйте лише перевіреним джерелам інформації. Усі заяви про грошову допомогу, компенсації чи соціальні виплати слід перевіряти виключно через офіційні канали — державні вебсайти, «гарячі лінії» профільних установ, а також у застосунку чи на порталі «Дія». Інформацію про легальні програми підтримки, зокрема від міжнародних організацій, варто шукати на порталі «єДопомога».

2. Остерігайтеся посилань із рекламних оголошень. Дізнавши пропозицію перейти за посиланням для «отримання допомоги», не натискайте одразу. Набагато безпечніше — ввести назву установи або програми в пошуковій системі та знайти офіційний сайт самостійно. Зверніть увагу: сайт, на який ви потрапили, не повинен мати позначки «реклама» і в нього має бути чітка, офіційна адреса (без підозрілих доменів на кшталт .space, .fun, .xyz, .page тощо).

3. Завжди перевіряйте URL-адресу сайту. Навіть незначна помилка у вебадресі (наприклад, diya замість diia) може свідчити про фішинговий сайт. Завжди перевіряйте, чи правильно написано назву сайту і чи збігається вона з тією, яку ви очікували побачити.

4. Ніколи не вводьте конфіденційні банківські дані на незнайомих сайтах. Ваш PIN-код, CVV-код (три цифри на звороті картки), логін і пароль до онлайн-банкінгу, SMS-паролі та push-коди від банку — це персональна інформація, яку не можна вводити ніде, окрім офіційного додатка або сайту вашого банку. Жоден державний орган чи серйозна організація не попросить вас поділитися цими даними через повідомлення, чатбот чи незахищений сайт.

5. Звертайтеся до банку або Кіберполіції при перших підозрах шахрайства. Якщо ви випадково розкрили дані платіжної картки на сумнівному сайті або підозрюєте, що стали жертвою шахраїв, — не зволікайте. Заблокуйте картку через онлайн-банкінг або телефоном (номер є на звороті картки). Одночасно подайте заяву до Кіберполіції України через сайт: ticket.cyberpolice.gov.ua.

2.1.3. Рекомендації для Meta

1. Автоматично виявляти і модерувати рекламу з ключовими словами на кшталт «фінансова допомога», «грошова виплата», «компенсація», якщо вони ведуть на підозрілі сторонні сайти.

2. Позначати оголошення, що використовують державну символіку або логотипи «Дії», як такі, що потребують додаткової модерації.

3. Запровадити попередження у стрічці новин, що повідомляють про найпоширеніші шахрайські схеми з виплатами.

4. Виявляти фішингові посилання на ранніх етапах через аналіз URL-адрес та пришвидшений розгляд скарг користувачів.

5. Ефективніше видаляти фейкові сторінки, що імітують офіційні державні органи або міжнародні організації. Запровадити додаткові механізми верифікації офіційних установ.

2.2. Клікбейт, що веде в Telegram

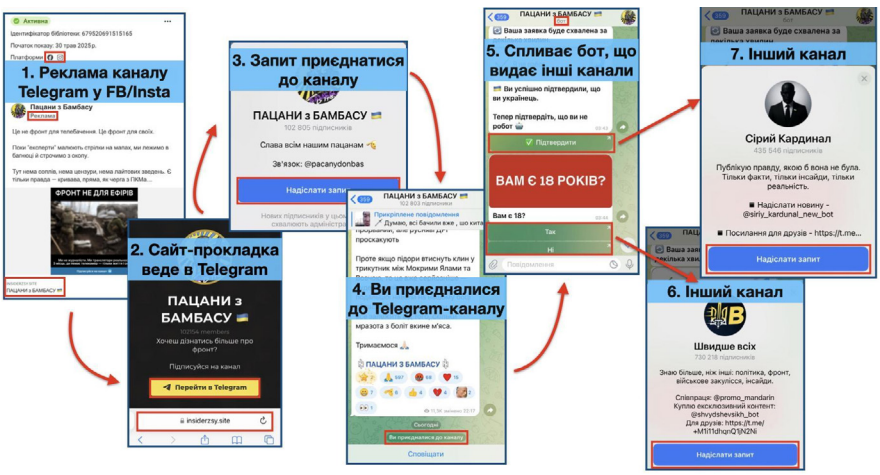
«Термінова заява уряду», «Правда, яку приховують медіа», «Отримай виплату 6500 грн вже зараз» — гучний заголовок у рекламному оголошенні змушує натиснути на посилання. Та в більшості випадків замість «термінової заяви», «правди» чи обіцяної виплати відкривається анонімний канал у Telegram.

На цьому заманювання не закінчується: відкривши один канал, людина мимоволі підписується ще на кілька десятків інших — із тими ж темами, тим самим стилем і тим самим маніпулятивним посилом.

2.2.1. Як розростається «гідра» Telegram-каналів

Шахрайські або пропагандистські Telegram-канали створюють мережі взаємопосилань, щоб підтримувати одне одного, нарощувати аудиторію та втягувати нових користувачів. Реклама у Facebook — лише перший гачок, далі запускається багаторівнева система впливу.

Приклад розростання «екосистеми» анонімних Telegram-каналів — від реклами у Facebook та Instagram до взаємних посилань:



Джерело: скриншоти ЦЕДЕМ

Одна з головних небезпек — **низький рівень модерації Telegram**. На відміну від Meta, де хоч і з вадами, але працюють стандарти спільноти, Telegram дозволяє публікувати майже будь-який контент. І цим активно користуються:

- **поширюють дезінформацію**, прикриваючись «анонімними інсайдами»;
- **використовують обіцянки фейкових виплат чи «компенсацій»**, щоб вивести користувача на шахрайський сайт;
- **продають псевдоінвестиційні схеми** з обіцянками швидких прибутків, часто із закликом зробити «невеликий стартовий внесок», після чого кошти безслідно зникають.

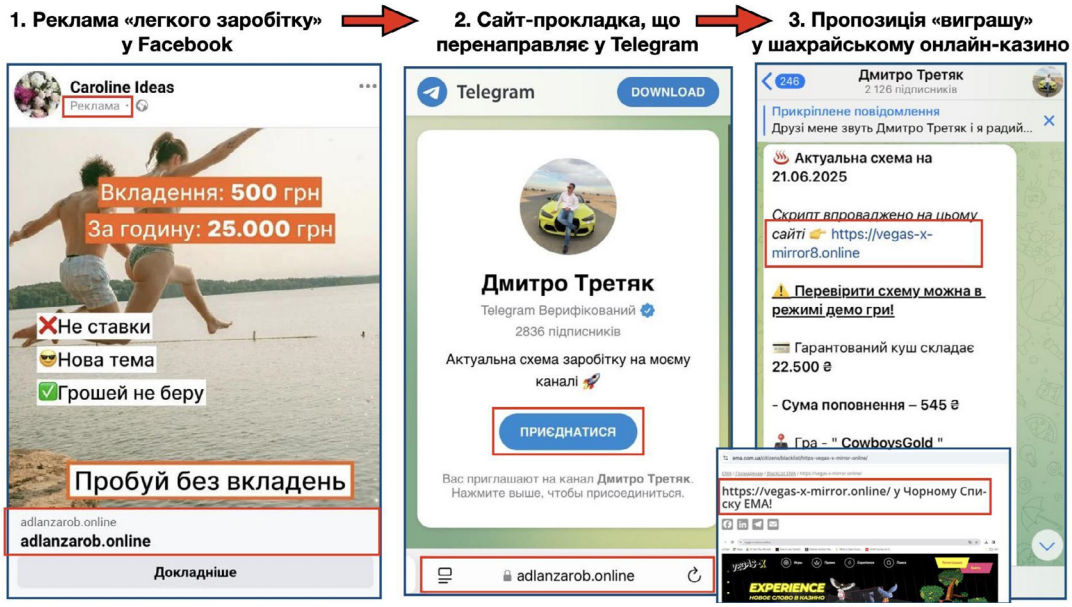
2.2.2. Від інформаційного впливу до фінансового шахрайства

Окрема категорія — **шахрайські Telegram-канали**, що заманюють користувача рекламою у Facebook з обіцянками заробітку: «інвестуй 100 грн і отримай 1000», «гарантована схема успіху». Заманливо, але нереалістично. Насправді за гучними обіцянками — або втрата грошей, або перехід на фішингові сайти, що викрадають ваші дані.

Нерідко такі Telegram-канали ведуть на небезпечні зовнішні ресурси, де шахраї просять:

- ввести дані платіжної картки;
- завантажити додатки зі шкідливим кодом;
- зареєструватися на сайті, вказавши особисту інформацію.

Приклад шахрайської схеми, яка перенаправляє користувача з реклами у Facebook до Telegram-каналу, де людину відправляють за «гарантованим кушем» на шкідливий сайт:



Джерело: скриншоти ЦЕДЕМ

2.2.3. Поради користувачам

1. Не піддавайтеся на гучні заголовки. Якщо заголовок волає про «термінову заяву», «виплати всім» чи «сенсаційну правду» — є високий шанс, що це клікбейт. Перевіряйте інформацію в надійних медіа або на офіційних сторінках державних установ.

2. Не вірте обіцянкам швидких грошей. Обіцянки на кшталт «легкого заробітку без вкладень» — це, найімовірніше, або обман, або схема, де ви ризикуєте втратити гроші, дані або наразитися на інші маніпуляції.

3. Не переходьте з Facebook-реклами у Telegram-канали. Якщо вас переспрямовують у месенджер Telegram — варто насторожитися.

4. Будьте обережні з підписками. Telegram дозволяє створювати ботів, що пропонують посилання на вступ до інших анонімних каналів, маскуючи їх за обіцянками виплат чи верифікації даних. Це ознака маніпулятивної «екосистеми».

5. Повідомляйте про маніпулятивні оголошення. Якщо ви бачите рекламу з маніпулятивним заголовком або неправдивими обіцянками — не полінуйтеся натиснути «Поскаржитися» до служби підтримки Meta.

2.2.4. Рекомендації для Meta

1. Виявляти і обмежувати рекламу, яка маніпуляціями заманює користувачів на Telegram-канали.

2. Позначати підозрілі дописи або рекламу з клікбейтними заголовками. Якщо оголошення містить слова на кшталт «терміново», «шок», «гроші зараз» — система має додатково перевіряти його на маніпулятивність.

3. Інформувати користувачів про небезпеку переходів у месенджери, такі як Telegram. Наприклад, виводити попередження: «Це посилання веде до стороннього месенджера. Переконайтеся, що довіряєте джерелу».

4. Надавати спрощений спосіб скаржитися на рекламу, яка веде в Telegram. Можна додати спеціальну категорію скарг — «Підозріле переспрямування в месенджери».

2.3. Диво-ліки та вдавані «держпрограми здоров'я»

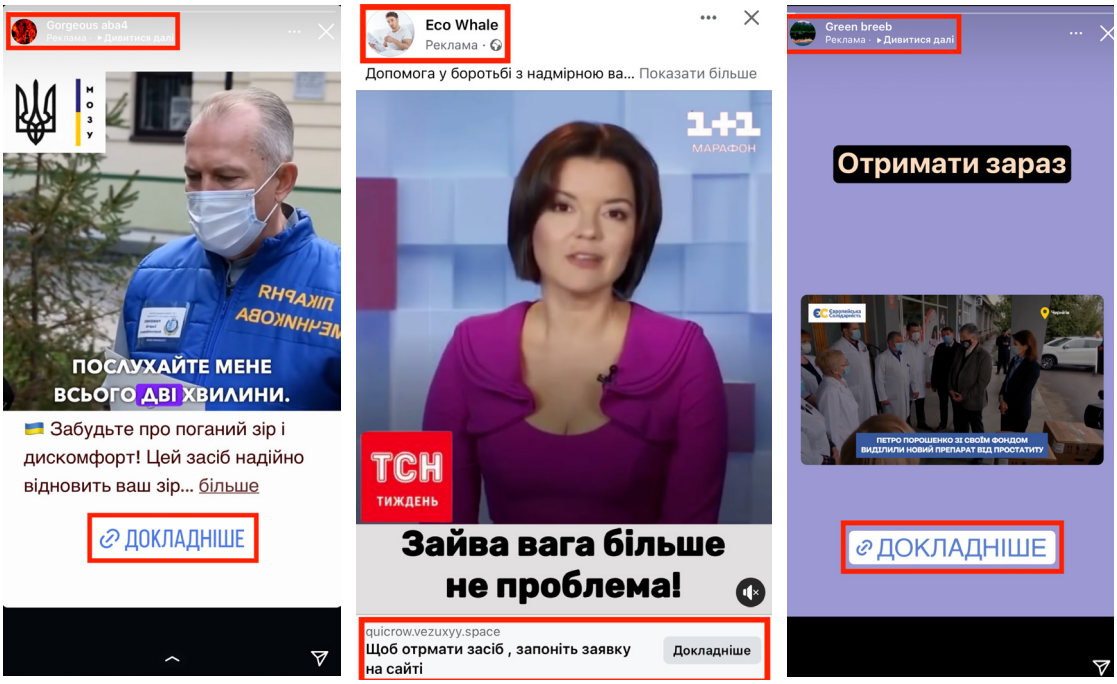
Вже кілька років — а надто з початком повномасштабного вторгнення — у стрічці Facebook з'являється реклама про «диво-ліки» від всіх хвороб і проблем. Відома телеведуча, лікар, політик чи ШІ-бабуся радять купити «чарівні таблетки», що лікують усе — від зайвої ваги й слабкого зору до потенції чи варикозу. Ще й безкоштовно! За «державною програмою»!

Очевидно, що ані лікар, ані телеведуча з рекламного допису ні сном ні духом не знали, що вони щось рекламують, — це був **дипфейк**.

Дипфейк — крадені відео, на яких обличчя або голос людей змінено штучним інтелектом, щоби ввести вас в оману.

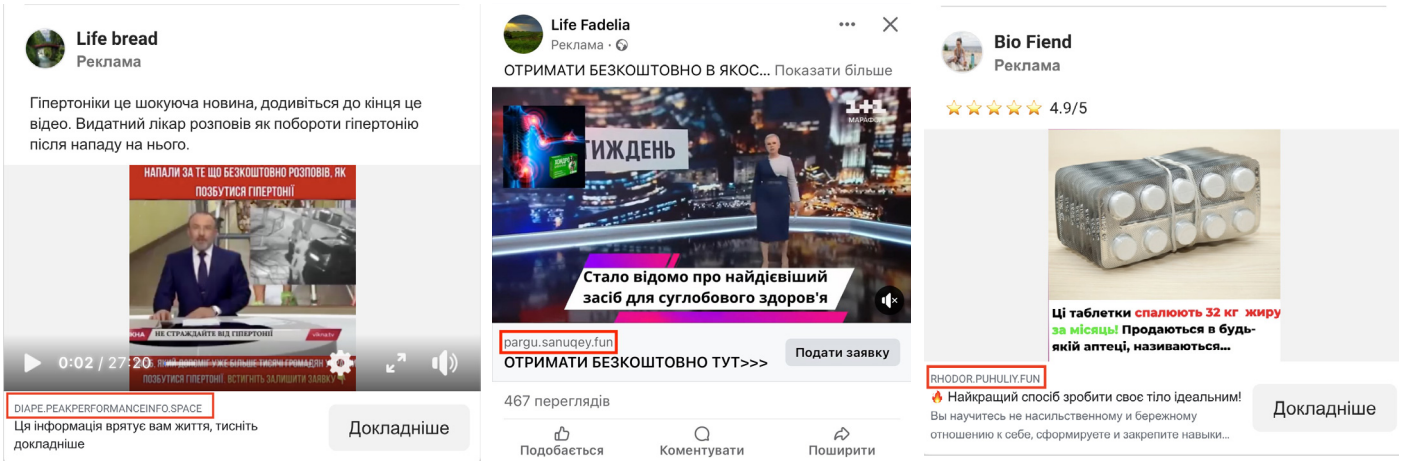
2.3.1. Як працює схема

1. Крок перший — реклама у стрічці. Ви бачите дипфейк, де знайомий ведучий чи авторитетний лікар нібито щиро радить купити унікальний препарат. Все виглядає переконливо — мова українська, фон студії знайомий, а на екрані — обличчя та ім'я відомої особи.



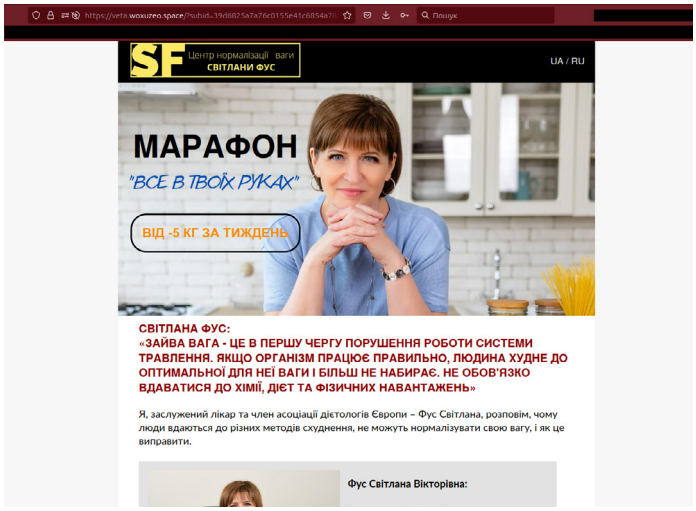
Джерело: скриншоти ЦЕДЕМ

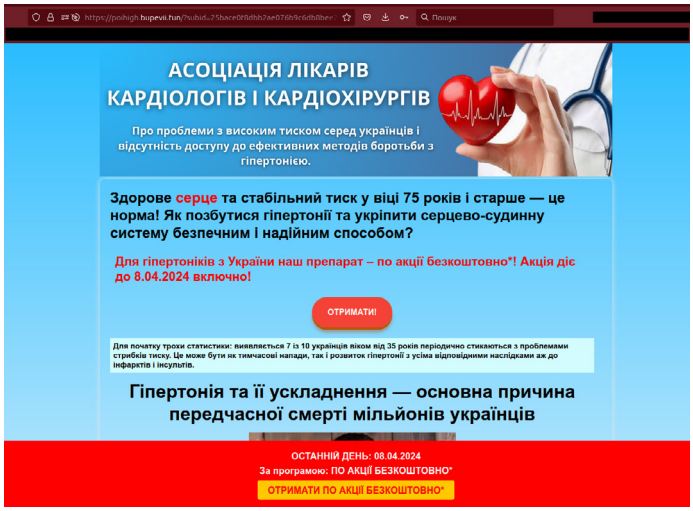
2. Крок другий — посилання на сторонній сайт. Дипфейк містить посилання на сайт із підозрілим доменом на кшталт *abra-kadabra.fun* чи *huba.buba.space*.



Джерело: скриншоти ЦЕДЕМ

3. Крок третій — сайт. Сайт виглядає «професійно»: інтерв'ю з лікарем чи героєм, «відгуки пацієнтів», логотипи, графіки, великі тексти.



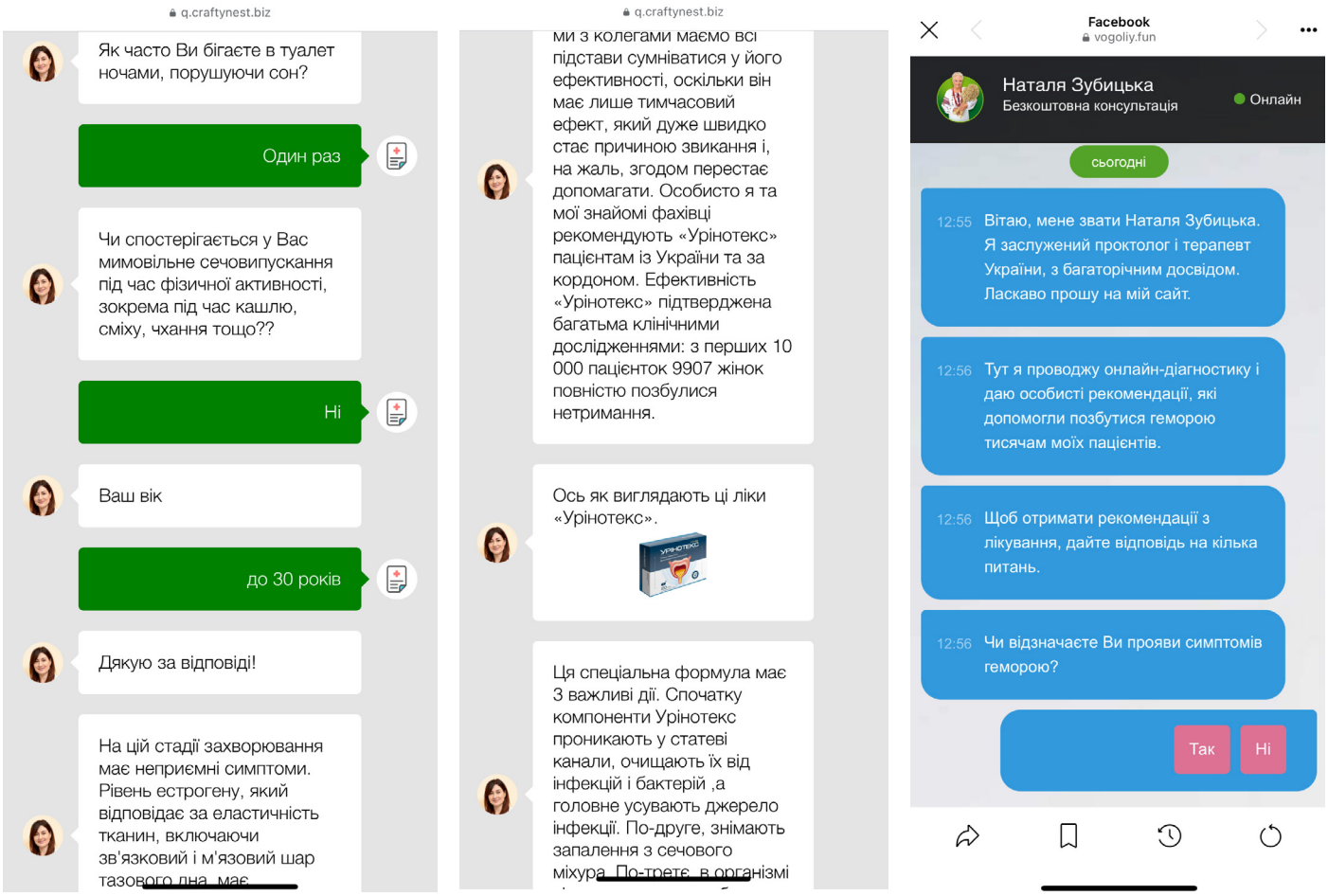


Джерело: скриншоти ЦЕДЕМ

Деякі сайти пропонують вам виграти знижку — звісно ж, вона буде 100%-ю. Далі просять вказати ім'я й телефон.

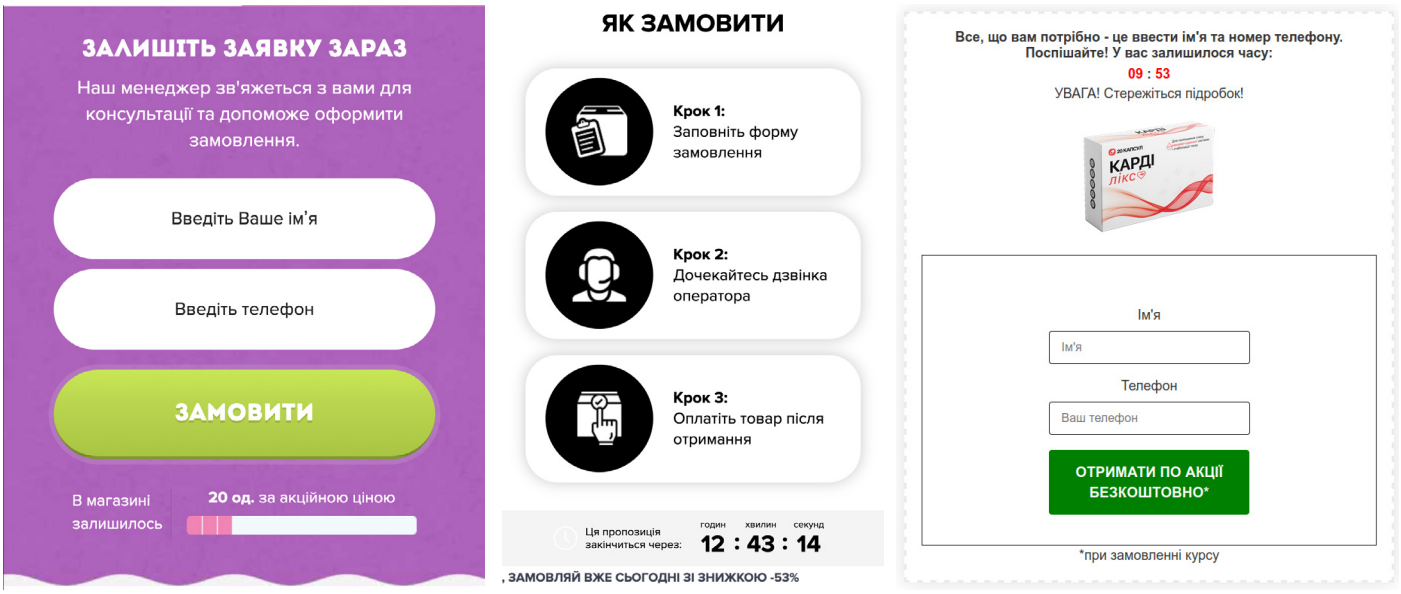
Джерело: скриншоти ЦЕДЕМ

Інші сайти пропонують «онлайн-консультацію» в чаті з лікарем. Нібито лікар запитує про проблему, каже, що звичайні ліки не допоможуть, але є «Суперпуперомін», який точно врятує.



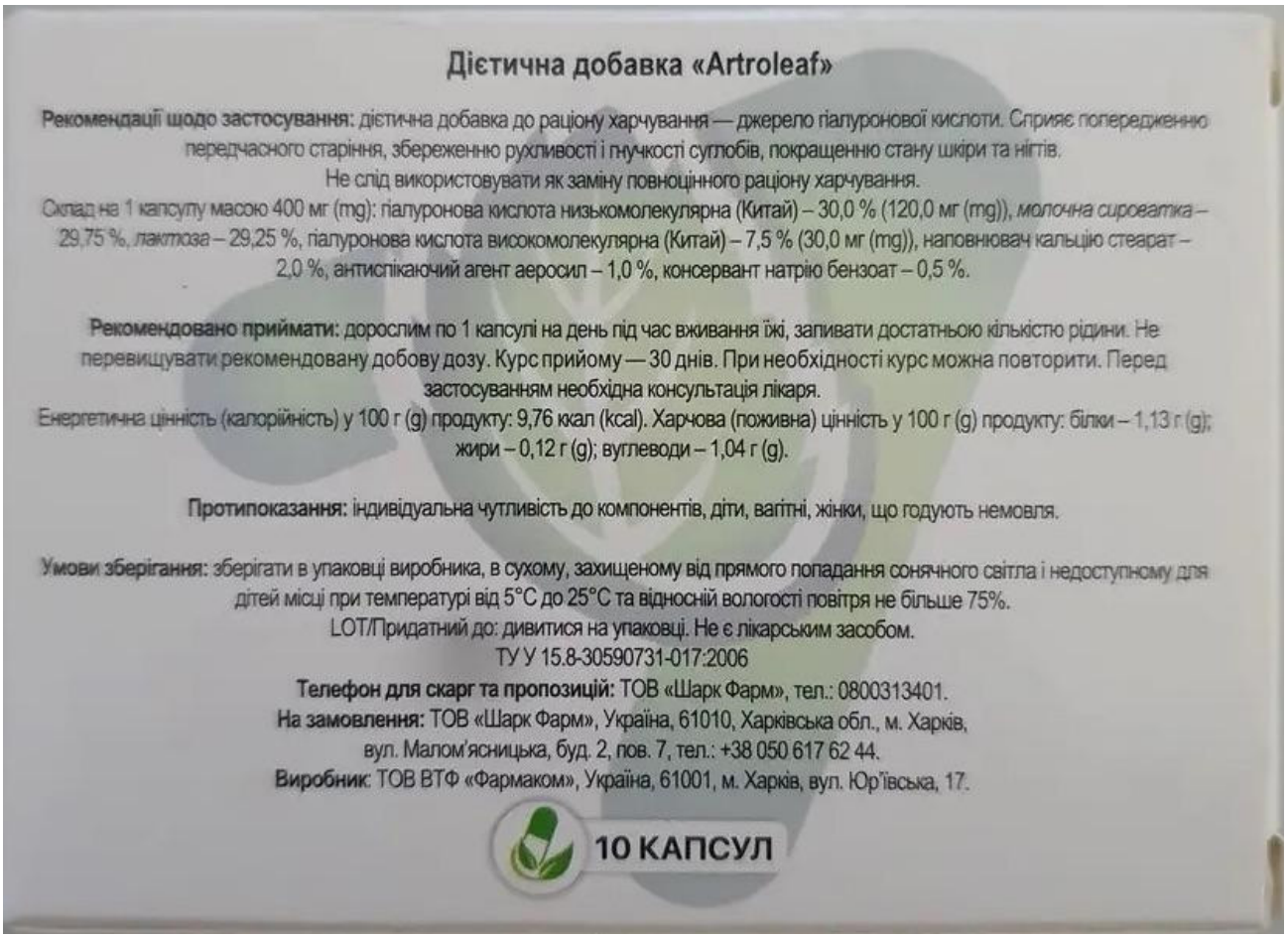
Джерело: скриншоти ЦЕДЕМ

4. Крок четвертий — контактні дані для зворотного зв'язку. Далі вам пропонують залишити свої контактні дані.



Джерело: скриншоти ЦЕДЕМ

5. Крок п'ятий — дзвінок для підтвердження замовлення. Потім телефонує «консультант» і переконує за великі гроші купити «диво-препарат». Насправді ж це звичайнісінька дієтична добавка (БАД).



Джерело: скриншоти ЦЕДЕМ

У чому ризик?

- **Небезпека для здоров'я.** Необхідно наголосити, що БАДи — це не ліки. Коли вам кажуть, що рецептурні препарати не потрібні, а вилікує БАД, — ви наражаєте себе на небезпеку. Особливо коли йдеться про діабет, онкологію, хворобу серця чи інші тяжкі недуги.
- **Фінансове шахрайство.** Часто «диво-препарати» продають за завищеною ціною. БАДи ж за потреби можна купити самостійно в аптеках за значно вигіднішими пропозиціями.
- **Цифрова безпека.** Залишаючи свої дані на фейкових сайтах, ви наражаєтесь на подальші спроби шахрайства — наприклад, з боку інших «проєктів» цієї ж мережі.
- **Відсутність відповідальності.** У випадку обману повернути гроші майже неможливо. Шахраї знають, що лишаться безкарними. Адже їхній сайт і сторінка у Facebook — фальшиві одноденки. А виробник БАДів на ваші претензії розведе руками, бо не він продавав вам їх як ліки — в сертифікаті написано «харчова добавка».

2.3.2. Поради користувачам

1. Не довіряйте рекламі з надто гучними обіцянками. Якщо «ліки» обіцяють вилікувати все одразу, ще й безкоштовно — це, найімовірніше, обман.

2. Перевіряйте джерело відео. Якщо знайомий політик чи ведучий раптом починає рекламувати диво-таблетки — перевірте, чи є такий запис на його офіційній сторінці.

3. Звертайте увагу на домени сайтів, куди спрямовує реклама. Домени на кшталт *abra-kadabra.fun* чи *huba.buba.space* — це сайти-одноденки, строк життя яких — кілька тижнів.

4. Не залишайте номер телефону на підозрілих сайтах. Це відкриє двері для нав'язливих дзвінків і нових схем.

2.3.3. Рекомендації для Meta

1. Вдосконалити виявлення дипфейків і фейкових відео. Алгоритми модерації мають аналізувати обличчя, голос і звукову синхронізацію, щоб ефективніше виявляти підроблені відео з ознаками маніпуляції.

2. Підвищену увагу приділяти рекламі, що містить посилання на домени із сірих зон. Наприклад: *.xyz, .fun, .space* тощо. Такі домени часто використовуються саме в шахрайських схемах, тож потребують пильнішої уваги.

3. Обмежити можливість рекламувати продукти медичного або «оздоровчого» характеру без чіткої перевірки документів. Рекламу будь-яких «ліків» і дієтичних добавок має розміщувати виробник чи офіційний представник.

4. Забезпечити прозору систему перевірки особистості рекламодавця. Якщо в рекламі використовується відоме обличчя, потрібна обов'язкова верифікація джерела та дозвіл від особи, яку зображено.

5. Розширити механізми скарг на модифіковані відео з публічними особами. В розділі скарг слід додати «використання публічних осіб у модифікованих відео (голос, ШІ тощо)».

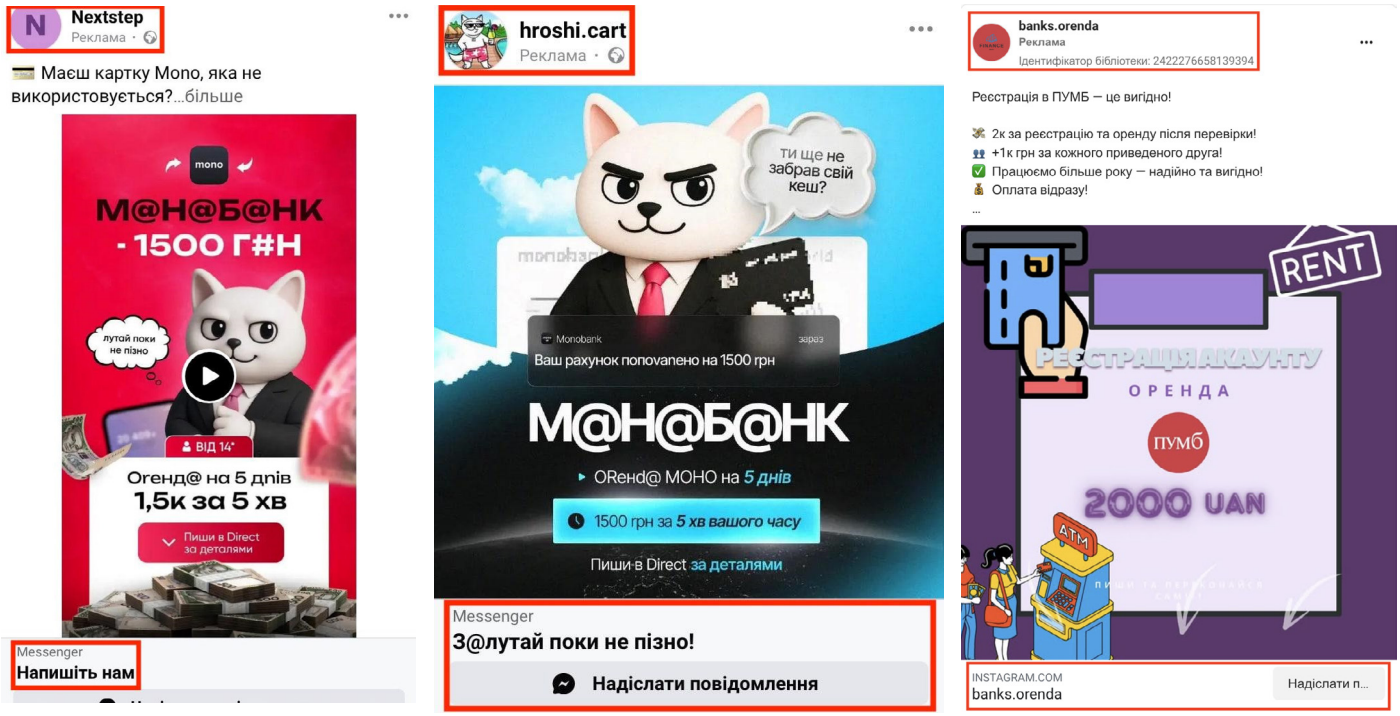
6. Інформувати користувачів про ознаки шахрайської реклами. Через сповіщення, картки безпеки у стрічці або навчальні відео. Особливо важливо показувати ці попередження людям, які взаємодіють із медичними темами.

2.4. Оренда банківської картки

Інша схема маскується під «**пасивний дохід**». Так, у Facebook з'являються оголошення на кшталт:

- «Здай свою банківську картку в оренду — отримай 1000 грн за 5 хв! Нічого робити не треба»;
- «Допоможи з переказами — заробляй онлайн легко і швидко»;
- «Зареєструйся в банку і здай рахунок в оренду. Напиши нам».

Пропонують лише надати доступ до рахунку — все інше «зробить команда».



Джерело: скриншоти ЦЕДЕМ

Звучить заманливо — хто б не хотів без зайвого клопоту отримати кілька тисяч гривень? Та безкоштовний сир буває тільки в мишоловці.

Насправді ж ви отримаєте проблеми з законом. Адже за такою пропозицією «легкого заробітку» ховається шахрайська схема відмивання грошей — і вас запрошують стати співучасником злочину.

2.4.1. Як працює схема

Шахраї шукають так званих грошових мулів, або дропів — людей, які за невелику плату погоджуються надати аферистам свою банківську картку або рахунок. Іноді аферисти пропонують «попрацювати» — відкрити рахунок на своє ім'я (якщо ще немає) і переказувати кошти.

Далі ваша банківська карта та рахунок стають частиною злочинної схеми:

- через них проходять гроші із шахрайств, фішингу, онлайн-біржі, торгівлі наркотиками, нелегальних азартних ігор, фінансування тероризму чи інших незаконних джерел;

- гроші «відмивають», пускаючи по ланцюгу таких самих «грошових мулів», щоби приховати їхнє походження;
- ви — те обличчя, яке фігурує в банку. Усі транзакції прив'язані до вас. І коли правоохоронці починають розслідування, першим на гачку опиняється не організатор, а саме ви — власник картки.

Шахраї — в тіні, а ви — під підозрою, усвідомлюєте ви це чи ні.

Що загрожує «грошовим мулам»?

- **Кримінальна відповідальність.** Закон не вибачає «я не знав» — зокрема, стаття 209 Кримінального кодексу України щодо відмивання коштів передбачає позбавлення волі строком від 3 до 12 років.
- **Обмеження банківських послуг.** Надалі вам можуть заблокувати доступ до банківських систем.
- **Репутаційні ризики і проблеми з працевлаштуванням.** Роботодавець може не взяти на роботу людину, яка фігурувала у справі про відмивання грошей.
- **Втрата грошей.** Шахраї можуть у будь-який момент просто зняти всі кошти з вашої картки, якщо ви надали їм доступ.
- **Моральна відповідальність.** Поки ви «допомагали з переказами», через ваш рахунок могли пройти гроші з торгівлі людьми чи фінансування тероризму. Ви, хай навіть несвідомо, могли допомогти злочинцям завдати реальної шкоди іншим людям.

Як розпізнати шахрайську рекламу про «легкий заробіток»?

Підозріла Facebook-сторінка, що поширює рекламу:

- створена нещодавно — як правило, дні або тижні тому;
- має дивну назву (може бути набір букв, якісь англійські слова);
- іноді маскується під банк або компанію (фейковий логотип, стиль оформлення мімікрує під стиль справжнього банку).

Ознаки шахрайського оголошення:

- просять використовувати ваш рахунок для переказу грошей;
- тільки онлайн-спілкування з «орендатором», без можливості особистої зустрічі;
- обіцяють великі гроші за мінімальні дії (наприклад, 1000 гривень за день).

2.4.2. Поради користувачам

1. Ніколи не передавайте стороннім особам свою банківську картку, її реквізити чи доступ до рахунків. Ніколи не розголошуйте:

- номер банківської картки, її термін дії, ПІН-код і CVV-код;

- логін та пароль від інтернет-банкінгу чи мобільного застосунку;
- одноразові коди з SMS або push-повідомлень.

2. Перевіряйте Facebook-сторінку, що поширює рекламне оголошення: яку вона має назву, коли вона створена тощо. Скаржтеся на підозрілі сторінки.

3. Ігноруйте будь-які оголошення про «легкі гроші», які просять переказати кошти чи надати доступ до картки або рахунку.

4. Якщо вже погодилися і зрозуміли, що потрапили в пастку, — одразу зверніться до Кіберполіції (https://ticket.cyberpolice.gov.ua/) та банку, в якому шахраї використовують картку чи рахунок.

2.4.3. Рекомендації для Meta

1. Автоматично блокувати рекламу з ключовими словами на кшталт «оренда картки», «заробіток через рахунок» тощо.

2. Ефективніше видаляти сторінки, що видають себе за банки або фінансові організації без офіційної верифікації.

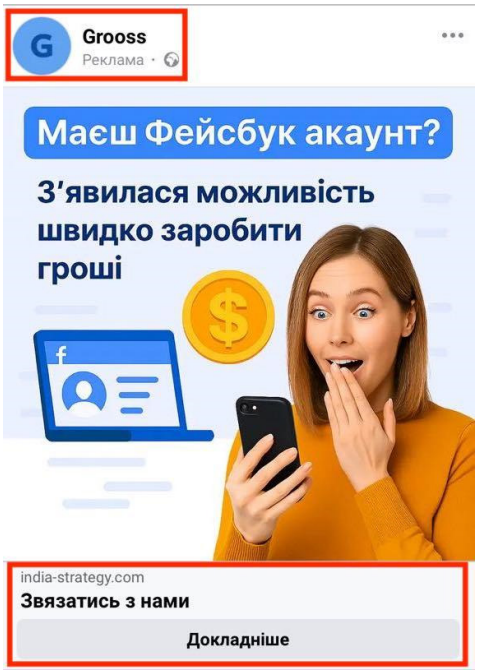
3. Позначати потенційно шахрайську рекламу та запускати інформаційні сповіщення для користувачів, які активно переглядають подібні оголошення.

4. Створити окрему категорію скарг на порушення стандартів спільноти Facebook, як-от «фінансове шахрайство», щоб користувачі могли скаржитися на таку рекламу.

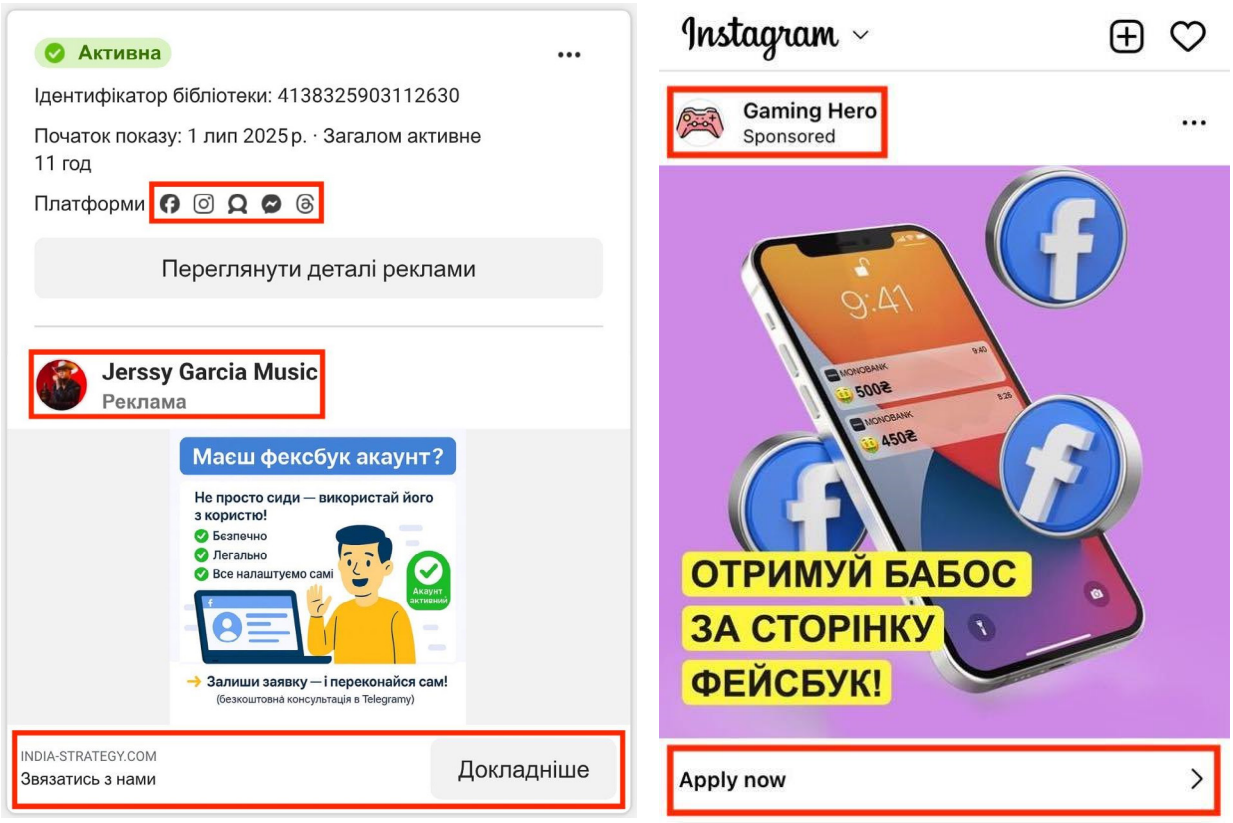
5. Сприяти інформаційним кампаніям про «грошових мулів». Особливо націленим на молодь, студентів, військовозобов'язаних, людей у скруті — бо саме ці аудиторії є головною мішенню таких схем.

2.5. Оренда Facebook-акаунтів

Рекламні оголошення на кшталт: *«Ваш акаунт старше року? Є фото й друзі? Орендуємо, платимо 500 гривень на тиждень, лише включимо рекламу»* почастішали у стрічці Facebook. Звучить привабливо: акаунт у вас уже є, зайвих грошей не буває — чому б і ні? Насправді ж це ще один різновид шахрайства, що експлуатує довіру користувачів.



На перший погляд, схеми з оренди акаунтів виглядають як проста можливість пасивного заробітку, та насправді вони становлять чималу загрозу для безпеки облікового запису, особистих даних і репутації власника.



Джерело: скриншоти ЦЕДЕМ

2.5.1. Як працює схема

Шахраї представляються «маркетологами» або «великими рекламними агенціями». Вони шукають справжні людські акаунти, які були створені щонайменше пів року тому, демонструють певний рівень активності, мають фото, друзів та інші ознаки автентичності, — і пропонують людям здати їх в оренду на вигідних умовах. Запевняють, нібито використовуватимуть лише рекламний кабінет і лише в законних цілях, а сам акаунт залишиться в повному доступі власника. Та насправді все інакше.

Мета зловмисників — запуск рекламних кампаній через «чисті» автентичні акаунти, які ще не потрапили під санкції Meta. Цей процес ще називають *«відмивання реклами»* (advertisement laundering): компанії чи особи, які не можуть (через санкції Meta) або не хочуть (через суперечливість рекламованого товару чи послуги) запускати рекламу напряму, «ховаються» за орендованими акаунтами і запускають рекламу через них.

Є кілька типових способів, як шахраї отримують доступ до акаунта:

- **через віддалений доступ до комп'ютера.** У деяких випадках користувача просять встановити спеціальну програму (наприклад, AnyDesk або TeamViewer), щоб «допомогти з налаштуванням реклами». В результаті зловмисник самостійно входить у Facebook із вашого пристрою, має повний доступ до браузера, файлів та акаунтів;

- **через передачу пароля.** Інші одразу запитують логін і пароль від акаунта — обіцяючи, що нічого змінювати не будуть. Це прямий шлях до повної втрати контролю над акаунтом, особливо якщо не увімкнена двофакторна автентифікація.

Навіщо зловмисникам чужі акаунти?

Шахраї можуть створювати нові сторінки від вашого імені, запускати шахрайську або маніпулятивну рекламу, залишати коментарі на інших сторінках, а в окремих випадках — змінити пароль і повністю захопити акаунт. Аферисти переслідують такі цілі:

- **використання рекламного кабінету** — для просування як звичайних невинних оголошень, так і скам-товарів: псевдокосметики, пігулок, фейкових інвест-платформ або онлайн-казино;
- **публікація шахрайських зборів коштів** — аферисти можуть публікувати дописи нібито зі збором коштів на лікування, амуніцію, дрони для ЗСУ тощо від імені власника акаунта;
- **звернення до друзів по гроші** — шахраї можуть писати вашим друзям від вашого імені і просити «терміново позичити 1000 грн»;
- **маніпулятивні коментарі** — на підтримку або дискредитацію сторінок, у тому числі з політичним підтекстом;
- **коментарі, що розпалюють ворожнечу**, — для посилення соціальних конфліктів і вкидання токсичного контенту.

Слід наголосити, що оренда акаунтів у такий спосіб грубо порушує правила Meta. Тож ваш акаунт можуть заблокувати. Разом із доступом до акаунту ви втратите й інші важливі дані — особисте листування, фото, доступ до бізнес-сторінок та інших функцій.

2.5.2. Поради користувачам

1. Ігноруйте всі пропозиції «легкого заробітку» через оренду сторінок. Це завжди ризиковано, навіть якщо обіцяють «нічого не змінювати у вашому акаунті».

2. Не передавайте нікому дані для входу — логін, пароль, коди двофакторної автентифікації.

3. Увімкніть двофакторну автентифікацію та регулярно перевіряйте активність входів у налаштуваннях безпеки Facebook.

4. Дбайте про свою «цифрову репутацію». Ваш акаунт — це не лише набір даних, а й цифрова особистість. Втрата контролю може обернутися втратою довіри ваших друзів, підписників і колег.

5. Реагуйте, не мовчіть. Скаржтеся на підозрілі рекламні дописи у Facebook, це допомагає зупиняти шахрайські кампанії. Якщо ви стали жертвою або зрозуміли, що потрапили у схему з «орендою» акаунта, — звертайтеся до Кіберполіції: https://ticket.cyberpolice.gov.ua/.

2.5.3. Рекомендації для Meta

Для боротьби з масовим поширенням цієї шахрайської схеми Meta має не лише реагувати постфактум, коли акаунт уже зламано або заблоковано, а й запровадити системні превентивні механізми. Серед найважливіших кроків:

1. Вдосконалити алгоритми штучного інтелекту для виявлення шахрайських рекламних оголошень. Алгоритми повинні краще виявляти підозрілі дописи, що містять характерні ключові слова на кшталт *«оренда акаунтів», «потрібен акаунт із доступом до реклами», «платимо за сторінку»* тощо. Такі оголошення повинні блокуватися до моменту публікації.

2. Автоматично виявляти й видаляти сторінки, які публічно декларують торгівлю акаунтами. Багато з таких сторінок прямо в назві вказують: *«Оренда акаунтів Facebook / Instagram», «Шукаємо акаунти з рекламним кабінетом»*. Такі назви не залишають сумнівів у порушенні правил платформи і мають видалятися без зволікань.

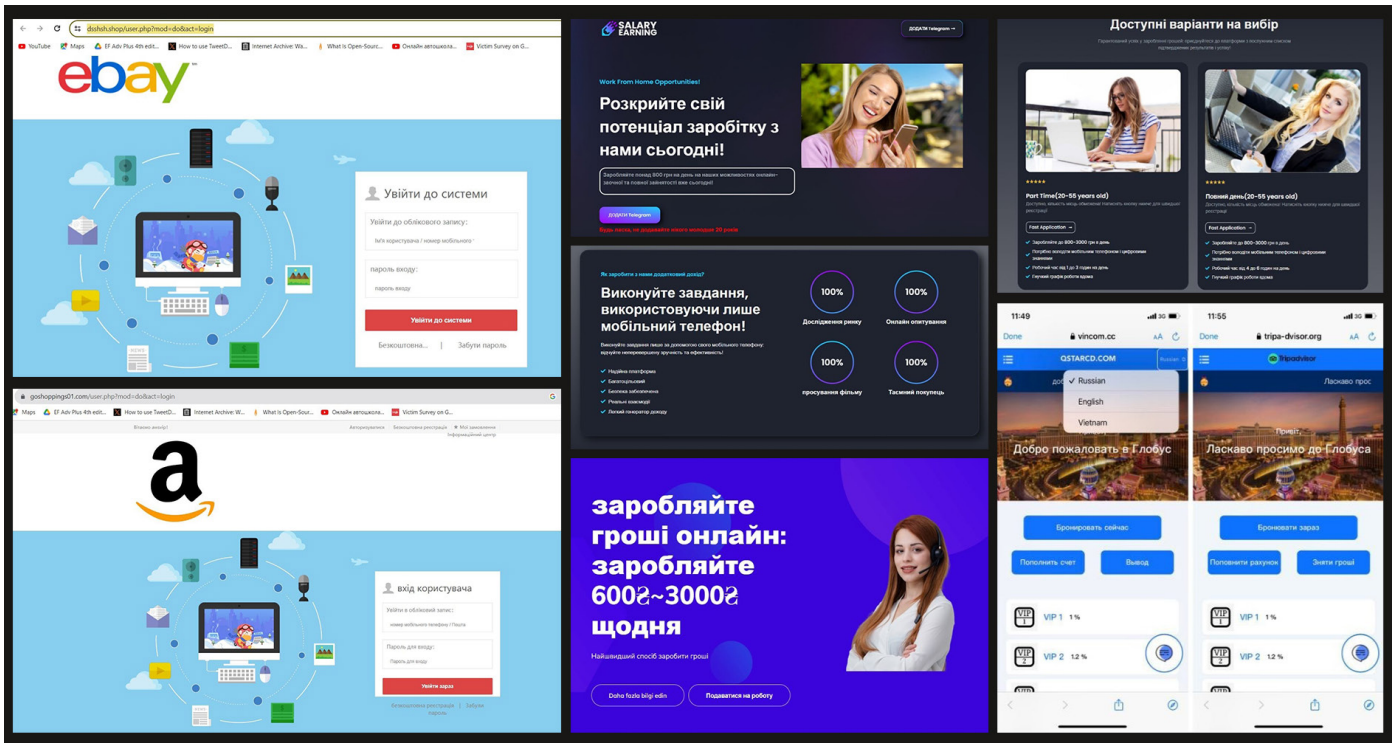
3. Запровадити систему сповіщень про незвичну активність в акаунті. Якщо з акаунта створюється нова сторінка або запускається рекламна кампанія, власник повинен отримувати сповіщення на електронну пошту або в додатку з можливістю миттєвого блокування цієї активності.

4. Показувати інформаційні попередження у стрічці новин про ризики «оренди акаунтів». Наприклад, Meta може запровадити невеликі банери або картки з текстом на кшталт: *«Не передавайте свій акаунт стороннім особам — це може призвести до його блокування»*, особливо у відповідь на взаємодію з підозрілими дописами.

5. Запровадити жорсткішу систему верифікації для першого запуску рекламних кампаній на фінансову тематику з нових акаунтів. Ввести додаткову ідентифікацію користувача, якщо профіль раніше ніколи не використовував рекламу. Це ускладнить використання «орендованих» акаунтів для шахрайських кампаній і захистить звичайних користувачів від того, що їхні профілі будуть використані у шахрайських схемах. без відома.

2.6. «Легкий заробіток» за лайки, перегляди, коментарі, скриншоти

Вам коли-небудь траплялася реклама з пропозиціями «лайкати відео на YouTube або TikTok за гроші»? Мовляв, ставте лайки, надсилайте скриншоти й отримуйте до 500 гривень на день. Спочатку все виглядає чесно: ви справді отримуєте 100 чи 200 гривень. Але насправді це лише гачок великої шахрайської афери.



Джерело: [скриншоти від асоціації ЄМА]

2.6.1. Як працює схема

1. «Гачок» — перші лайки і реальні виплати. Аферисти заманюють жертв через рекламу в соцмережах, месенджерах або навіть у коментарях до відео. Обіцяють гроші за перегляд контенту, лайки, коментарі, оцінки в Google-картах, Ebay або Amazon. За виконані «завдання» переказують дрібні суми — це створює ілюзію легкого заробітку і викликає довіру.

2. «Підвищення ставок» — перші вкладення. Наступний крок — приєднання до «робочої групи» в месенджері. Тут вам обіцяють ще більше грошей, але за умови, що ви купите товар у «партнерському магазині», поповните рахунок на фейковій криптобіржі або пройдете платну «реєстрацію».

Іноді ці сайти — фішингові, спрямовані на отримання ваших банківських даних зловмисниками.

В інших випадках аферисти можуть справді повернути вам першу «інвестицію» — із бонусом. Це ще більше заохочує до нових переказів. А далі — все, ви у пастці. Кожне наступне «завдання» коштує дорожче: 500 грн, 2000 грн, 10 000 грн. А щоб «отримати зароблене» — треба внести ще більше.

3. Фінал — втрата всіх коштів. Чати раптово зникають, адміністратори блокують вас або повідомляють, що «ви порушили правила», «вийшли з групи» чи «відмовились від завдання». Гроші не повертаються. Жертви часто лишаються з боргами, кредитами й скомпрометованими банківськими даними.

Насправді це класична фінансова піраміда

Ці «виплати за лайки» найчастіше надходять не від шахраїв, а від інших жертв — дропів, через яких зловмисники запускають обіг грошей. Усе це — схема, схожа на фінансову піраміду: одні новачки отримують невеликі виплати за рахунок інших, щоби спонукати їх інвестувати більше в ці схеми, а прибутки справжніх організаторів схеми — величезні.

Ви або жертва, або співучасник

Багато хто вважає: «Я візьму 200 гривень — і зникну. Переграю шахраїв!» Але ні, ви не переграєте схему. Якщо ви отримали переказ — це, ймовірно, кошти інших ошуканих. Ви вже частина шахрайської мережі, а не її переможець.

Отримавши кошти або переславши їх далі, ви можете наразити себе на такі ризики:

- **втрата особистих коштів.** Шахраї можуть витягнути з жертви значні суми, використовуючи методи психологічного тиску та обіцянки компенсацій;
- **компрометація персональних даних.** Під час «реєстрації» жертва часто вводить свої банківські дані, логін і пароль до онлайн-банкінгу або навіть завантажує копії документів;
- **юридична відповідальність.** Якщо кошти, отримані через подібні «завдання», мають шахрайське походження — користувач ризикує стати співучасником злочину і фігурантом справи за статтею 190 ККУ «Шахрайство»
- **підтримка шахрайських мереж.** Лайки, коментарі та поширення зловмисних сторінок сприяють видимості афери і втягненню нових жертв.

2.6.2. Поради користувачам

1. Віддавайте перевагу вакансіям на перевірених ресурсах (на кшталт lobby x, robota ua, work ua, happy monday) з офіційним працевлаштуванням.

2. Не вірте в «легкі гроші за лайки». Навряд легітимна компанія буде платити за перегляди чи лайки випадковим людям з соціальних мереж.

3. Не вводьте свої банківські дані на сторонніх або підозрілих сайтах.

4. Не переходьте за підозрілими гіперпосиланнями. Уважно перевіряйте URL — будь-яка дрібна помилка чи дивний домен можуть свідчити про фішинг.

5. Не переказуйте гроші на невідомі рахунки для «реєстрації», «покупки товарів» або «виведення бонусів».

6. Не повідомляйте незнайомцям номер картки, CVV-код, логіни та паролі до онлайн-банкінгу — навіть якщо вже отримали «виплату».

7. Якщо ви розголосили дані банківської картки — негайно зверніться до банку та заблокуйте її.

8. Сумніваєтесь — зверніться до Кіберполіції: ticket.cyberpolice.gov.ua.

2.6.3. Рекомендації для Meta

1. Впровадити проактивне виявлення реклами із фразами «заробіток на лайках», «гроші за перегляди», «доходи без досвіду» — як потенційно шахрайської.

2. Позначати небезпечні сайти, групи й чати, на які веде реклама, як потенційно шахрайські.

3. Інформувати користувачів про подібні схеми через вбудовані попередження у стрічці та на сторінках сповіщень. Наприклад, картками на кшталт: «Обережно: легкий онлайн-заробіток часто є частиною шахрайської схеми».

4. Пришвидшити розгляд скарг на рекламу, коли користувачі повідомляють про підозрілу схему із фінансовими втратами.

2.7. Висновки до другого розділу

Проведений аналіз шахрайських схем і дезінформації, поширюваних через рекламні інструменти Facebook, засвідчує високий рівень загроз для українських користувачів цієї соціальної мережі. Шахрайські оголошення, які експлуатують актуальні суспільні потреби, страхи чи очікування (зокрема теми фінансової допомоги, здоров'я чи легкого заробітку), масово залучають громадян у пастки, наслідками яких стають як фінансові втрати, так і витік персональних даних.

Характерною ознакою таких схем є їхня швидка адаптивність до реальних інформаційних приводів, що суттєво ускладнює ідентифікацію загроз користувачами та модераторами. Під час війни подібна реклама є не лише джерелом матеріальних збитків, а й фактором дестабілізації інформаційного простору через поширення паніки, зневіри й дезінформації.

Для ефективного протистояння цим загрозам критично важливим є підвищення прозорості рекламних інструментів Meta, удосконалення алгоритмів автоматичного виявлення шахрайських оголошень та регулярне інформування користувачів про актуальні ризики. Крім того, важливо продовжувати моніторинг українського сегменту Facebook для своєчасної ідентифікації та блокування нових шахрайських схем.

Таким чином, захист користувачів від рекламних шахрайств та дезінформації є не лише питанням їхньої особистої безпеки, але й умовою збереження довіри до самої платформи як інформаційного середовища у воєнних умовах.

Висновки

Проведене дослідження дозволило виявити й описати ключові ризики, пов'язані з поширенням маніпулятивного клікбейтного й шахрайського контенту в українському сегменті Facebook.

Як продемонстрував аналіз, феномен клікбейту є одним із центральних інструментів привернення уваги українських користувачів із подальшим втягненням їх у схеми фінансових шахрайств або інформаційних маніпуляцій.

Через таргетовану рекламу на платформі Meta зловмисники активно використовують соціальну вразливість громадян, пропонуючи фейкові соціальні виплати, псевдомедичні послуги чи «легкі заробітки», або підсовуючи дезінформацію, що становить значну загрозу фінансовій, фізичній та інформаційній безпеці.

Результати дослідження підтверджують, що ефективність таких схем обумовлена як складною соціально-економічною ситуацією під час війни, так і недостатньо ефективною модерацією клікбейтного і рекламного контенту з боку Meta. Саме тому вкрай важливо підвищувати цифрову грамотність українських користувачів та вдосконалювати політики модерації й перевірки рекламного контенту з боку самої платформи.

Для користувачів критично важливо навчитися розпізнавати ознаки клікбейту, не піддаватися на маніпулятивні заголовки та перевіряти інформацію виключно в надійних, офіційних джерелах.

Водночас для платформи Meta необхідно посилити модерацію клікбейтного й рекламного контенту, активніше боротися з поширенням фішингових посилань і шахрайських схем, а також систематично інформувати користувачів про найпоширеніші види онлайн-загроз.

Забезпечення ефективного захисту від клікбейту, маніпуляцій та онлайн-шахрайства є ключовою передумовою формування безпечного й надійного цифрового середовища, яке має не підривати, а підтримувати стійкість українського суспільства.

HEINRICH BÖLL STIFTUNG
КИЇВ
Україна

ЦЕНТР ДЕМОКРАТІЇ ТА
ВЕРХОВЕНСТВА ПРАВА