Електронний журнал «Ефективна економіка» включено до переліку наукових фахових видань України з питань економіки (Категорія «Б», Наказ Міністерства освіти і науки України № 975 від 11.07.2019). Спеціальності – 051, 071, 072, 073, 075, 076, 292.

Ефективна економіка. 2025. № 12.

DOI: http://doi.org/10.32702/2307-2105.2025.12.35

УДК 004.056:316.77

Г. М. Яровенко,

д. е. н., доцентка, доцентка кафедри економічної кібернетики,

Сумський державний університет

ORCID ID: https://orcid.org/0000-0002-8760-6835

М. С. Рожкова,

аспірантка, Сумський державний університет

ORCID ID: https://orcid.org/0000-0002-5444-9095

СЕНТИМЕНТ ЯК ІНДИКАТОР КІБЕРПАНІКИ: АНАЛІЗ МЕДІЙНОГО ДИСКУРСУ ПРО КІБЕРЗАГРОЗИ

H. Yarovenko,

Doctor of Economic Sciences, Associate Professor, Associate Professor of the Department of Economic Cybernetics, Sumy State University

M. Rozhkova,

Postgraduate student, Sumy State University

SENTIMENT AS AN INDICATOR OF CYBER PANIC: AN ANALYSIS OF MEDIA DISCOURSE ABOUT CYBER THREATS

У статті розглядається актуальна проблема формування кіберпаніки в суспільстві, зумовлена зростанням масштабу та складності кіберзагроз і впливом медійного середовища на сприйняття ризиків. Метою дослідження

є аналіз медійного дискурсу щодо кіберінцидентів для виявлення масових проявів кіберпаніки та визначення закономірностей формування емоційного фону у новинах, а також оцінка залежності тональності повідомлень від типу кібератак та їх економічних наслідків. Дослідження базується на емпіричному кількісному аналізі новин за 2020–2025 рр. із застосуванням структурування вибірки, аналізу часової динаміки та порівняння медіаджерел. Проведено класифікацію дискурсу за видами загроз, економічним впливом та емоційною тональністю. Новизна роботи полягає у демонстрації механізму формування кіберпаніки через взаємозв'язок між фактом атаки, економічною інтерпретацією та медійним сентиментом; підтверджено домінування негативного дискурсу. Методика охоплює використання Python, бібліотеки NLTK та інструмента VADER для автоматичного визначення тональності, а також контент-аналіз, нормалізацію даних і побудову графічних візуалізацій, включаючи Sankey-діаграму. У результаті оцінено дисбаланс медійної тональності, охарактеризовано сезонні коливання сентименту, поляризацію між видами ЗМІ, залежність емоційного фону від типів атак та виділено ключові тематичні кластери. Теоретичне значення полягає в розвитку підходів до дослідження інформаційних ризиків, практичне – у можливості створення індикаторів кіберпаніки та удосконалення комунікаційних стратегій. Оригінальність полягає в комплексному поєднанні сентимент-аналізу з економічною інтерпретацією дискурсу, а перспективи подальших досліджень охоплюють економетричне моделювання впливу медійного сентименту на фінансові ринки.

This article addresses the urgent issue of cyber panic formation in society, intensified by the growing scale and complexity of cyber threats. The relevance of the topic is driven by the influence of the media environment on risk perception and information security. The aim of the study is to analyze media discourse on cyber incidents to identify mass manifestations of cyber panic and determine the

patterns shaping the emotional background in the news environment. The study employs an empirical research design based on quantitative text analysis. The sample of news articles from 2020–2025 is structured, followed by time-series analysis and comparison across media sources. The discourse is classified by types of threats, economic impact, and emotional tone. The novelty of the study lies in demonstrating the logical mechanism of cyber panic formation through the connection between the occurrence of an attack, the interpretation of its economic implications, and media sentiment. The hypothesis regarding the dominance of negative discourse is confirmed by empirical data. The methodology involves the use of Python, the NLTK library, and the VADER tool for automatic sentiment detection. Content analysis, data normalization, graphical visualization, and Sankey diagrams were applied to identify key relationships. As a result, the media sentiment imbalance was assessed, the dominance of negative narratives was demonstrated, seasonal fluctuations in sentiment were identified, polarization among media types was characterized, sentiment dependence on cyberattack types was systematized, thematic clusters were highlighted, and the mechanism of cyber panic formation was generalized. The theoretical significance of the article lies in advancing approaches to studying information risks through media analysis. The practical significance is reflected in the potential application of the results for developing cyber panic indicators and communication security strategies. The originality rests in the comprehensive integration of sentiment analysis and economic interpretation of discourse. Future research may include econometric modelling of the impact of media sentiment on global financial markets.

Ключові слова: *кіберзагрози; медійний дискурс; сентимент-аналіз; кіберпаніка; кіберінциденти; інформаційна безпека; тональність новин.*

Keywords: *cyber threats; media discourse; sentiment analysis; cyber panic; cyber incidents; information security; news tone.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Сучасний світ і стрімка цифровізація стали ключовими факторами ризику, що суттєво впливають на економіку, політику та суспільство. Кіберінциденти, які раніше вважалися вузькотехнічною проблемою, сьогодні перетворилися на системний виклик, здатний паралізувати критичну інфраструктуру, бізнес-процеси та державні послуги, провокуючи кризи на різних ринках. Кібершахраї дедалі частіше атакують енергетику, транспорт, телекомунікації, фінансовий сектор і держуправління, що робить кіберзагрози важливою складовою національної та глобальної безпеки.

Масштаби проблеми швидко зростають. За даними Qualys, у січні–липні 2024 року кількість зареєстрованих вразливостей збільшилася на 30 %, а випадки активної експлуатації – на 20 % [1]. Це свідчить про скорочення «вікна безпеки» між виявленням недоліків і їхнім використанням у атаках. Найбільш уразливими залишаються сектори, що працюють із критично важливими даними. Наприклад, у сфері охорони здоров'я 2024 року кількість атак зросла на 32 % [2], що створює ризики не лише фінансових втрат, а й підриву довіри та загрозу життю людей.

Масштабність проблеми підтверджують інциденти 2024–2025 років. Збій у продукті CrowdStrike вивів з ладу 8,5 млн пристроїв і спричинив збитки понад 10 млрд доларів [3]. CDK Global була змушена сплатити 25 млн доларів викупу після атаки ransomware [3–4], а масові атаки на AT&T, Verizon і T-Mobile призвели до витоку даних користувачів [5]. У 2025 році середня вимога викупу сягнула 1,13 млн доларів, що на 104 % більше, ніж раніше [6].

Ці події демонструють багатовимірний вплив кіберінцидентів на ринки, інвестиційну поведінку та довіру споживачів. Найуразливішим елементом залишається інформаційний простір, адже саме новини формують емоційні сигнали, що перетворюються на фінансові реакції – від панічних продажів до підвищеного попиту на захисні технології.

Аналіз останніх досліджень і публікацій. Загалом масштабні інциденти, що уражають критичну інфраструктуру, корпоративний сектор чи державне управління, дедалі частіше стають джерелом фінансової

нестабільності, впливаючи на ціни активів, ліквідність і довіру інвесторів. Тому дослідження наслідків кіберінцидентів за останнє десятиліття перейшли від аналізу окремих прикладів до систематичних оцінок на великих вибірках. Tweneboah-Koduah, Atsu та Prasad довели, що новини про витік даних знижують ціни акцій і підвищують їхню волатильність, відображаючи зростання невизначеності [7].

У прикладних дослідженнях Day та Booker підтвердили, що ринки негативно реагують на масштабні атаки, зберігаючи спадний тренд після їх розкриття [8]. Kammoun, Rekik та Boujelbène показали, що навіть добровільне повідомлення про інцидент супроводжується падінням ринкової вартості, хоча прозорість частково пом'якшує його глибину [9]. Таким чином, ринки реагують не лише на сам факт атаки, а й на спосіб її подання в медіа.

Це зумовило розвиток досліджень тональності новин. Від словникових підходів наука перейшла до глибинних моделей: так, Huang та інші розробили FinBERT, який демонструє значно вищу точність класифікації фінансових новин [10]. Fatouros та інші показали високу результативність ChatGPT у zero-shot аналізі текстів [11]. Проте Todd, Bowdenn і Moshfeghi довели, що словникові методи легко маніпулюються, тоді як контекстні моделі значно стійкіші [12].

З'явилися спеціалізовані корпуси, наприклад SEntFiN, які дозволяють визначати сентимент щодо кожної компанії в багатооб'єктних новинах [13]. Це особливо важливо для кіберінцидентів, де негатив щодо постраждалої компанії може супроводжуватися позитивом щодо виробників засобів захисту. Islam та інші встановили, що атаки конкурентів інколи створюють позитивні доходності для компаній кібербезпеки [14]. Регуляторні аспекти також відіграють роль: Cao та інші довели, що посилення вимог до розкриття інцидентів у США підвищує ризик цінових обвалів [15].

Узагальнюючи, сучасні дослідження сходяться на тому, що ринки швидко та переважно негативно реагують на кіберінциденти; ключовим каналом впливу є медійний дискурс; а нові інструменти, від FinBERT до ChatGPT, відкривають можливості точнішої та оперативнішої оцінки ринкових настроїв. Зростання прозорості у сфері кіберризиків робить

сентимент-аналіз особливо важливим для кількісного вимірювання ефектів, які традиційні моделі часто не фіксують.

Формулювання цілей статті. Метою статті є реалізація аналізу медійного дискурсу про кіберзагрози для ідентифікації масових кіберпанік у світі.

Виклад основного матеріалу дослідження. Для реалізації поставленої мети дослідження проводився сентиментний аналіз глобальних новин про кіберінциденти за період 2020-2025 рр. за допомогою мови програмування Python, з акцентом на виявленні ключових закономірностей у їхній тональності та часовій динаміці. Дані було зібрано на платформі Media Cloud за ключовими словами, які відповідають термінам кіберзагроз, наприклад, "DDoS", "Phishing", "Ransomware", "Malware", "Data Breach", тощо [16].

Сентиментний аналіз – це метод автоматичного визначення емоційного забарвлення тексту: позитивного, нейтрального або негативного. У Python для такого завдання є бібліотека NLTK (Natural Language Toolkit), яка містить готові лексикони та моделі для аналізу тональності. У даному дослідженні застосовувався модуль Valence Aware Dictionary and sEntiment Reasoner (VADER) із складу NLTK. Це лексикон та набір правил, спеціально розроблені для роботи з короткими текстами, повідомленнями в соцмережах, заголовками новин та неформальною мовою.

У сучасних умовах, коли офіційні індекси кібербезпеки оновлюються лише раз на рік і не здатні відображати динаміку подій у режимі реального часу, саме аналіз тональності медіа може стати індикатором «миттєвого» рівня загрози. Негативні сплески сентименту відображатимуть підвищену напругу, тоді як позитивні чи нейтральні повідомлення сигналізуватимуть про відновлення стабільності або успішне подолання кризи, викликаної кіберзагрозами.

Проведений сентиментний аналіз дозволив отримати наступні результати. Так, Рисунок 1 розкриває структурний дисбаланс у тональності медіа-висвітлення кібербезпекових тем: майже половина (44,5%) всіх аналізованих медіа публікацій має нейтральне забарвлення, що свідчить про переважання фактологічного, безоціночного висвітлення інцидентів. Проте

негативні новини становлять значну частку – 33.4%, що підтверджує тенденцію до драматизації та акцентування на ризиках і наслідках кібератак. На тлі цього частка позитивних матеріалів (22.1%) виглядає маргінальною, вказуючи на системну проблему – медіа рідко висвітлюють успішні кейси запобігання загрозам, технологічні прориви в галузі безпеки чи позитивні регуляторні зміни, формуючи таким чином перекошену картину реальності.

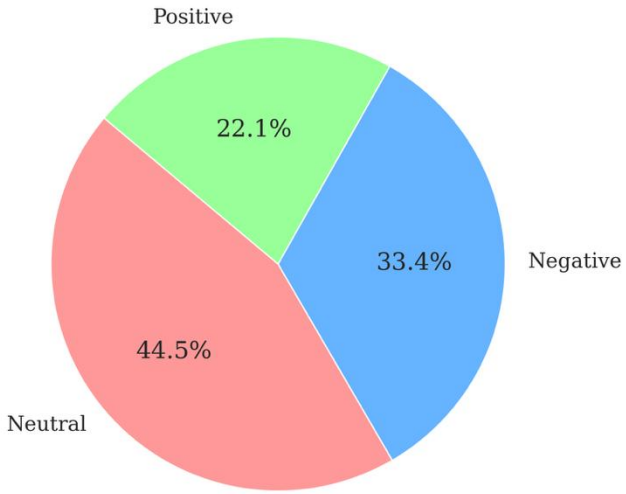

Рис. 1. Діаграма розподілу медіа-новин за тональністю

Джерело: власна розробка авторів

Проаналізуємо більш предметно динаміку новин в залежності їх емоційного забарвлення. Рисунок 2 демонструє чітку циклічність у середній тональності новин про кіберзагрози: різкі піки негативності у 2020 та 2022 роках, що корелюють з хвилями масштабних витоків даних і ransomware-атак, змінюються відносним затишшям у 2021 та 2023 роках, тоді як 2024-2025 роки виявляють нову хвилю ескалації, ймовірно, пов'язану з поширенням штучного інтелекту в кіберзлочинності та геополітичними конфліктами в кіберпросторі.

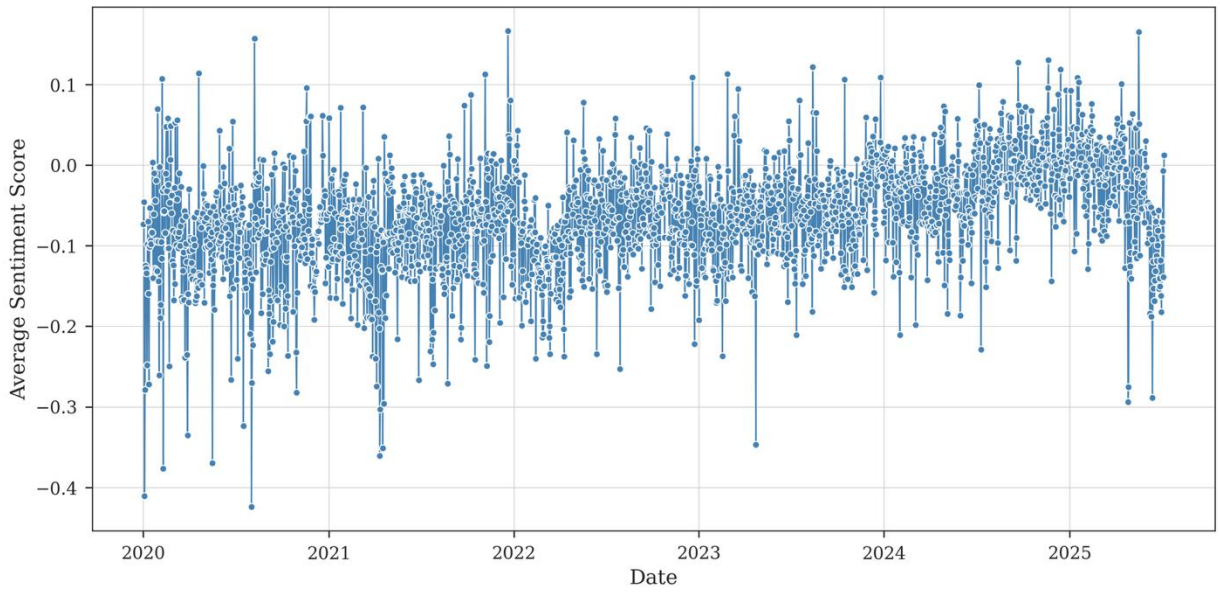

Рис. 2. Динаміка середньої тональності новин за 2020-2025 роки

Джерело: власна розробка авторів

Рисунок 3 фіксує експоненційне зростання кількості негативних новин про кіберзагрози: після різкого зльоту у 2021-2022 роках, коли їх число зросло майже втричі, спостерігається стабілізація на високому плато у 2023 році, проте вже з 2024 року траєкторія знову набирає підйом, прогнозуючи до 2025 року подвоєння показників порівняно з піковими значеннями 2022 року.

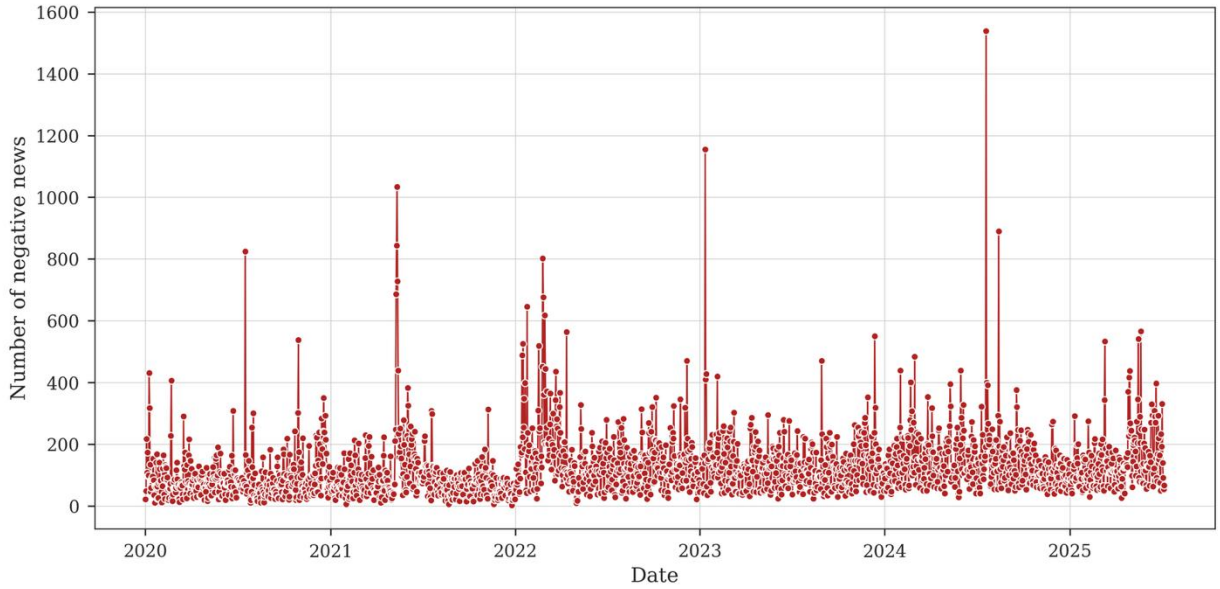

Рис. 3. Динаміка негативної тональності новин за 2020-2025 роки

Джерело: власна розробка авторів

На відміну від динаміки негативних новин, кількість позитивних повідомлень про кібербезпеку демонструє стабільно низькі значення (Рисунок 4), лише з незначними коливаннями на рівні 100-200 одиниць щороку, що вказує на хронічний дефіцит уваги ЗМІ до профілактичних заходів, технологічних проривів та успішних операцій з нейтралізації кіберзагроз упродовж усього аналізованого періоду.

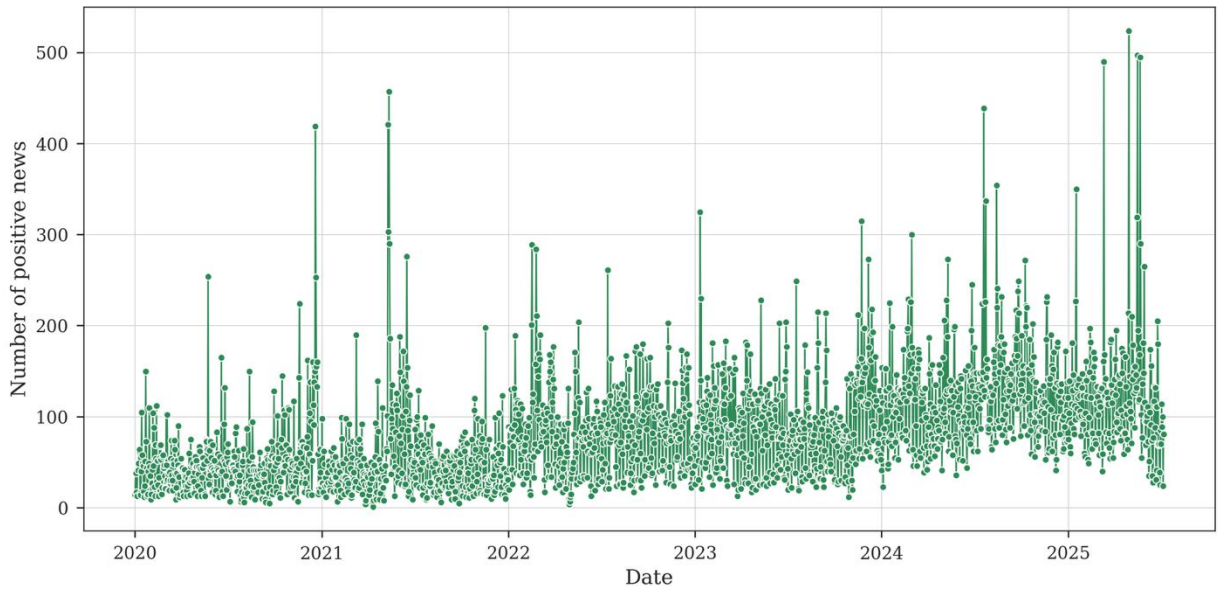

Рис. 4. Динаміка позитивної тональності новин за 2020-2025 роки

Джерело: власна розробка авторів

Якщо аналізувати періодичність, то Рисунок 5 демонструє чітку сезонність у висвітленні кіберзагроз із періодичними спалахами активності, які чітко корелюють з конкретними глобальними подіями – різкі піки припадають на перші квартали 2020 та 2022 років, що відповідає початку масових хвиль шантажувального ПЗ та конфліктів, пов’язаних з війною в Україні та загострення конфліктів на сході. З 2023 року спостерігається структурна зміна медіа-ландшафту: коливання кількості публікацій згладжуються, утворюючи стабільно високе плато, що вказує на інституціоналізацію кібербезпеки як постійної теми в інформаційному просторі. Прогноз на 2024-2025 роки підтверджує цю тенденцію, демонструючи відхід від чітко виражених сезонних спалахів на користь

сталого високого фону, що свідчить про перехід кіберзагрози з категорії епізодичних інцидентів до статусу хронічного ризику.

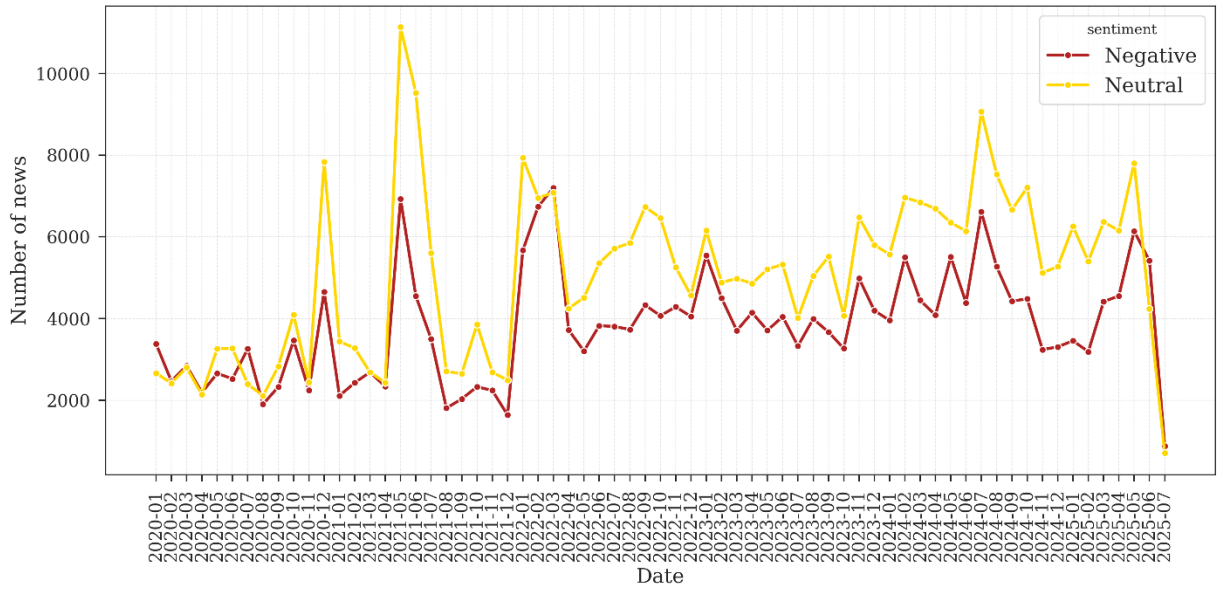

Рис. 5. Щомісячна динаміка тональності новин за 2020-2025 роки

Джерело: власна розробка авторів

Аналіз тональності медіа-висвітлення кіберзагроз виявляє значну поляризацію між окремими джерелами (рисунок 6). Такі видання як Forbes, MakeUseOf та Zawya демонструють нейтральну або помірно позитивну позицію (діапазон від -0.05 до +0.15), тоді як низка джерел, зокрема The Sun, Daily Mail, The Gardiant, Independent та інші виявляють стабільно негативну тональність з показниками -0.25 та вище. Ця дисперсія може бути пояснена кількома факторами:

1) цільова аудиторія та редакційна політика. Видання, орієнтовані на масового читача, часто використовують більш емоційну та алармістську мову для залучення уваги, що безпосередньо впливає на негативний сентимент. У той же час, бізнес-орієнтовані (Forbes, Business Standard) або технологічні (TechRadar, TechTarget) ресурси дотримуються більш об'єктивного та аналітичного стилю;

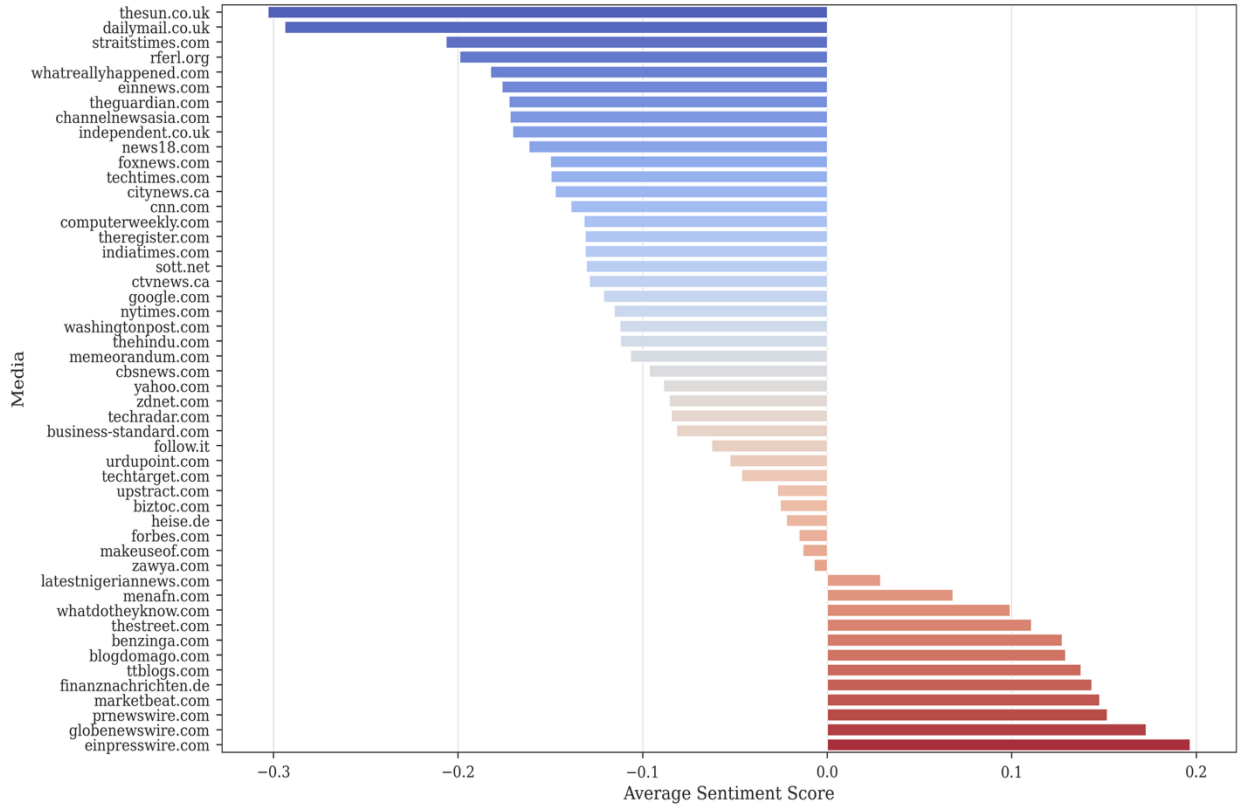

Рис. 6. Тональність новин за джерелами інформації

Джерело: власна розробка авторів

2) характер висвітлення. Джерела з позитивним або нейтральним сентиментом часто акцентують увагу на рішеннях, методах захисту та успішних кейсах кібербезпеки. На противагу цьому, видання з різко негативним тоном зосереджені на описі наслідків атак, фінансових збитках та соціальній тривозі, що безпосередньо формує «кіберпаніку»;

3) геополітичний контекст. Наявність у списку таких джерел, як rferi.org (Радіо Вільна Європа/Радіо Свобода) та heise.de (німецьке видання), може вказувати на регіональні особливості висвітлення, де кіберзагрози часто подаються через призму геополітичної конфронтації, що також посилює негативний фон.

Розподіл сентименту підтверджує, що медіа-ландшафт щодо кіберзагроз є неоднорідним. Однак переважна концентрація великих ЗМІ в області негативного сентименту свідчить про те, що саме алармістський нарратив домінує в інформаційному полі. Це створює ґрунт для соціальної

тривоги, навіть якщо експертні та нішеві видання намагаються балансувати картину. Таким чином, поляризація не лише відображає різні редакційні підходи, але й виступає ключовим механізмом у формуванні суспільного сприйняття кіберризиків.

Рисунок 7 виявляє різку диспропорцію у медійному висвітленні різних типів кіберзагроз, де хакінг домінує з показником у 71138 згадок, що більш ніж утричі перевищує показники наступних за ним категорій – malware (22192) та ransomware (20743). Ця статистика свідчить про те, що медіа схильні використовувати загальний термін "хакінг" як універсальний дескриптор для будь-яких кібератак, часто ігноруючи технічні деталі. Класичні загрози, такі як витоки даних (16973) та фішинг (14712), посідають помірну частку у висвітленні, тоді як складні та спеціалізовані атаки, зокрема zero-day (383) та defacement (106), залишаються практично непоміченими, що формує в аудиторії спотворене уявлення про реальний спектр кіберзагроз.

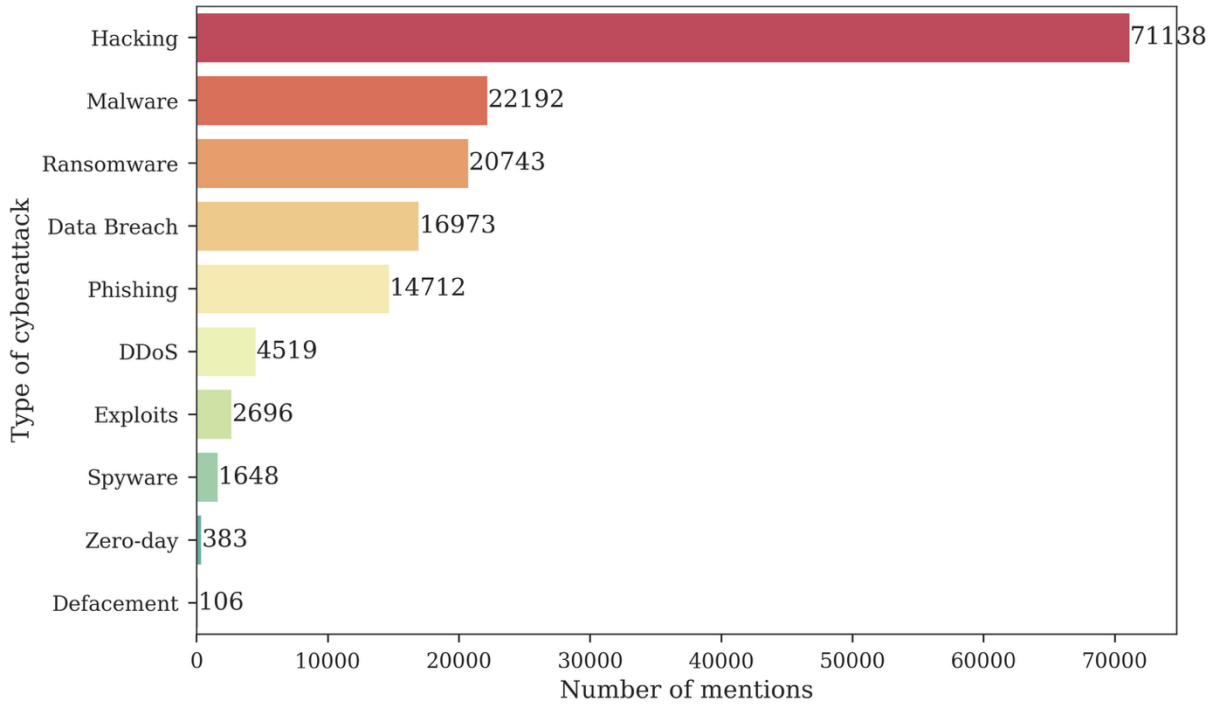

Рис. 7. Аналіз новин за видом кіберзагроз

Джерело: власна розробка авторів

Рисунок 8 відображає динаміку кількості новинних заголовків, пов’язаних із різними типами кіберінцидентів, у період з 2020 по 2025 рік.

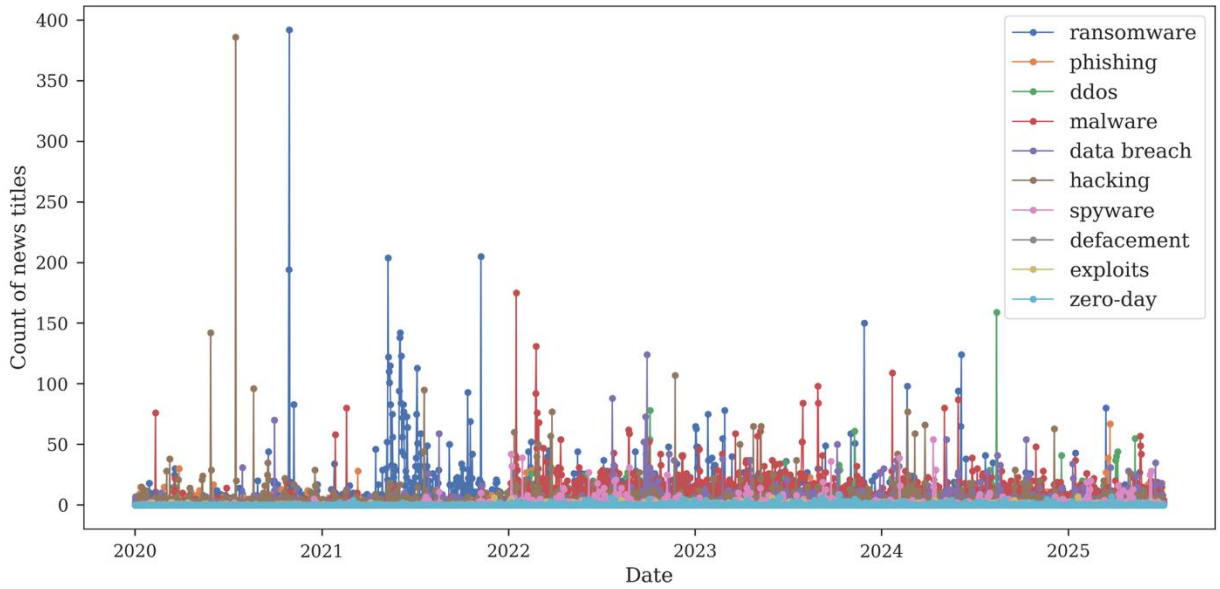

Рис. 8. Аналіз середньої тональності висвітлення різних типів кіберзагроз у ЗМІ

Джерело: власна розробка авторів

Аналіз розподілу даних свідчить про значну варіативність інтенсивності інформаційного висвітлення окремих типів атак у часі. Зокрема, спостерігається, що тематика, пов’язана з програмами-вимагачами («ransomware»), має найбільшу частоту появи у новинному просторі, що проявляється численними піковими значеннями, зокрема у 2020–2021 роках. Інші категорії, такі як «malware» та «data breach», демонструють відносно стабільну активність протягом усього періоду, із помірними коливаннями. Натомість повідомлення, що стосуються «phishing», «ddos» та «zero-day» атак, відзначаються меншою інтенсивністю та нерегулярними сплесками.

Загальна тенденція графіка свідчить про циклічний характер інтересу до теми кіберзагроз, що може бути пов’язано з періодичними сплесками активності зловмисників, великими інцидентами безпеки або зростанням уваги ЗМІ до певних типів атак. Незважаючи на коливання, протягом досліджуваного періоду простежується поступове підвищення частоти згадок

про кіберінциденти, що вказує на зростаючу актуальність проблеми кібербезпеки у глобальному інформаційному просторі.

Аналізуючи графік частки негативних заголовків за типами кіберзагроз (Рисунок 9), виявляється чітка закономірність: чим більш візуально демонстративною та публічною є атака, тим вищий відсоток негативного висвітлення вона отримує. Безумовним лідером за цим показником є дефейсменти (78,8%) – ці атаки, спрямовані на зміну зовнішнього вигляду веб-сайтів, є найбільш очевидними для масової аудиторії, що робить їх ідеальним матеріалом для сенсаційних заголовків.

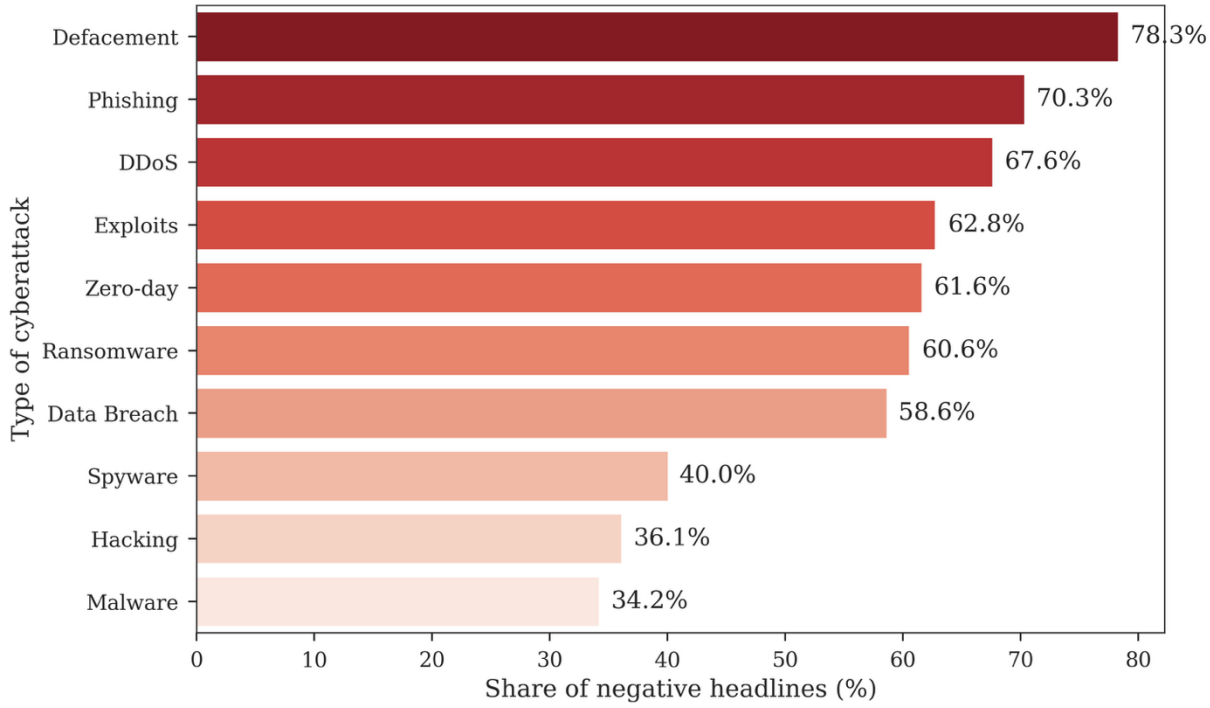

Рис. 9. Аналіз частки негативних заголовків за типами кіберзагроз

Джерело: власна розробка авторів

Близькі за рівнем негативу DDoS-атаки (67,6%) також належать до категорії "спектакльних" загроз, оскільки їх наслідки – недоступність популярних сервісів – миттєво відчують мільйони користувачів, що породжує хвилю негативного резонансу. Високі показники для експлойтів (62,8%) та zero-day вразливостей (61.6%) пояснюються їхнім "невидимим" та непередбачуваним характером, який журналісти часто подають через призму

"бомбо відкладного" механізму, створюючи відчуття постійної прихованої загрози.

Цікаво, що навіть такі рутинні, хоча й руйнівні, загрози, як витоки даних (58,6%) та ransomware (60,6%), демонструють лише трохи нижчі, але все одно критично високі рівні негативу. Це вказує на те, що сама тема кіберзлочинності в медіа-просторі стала універсальним тригером негативного сприйняття. Медіа, орієнтовані на кліки, інстинктивно використовують будь-яку кіберподію як привід для генерації тривоги, незалежно від реальних масштабів загрози, формуючи у суспільстві стійкий зв'язок між поняттям "кібербезпека" та почуттям небезпеки.

Графік середньої тональності висвітлення різних типів кіберзагроз у ЗМІ (Рисунок 10) виявляє цікаву та важливу закономірність.

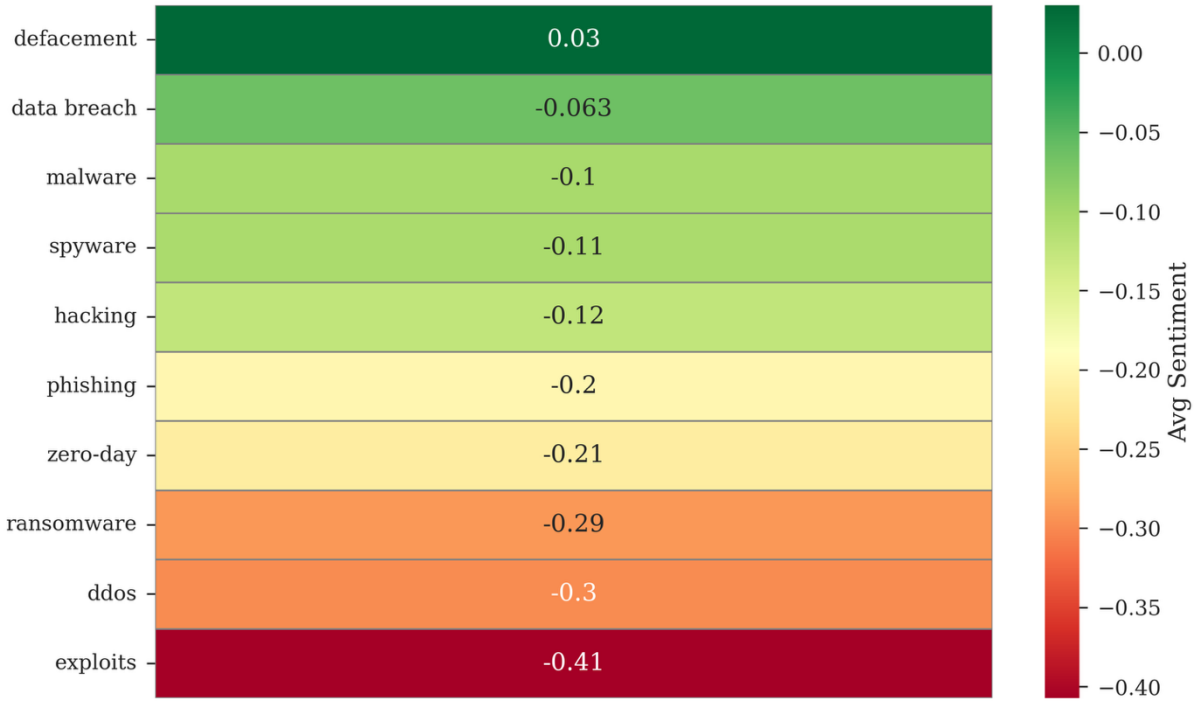

Рис. 10. Аналіз середньої тональності висвітлення різних типів кіберзагроз у ЗМІ

Джерело: власна розробка авторів

Єдиною загрозою з позитивним показником (+0,03) є дефейсмент. Це може пояснюватися тим, що такі атаки часто сприймаються як акти

вандалізму чи хактивізму, інколи з елементом символічного протесту, що місцями подається медіа не лише осудливо, а й із певною часткою схвалення. Натомість усі інші загрози мають негативну тональність, яка суттєво різниться за рівнем. Витоки даних (-0,063) та malware (-0,1) демонструють відносно помірний негатив, ймовірно через їхню буденність у цифровому середовищі.

Найбільш негативні значення притаманні технічно складним і кризовим загрозам: zero-day (-0,21), ransomware (-0,29), DDoS (-0,3) та exploits (-0,41). Вони асоціюються з раптовістю, значними збитками та відчуттям незахищеності, що формує похмурий медіаобраз. Показник експлойтів (-0,41) фактично виступає антирекордом і відображає найбільший рівень страху, спричинений непередбачуваністю та потенційно катастрофічними наслідками таких атак. Таким чином, графік демонструє залежність медійної тональності не лише від типу загрози, а й від її складності, раптовості та можливого масштабу руйнувань.

Рисунок 11 також відображає частоту ключових слів у медійному дискурсі. Найвищі піки пов’язані з ширшим контекстом — "business news community" та "2020 presidential election". Це свідчить, що кіберзагрози обговорювалися не ізольовано, а в поєднанні з бізнес-середовищем та політичними подіями, зокрема темою кібервтручання у вибори США, що вказує на політизацію проблематики кібербезпеки.

Значна група словосполучень зосереджена на конкретній компанії та пов’язаній із нею загрозі: "palo alto networks", "networks nasdaq panw", "alto networks nasdaq". Це демонструє, що медіа часто фокусуються на конкретних інцидентах, вказуючи на постраждалі організації, через що абстрактна загроза набуває конкретних обрисів і може посилювати кіберпаніку.

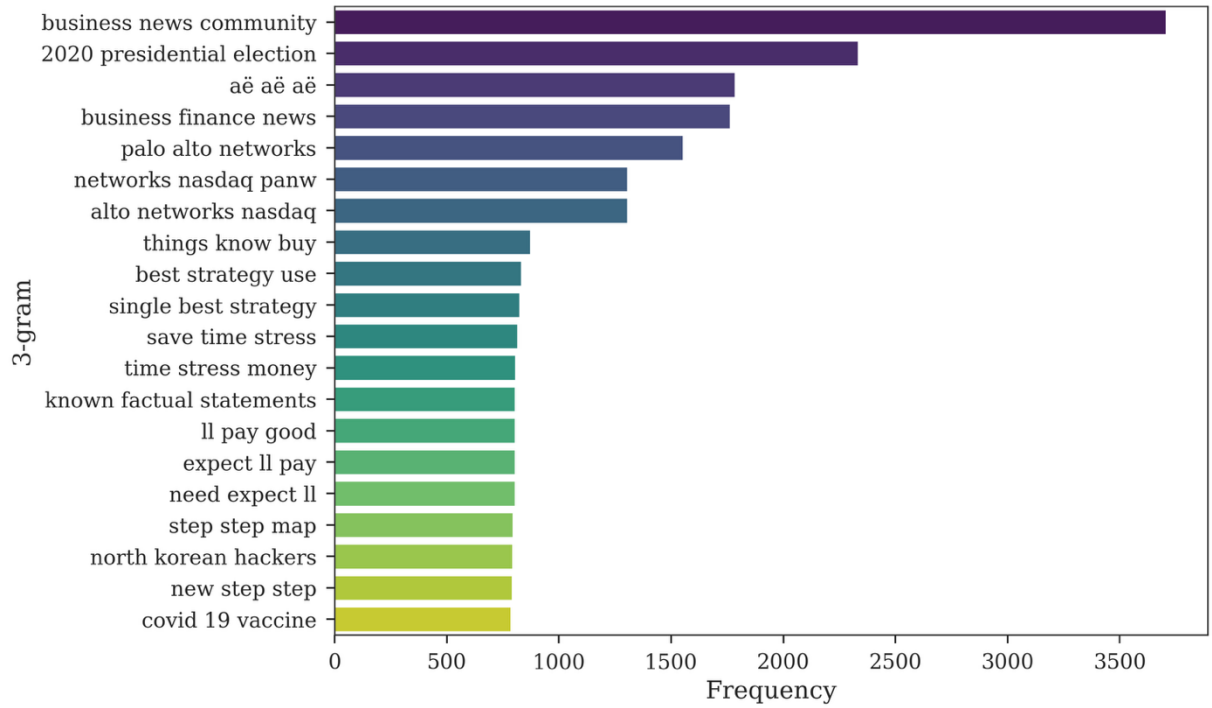

Рис. 11. Тематичні кластери медіадискурсу про кіберзагрози

Джерело: власна розробка авторів

Помітний кластер слів стосується реакції та порад: "things know buy", "best strategy use", "single best strategy", "save time stress", "time stress money", "step step map", "new step step". Ці фрази свідчать про прагнення медіа не лише констатувати проблему, а й пропонувати шляхи її вирішення. Використання слів "stress" і "money" підкреслює емоційний акцент, орієнтований на страхи щодо фінансових втрат і психологічного тиску.

Фрази "known factual statements" та "ll pay good", "expect ll pay", "need expect ll" можуть вказувати як на бажання медіа спиратися на факти (що частково знижує паніку), так і на акцент на фінансових наслідках, пов’язаних з економічним страхом. Наявність фрази "covid 19 vaccine" разом із термінами кіберзагроз свідчить, що дослідження охоплює період пандемії, коли теми цифрової та медичної безпеки переплiталися в інформаційному просторі.

Рисунок 11 підтверджує, що медійний дискурс про кіберзагрози не є суто технічним: він тісно пов’язаний із політикою, бізнесом та соціальними подіями. Медіа одночасно подають конкретику (компанії, хакерів) і використовують емоційно заряджену лексику, апелюючи до страхів щодо втрат, стресу та невизначеності. Саме поєднання конкретизації, політичного контексту й емоційної подачі формує та підсилює кіберпаніку в суспільстві.

Для аналізу логіки, як конкретні типи атак (наприклад, Ransomware, Data Breach) асоціюються в медійному дискурсі з певним рівнем економічного впливу, який, у свою чергу, формує загальний емоційний фон або сентимент (Негативний, Нейтральний, Позитивний) у публікаціях, було побудовано Sankey діагарму (Рисунок 12). Вона візуалізує потік зв'язків між трьома ключовими категоріями:

Категорія 1: Тип кібератаки (Hacking) – вихідна точка потоку.

Категорія 2: Економічний вплив (Economic Impact) – проміжна ланка.

Категорія 3: Сентимент (Sentiment) – кінцева точка потоку.

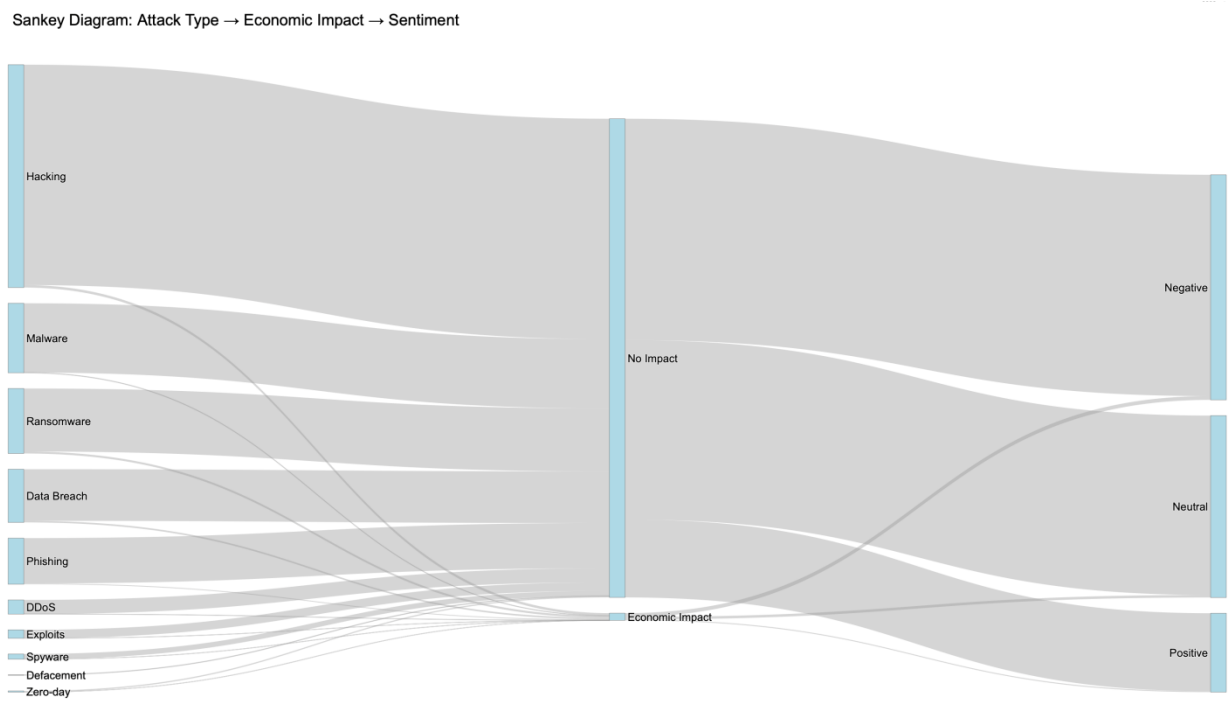

Рис. 12. Діаграма Sankey: Взаємозв'язок типів кібератак, економічного впливу та медійного сентименту

Джерело: власна розробка авторів

Ліва частина діаграми перераховує спектр кіберзагроз. Важливо відзначити наявність як широких категорій (наприклад, Data Breach), так і специфічних векторів атак (наприклад, Zero-day, DDoS). Це вказує на те, що медіа дискурс охоплює як загальні поняття, так і технічно складні та актуальні загрози. Присутність Ransomware та Malware як окремих категорій підкреслює їхню значущість і, ймовірно, високу частоту згадувань, що може бути прямим індикатором формування паніки, оскільки саме ці загрози найбільш відчутні для широкої аудиторії та бізнесу.

Центральна ланка – Economic Impact – є ключовим концептом у ланцюжку "загроза → наслідок → емоційна реакція". Це підтверджує гіпотезу про те, що саме матеріальні збитки та фінансові ризики є основним механізмом, через який технічні загрози трансформуються у соціальну тривогу. Потік від більшості типів атак саме до цієї категорії свідчить про домінування економічного наративу в освітленні кіберінцидентів. Окрема категорія No Impact може вказувати на публікації, де загроза лише констатується без оцінки її матеріальних наслідків, що, однак, не виключає формування негативного сентименту.

Права частина діаграми відображає емоційний результат медійного висвітлення. Потік, що сходиться переважно до категорії Negative, є прямим візуальним доказом формування негативного інформаційного фону навколо кіберзагроз. Це центральний висновок: незалежно від конкретного типу атаки та ступеня її економічного впливу, домінуючою медійною реакцією є негативний сентимент. Наявність Neutral та Positive потоків (останній, ймовірно, мінімальний) важлива для демонстрації того, що дискурс не є абсолютно одноманітним.

Ця триетапна модель підтверджує, що кіберпаніка не є спонтанною емоційною реакцією, а є структурованим соціальним явищем, що конструюється медіа через певні логічні зв'язки між фактами, їх економічною інтерпретацією та емоційним забарвленням.

Висновки та перспективи подальших розвідок у даному напрямі. Проведене дослідження довело, що сентимент-аналіз є ефективним інструментом для виявлення та оцінки явища кіберпаніки в медійному дискурсі. Отримані результати повністю корелюють з метою роботи та підтверджують ключову гіпотезу про те, що медіа виступають основним каталізатором формування соціальної тривоги навколо кіберзагроз.

Встановлено, що медіа-простір щодо кібербезпеки характеризується структурним перекосом у бік негативного висвітлення (33,4%), тоді як позитивні новини залишаються маргінальними (22,1%). Це свідчить про системну тенденцію до драматизації загроз та ігнорування успішних кейсів їх нейтралізації. Аналіз показав, що кіберзагрози рідко обговорюються ізольовано. Натомість, вони тісно переплетені з політичним контекстом (наприклад, втручання у вибори) та економічними наслідками. Економічний вплив виступає ключовою ланкою у ланцюжку трансформації технічної загрози в соціальну паніку, що наочно підтверджує діаграма Sankey.

Виявлено, що існує чітка залежність між типом видання та тональністю висвітлення. Масові таблоїди демонструють стабільно негативний сентимент, тоді як бізнес-орієнтовані та технологічні ресурси дотримуються більш нейтральної або об'єктивної позиції. Ця поляризація є ключовим механізмом формування суспільного сприйняття кіберризиків. Медійна тональність безпосередньо залежить від характеру кібератаки. Найбільш негативно висвітлюються "спектакльні" (DDoS, дефейсменти) або технічно складні та непередбачувані загрози (експлойти, zero-day), які асоціюються з раптовістю та масштабними збитками. Динаміка тональності має виражену циклічність, що корелює з реальними масштабними інцидентами. Одночасно спостерігається перехід від чітких сезонних спалахів до стабільно високого рівня висвітлення, що свідчить про інституціоналізацію кібербезпеки як постійної теми в глобальному інформаційному просторі.

Подальша робота може бути спрямована на кореляційний аналіз між конкретними лінгвістичними конструкціями в заголовках (наприклад,

використання метафор, категоричних тверджень) та силою негативного сентименту. Перспективним напрямом є побудова економетричних моделей для кількісної оцінки впливу медійного сентименту про кіберінциденти на волатильність акцій компаній кібербезпекового сектору та ринкових індексів.

Отже, запропонований підхід до моніторингу кіберпаніки через аналіз медійного сентименту відкриває нові можливості для проактивного управління інформаційними ризиками та розробки превентивних комунікаційних стратегій у сфері кібербезпеки.

Література

1. Cybersecurity threat landscape 2024 midyear review. URL: https://blog.qualys.com/vulnerabilities-threat-research/2024/08/06/2024-midyear-threat-landscape-review (дата звернення: 01.10.2025).
2. Cybersecurity statistics of 2024: Key trends and insights. URL: https://nordlayer.com/blog/cybersecurity-statistics-of-2024/ (дата звернення: 01.10.2025).
3. CrowdStrike deploys fix for issue causing global tech outage. URL: https://www.reuters.com/technology/crowdstrike-says-actively-working-with-customers-impacted-by-outage-2024-07-19/ (дата звернення: 01.10.2025).
4. Cimpanu, C. (2024). CDK reportedly paid $25 million ransom following cyberattack. URL: https://cyberscoop.com/cdk-ransom-blacksuit-25-million (дата звернення: 01.10.2025).
5. AT&T breach 2024: Customer data exposed in massive cyber attack. URL: https://www.cyberdefensemagazine.com/att-breach-2024-customer-data-exposed-in-massive-cyber-attack/ (дата звернення: 01.10.2025).
6. Average ransomware payment doubles in a single quarter. URL: https://www.itpro.com/security/ransomware/average-ransom-payment-doubles-in-a-single-quarter (дата звернення: 01.10.2025).

7. Tweneboah-Koduah S., Atsu F., Prasad R. Reaction of stock volatility to data breach: An event study. *Journal of Cyber Security and Mobility.* 2020. Vol. 9, No 3. P. 355-384.

8. Day K., Booker Q. Market reactions to cybersecurity incidents: A case study approach. *Issues in Information Systems*. 2024. Vol. 25, No 4. P. 260-276.

9. Kammoun N., Rekik Y. M., Boujelbène M. A. Financial market reaction to cyberattacks. *Cogent Economics & Finance*. 2019. Vol. 7, No 1. Article 1645584.

10. Huang A. H., Wang H., Yang Y. FinBERT: A large language model for extracting information from financial text. *Contemporary Accounting Research*. 2023. Vol. 40, No 2. P. 806-841.

11. Fatouros G., Soldatos J., Kouroumali K., Makridis G., Kyriazis D. Transforming sentiment analysis in the financial domain with ChatGPT. *Machine Learning with Applications*. 2023. Vol. 14. Article 100508.

12. Todd A., Bowden J., Moshfeghi Y. Text-based sentiment analysis in finance: Synthesising the existing literature and exploring future directions. *Intelligent Systems in Accounting, Finance and Management*. 2024. Vol. 31. Article e1549.

13. Sinha A., Kedas S., Kumar R., Malo P. SEntFiN 1.0: Entity-aware sentiment analysis for financial news. *Journal of the Association for Information Science and Technology.* 2022. Vol. 73, No 9. P. 1314-1335.

14. Islam M. S., Wang T., Farah N., Stafford T. F. The spillover effect of focal firms' cybersecurity breaches on rivals and the role of the CIO: Evidence from stock trading volume. *Journal of Accounting and Public Policy.* 2022. Vol. 41, No. 2. Article 106916.

15. Cao H., Phan H. V., Silveri S. Data breach disclosures and stock price crash risk: Evidence from data breach notification laws. *International Review of Financial Analysis*. 2024. Vol. 93. Article 103164.

16. Media Cloud, an open-source platform for media analysis. URL: https://www.mediacloud.org (дата звернення: 01.10.2025).

References

1. Qualys (2024), “Cybersecurity threat landscape 2024 midyear review”, available at: https://blog.qualys.com/vulnerabilities-threat-research/2024/08/06/2024-midyear-threat-landscape-review, (Accessed 1 October 2025).

2. NordLayer (2024), “Cybersecurity statistics of 2024: Key trends and insights”, available at: https://nordlayer.com/blog/cybersecurity-statistics-of-2024/, (Accessed 1 October 2025).

3. Reuters (2024), “CrowdStrike deploys fix for issue causing global tech outage”, available at: https://www.reuters.com/technology/crowdstrike-says-actively-working-with-customers-impacted-by-outage-2024-07-19/, (Accessed 1 October 2025).

4. Cimpanu, C. (2024), “CDK reportedly paid $25 million ransom following cyberattack”, *CyberScoop*, [Online], available at: https://cyberscoop.com/cdk-ransom-blacksuit-25-million, (Accessed 1 October 2025).

5. CyberDefense Magazine (2024), “AT&T breach 2024: Customer data exposed in massive cyber attack”, available at: https://www.cyberdefensemagazine.com/att-breach-2024-customer-data-exposed-in-massive-cyber-attack/, (Accessed 1 October 2025).

6. ITPro (2025), “Average ransomware payment doubles in a single quarter”, available at: https://www.itpro.com/security/ransomware/average-ransom-payment-doubles-in-a-single-quarter, (Accessed 1 October 2025).

7. Tweneboah-Koduah, S. Atsu, F. and Prasad, R. (2020), “Reaction of stock volatility to data breach: An event study”, *Journal of Cyber Security and Mobility*, vol. 9(3), pp. 355-384.

8. Day, K. and Booker, Q. (2024), “Market reactions to cybersecurity incidents: A case study approach”, *Issues in Information Systems*, vol. 25(4), pp. 260-276.

9. Kammoun, N. Rekik, Y.M. and Boujelbène, M.A. (2019), "Financial market reaction to cyberattacks", *Cogent Economics & Finance,* vol. 7(1), 1645584.

10. Huang, A.H. Wang, H. and Yang, Y. (2023), "FinBERT: A large language model for extracting information from financial text", *Contemporary Accounting Research,* vol. 40(2), pp. 806-841.

11. Fatouros, G. Soldatos, J. Kouroumali, K. Makridis, G. and Kyriazis, D. (2023), "Transforming sentiment analysis in the financial domain with ChatGPT", *Machine Learning with Applications,* vol. 14, 100508.

12. Todd, A. Bowden, J. and Moshfeghi, Y. (2024), "Text-based sentiment analysis in finance: Synthesising the existing literature and exploring future directions", *Intelligent Systems in Accounting, Finance and Management,* vol. 31, e1549.

13. Sinha, A. Kedas, S. Kumar, R. and Malo, P. (2022), "SEntFiN 1.0: Entity-aware sentiment analysis for financial news", *Journal of the Association for Information Science and Technology,* vol. 73(9), 1314-1335.

14. Islam, M.S. Wang, T. Farah, N. and Stafford, T.F. (2022), "The spillover effect of focal firms' cybersecurity breaches on rivals and the role of the CIO: Evidence from stock trading volume", *Journal of Accounting and Public Policy,* vol. 41(2), 106916.

15. Cao, H. Phan, H.V. and Silveri, S. (2024), "Data breach disclosures and stock price crash risk: Evidence from data breach notification laws", *International Review of Financial Analysis,* vol. 93, 103164.

16. Media Cloud (2025), "Media Cloud, an open-source platform for media analysis", available at: https://www.mediacloud.org, (Accessed 1 October 2025).

Стаття виконана в рамках науково-дослідної роботи № 0124U000544 Кібербезпекові та цифрові трансформації економіки країни воєнного часу: боротьба із кіберзлочинами, корупцією та тіньовим сектором.

Стаття надійшла до редакції 07.12.2025 р.