

В.В. Лавров¹

А.В. Дудатьєв²

ЕПІДЕМІОЛОГІЧНІ ТА МЕРЕЖЕВІ МОДЕЛІ ПОШИРЕННЯ ДЕЗІНФОРМАЦІЇ: ОГЛЯД ПІДХОДІВ І КЕЙСІВ

¹ Вінницький національний технічний університет;

Анотація

У статті здійснено аналіз епідеміологічних та мережевих моделей поширення дезінформації у цифрових соціальних мережах. Представлено порівняльний огляд основних підходів, таких як компартментні моделі (SIR, SIS, SEIR, SEIZ, модель чутток Дейлі–Кендалла) та мережеві моделі (модель незалежних каскадів, порогові моделі, агент-орієнтовані моделі). Описано переваги та обмеження кожної групи моделей, наведено практичні кейси та застосування у сферах медіаграмотності та фактчекінгу. Дослідження підкреслює важливість комбінування епідеміологічного і мережевого аналізу для ефективного прогнозування та протидії інфодеміям.

Ключові слова: дезінформація, фейкові новини, епідеміологічні моделі, мережеві моделі, інфодемія, компартментні моделі, SIR, SEIZ, модель чутток Дейлі–Кендалла, модель незалежних каскадів, порогові моделі, агент-орієнтовані моделі, медіаграмотність, фактчекінг, мережевий аналіз.

Abstract

The article reviews epidemiological and network models for the spread of misinformation in digital social networks. A comparative analysis of main approaches, including compartmental models (SIR, SIS, SEIR, SEIZ, Daley-Kendall rumor model) and network-based models (independent cascade model, threshold models, agent-based models), is provided. Advantages and limitations of each model type are discussed along with practical case studies and applications in media literacy and fact-checking. The study emphasizes the importance of integrating epidemiological and network analyses for effectively predicting and combating infodemics.

Keywords: disinformation, fake news, epidemiological models, network models, infodemics, compartmental models, SIR, SEIZ, Daley-Kendall rumor model, independent cascade model, threshold models, agent-oriented models, media literacy, fact-checking, network analysis.

Вступ

Поширення фейкових новин та дезінформації у цифрових мережах часто відбувається за «вірусними» законами – інформація стрімко передається від людини до людини, охоплюючи дедалі більшу аудиторію. Це наштовхнуло науковців на аналогії з епідеміями: неправдивий контент розглядають як «інфекцію», що заражає довіру людей, а користувачів – як сприйнятливих або «імунних» до цієї інфекції [1]. Такий підхід не лише метафоричний – він забезпечує формальні моделі для оцінювання ризиків вірусного поширення дезінформації. У цьому огляді проаналізовано два основні підходи до моделювання «інфодемій»: епідеміологічні моделі (компартментні, математичні моделі на кшталт SIR) та мережеві моделі (моделі розповсюдження на графах соціальних мереж). Розглянемо, як кожен підхід використовується в академічних дослідженнях і на практиці, їх ефективність у різних контекстах, а також сильні та слабкі сторони. Наприкінці подано порівняльну таблицю основних моделей (назва, опис, переваги, обмеження, застосування) та візуалізації для ілюстрації їх роботи.

Результати дослідження

Епідеміологічні моделі поділяють населення на кілька станів (компартментів) і описують динаміку переходів між ними за допомогою рівнянь. Класичний приклад – модель SIR (Susceptible-Infected-Recovered), що в контексті інформації можна інтерпретувати так: S (сприйнятливі) – особи, які ще не бачили дану дезінформацію, але можуть повірити в неї; I (інфіковані) – ті, хто повірив або поширює фейк; R (вилікувані/резистентні) – ті, хто перестав вірити чи поширювати (наприклад, дізнався правду або просто втратив інтерес) [1]. Поширення дезінформації описується аналогами «швидкості інфікування» (ймовірність, що сприйнятлива особа стане інфікованою після контакту з фейком) та «швидкості одужання» (ймовірність, що інфікована перестане вірити/поширювати). Якщо базове репродуктивне число R_0 (середня кількість людей, яких одна «інфікована» особа заражає) перевищує 1, дезінформація здатна викликати масштабну «епідемію» на платформі [1]. Дослідження показують, що в більшості великих соцмереж оцінене $R_0 > 1$, тобто вони мають потенціал для епідемічного поширення фейків [1]. Простий SIR – не єдиний компартментний підхід. Застосовуються й інші схеми, запозичені з епідеміології та теорії чуток:

- SIS (Susceptible-Infected-Susceptible): відсутня довготривала «імунітет» – аналог ситуації, коли людина може неодноразово піддаватися впливу різних фейків або знову повірити у спростований фейк через деякий час. Така модель корисна для опису рециркуляції чуток або повторних спалахів дезінформації.
- SEIR (Susceptible-Exposed-Infected-Recovered): вводить стан E (Exposed, тобто «експонований») – людина отримала дезінформацію, але ще не почала її поширювати. Це відповідає латентному періоду – наприклад, користувач бачить фейк, думає чи перевіряє певний час, перш ніж вирішити поділитися. Стан E дозволяє моделювати затримки у поширенні.
- SEIZ (Susceptible-Exposed-Infected-Skeptic): розширює попередню модель, додаючи стан Z – скептики [2]. Skeptic – це особа, яка була експонована до фейку, але свідомо вирішила не вірити і не поширювати (наприклад, розпізнала неправду). Дослідники відзначають, що модель SEIZ дає більш реалістичні результати порівняно з базовими моделями, оскільки враховує частку людей, які бачать фейк, але не реагують (Z), а також тих, хто потребує часу на обдумування (E) [2]. Наприклад, в аналізі поширення хештегу #DCblackout у Twitter (чутки про “відключення зв’язку” у Вашингтоні) модель SEIZ показала добру відповідність реальним даним [2].
- Модель чуток Дейлі–Кендалла (DK): спеціалізована епідеміологічна модель для поширення чуток, вперше описана ще в 1960-х. Подібно до SIR, вона має три стани, але інтерпретація інша: «невігласи» (ignorants) – ті, хто ще не чув чутку; «розповсюджувачі» (spreaders) – активні носії чутки; «згуджені» або «гасителі» (stiflers) – ті, хто вже не поширює (бо дізнався, що чутка стара або хибна, чи просто втратив інтерес). DK-модель вважається реалістичною для опису стихійних чуток і маркетингових вірусних кампаній [3]. Цікаво, що сучасні дослідники доповнюють її новими компонентами – наприклад, вводять окремий клас перевіряючих (fact-checkers), які здатні перевести «інфікованих» у стан невразливих, тим самим пригнічуючи епідемію фейків [3]. Зокрема, було показано, що наявність навіть відносно невеликої групи перевіряючих і спростовувачів (аналог «імунізації правдою») може суттєво обмежувати максимальне охоплення фейку.

Епідеміологічні моделі надають корисний інструментарій для кількісної оцінки динаміки дезінформації. Вони дозволяють розрахувати важливі показники ризику – наприклад, максимальну частку «зараженого» неправдою населення, час до піку зараження, довжину «хвоста» поширення тощо. За їх допомогою можна прогнозувати, чи стане певна неправдива історія вірусною і випереджати події [4]. Більше того, такі моделі слугують віртуальними «лабораторіями» для тестування контрзаходів. Наприклад, моделюючи введення “вакцинації” проти дезінформації – тобто попереджувального навчання, препозиції правди (prebunking) – вчені досліджують, як зміняться криві зараження у порівнянні з базовим сценарієм [4]. На рис. 1 наведено приклад симуляції: лівий графік відображає поширення «інфекції» дезінформації за умови лише післяфактумного спростування (debunking), а правий – якщо додати превентивне «щеплення» (prebunking) перед появою фейку. Видно, що без превенції частка дезінформованих різко зростає (помаранчева крива, ліворуч) і досягає ~60%, тоді як

масова превентивна просвіта значно знижує піковий рівень зараження (помаранчева крива праворуч ледве перевищує 20%) та швидше зупиняє епідемію фейку [4].

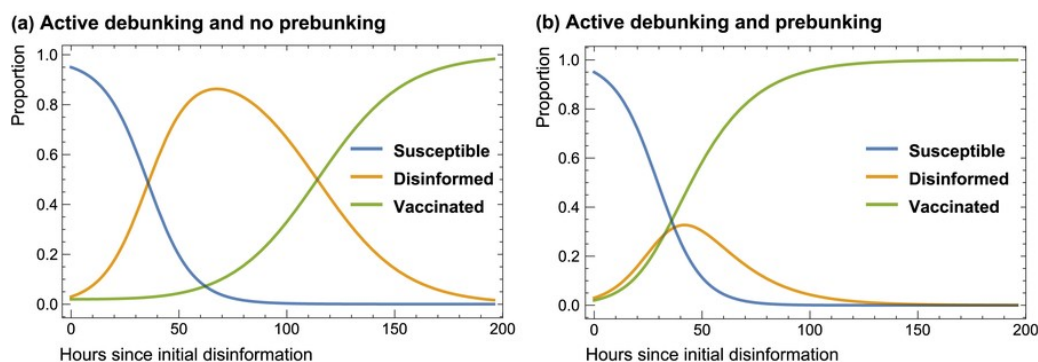


Рис. 1. Симуляція «епідемії» дезінформації (помаранчева крива) серед онлайн-користувачів при різних стратегіях протидії

Тільки активне спростування після поширення: фейк інфікує більшість сприйнятливих (синя крива падає до нуля, помаранчева зростає до піку), поки поступово не виробляється «імунітет» (зелені – вакциновані/пропущені через спростування). (b) Додавання превентивного «щеплення» (prebunking, зелені з самого початку) різко обмежує масштаби та швидкість зараження помилковою інформацією [4]. Подібні дослідження підтверджують ефективність “психологічного вакцинування” аудиторії: введення невеликих доз дезінформації з навчальними поясненнями наперед формує стійкість до майбутніх атак фейків [4]. Цей прийом вже впроваджується на практиці – наприклад, у інформаційних кампаніях з медіаграмотності, урядових програмах та ініціативах технологічних компаній (платформа Google Jigsaw у 2023 році запустила серію відео-пребанків для «щеплення» користувачів проти дезінформації про біженців і вибори). Мережеві моделі розглядають не суцільну масу населення, а граф взаємодій – хто з ким пов’язаний у інформаційному просторі. Соціальна мережа моделюється у вигляді вершин (користувачів) та ребер (зв’язків: дружиби, підписки, ретвіти тощо). На цю структуру «накладається» динаміка поширення: спрощено, якщо користувач А побачив фейк і поділився ним, всі його сусіди в графі В, С, D отримають цей контент і можуть теж стати носіями. Таким чином, зараження поширюється по ребрах графа – аналогічно тому, як інфекція передається по соціальних контактах, але тепер конкретна топологія цих контактів враховується явно. Мережеві моделі можуть бути різних типів, серед них популярні: стохастичні моделі поширення на графах (на кшталт моделі незалежних каскадів) та порогові моделі (з урахуванням множинних впливів), а також більш складні агент-орієнтовані симуляції.

- Модель незалежних каскадів (Independent Cascade, IC). Це класична модель дифузії на графі, яка фактично реалізує принцип SIR дискретно: кожен раз, коли вузол А вперше стає «інфікованим» (отримує і повірив у фейк), він має один шанс «заразити» кожного свого ще не зараженого сусіда В з деякою ймовірністю p . Якщо успішно – сусід також інфікується (наступного кроку), і далі сам намагається заразити своїх сусідів, і т.д. Таким чином формується каскад поширення по мережі. Ця модель широко використовується для вивчення інформаційних каскадів у соцмережах і задач на кшталт максимізації впливу (вибір початкових вузлів, здатних дати найбільший каскад). Для дезінформації вона дозволяє змодельовати, як випадкові перешкоди (не всякий контакт призводить до інфікування) і структура зв’язків впливають на охоплення фейку. На відміну від агрегованого SIR, тут епідемія може згаснути навіть при високому середньому p , якщо фейк не потрапить у потрібні вузли чи «захлинеться» у ізольованих кластерах.
- Порогові моделі (лінійний поріг). В цих моделях кожен вузол має поріг впливу: він перейде у стан «інфікований» лише коли достатня кількість сусідів (або вага впливу сусідів) перевищить його особистий поріг. Це відображає явище “соціального підкріплення”: людина може не повірити першому-ліпшому фейку, але якщо «всі навколо говорять» (кілька друзів уже поширили), то вона теж почне довіряти і ділитися. Порогові моделі придатні для опису

складної дифузії, що потребує кількох дотиків. З їх допомогою можна визначати критичну масу: наприклад, якщо частка інфікованих у спільноті перевищить X%, відбудеться лавина, а якщо ні – фейк залишиться локальним. Деякі дослідження зіставляють ці дві ситуації з аналогією «простого vs. комплексного зараження» для фейкових новин [5].

- Агент-орієнтовані моделі та симуляції. Це більш загальна категорія: тут кожен користувач моделюється як агент з певними атрибутами (ступінь довіри, частота онлайн-активності, політичні уподобання тощо), а між агентами існує мережа контактів. Визначаються правила оновлення станів агентів – наприклад, правило IC чи порогу, або навіть більш складні, наприклад байєсівське оновлення переконань, модель виборця (voter model, де агент приймає стан більшості сусідів) тощо. Агент-орієнтовані підходи дають змогу імітувати поширення дезінформації з високою реалістичністю, включаючи конкуренцію правдивої та фейкової інформації, вплив ботів, повторні взаємодії тощо. Наприклад, у свіжому дослідженні 2023 р. запропоновано “бінарну модель згоди” на зваженому реальному графі, щоб перевірити ефективність різних стратегій боротьби [5]. В мережі агентів запускали три типи втручання: модерацію контенту (вилучення частини активних дезінформаторів), освіту/підвищення скептицизму у частини населення та контр-кампанію (агенти, які поширюють спростування). Результат – випадкове видалення навіть небагатьох акаунтів-дезінформаторів знижує поширення майже так само, як цілеспрямоване видалення найбільш впливових акаунтів [5]. Інакше кажучи, масове «прочищення» фейкового контенту по мережі, навіть без точкового націлювання, може бути ефективним заходом (це цікавий висновок для платформ – він підтверджує, що політика загального видалення дезінформації здатна працювати, не завжди обов’язково шукати “суперрозповсюджувачів”). Також з’ясувалося, що підвищення скептичності широкої аудиторії (через освіту, медіаграмотність) дієвіше, ніж спроби «переконати фанатиків» (цілитися зусилля лише в тих, хто вже глибоко заражений) [5]. А для успіху контр-наративів потрібно, щоб суттєва частка мережі їх просувала – інакше фейк домінуватиме [5].

Особливості мережевого поширення. Мережеві моделі дозволяють дослідити феномени, невидимі в агрегатних підходах. По-перше, це роль надвпливових вузлів – так званих “superspreaders” або «суперрозповсюджувачів». У соціальних мережах такими можуть бути акаунти з гігантською аудиторією або боти, що постять тисячі повідомлень. Дослідження підтверджують, що більшість дезінформації розганяється відносно малою кількістю джерел: «левова частка» фейків дифундує через кілька популярних акаунтів [5]. Наприклад, у виборчих кампаніях кілька ключових дезінформаторів (зірки, політики, або координовані тролі) можуть запустити хвилю, яку вже підхоплюють маси. Мережевий аналіз дозволяє виявити цих суперрозповсюджувачів – через метрики на кшталт ступеня вузла, централізованості, рангування за охопленням тощо. Практичне застосування: платформи й державні органи можуть цілеспрямовано стежити за цими «вузлами ризику» і при потребі гасити епідемію у зародку, блокуючи або позначаючи їхні пости. По-друге, мережевий підхід враховує структурні бар’єри та провідники. В реальних соцмережах люди утворюють спільноти за інтересами – так звані «ехо-камери», де всі учасники мають схожі погляди. Фейк може дуже ефективно розійтися всередині однієї такої камери, але не одразу перескочити в іншу (бо між групами мало контактів). З іншого боку, якщо є «міст» між кластерами – користувач, що перебуває у двох спільнотах, – він може перенести дезінформацію далі, подібно до міжміського поширення вірусу. Отже, топологія мережі визначає масштаб епідемії: високозв’язані, інтегровані мережі більш піддатливі до глобального поширення, а сегреговані – можуть локалізувати фейк у межах сегмента [6]. Цей висновок має і позитивний аспект: інтегровані мережі також мають більшу здатність “самоочищуватися”, бо в них і правда та фейки циркулюють спільно, і критичні голоси можуть швидше сягнути аудиторії фейку [6]. Навпаки, ізольовані групи ризикують залишитися сам на сам з брехнею. Тому платформи часто прагнуть обмежити зловмисну координацію (щоб боти не створювали штучно посилені осередки) і роз’єднувати мережі дезінформації. Нижче у таблиці узагальнено основні моделі і підходи, що використовуються для оцінювання ризиків вірусного поширення дезінформації, з їхніми ключовими характеристиками.

Табл. 1. — Порівняльна таблиця моделей

Модель/підхід	Опис і призначення	Переваги	Обмеження	Застосування (приклади)
SIR модель (епідеміологічна компартментна)	Базова трисекторна модель: Susceptible (сприйнятливий), Infected (інфікований фейком), Recovered (невразливий після «одужання» або імунізації). Описує загальну динаміку поширення з допомогою рівнянь.	– Простота, наявність аналітичних рішень – Інтуїтивні метрики (R_0 , піки, фінальна доля) – Швидке тестування глобальних сценаріїв	– Ігнорує структуру мережі (припускає однорідні контакти) – Не відображає повторних впливів (один контакт = зараження) – Параметри важко точно оцінити з даних	– Оцінка, чи стане інформація вірусною (при $R_0 > 1$) – Прогноз охоплення фейку без втручання – Моделювання масових інтервенцій: напр. видалити X% «інфікованих» (бан акаунтів) чи зробити Y% «вакцинованими» (підготовленими) і побачити зміну динаміки
SEIZ модель (епідем. модель з «Експонованими» та «Скептиками»)	Розширення SIR: додає стан Exposed (E) – особи, що бачили фейк, але ще не поширили, і Skeptic (Z) – бачили, але не повірили і не поширять. Ближче до реальної поведінки онлайн-користувачів	– Врахування затримки прийняття рішення (E) – Врахування стійкої частки скептиків, що ігнорують фейки – Точніше моделює реальні дані соцмереж (більш гнучка крива)	– Більше параметрів, складніше оцінити – Потребує даних про частку скептиків (не завжди відомо) – Як і SIR, не враховує явної структури зв'язків (можна застосувати в «середньому» по мережі)	– Аналіз конкретних кампаній: застосовано для Twitter-хештегів (протестні фейки), поширення теорій змови – Допомогає оцінити ефект пасивної більшості (яка бачить фейк, але не реагує) на уповільнення епідемії
Модель чуток (Daley–Kendall) (епідем. модель з «гасителями» та перевіркою фактів)	Компартментна модель: Ignorant (не поінформовані), Spreader (поширювачі), Stifler (тих, хто припинив поширення). Особливість – «гасіння» чуток: коли спредер контактує з іншим спредером чи вже освідомленим, він сам перестає поширювати (втрачає інтерес). Сучасні варіації додають окремий клас фактчекерів або правдивої інформації, що переводять спредерів у stiflers.	– Спеціально пристосована для вірусних чуток (враховує ефект пересичення інформацією) – Може моделювати самопоширення спростувань (через окремий канал перевірки) – Добре підходить для короткотривалих інфовсплесків (де люди швидко втомлюються від теми)	– Менш підходить для тривалих кампаній дезінформації (де не настає «насичення» аудиторії) – Параметри гасіння часто доводиться припускати (скільки раз людина має почути, щоб перестати ділитися) – Як і інші компартментні – середньому по населенню, неявно припускає довільні контакти	– Моделювання чуток і вірусного маркетингу – Оцінка впливу фактчекінгу: наскільки наявність перевіряючих зменшить охоплення (модель дозволяє задати частку «знезаражувачів» і виміряти ефект)
Модель незалежних каскадів (IC) (стохастична модель на мережі, просте зараження)	Дискретна модель поширення по графу соціальної мережі. Кожен інфікований вузол з певною ймовірністю р заражає кожного зі своїх сусідів (один раз). Процес іде каскадами хвилеподібно по зв'язках, поки нові інфікування вичерпуються. Еквівалент моделювання SIR на конкретній мережі (без повторного	– Враховує реальну структуру зв'язків (хто кого може інфікувати) – Дозволяє випадкове затухання – навіть при високому р епідемія може не піти, якщо не пощастить (моделює реальність, де не кожен фейк «вистрілює») – Можна кількісно оцінити внесок кожного вузла (якщо зробити його дже-	– Потрібен граф соцмережі (не завжди доступний, доводиться брати вибірки або моделі графів) – Результати імовірнісні: треба багато прогонів для оцінки середнього охоплення – Не враховує ефекту багаторазових впливів з різних джерел – зараження або стається від одного	– Оцінка охоплення: моделюючи каскад, можна прогнозувати скільки користувачів побачать/ повірять у фейк – Виявлення ключових вузлів: перебір різних початкових вузлів (або поєднань) вказує, чий запуск фейку найнебезпечніший – корисно для превентивного моніторингу (за акаунтами, які

	зараження та без одужання – кожен може заразити сусідів тільки при переході з S в I).	релом, який каскад)	сусіда, або ні (модель “простого” інфікування)	можуть спричинити найбільші спалахи) – Задача “інфлюенсерів”: навпаки, визначення вузлів для поширення правди (щоб максимально покрити мережу контр-нарративом) – аналог задачі впливу, але для правдивої інфо
Порогова модель (мережева модель комплексного зараження)	Детерміністична або стохастична модель, де кожен вузол має поріг (від 0 до 1, або певне число сусідів). Вузол переходить у стан «інфікований» тільки якщо частка (або число) його сусідів, які вже інфіковані, перевищує поріг. До досягнення порогу вузол лишається несприйнятливим. Модель може мати порог і для правдивої інформації – одночасна дифузія двох конкуруючих ідей.	– Урахування ефекту соціального підтвердження: моделює ситуації, коли одна згадка фейку недостатня для віри – Дозволяє досліджувати стабільні та нестабільні рівноваги: існує критична маса, після якої фейк самопідтримується – Може показати випадки, коли фейк не пошириться, хоч деякі носії його запускають (якщо всі мають високі порог)	– Важко обрати порог для реальних людей (потрібні опитування або припущення) – При детерміністичних порогах – модель не враховує випадковості (у реальності хтось може повірити й від однієї появи, інший й після десятої сумнівається) – Складно калібрувати на даних: потрібно знати послідовність впливів на кожну особу	– Моделювання конспірології та радикалізації: тут часто потрібні повторні впливи. Порогові моделі використовують, щоб зрозуміти, скільки “друзів-адептів” потрібно, аби людина прийняла хибну ідею. – Дифузія правди vs фейку: дві мережеві думки конкурують (хто першим досягне порогу у більшості – той і домінує). Застосовується для вивчення, за яких умов спростування може перемагати дезінформацію.

Висновки

Епідеміологічні та мережеві моделі забезпечують взаємодоповнюючі інструменти для розуміння і протидії вірусному розповсюдженню фейкових новин. Епідеміологічні підходи дають нам мову і математичний апарат для того, щоб говорити про “інфікованість” суспільства неправдою, вимірювати “репродуктивне число” дезінформації та “імунітет” до неї. Це не лише теорія – подібні моделі дозволяють на практиці перевірити, наскільки ефективними будуть різні втручання (від звичайного спростування до превентивного навчання) ще до того, як їх реалізовано. Мережеві моделі, зі свого боку, занурюються глибше в механіку розповсюдження: вони показують, через які саме канали ідуть “зарази” неправди, хто їх прискорює, а де вони зупиняються. Це критично для цільового реагування – знати свої “слабкі місця” (ключові вузли і спільноти ризику) означає мати змогу вчасно перерізати ланцюги поширення. На практиці вже створено низку систем, що в реальному часі відслідковують мережі дезінформації і допомагають аналітикам та платформам реагувати (Noaxu, Botometer, інфодемічні панелі ВООЗ тощо). Жоден з підходів не є ідеальним чи самодостатнім: моделі – це спрощення дійсності, і вони не враховують усіх соціальних чинників (емоції, контекст, мотивації людей). Проте, як свідчать дослідження, багато фейкових історій дійсно підкоряються законам, подібним до епідемічних. Отже, запозичуючи найкраще з епідеміології та науки про мережі, ми отримуємо потужний інструментарій для оцінки ризиків і вироблення стратегій протидії “вірусній” дезінформації на благо інформаційної безпеки суспільства.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science*, 359(6380), 1146–1151. DOI: 10.1126/science.aap9559
2. Epstein, Z., Berinsky, A. J., Rand, D. G., & Pennycook, G. (2022). Cognitive cascades: How to model (and potentially counter) the spread of fake news. *PLOS One*, 17(1), e0261811.
3. Zhao, Z., et al. (2021). Why cannot long-term cascade be predicted? Exploring temporal dynamics in information diffusion processes. *PMC*
4. Dhiman, M. (2024). A novel integration of multiple learning methods for detecting misinformation. *Expert Systems with Applications*.
5. DARPA SocialSim Program. (2023). Modeling information diffusion in social media: data-driven observations.
6. Frameworks, Modeling and Simulations of Misinformation and Disinformation: A Systematic Literature Review. (2024).

Лавров Вадим Валерійович —аспірант кафедри захисту інформації, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: vadosssss228@gmail.com

Науковий керівник: **Дудатьєв Андрій Веніамінович** — кандидат технічних наук, доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця

Lavrov Vadym V.— Department of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email : vadosssss228@gmail.com

Supervisor: **Andriy Veniaminovich Dudatyev.** — Candidate of Technical Science, Associate Professor of Information Protection, Vinnytsia National Technical University, Vinnytsia