МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Кваліфікаційна наукова
праця на правах рукопису

ВЕТЛИЦЬКА ОЛЕНА СЕРГІЇВНА

УДК 004.056.5:316.776(043)

ДИСЕРТАЦІЯ
МОДЕЛЬ ІНФОРМАЦІЙНОЇ ЗАХИЩЕНОСТІ ОСОБИСТОСТІ В УМОВАХ ВПЛИВУ РЕЗУЛЬТАТІВ СОЦІОЛОГІЧНИХ ДОСЛІДЖЕНЬ

Спеціальність 125 – Кібербезпека
Галузь знань 12 – Інформаційні технології

Подається на здобуття наукового ступеня доктора філософії.

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.
_____ Олена ВЕТЛИЦЬКА

Науковий керівник:
МУЖАНОВА Тетяна Михайлівна, кандидат наук з державного управління, доцент

Київ – 2024

АНОТАЦІЯ

Ветлицька О.С. Модель інформаційної захищеності особистості в умовах впливу результатів соціологічних досліджень. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 125 – Кібербезпека. – Державний університет інформаційно-комунікаційних технологій, МОН України, Київ, 2024.

В сучасному інформаційному світі людина постійно піддається впливу різноманітних медіа і цифрових технологій, що визначає необхідність її захисту від маніпуляцій, фейкових новин, дезінформації та кібербулінгу. Здатність людини розпізнавати і протидіяти шкідливому впливу інформації сприяє збереженню психічного здоров'я, підвищує стійкість до стресів і сприяє більшій впевненості у власних діях та рішеннях в умовах постійного інформаційного тиску. Серед інформації, яка щодня впливає на сучасну людину, до особливої категорії відноситься інформація про результати соціологічних досліджень, які віддзеркалюють узагальнене ставлення суспільства до тієї чи іншої проблеми. Сприймаючи таку інформацію та дослухаючись до більшості, людина може змінювати свої переконання у відповідності до "думки народу". Враховуючи конформізм людського мислення, численні медіа можуть використовувати результати соціологічних досліджень з негативною метою (маніпуляція громадською думкою, створення паніки або страху, політична пропаганда, відволікання уваги, тощо).

Поняття інформаційної безпеки (людини, особистості) є вкрай складним для кількісного вимірювання і тому у роботі досліджується інформаційна захищеність особистості, як складова її інформаційної безпеки, яка може бути оцінена кількісно на основі аналітичних чи

статистичних моделей. Основна проблема, яка обумовлює необхідність досліджень в області інформаційної безпеки та захищеності особистості, випливає з протиріччя, пов'язаного з конфліктом між необхідністю доступу до інформації та потребою захистити особистість від маніпуляцій і дезінформації.

Все це визначає необхідність вирішення актуального наукового завдання щодо *створення моделі інформаційної захищеності особистості в умовах впливу результатів соціологічних досліджень.*

Метою дослідження є підвищення інформаційної захищеності особистості в умовах впливу результатів соціологічних досліджень. Для досягнення зазначеної мети у роботі одержано основні наукові результати:

удосконалено модель поведінки особистості під впливом соціологічної інформації, в основу якої покладено базову модель конформної поведінки людини з урахуванням її апріорних переконань та ступеня незалежності мислення, і яку було розширено за рахунок використання коефіцієнтів впливу на особистість джерел соціологічної інформації, що дозволяє враховувати рівень довіри особистості до джерела соціологічної інформації та особливості сприйняття особистістю результатів соціологічних досліджень;

вперше розроблено модель інформаційної захищеності особистості яка базується на концепції управління на основі ймовірнісного контролю з використанням результатів моделювання поведінки особистості під впливом соціологічної інформації, що дає можливість досліджувати різноманітні стратегії керування інформаційним впливом результатів соціології на особистість та обирати доцільну стратегію керування інформаційним потоком з метою забезпечення необхідного рівня інформаційної захищеності особистості;

набули подальшого розвитку методи обробки соціологічної інформації, які були адаптовані для використання у моделях поведінки та інформаційної

захищеності особистості за рахунок бінаризації багатовимірних результатів досліджень з використанням методів кластерного аналізу та визначенням ймовірностей для бінарних кластерів. Застосування такого підходу дозволяє кількісно оцінювати вплив результатів соціології на особистість, обирати раціональну стратегію керування інформаційним впливом та забезпечувати необхідний рівень інформаційної захищеності особистості.

Практичне значення одержаних результатів полягає в тому, що розроблені у дисертаційній роботі моделі інформаційного впливу та захищеності особистості дають можливість кількісно оцінювати вплив результатів соціологічних досліджень на особистість та визначати раціональну стратегію керування впливом, чим підвищують ефективність інформаційного захисту особистості. На базі них розроблено рекомендації для психологів, психотерапевтів, соціальних психологів, фахівців з медіаграмотності, фахівців з комунікацій та PR, юристів з питань захисту особистих прав з покращення інформаційної захищеності особистості в умовах впливу соціології. Середнє значення покращення інформаційної захищеності особистості: для стратегії перемикання каналів при найменшому впливі складає 27.9%, для стратегії перемикання каналів при суттєвому впливі складає 54.2%. При цьому, статистична похибка результату (з імовірністю 0.95) складає від 2.3% до 3.4%.

У вступі обґрунтовується важливість та актуальність теми дисертаційного дослідження, сформульовано мету та задачі роботи, визначено основні результати дослідження, їх наукову та практичну цінність та визначено особистий внесок автора у спільних публікаціях.

У першому розділі здійснено аналіз проблематики забезпечення інформаційної захищеності особистості в умовах інформаційного впливу; аналіз технологій використання соціологічної інформації як інструмента інформаційного впливу на особистість; аналіз теоретичних підходів до вирішення проблеми створення моделі інформаційної захищеності

особистості в умовах впливу соціологічної інформації. Здійснено постановку наукового завдання щодо створення моделі інформаційної захищеності особистості в умовах впливу соціологічної інформації.

У другому розділі удосконалено та досліджено модель поведінки особистості під впливом соціологічної інформації; обґрунтувано підхід щодо забезпечення інформаційної захищеності особистості та розроблено модель інформаційної захищеності особистості під впливом соціологічної інформації.

У третьому розділі здійснено розвиток технологій обробки результатів соціологічних досліджень для їх використання в моделі інформаційної захищеності особистості.

У четвертому розділі проведено дослідження моделей поведінки та інформаційної захищеності особистості, розроблено рекомендації щодо їх впровадження.

Результати наукових досліджень були впроваджені в освітній процес на кафедрі управління кібербезпекою та захистом інформації Державного університету інформаційно-комунікаційних технологій, зокрема при викладанні дисциплін: “Основи національної безпеки”, “Інформаційна безпека держави”, “Стратегічні комунікації” та ін. при підготовці здобувачів освіти за спеціальністю 125 Кібербезпека та захист інформації.

Результати наукових досліджень були використані на кафедрі Управління інформаційною та кібернетичною безпекою Державного університету інформаційно-комунікаційних технологій під час виконання науково-дослідної роботи на тему “Запобігання і протидія методам соціальної інженерії у забезпеченні інформаційної безпеки підприємства” (№ держ. реєстрації 0123U100743, ДУІКТ, м. Київ).

Також результати наукових досліджень прийняті до впровадження в діяльність ТОВ “ІТ Спеціаліст”.

Ключові слова: кібербезпека, інформаційна безпека, інформаційна захищеність, особистість, поведінка особистості, соціальні мережі, соціальна інженерія, соціологічні дослідження, медіа, інформаційний вплив, неправдива інформація, математична модель, стратегія керування, кластерний аналіз

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Ветлицька, О. С., & Дзюба, Т. М. (2022). Модель оцінки впливу соціологічної інформації на поведінку людини в контексті її інформаційної безпеки. Телекомунікаційні та інформаційні технології, 4(77), 35–45. https://doi.org/10.31673/2412-4338.2022.043545.

2. Ветлицька, О. С., & Треньов, М. Г. (2024). Проблеми кіберстійкості ІКТ-систем в умовах цифрової трансформації. Телекомунікаційні та інформаційні технології, 1(82), 64–72. https://doi.org/10.31673/2412-4338.2024.016472.

3. Ветлицька, О. С., & Треньова, К. О. (2024). Виявлення атак у мережах Інтернету речей методами машинного навчання. Сучасний захист інформації, 1(57), 39–49. https://doi.org/10.31673/2409-7292.2024.010005.

4. Ветлицька, О. С. (2024). Модель інформаційної захищеності особистості від впливу соціологічної інформації. Сучасний захист інформації, 3(59), 29–41. https://doi.org/10.31673/2409-7292.2024.030003.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

1. Ветлицька, О. С. (2022, жовтень 27). Сучасні методи виявлення автоматизованих аккаунтів у соціальних мережах. Актуальні проблеми кібербезпеки: матеріали всеукр. наук.-практ. конф., м. Київ, 186–187. URL: https://dut.edu.ua/uploads/p_2121_20358827.pdf

2. Ветлицька, О. С. (2023, квітень 27). Соціологічна концептуалізація інформаційної безпеки. Цифрова трансформація кібербезпеки: матеріали

всеукр. наук.-практ. конф., м. Київ, 14–16. URL: https://dut.edu.ua/uploads/p_2626_12162422.pdf

3. Ветлицька, О. С. (2023, травень 16). Методика виявлення вразливостей, пов’язаних з параметрами нейронної мережі, в алгоритмах на основі машинного навчання. Сучасні інтелектуальні інформаційні технології в науці та освіті: матеріали всеукр. наук-практ. конф., м. Київ, 45–46. URL: https://duikt.edu.ua/uploads/n_11208_13331372.pdf

4. Ветлицька, О. С., & Треньова, К. О. (2024, лютий 22). Проблеми кіберстійкості ІКТ-систем в умовах цифрової трансформації. Стратегії кіберстійкості: управління ризиками та безперервність бізнесу: матеріали IV Всеукр. наук.-практ. конф., м. Київ, 71–73. URL: https://duikt.edu.ua/uploads/p_2661_62255520.pdf

5. Ветлицька, О. С. (2024, квітень 26). Вплив цифрових технологій на стійкість ланцюгів поставок. Цифрова трансформація кібербезпеки: матеріали всеукр. наук.-практ. конф., м. Київ, 19–22. URL: https://duikt.edu.ua/uploads/n_12581_11703414.pdf

6. Ветлицька, О. С. (2024, квітень 18). Виявлення атак у мережах інтернету речей методами машинного навчання. Сучасний стан та перспективи розвитку IoT: матеріали V Наук.-техніч. конф., м. Київ, 165–167. URL: https://duikt.edu.ua/uploads/p_2661_70423010.pdf

Наукові праці, які додатково відображають наукові результати дисертації:

1. Ветлицька, О. С., & Мужанова, Т. М. (2023). Математична модель інформаційної безпеки особистості під впливом медіаінформації. Сучасний захист інформації, 2(54), 6–12. https://doi.org/10.31673/2409-7292.2023.020001.

2. Ветлицька, О. С. (2023). Інформаційна безпека: соціологічна концептуалізація. Сучасний захист інформації, 3(55), 52–56. URL: https://doi.org/10.31673/2409-7292.2023.030007.

ANOTATION

Vetlytska O. S. The model of information protection of the individual under the influence of the results of sociological research. – Qualifying scientific work on manuscript rights.

Dissertation for obtaining the scientific degree of Doctor of Philosophy in specialty 125 – Cybersecurity. – State University of Information and Communication Technologies, MES of Ukraine, Kyiv, 2024.

In the modern information world, a person is constantly exposed to various media and digital technologies, which determines the need to protect him from manipulation, fake news, misinformation, and cyberbullying. A person's ability to recognize and counteract the harmful effects of information contributes to the preservation of mental health, increases stress resistance, and promotes greater confidence in one's actions and decisions in conditions of constant information pressure. Among the information that affects modern people every day, a special category includes information about the results of sociological studies, which reflect the general attitude of society to one or another problem. Perceiving such information and listening to the majority, a person can change his beliefs following the “opinion of the people”. Given the conformism of human thinking, numerous media can use the results of sociological research for a negative purpose (manipulation of public opinion, creation of panic or fear, political propaganda, diversion of attention, etc.).

Information security (person, individual) is complicated for quantitative measurement. Therefore the work examines the information security of an individual as a component of his information security, which can be evaluated quantitatively based on analytical or statistical models. The main problem, that determines the need for research in the field of information security and personal protection, stems from the contradiction associated with the conflict between the

need for access to information and the need to protect the individual from manipulation and misinformation.

All this determines the need to solve the actual scientific task of creating a model of information security for the individual under the influence of the results of sociological research.

The purpose of the study is to increase the information security of the individual under the influence of the results of sociological research. To achieve the specified goal, the main scientific results were obtained in the work:

the model of personality behavior under the influence of sociological information has been improved, which is based on the basic model of conforming behavior of a person taking into account his a priori beliefs and the degree of independence of thinking, and which was expanded due to the use of coefficients of influence on the personality of sources of sociological information, which allows taking into account the level of trust of the individual in sources of sociological information and peculiarities of personal perception of the results of sociological research;

for the first time, a model of information security of the individual was developed, which is based on the concept of management based on probabilistic control using the results of modeling the behavior of the individual under the influence of sociological information, which makes it possible to explore various strategies for managing the information impact of the results of sociology on the individual and to choose an appropriate strategy for managing the information flow to ensure the necessary the level of individual information security;

methods of processing sociological information, which were adapted for use in models of behavior and information security of the individual due to binarization of multidimensional research results using methods of cluster analysis and determination of probabilities for binary clusters, were further developed. The use of this approach allows you to quantitatively assess the impact of the results of sociology on the individual, to choose a rational strategy for

managing informational influence, and to ensure the necessary level of personal information security.

The practical significance of the obtained results is that the models of informational influence and personal protection developed in the dissertation make it possible to quantitatively assess the impact of the results of sociological research on the individual and to determine a rational strategy for managing the influence, thereby increasing the effectiveness of informational personal protection. Based on them, recommendations have been developed for psychologists, psychotherapists, social psychologists, media literacy specialists, communications and PR specialists, and lawyers on the protection of personal rights to improve personal information security under the influence of sociology. The average value of the improvement of the information security of the individual: for the strategy of switching channels with the least influence is 27.9%, and for the strategy of switching channels with significant influence is 54.2%. At the same time, the statistical error of the result (with a probability of 0.95) is from 2.3% to 3.4%.

The introduction substantiates the importance and relevance of the topic of the dissertation research, formulates the purpose and tasks of the work, defines the main results of the research, and their scientific and practical value, and defines the personal contribution of the author in joint publications.

In the first section, an analysis of the issues of ensuring the information security of the individual in the conditions of information influence was carried out; an analysis of the technologies of using sociological information as a tool of informational influence on the individual; an analysis of theoretical approaches to solving the problem of creating a model of personal information security under the influence of sociological information. The scientific task of creating a model of information security for the individual under the influence of sociological information was carried out.

In the second chapter, the model of personality behavior under the influence of sociological information is improved and researched; the approach to ensuring personal information security is substantiated, and a model of personal information security under the influence of sociological information is developed.

In the third chapter, the development of technologies for processing the results of sociological research for their use in the model of information security of the individual is carried out.

In the fourth chapter, a study of behavioral models and information security of the individual was carried out, and recommendations for their implementation were developed.

The results of scientific research were implemented in the educational process at the Department of Information and CyberSecurity Management of the State University of Information and Communication Technologies, in particular when teaching the disciplines: “Fundamentals of national security”, “Information security of the state”, “Strategic communications” and others, when preparing students in the specialty 125 Cybersecurity and information protection.

The results of scientific research were used at the Department of Information and CyberSecurity Management of the State University of Information and Communication Technologies during the implementation of research work on the topic “Prevention and countermeasures to social engineering methods in ensuring the information security of the enterprise” (state registration number 0123U100743, DUIKT, m Kyiv).

Also, the results of scientific research were accepted for implementation in the activities of “IT Specialist” LLC.

Keywords: cybersecurity, information security, information safety, personality, personality behavior, social networks, social engineering, sociological research, media, information influence, false information, mathematical model, management strategy, cluster analysis.

LIST OF AUTHOR'S PUBLICATIONS

Scientific papers, in which the main scientific results of the dissertation are published:

1. Vetlytska, O. S., & Dzyuba, T. M. (2022). A model for assessing the impact of sociological information on human behavior in the context of its information security. Telecommunications and Information Technologies, 4(77), 35–45. https://doi.org/10.31673/2412-4338.2022.043545.

2. Vetlytska, O. S., & Trenyov, M. G. (2024). Problems of cyber resilience of ICT systems in the conditions of digital transformation. Telecommunications and Information Technologies, 1(82), 64–72. https://doi.org/10.31673/2412-4338.2024.016472.

3. Vetlytska, O. S., & Trenyova, K. O. (2024). Detection of attacks in Internet of Things networks using machine learning methods. Modern Information Security, 1(57), 39–49. https://doi.org/10.31673/2409-7292.2024.010005.

4. Vetlytska, O. S. (2024). The model of information security of the individual against the influence of sociological information // Modern information Security. 3(59), 29–41. https://doi.org/10.31673/2409-7292.2024.030003.

Scientific papers certifying the approbation of the dissertation materials:

1. Vetlytska, O. S. (2022, October 27). Modern methods of detecting automated accounts in social networks. Actual problems of cyber security: materials of the All-Ukrainian. science and practice conference, Kyiv, 186–187. URL: https://dut.edu.ua/uploads/p_2121_20358827.pdf

2. Vetlytska, O. S. (2023, April 27). Sociological conceptualization of information security. Digital transformation of cyber security: all-Ukrainian materials. science and practice conference, Kyiv, 14–16. URL: https://dut.edu.ua/uploads/p_2626_12162422.pdf

3. Vetlytska, O. S. (2023, May 16). Techniques for detecting vulnerabilities related to neural network parameters in algorithms based on machine learning.

Modern intellectual information technologies in science and education: materials all over Ukraine. science and practice conference, Kyiv, 45–46. URL: https://duikt.edu.ua/uploads/n_11208_13331372.pdf

4. Vetlytska, O. S., & Trenyova, K. O. (2024, February 22). Problems of cyber resilience of ICT systems in the conditions of digital transformation. Cyber resilience strategies: risk management and business continuity: materials IV Vseukr. science and practice conference, Kyiv, 71–73. URL: https://duikt.edu.ua/uploads/p_2661_62255520.pdf

5. Vetlytska, O. S. (2024, April 26). The impact of digital technologies on the sustainability of supply chains. Digital transformation of cyber security: all-Ukrainian materials. science and practice conference, Kyiv, 19–22. URL: https://duikt.edu.ua/uploads/n_12581_11703414.pdf

6. Vetlytska, O. S. (2024, April 18). Detection of attacks in Internet of Things networks using machine learning methods. The current state and prospects of IoT development: materials V Scientific and technical. conference, Kyiv, 165–167. URL: https://duikt.edu.ua/uploads/p_2661_70423010.pdf

Scientific papers that additionally reflect the scientific results of the dissertation:

1. Vetlytska, O. S., & Muzhanova, T. M. (2023). Mathematical model of personal information security under the influence of media information. Modern information protection, 2(54), 6–12. https://doi.org/10.31673/2409-7292.2023.020001.

2. Vetlytska, O. S. (2023). Information security: sociological conceptualization. Modern information protection, 3(55), 52–56. URL: https://doi.org/10.31673/2409-7292.2023.030007.

ЗМІСТ

ВСТУП

Актуальність теми. В сучасному інформаційному просторі, де людина постійно піддається впливу різноманітних медіа і цифрових технологій, забезпечення її інформаційної захищеності є актуальною проблемою. Інформаційна захищеність включає в себе захист від маніпуляцій, фейкових новин, дезінформації та кібербулінгу, що можуть мати негативний вплив на психічне здоров'я та емоційний стан людини. Захист психологічного стану людини вимагає не лише технічних заходів, але й розвитку критичного мислення, медіаграмотності та навичок саморегуляції. Здатність розпізнавати і протидіяти шкідливому впливу інформації сприяє збереженню психічного здоров'я, підвищує стійкість до стресів і сприяє більшій впевненості у власних діях та рішеннях в умовах постійного інформаційного тиску.

Людина – істота соціальна. Вона хоче не тільки знати, що і як відбувається в навколишньому світі, але й розуміти, що думають інші люди і як вони оцінюють те, що відбувається, чи є в неї однодумці та опоненти і яке місце вона, з її позицією та поведінкою, займає серед членів товариства. Серед інформації, яка щодня впливає на сучасну людину, до особливої категорії можна віднести інформацію про результати соціологічних досліджень, які віддзеркалюють узагальнене ставлення суспільства до тієї чи іншої проблеми. Сприймаючи таку інформацію та дослухаючись до більшості, людина може змінювати свої переконання у відповідності до "думки народу". Така особливість людської психіки носить назву "конформізм". Враховуючи її, численні медіа можуть використовувати результати соціологічних досліджень як для позитивних цілей (інформування громадськості, формування громадської думки, підтримка демократичних процесів), так і з негативною метою (маніпуляція

громадською думкою, створення паніки або страху, політична пропаганда, відволікання уваги, тощо).

Ключовим об’єктом інформаційного впливу, який розглядається у даній дисертаційній роботі, є особистість, як комплекс соціально-психологічних характеристик людини, що включає її свідомість, характер, поведінкові моделі, цінності та самосвідомість. Поняття інформаційної безпеки (людини, особистості) є вкрай складним для кількісного вимірювання і тому у роботі досліджується інформаційна захищеність особистості, як складова її інформаційної безпеки, яка може бути оцінена кількісно на основі аналітичних чи статистичних моделей. Маючи можливість оцінювати вплив результатів соціології на поведінку особистості у дослідників та практиків з інформаційної безпеки з’являється інструмент для оцінки поточного стану та розробки ефективних заходів щодо забезпечення інформаційної захищеності особистості.

Основна проблема, яка обумовлює необхідність досліджень в області інформаційної безпеки та захищеності особистості, випливає з протиріччя, пов’язаного з конфліктом між необхідністю доступу до інформації та потребою захистити особистість від маніпуляцій і дезінформації.

Дослідженням інформаційної безпеки та захищеності особистості вже давно займаються як закордонні, так і вітчизняні вчені. Дослідження та моделювання поведінки людини: В. Ліпман [1], Р. К. Мертон [2], І. Айзен [3], М. Фішбейн [3], Е. Ноеле-Н’юман [4], Д. Р. Заллер [5], Д. Ф. Бішоп [6], С. Пейдж [7]. Вплив медіа на людину: О. О. Разуваєва [8], Д. Брайант [9], С. Томпсон [9]. Захист людини в соціальних мережах: В. А. Савченко [10 – 16], В. М. Ахрамович [10 – 12, 14 – 16], Г. І. Гайдур [17], Т. М. Дзюба [11, 16], О. А. Лаптєв [16, 18, 19], К. В. Молодецька [20, 21]. Моделювання конформної поведінки людини: В. В. Бреєр [22], П. С. Краснощоков [23].

Аналіз робіт цих та багатьох інших авторів дає змогу зробити висновок, що на теперішній час питання формалізації процесів впливу результатів

соціології на поведінку особистості досліджені вкрай недостатньо. У математичних моделях, які були запропоновані різними авторами, можна відзначити наступні недоліки, зокрема:

моделі, побудовані на емпіричних даних, можуть бути застосовані лише після завершення збору статистичних даних;

соціально-когнітивні моделі не надають доступної формалізації для оцінки процесів впливу, що ускладнює практичне їх застосування;

моделі з використанням евентуально-статистичного підходу переобтяжені внутрішнім психологічним аналізом особистості, який складно підлаштовується до методів соціології;

підходи на основі концепції багатомодельного мислення вимагають розробки додаткових механізмів переходу між моделями;

моделі захисту особистості в соціальних мережах розглядають особистість без урахування ступеня її конформізму;

математичні моделі конформності та конформної поведінки є найбільш близькими, хоча і потребують удосконалення для можливості використання в них результатів соціології.

Сформульоване протиріччя та недоліки, виявлені в у попередніх публікаціях, дають змогу окреслити завдання, які на сьогодні залишаються невирішеними в науці: вимірювання впливу маніпуляцій в сучасних медіа; моделювання захисних механізмів особистості; визначення балансу між доступністю інформації та захистом особистості; етичні аспекти регулювання інформації. Все це визначає необхідність вирішення актуального наукового завдання щодо *створення моделі інформаційної захищеності особистості в умовах впливу результатів соціологічних досліджень.*

Зв’язок роботи з науковими програмами, планами, темами.

Напрям дисертаційного дослідження безпосередньо пов’язаний з реалізацією Законів України “Про інформацію” [24], “Про медіа” [25], “Про

національну безпеку України” [26], “Про захист персональних даних” [27], “Про основні засади забезпечення кібербезпеки України” [28] та Стратегією інформаційної безпеки України [29]. Дисертаційна робота виконана відповідно до планів наукової і науково-технічної діяльності Державного університету інформаційно-комунікаційних технологій в рамках науково-дослідної роботи “Запобігання і протидія методам соціальної інженерії у забезпеченні інформаційної безпеки підприємства” (№ держ. реєстрації 0123U100743, ДУІКТ, м. Київ).

Мета і завдання дослідження.

Метою дослідження є підвищення інформаційної захищеності особистості в умовах впливу результатів соціологічних досліджень.

Для досягнення поставленої мети визначено наступні *окремі завдання дослідження*:

проаналізувати проблематику та сучасні підходи до забезпечення інформаційної захищеності особистості;

проаналізувати технології використання соціологічної інформації як інструмента інформаційного впливу на особистість;

удосконалити модель поведінки особистості під впливом соціологічної інформації;

розробити модель інформаційної захищеності особистості;

адаптувати технології обробки результатів соціологічних досліджень для використання в моделях поведінки та інформаційної захищеності особистості;

дослідити моделі та розробити рекомендації щодо їх впровадження.

Об’єкт дослідження – інформаційна захищеність особистості.

Предмет дослідження – моделі поведінки та інформаційної захищеності особистості в умовах впливу результатів соціологічних досліджень.

Методи дослідження. Дослідження проведено на основі системного підходу з застосуванням:

морфологічного аналізу (для систематизації різних аспектів інформаційної безпеки, визначення місця і ролі інформаційної захищеності у цій системі; визначення особливостей інформаційного захисту особистості на відміну від захисту людини чи індивіда);

методів теорії ймовірностей (для визначення змінних, що описують апріорні та апостеріорні переконання особистості, ступінь незалежності її мислення, рівень довіри до інформаційних джерел);

методів теорії ігор (для моделей взаємодії між особистістю та каналом інформаційного впливу);

статистичних методів (для адаптації результатів соціологічних досліджень до моделей поведінки та інформаційної захищеності особистості).

Наукова новизна одержаних результатів полягає в тому, що у дисертаційній роботі:

удосконалено модель поведінки особистості під впливом соціологічної інформації, в основу якої покладено базову модель конформної поведінки людини з урахуванням її апріорних переконань та ступеня незалежності мислення, і яку було розширено за рахунок використання коефіцієнтів впливу на особистість джерел соціологічної інформації, що дозволяє враховувати рівень довіри особистості до джерела соціологічної інформації та особливості сприйняття особистістю результатів соціологічних досліджень;

вперше розроблено модель інформаційної захищеності особистості яка базується на концепції управління на основі ймовірнісного контролю з використанням результатів моделювання поведінки особистості під впливом соціологічної інформації, що дає можливість досліджувати різноманітні стратегії керування інформаційним впливом результатів

соціології на особистість та обирати доцільну стратегію керування інформаційним потоком з метою забезпечення необхідного рівня інформаційної захищеності особистості;

набули подальшого розвитку методи обробки соціологічної інформації, які були адаптовані для використання у моделях поведінки та інформаційної захищеності особистості за рахунок бінаризації багатовимірних результатів досліджень з використанням методів кластерного аналізу та визначенням ймовірностей для бінарних кластерів. Застосування такого підходу дозволяє кількісно оцінювати вплив результатів соціології на особистість, обирати раціональну стратегію керування інформаційним впливом та забезпечувати необхідний рівень інформаційної захищеності особистості.

Практичне значення одержаних результатів полягає в тому, що розроблені у дисертаційній роботі моделі інформаційного впливу та захищеності особистості дають можливість кількісно оцінювати вплив результатів соціологічних досліджень на особистість та визначати раціональну стратегію керування впливом, чим підвищують ефективність інформаційного захисту особистості. На базі них розроблено рекомендації для психологів, психотерапевтів, соціальних психологів, фахівців з медіаграмотності, фахівців з комунікацій та PR, юристів з питань захисту особистих прав з покращення інформаційної захищеності особистості в умовах впливу соціології. Середнє значення покращення інформаційної захищеності особистості: для стратегії перемикання каналів при найменшому впливі складає 27.9%, для стратегії перемикання каналів при суттєвому впливі складає 54.2%. При цьому, статистична похибка результату (з імовірністю 0.95) складає від 2.3% до 3.4%.

Результати досліджень прийняті до впровадження в діяльність ТОВ “ІТ Спеціаліст”, а також реалізовані в освітньому процесі кафедри Управління кібербезпекою та захистом інформації Державного університету інформаційно-комунікаційних технологій.

Особистий внесок здобувача. Основні наукові та прикладні результати дисертаційної роботи, що виносяться на захист, отримані автором особисто. У наукових роботах, що опубліковані у співавторстві, автору належать: у [30] автором розроблено основні елементи моделі оцінки впливу соціологічної інформації на поведінку людини в контексті її інформаційної безпеки; у [31] розроблено математичний апарат моделі інформаційної безпеки особистості під впливом медіаінформації; у [32] обґрунтовано, що інформаційна захищеність особистості є одним з ключових елементів кіберстійкості ІКТ-систем в умовах цифрової трансформації; у [33, 34] досліджено залежність рівня захищеності систем від інтенсивності вхідного впливу на прикладі інтернету-речей.

Апробація результатів дисертації. Основні теоретичні та практичні результати були представлені та обговорені в ході низки наукових конференцій:

Всеукраїнська науково-практична конференція “Актуальні проблеми кібербезпеки” (27 жовтня 2022 року) [35];

Всеукраїнська науково-практична конференція “Цифрова трансформація кібербезпеки” (27 квітня 2023 року) [36];

Всеукраїнська науково-практична конференція “Сучасні інтелектуальні інформаційні технології в науці та освіті” (16 травня 2023 року) [37];

IV Всеукраїнська науково-практична конференція “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” (22 лютого 2024 року) [34];

Всеукраїнська науково-практична конференція “Цифрова трансформація кібербезпеки” (26 квітня 2024 року) [38];

V науково-технічна конференція “Сучасний стан та перспективи розвитку IoT” (18 квітня 2024 року) [39].

Публікації. За результатами дисертаційних досліджень опубліковано 12 наукових праць. Основні наукові результати викладено в 6 наукових статтях [30 – 33, 40, 41], серед яких [30, 32, 33, 41] опубліковані у спеціалізованих фахових виданнях, затверджених наказом МОН України, [31, 40] опубліковані в інших виданнях. Матеріали виступів на наукових та науково-практичних конференціях опубліковано у 6 збірниках тез доповідей [34 – 39].

Структура та обсяг дисертаційної роботи. Дисертація складається зі вступу, чотирьох розділів, висновків, списку використаних джерел із 97 найменувань на 13 сторінках. Загальний обсяг роботи становить 185 сторінок серед яких 152 сторінки основного тексту, 33 рисунки, 12 таблиць.

РОЗДІЛ 1
АНАЛІЗ ПРОБЛЕМАТИКИ ТА СУЧАСНИХ ПІДХОДІВ ДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ ЗАХИЩЕНОСТІ ОСОБИСТОСТІ

1.1. Аналіз проблематики забезпечення інформаційної захищеності особистості в умовах інформаційного впливу

В умовах сучасного інформаційного суспільства, де обсяг та швидкість поширення інформації постійно зростають, забезпечення інформаційної захищеності особистості набуває все більшої актуальності. Кожен день ми стикаємося з безліччю інформаційних потоків, які можуть нести як корисну, так і шкідливу інформацію. Інформаційні загрози, такі як дезінформація, кібератаки, фішинг та маніпуляції в соціальних мережах, можуть серйозно впливати на приватне життя, здоров’я та безпеку особистості [31, 42, 43].

Метою даного розділу є аналіз сучасних підходів до забезпечення інформаційної захищеності особистості в умовах зростаючого інформаційного впливу. Для цього необхідно спочатку визначити поняття інформаційної захищеності та основні інформаційні загрози, з якими стикається особистість у повсякденному житті. Потім проаналізувати різні підходи до захисту, включаючи технологічні рішення та психологічні методи забезпечення інформаційної захищеності. У висновку необхідно оцінити розглянуті аспекти на основі комплексного підходу до забезпечення інформаційної захищеності особистості в сучасному світі.

Поняття інформаційної захищеності особистості. У роботі [44] наводиться низка визначень та етимологія понять “інформаційна безпека” і “інформаційно-психологічна безпека” стосовно держави, суспільства та

окремої особистості. Традиційно, протягом тривалого часу людство використовувало поняття інформаційно-психологічної безпеки, під яким вбачалась “захищеність психіки і свідомості людини від небезпечних інформаційних впливів: маніпулювання свідомістю, дезінформування, спонукання до образ, самогубства тощо”. Разом з тим, кінець XX та початок XXI сторіччя, які характеризуються стрімким розвитком інформаційних технологій та засобів передачі інформації, призводять до необхідності говорити вже про інформаційну безпеку особистості, як “стан людини, у якому його особистості не може бути завдано істотної шкоди шляхом здійснення впливу на навколишній (для особистості) інформаційний простір” [44].

Такий підхід відображений в низці наукових публікацій та в керівних документах держави, зокрема в Стратегії інформаційної безпеки України [29], де людина визначається у якості суб’єкта інформаційної безпеки, який перебуває під дією медіа та соціальних мереж. Таким чином, у подальшому у роботі буде вживатися термін “інформаційна безпека”, як стан захищеності життєво важливих інтересів людини, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об’єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів [29]. Як бачимо, базовою складовою терміну “інформаційна безпека”, який є вкрай складним для кількісного вимірювання, є поняття “захищеності”, яке може бути оцінене кількісно на основі аналітичних чи статистичних моделей.

Інформаційна (інформаційно-психологічна) захищеність особистості є надзвичайно важливою в сучасному світі, де інформаційні потоки та психологічні впливи комбіновано, з різним ступенем поєднання проникають у всі сфери людського життя. Вона полягає у захисті психічного

здоров’я та особистої інформації індивідуума від несанкціонованого доступу, використання, маніпуляції, порушення, зміни або знищення. Метою інформаційної (інформаційно-психологічної) захищеності є забезпечення психічної стійкості, критичного мислення та здатності особистості протистояти інформаційним загрозам [45].

Отже, *інформаційна захищеність особистості* – це стан, при якому персональні дані та психічне здоров’я особистості захищені від загроз, які можуть призвести до витоку її персональних даних, їх спотворення чи знищення, а також до психологічного впливу на особистість шляхом маніпуляцій інформацією або деструктивного впровадження дезінформації у її свідомість чи підсвідомість [46].

Цей термін охоплює широкий спектр заходів, спрямованих на захист персональних даних, інформаційних систем, а також на підвищення обізнаності особистості про можливі загрози та методи їх запобігання.

Основні загрози інформаційній безпеці особистості

Дезінформація – розповсюдження неправдивої або спотвореної інформації з метою маніпуляції думками або поведінкою індивідуума. Дезінформація може впливати на прийняття рішень, політичні погляди та особисті переконання, що може мати серйозні наслідки для психічного здоров’я та стабільності людини [47].

Психологічні атаки – несанкціоновані дії, спрямовані на вплив на психічний стан та поведінку особистості з метою викликати страх, стрес або паніку. Приклади включають використання пропаганди, шокуючих зображень або відеоматеріалів, що можуть викликати сильний емоційний вплив [48].

Фішинг та соціальна інженерія – методи шахрайства, при яких зловмисники намагаються отримати конфіденційну інформацію (наприклад, паролі, дані кредитних карток) шляхом видавання себе за

надійне джерело або використовуючи методи соціальної інженерії. Такі дії можуть призвести до психологічного стресу та відчуття безпорадності [49].

Маніпуляції в соціальних мережах – використання соціальних мереж для розповсюдження пропаганди, маніпуляцій або фальшивих новин з метою впливу на погляди та поведінку користувачів. Соціальні мережі можуть стати інструментом для організованих інформаційних атак, спрямованих на певних осіб або групи людей, викликаючи психологічний дискомфорт або тривогу [35, 50].

Порушення конфіденційності та стеження – неавторизований доступ до приватних даних особистості або стеження за її поведінкою, що може призвести до розголошення або використання без згоди власника. Це включає витік персональних даних, несанкціоноване спостереження, що може серйозно вплинути на психічний стан та відчуття безпеки людини [51].

Визначивши основні загрози інформаційній безпеці особистості, можна перейти до аналізу підходів, які використовуються для забезпечення захисту психічного здоров’я та особистих даних. До них включаються технологічні, освітні, психологічні та правові аспекти цієї проблеми, щоб зрозуміти, як можна ефективно протистояти інформаційним загрозам і захистити психічне здоров’я та особисті дані в умовах сучасного інформаційного впливу.

Технологічні та психологічні підходи щодо забезпечення інформаційної захищеності особистості

Технологічні підходи.

Антивірусне програмне забезпечення. Використання антивірусних програм для захисту комп’ютерів та мобільних пристроїв від шкідливого програмного забезпечення. Антивіруси здійснюють регулярне сканування системи на наявність вірусів, троянів та іншого шкідливого ПЗ, забезпечуючи захист особистих даних від кібератак [32, 52].

Мережеві фільтри та фаєрволи. Використання мережевих фільтрів та фаєрволів для контролю та обмеження доступу до інтернет-ресурсів. Ці технології допомагають запобігати несанкціонованому доступу до особистої інформації, блокуючи потенційно небезпечні підключення та забезпечуючи безпеку мережі [34].

Шифрування даних. Застосування шифрування для захисту конфіденційної інформації. Шифрування дозволяє перетворювати дані у форму, яку можуть прочитати лише авторизовані користувачі, тим самим запобігаючи несанкціонованому доступу до особистих даних у разі їх перехоплення [37, 39].

Безпека в соціальних мережах. Використання налаштувань конфіденційності та двофакторної автентифікації у соціальних мережах для захисту облікових записів. Ці заходи допомагають запобігти несанкціонованому доступу до особистої інформації та знижують ризик маніпуляцій та психологічного впливу [53].

Постійне оновлення програмного забезпечення. Регулярне оновлення операційних систем, антивірусних програм та іншого програмного забезпечення для забезпечення актуальності засобів захисту від нових загроз. Оновлення включають виправлення вразливостей, що можуть бути використані зловмисниками для атак на особисті дані [33, 53].

Психологічні підходи

Розвиток критичного мислення. Навчання особистості критично оцінювати отримувану інформацію. Це включає аналіз джерел інформації, перевірку фактів та свідоме сприйняття контенту, що допомагає уникати дезінформації та маніпуляцій [54].

Тренінги з психологічної стійкості. Проведення тренінгів, спрямованих на розвиток психологічної стійкості до стресу та інформаційного впливу. Такі тренінги допомагають особистості зберігати спокій та раціонально реагувати на інформаційні загрози [55].

Освітні програми з кібербезпеки. Впровадження освітніх програм, що підвищують обізнаність про загрози в Інтернеті та методи їх запобігання. Це включає навчання з безпечного користування інтернет-ресурсами, розпізнавання фішингових атак та правил безпечного поводження з особистими даними [56].

Психологічна підтримка та консультування. Надання психологічної підтримки та консультування особам, які зазнали інформаційного або психологічного впливу. Це допомагає впоратися зі стресом, розвинути навички управління емоціями та підвищити загальний рівень психічного здоров'я [55].

Підвищення інформаційної грамотності. Організація кампаній з підвищення інформаційної грамотності серед населення. Інформаційна грамотність включає вміння ефективно використовувати інформаційні ресурси, розуміти та критично оцінювати медійний контент, що знижує ризик піддавання маніпуляціям та дезінформації.

Об'єднання технологічних та психологічних підходів є критичним для забезпечення комплексної інформаційної захищеності особистості. Використання сучасних технологій у поєднанні з розвитком критичного мислення, психологічної стійкості та інформаційної грамотності створює надійний захист від інформаційних загроз, забезпечуючи безпеку та психічне здоров'я індивідуума в умовах сучасного інформаційного впливу.

1.2. Аналіз технологій використання соціологічної інформації як інструмента інформаційного впливу на особистість

Соціологічні дослідження вже давно стали науковим методом збору, аналізу та інтерпретації даних, який дозволяє вивчати різноманітні аспекти

соціального життя, поведінку людей, їхні стосунки, установи та структури суспільства. Основною метою соціологічного дослідження є отримання об’єктивних даних про соціальні явища, процеси та тенденції, що відбуваються в суспільстві [24, 57].

Замовниками соціологічних досліджень можуть бути різноманітні організації та інституції, які зацікавлені у зборі соціальної інформації для прийняття обґрунтованих рішень. Серед них можна виділити наступні групи: урядові організації та установи, неприбуткові організації та фонди, приватний сектор, академічні та наукові установи, медіа та соціологічні служби.

Результати соціологічних досліджень можуть використовуватися для різних цілей, в залежності від замовника та контексту дослідження, зокрема [58]:

для прийняття управлінських рішень, як урядових, так і органами місцевого самоврядування;

для бізнесу та маркетингу – оцінка потреб споживачів, аналіз конкурентного середовища, розробка маркетингових стратегій та рекламних кампаній;

з метою аналізу громадської думки та соціальних настроїв під час політичних кампаній;

для соціального контролю та у сфері права, наприклад, для виявлення проблемних груп, боротьби зі злочинністю та розробки програм соціальної підтримки;

з метою наукових досліджень та вивчення освітніх потреб.

Таким чином, соціологічні дослідження є потужним інструментом для розуміння соціальних процесів і прийняття ефективних рішень у різних сферах життя [41]. Соціологічні дослідження проводяться різноманітними організаціями та установами, які можуть відрізнятися за своєю структурою,

цілями і методами роботи. Основні категорії організацій, які проводять соціологічні дослідження [59]:

1. Академічні та науково-дослідні інститути.

Університети та інститути: вони проводять фундаментальні та прикладні дослідження з метою розвитку науки та освіти. Приклади: Інститут соціології НАН України; Кафедри соціології в університетах, наприклад, Київський національний університет імені Тараса Шевченка.

Науково-дослідні центри: спеціалізуються на вивченні певних соціальних проблем. Наприклад, Інститут соціальних досліджень ім. Олександра Яременко.

2. Соціологічні служби та центри.

Недержавні дослідницькі організації: виконують замовлення як від державних, так і від приватних замовників. Приклади: Київський міжнародний інститут соціології (КМІС); Центр Разумкова; Соціологічна група “Рейтинг”; Фонд “Демократичні ініціативи” імені Ілька Кучеріва та ін.

Державні соціологічні служби: здійснюють дослідження з метою підтримки державної політики. Приклад: Державна служба статистики України, яка займається також соціологічними аспектами.

3. Громадські та міжнародні організації.

Громадські організації: проводять дослідження для підтримки своїх соціальних ініціатив. Наприклад, Центр економічної стратегії.

Міжнародні організації: вивчають соціальні питання на глобальному або регіональному рівні. Приклади: ЮНІСЕФ (UNICEF); Світовий банк; Міжнародний республіканський інститут (IRI).

4. Приватні дослідницькі компанії, комерційні організації: проводять дослідження на замовлення бізнесу та інших організацій. Приклади: GfK Ukraine; TNS Ukraine; Ipsos Ukraine.

5. Урядові та державні установи.

Міністерства та агентства: Проводять дослідження для розробки та оцінки політик. Наприклад, Міністерство соціальної політики України.

Національні статистичні служби: Займаються збором та аналізом соціально-економічних даних. Приклад: Державна служба статистики України.

6. Аналітичні та консалтингові компанії.

Аналітичні центри: Проводять дослідження для розробки рекомендацій та аналізу політик. Приклади: Український інститут майбутнього; Центр соціально-економічних досліджень CASE Україна.

Консалтингові фірми: Проводять дослідження для бізнесу та організацій. Наприклад, консалтингова компанія Advanter Group.

7. Медіа та інформаційні агентства, медіа організації: Замовляють і проводять соціологічні дослідження для аналізу громадської думки та актуальних соціальних питань. Приклади: Інтерфакс-Україна; Укрінформ.

8. Освітні заклади та центри професійного розвитку.

Навчальні заклади: Проводять дослідження в рамках навчальних програм та наукових проектів. Наприклад, кафедра соціології в університеті.

Центри розвитку: Виконують дослідження для підготовки кадрів та розробки навчальних програм.

Таким чином, як бачимо, соціологічні дослідження в Україні проводяться численними організаціями, які можуть спеціалізуватися на різних аспектах соціального життя і використовувати різні методи досліджень. Від державних установ до приватних компаній, всі вони роблять вагомий внесок у розуміння соціальних процесів і допомагають у прийнятті обґрунтованих рішень на різних рівнях. З іншого боку, результати соціологічних досліджень, які поширюються різноманітними медіа є вагомим інструментом впливу на свідомість та поведінку людини, яка у

своєму повсякденному житті перебуває під дією численних інформаційних потоків. Вивченню цього впливу і присвячено подальше дослідження.

Вплив соціологічної інформації на особистість визначається багатьма чинниками: інтенсивністю та частотою самого впливу, засобами впливу, умовами, за яких цей вплив відбувається, а також характеристиками особистості, зокрема її здатністю та готовністю сприймати і довіряти інформації від джерел інформації.

Широко поширена думка, що політична свідомість і поведінка людей значно залежать від інформаційного середовища, створюваного різними медіа. Сьогодні є підстави вважати, що медіа формують наше мислення, впливають на наші думки й поведінку, підштовхуючи до певних рішень, таких як, наприклад, голосування за конкретного кандидата на виборах [8]. Інші дослідники стверджують, що вплив медіа на поведінку громадян здійснюється шляхом створення певної суспільної думки. Сучасні медіа, завдяки своїй здатності надавати суспільній думці масовості, мають можливість керувати і навіть маніпулювати нею [8]. Крім того, останнім часом серед дослідників масових комунікацій, політиків і журналістів, вже давно ведуться розмови про початок епохи “медіаполітики” – влади медіа, які не лише відображають та інтерпретують дійсність, але й створюють її за власними правилами. При цьому людина стає повноправним суб’єктом комунікативної взаємодії, зважаючи на те, що вплив медіа на особистість залежить від того, яку роль відіграє сама особистість в інформаційному процесі.

В той же час, недобросовісні гравці у сфері діяльності медіа можуть сприймати громадян як об’єкт маніпулювання, застосовуючи до них які завгодно визначення – “гурт”, “натовп”, “піпл”, який “хаває все підряд”. Більшість політичних “технологій”, які застосовуються сьогодні, базуються саме на такому підході [8].

В основі інформаційного впливу, який здійснюють медіа на людей, лежить контент, який являє собою сукупність інформаційного змісту (новини, аналітика, розважальні програми, реклама тощо) та наративів, які просуваються через контент, включаючи підбір і подачу фактів, акцент на певних аспектах подій або проблем [60]. При цьому, для надання більшої вагомості меседжам та наративам, які розповсюджуються через медіа, використовується “колективна думка”, як узгоджений набір уявлень, поглядів, переконань або суджень, які сформовані серед великої групи людей. Для підкріплення чи обґрунтування такої колективної думки дуже часто використовуються результати соціологічних досліджень.

Наприклад, людина може вирішувати проблему: за кого з кандидатів голосувати на виборах. При цьому, на певному етапі кампанії людина може і не мати чітких політичних вподобань. В цей же час результати соціології, які транслюються численними медіа, дають їй сконцентровану колективну думку суспільства, яка “підштовхує” людину до певних дій. І, у багатьох випадках, через деякий час, така людина набуває “власних” переконань щодо кандидатів.

Соціологічні дослідження можуть значно впливати на індивідуальну поведінку особистості через декілька механізмів [57]:

1. Інформаційний вплив (Information Influence): люди часто орієнтуються на думки та поведінку інших, щоб прийняти рішення або сформувати свою точку зору. Соціологічні дослідження можуть надати інформацію про те, як інші люди думають і діють, що впливає на індивідуальні рішення та дії [36].

2. Нормативний вплив (Normative Influence): результати соціологічних досліджень можуть показувати соціальні норми та очікування. Коли люди дізнаються про загальноприйняті стандарти чи типову поведінку в їх спільноті, вони можуть змінити свою поведінку, щоб відповідати цим нормам.

3. Механізм зворотного зв’язку (Feedback Mechanism): результати досліджень можуть використовуватися для оцінки ефективності певних політик або програм. Якщо результати показують позитивні або негативні наслідки, це може стимулювати зміну поведінки як на індивідуальному, так і на суспільному рівні.

4. Вплив через медіа (Media Influence): соціологічні дослідження часто висвітлюються у різноманітних медіа. Це може спричиняти широке розповсюдження інформації та впливати на суспільну думку, що, в свою чергу, впливає на поведінку окремих людей [38].

5. Соціальне порівняння (Social Comparison): люди схильні порівнювати себе з іншими. Коли результати соціологічних досліджень показують, як поводяться інші, це може стимулювати людей до змін у власній поведінці, щоб відповідати або виділятися на фоні загальних тенденцій.

6. Вплив на формування громадської думки (Influence on Public Opinion Formation): результати досліджень можуть допомагати у формуванні громадської думки, що, в свою чергу, впливає на індивідуальні переконання та дії. Наприклад, якщо дослідження показують високий рівень підтримки певної політики, це може змінити ставлення людей до цієї політики [40].

7. Вплив на особисту рефлексію (Impact on Personal Reflection): ознайомлення з результатами соціологічних досліджень може спонукати людей до самоаналізу та критичного осмислення власних цінностей, переконань та поведінки, що може призвести до їхньої зміни.

Через ці механізми соціологічні дослідження можуть значно впливати на індивідуальну поведінку, сприяючи змінам як на рівні окремих людей, так і на рівні суспільства в цілому.

Суперечливість різних поглядів на характер і ступінь впливовості медіа обумовлює необхідність теоретично та експериментально побудувати модель оцінки впливу соціологічної інформації на поведінку людини.

1.3. Аналіз теоретичних підходів до вирішення проблеми створення моделі інформаційної захищеності особистості в умовах впливу соціологічної інформації

Вплив результатів соціологічних досліджень на поведінку людини є предметом досліджень у багатьох галузях соціальних наук, включаючи соціологію, психологію та політичні науки. Так, відомими є роботи В. Ліпмана [1], який у 20-х роках минулого сторіччя досліджував, як громадська думка формується під впливом мас-медіа і соціальних досліджень, а також як вона впливає на поведінку індивідів і суспільства в цілому. Пізніше, у 40-х роках Р. К. Мертон [2] досліджує феномен самоздійснюваного пророцтва, коли прогнози або результати опитувань впливають на поведінку людей, змушуючи їх діяти у відповідності з очікуваннями, що призводить до здійснення цих прогнозів.

У 70-х І. Айзен та М. Фішбейн [3] досліджують взаємозв’язок між громадською думкою та поведінкою, що є центральною темою багатьох соціологічних досліджень. Далі, у 80-х Е. Ноеле-Н’юман [4] встановлює, як страх бути ізольованим або осудженим за висловлювання менш популярної думки змушує людей замовчувати свої справжні погляди, що впливає на поведінку індивідів і груп.

Д. Р. Заллер у 90-х [5] вивчає механізми формування громадської думки і вплив на неї соціологічних досліджень і медіа. Показує, як інформація, яку люди отримують з опитувань, може змінювати їхні політичні та соціальні

погляди. А Д. Ф. Бішоп у статті [6] розглядає, як результати соціологічних опитувань впливають на виборчу поведінку, зокрема на явку виборців та їх вибір.

Крім фундаментальних публікацій, різним аспектам соціальних досліджень присвячено низку періодичних видань, зокрема “The Public Opinion Quarterly”, де публікуються численні статті, які досліджують вплив результатів соціологічних опитувань на громадську думку та поведінку людей, включаючи формування громадської думки, політичну поведінку та вплив мас-медіа. В той же час, ні фундаментальні праці, ні публікації у періодичних виданнях не досліджують можливості формалізації процесів впливу соціальної думки на поведінку окремих особистостей. Дуже мало публікацій присвячено питанням створення математичних моделей поведінки людини під впливом медіа та соціологічної інформації. Серед існуючих спроб створення таких моделей можна визначити декілька робіт вітчизняних та закордонних авторів.

У статті [8] узагальнено емпіричні дані, отримані в результаті соціологічних опитувань з використанням методів кореляційного аналізу та запропоновано модель реагування виборців на медіа-вплив під час президентських передвиборчих кампаній. Основним елементом запропонованої моделі є залежність кількості голосів, відданих за кандидатів на різних етапах президентських виборів, від обсягу присвяченого їм ефірного часу на державних телеканалах. Такий підхід, хоча і достатньо реалістичний, може бути застосований лише після завершення виборів. Крім того, ця модель не враховує якісні характеристики ефірного часу, такі як час доби та популярність програм.

У статті [9] автори аналізують вплив медіа на глядачів та слухачів, досліджуючи феномен медіа-впливу на масову аудиторію. В основі дослідження лежать різні концепції, такі як соціально-когнітивна теорія, ефект праймінгу, гіпотеза культивації, дифузія інновацій тощо, які

пояснюють феномен медіа-впливу за допомогою численних прикладів, включаючи вплив новин, сцен насильства, відвертих сцен та розважальних передач. Основною метою авторів є підвищення медіаграмотності споживачів, що дозволить їм контролювати та зменшувати негативний вплив мас-медіа. Масова комунікація забезпечується єдиним джерелом, яке передає інституціалізовану інформацію мільйонам споживачів. Аудиторія часто гетерогенна, характеризується різними демографічними параметрами і зазвичай невідома джерелу інформації. Хоча автори досліджують цю тему досить глибоко, вони не надають простої формалізації для оцінки процесів впливу, що ускладнює практичне застосування моделі медіа-впливу.

У дослідженні [61] для розробки евристичних математичних моделей людської поведінки пропонується евентуально-статистичний підхід. Основна суть цього підходу полягає в тому, що людина, виступаючи в ролі економічного агента, здійснює економічну діяльність у рамках конкретних подій у часі. У кожній з цих подій агент має можливість вибору та реалізації кількох стратегій поведінки відповідно до різних критеріїв, що базуються на описаних локальних концептуальних моделях, таких як економічна, соціологічна, психологічна, інституційна та інші. Зазначається, що акти вибору та реалізації стратегій поведінки є взаємопов’язаними. Проте, для адекватної оцінки поведінки людини необхідно спиратися на конкретні вчинки, а не на внутрішній психологічний аналіз, який слугує основою для вибору стратегії . Процес і результати такого аналізу практично неможливо піддати якісній та кількісній оцінці.

У роботі [7] досліджується концепція багатомодельного мислення, яка передбачає використання набору моделей для осмислення складних явищ. Основна ідея полягає в тому, що багатомодельне мислення сприяє формуванню мудрості через застосування різноманітних логічних структур. Кожна модель акцентує увагу на окремих причинно-наслідкових факторах. У роботі наведено формальні аргументи, що обґрунтовують концепцію

множини моделей, а також численні приклади з реального життя. Багатомодельне мислення не лише підвищує ефективність роботи, але й сприяє успіху в суспільному житті, що дозволяє стати справжніми експертами в оцінках економічних та політичних подій. Проте, використання запропонованих моделей для формалізації впливу результатів соціальних досліджень виявляється досить проблематичним.

Низка робіт вітчизняних авторів присвячена захисту людини в соціальних мережах. Так у [10 – 12] досліджуються параметри безпеки персональних даних особистості у залежності від топології та взаємовпливу користувачів соціальної мережі. Робиться висновок щодо необхідності управління топологією зв’язків та управління контентом користувача у соціальній мережі. Пропонується модель такого управління на основі теорії графів. У [13 – 16] розглядається залежність інформаційної захищеності особистості у соціальній мережі від впливу методів соціальної інженерії. Пропонуються моделі захисту на основі кластеризації зв’язків та оцінки ступеня зв’язності особистості у соціальній мережі. У роботах [17 – 19] досліджуються питання роботи з інформаційним контентом. Застосовуються різноманітні методи для виявлення мережевих атак на основі аналізу контенту. В публікаціях [20, 21] аналізуються різні методи соціального контролю як механізму самоорганізації, а також процес прийняття рішень у антагоністичних цифрових комунікаціях. Реалізація таких підходів дозволяє мінімізувати негативний вплив поширення деструктивного контенту та дій недобросовісних конкурентів в соціальних інтернет-сервісах. В той же час, особистість у всіх цих роботах розглядається як пасивний сприймач інформації, який не змінює лінію поведінки у залежності від обсягу та джерела інформації. Поза увагою залишаються також питання впливу контенту на зміну лінії поведінки особистості, а саме – її конформності.

У роботі [22] аналізуються сучасні математичні моделі конформності, які досліджуються за допомогою методів теорії ймовірностей, теорії ігор та статистичної фізики. Автор намагається узагальнити порогові моделі Грановеттера та модель обмеженого оточення Шеллінга, пропонуючи на їх базі загальне формулювання теоретико-ігрової моделі конформної поведінки в рамках гри в нормальній формі. У межах цієї загальної моделі автором отримано результати для низки її змістовно інтерпретованих варіацій, а також досліджено властивості відповідних рівноваг Неша. У роботі також наведено численні приклади соціальних та економічних ситуацій, які можуть бути інтерпретовані як прояви стадної поведінки. Однак у рамках цього дослідження навряд чи можна обмежитися лише варіантом стадної поведінки, що вимагає застосування інших підходів до побудови моделі впливу результатів соціологічних досліджень.

У роботі [23] досліджується побудова моделі поведінки індивіда, який при прийнятті рішень з певних питань спирається як на власну думку, так і на ставлення оточуючих його суб’єктів (колективу). Основна ідея дослідження полягає в урахуванні індивідуального сприйняття інформації, що оточує особу. Такий підхід може бути використаний для створення загальної моделі оцінки впливу соціологічної інформації на поведінку окремого індивіда. Його переваги: простота і доступність, а також можливість до розширення, оскільки автором пропонується лише основа, яка у подальшому може бути доповнена іншими аспектами.

Отже, з проведеного розгляду можна зробити висновок, що на теперішній час питання формалізації процесів впливу результатів соціології на поведінку особистостей досліджені вкрай недостатньо. У математичних моделях, які були запропоновані різними авторами, можна відзначити наступні недоліки, зокрема:

моделі, побудовані на емпіричних даних, можуть бути застосовані лише після завершення збору статистичних даних;

моделі на базі соціально-когнітивної теорії не надають доступної формалізації для оцінки процесів впливу, що ускладнює практичне їх застосування;

моделі з використанням евентуально-статистичного підходу переобтяжені внутрішнім психологічним аналізом особистості, який складно підлаштовується до методів соціології;

підходи на основі концепції багатомодельного мислення вимагають розробки додаткових механізмів переходу між моделями;

моделі захисту особистості в соціальних мережах розглядають особистість як стабільного реципієнта інформації без урахування ступеня її конформізму;

математичні моделі конформності та конформної поведінки є найбільш близькими, хоча і потребують удосконалення для можливості використання в них результатів соціології.

1.4. Постановка наукового завдання щодо створення моделі інформаційної захищеності особистості в умовах впливу соціологічної інформації

Протиріччя на практиці. Сучасна людина існує в інформаційному просторі де щоденно перебуває під впливом десятків або сотень повідомлень з різних джерел інформації. Біологічно, індивідууми Homo Sapiens не мають природних інформаційних фільтрів, що робить їх беззахисними перед суцільним інформаційним потоком. Крім того, існування у людини схильності до конформізму, як поведінки, яка відображає прагнення індивідів слідувати груповим нормам, цінностям і звичаям, призводить до того, що майже будь-яка інформація, підкріплена

результатами соціологічних досліджень, може стати тим тригером, що змінює поведінку особистості наперекір її вподобанням чи, навіть, здоровому глузду.

Відтак, виникає протиріччя, яке пов'язане з конфліктом між необхідністю доступу до інформації та потребою захистити особистість від маніпуляцій і дезінформації. При цьому, можна виділити кілька ключових аспектів цього протиріччя:

1. *Доступність інформації* vs *захист від дезінформації*. Люди потребують доступу до різноманітної інформації для формування власних думок і прийняття рішень. Однак, зростання кількості дезінформації, фейкових новин та маніпулятивних соціологічних опитувань підвищує ризик впливу на їх поведінку та світогляд. *Ключове питання протиріччя*: Як забезпечити відкритий доступ до інформації, водночас захищаючи особистість від маніпулятивного контенту?

2. *Свобода вираження* vs *контроль інформації*. Свобода вираження є фундаментальною цінністю демократичного суспільства, але вона може використовуватися для поширення шкідливої інформації або для маніпуляцій. *Ключове питання протиріччя*: Як балансувати між забезпеченням свободи слова і необхідністю контролювати поширення неправдивої або маніпулятивної інформації?

3. *Прозорість опитувань* vs *захист від маніпуляцій*. Прозорість і доступність результатів соціологічних опитувань важливі для громадського контролю за владою. Однак, ті самі опитування можуть бути використані для маніпуляцій суспільною думкою або для впливу на виборчу поведінку. *Ключове питання протиріччя*: Як зробити результати соціологічних опитувань доступними для громадськості, водночас захищаючи її від маніпуляцій?

4. *Ефективність комунікації* vs *критичне мислення*. Для ефективної комунікації важливо, щоб інформація була зрозумілою і доступною. Однак,

спрощення інформації може призвести до втрати важливих деталей і критичного аналізу. *Ключове питання протиріччя*: Як забезпечити ефективну комунікацію інформації, водночас стимулюючи критичне мислення і аналіз?

5. *Глобалізація* vs *приватність*. Сучасні технології, такі як соціальні мережі і великі дані, дозволяють збирати і аналізувати величезні обсяги інформації про користувачів, що може бути використано для більш точного таргетування та маніпуляцій. *Ключове питання протиріччя*: Як використовувати переваги глобалізації для отримання достовірної інформації, водночас захищаючи приватність і дані користувачів?

Для демонстрації реалізації протиріччя на практиці можна розглянути приклад виборів та опитування громадської думки перед виборами. Публікація результатів соціологічних опитувань перед виборами може вплинути на рішення виборців, сприяючи ефекту приєднання до більшості (bandwagon effect) або, іноді і навпаки, підтримуючи менш популярного кандидата (underdog effect). Отже, виникає протиріччя: Як забезпечити право громадськості на інформацію про громадську думку, не допускаючи маніпуляцій виборчою поведінкою?

Виявлені аспекти протиріччя підкреслюють необхідність розробки моделей інформаційної захищеності, які допомагатимуть знаходити баланс між відкритістю та захистом, свободою вираження та контролем, прозорістю та захистом від маніпуляцій. Вони також вказують на важливість міждисциплінарного підходу, що враховує як технічні, так і соціальні аспекти проблеми.

Протиріччя в теорії. У теоретичній площині виявлені раніше практичні аспекти протиріччя зводяться до формули: *раціональний вибір* vs *когнітивні упередження та маніпуляції*.

Раціональний вибір: Теорія раціонального вибору передбачає, що люди приймають рішення, оцінюючи наявну інформацію та вибираючи

найкращий варіант для досягнення своїх цілей. Ця концепція передбачає, що люди можуть обробляти інформацію об’єктивно і робити зважені рішення.

Когнітивні упередження та маніпуляції: Проте численні дослідження в області когнітивної психології та поведінкової економіки (наприклад, роботи Деніела Канемана [62] та Амоса Тверськи [63]) показують, що люди схильні до когнітивних упереджень, які можуть спотворювати їх сприйняття інформації та впливати на рішення. Маніпулятивні техніки, такі як фреймування, соціальний доказ (social proof), та ефект приєднання до більшості (bandwagon effect) на основі конформізму, можуть значно впливати на поведінку людей.

Відтак, завдання, які залишаються невирішеними в науці:

1. *Вимірювання впливу маніпуляцій*: Наукова задача полягає в тому, щоб точно виміряти, наскільки різні форми маніпуляцій (наприклад, медіа маніпуляції, фреймування питань в опитуваннях) впливають на прийняття рішень людьми. Як можна кількісно оцінити цей вплив і передбачити його наслідки?

2. *Моделювання захисних механізмів*: Як можна моделювати та розробити ефективні захисні механізми для захисту людей від маніпулятивного впливу, враховуючи їхні когнітивні упередження? Які методи можуть допомогти людям краще розпізнавати маніпуляції та захищатися від них?

3. *Баланс між доступністю інформації та захистом*: Як знайти баланс між забезпеченням доступу до інформації та необхідністю захистити особистість від дезінформації та маніпуляцій? Які підходи можуть бути використані для забезпечення цього балансу в різних контекстах (наприклад, у соціальних мережах, новинних медіа)?

4. *Етичні аспекти регулювання інформації*: Які етичні принципи повинні лежати в основі регулювання інформаційного простору для захисту

особистості? Як уникнути надмірного контролю та цензури, забезпечуючи водночас захист від шкідливого впливу?

Ці теоретичні протиріччя підкреслюють необхідність подальших досліджень і розробки моделей, які можуть допомогти краще зрозуміти і захистити особистість від негативного впливу соціологічної інформації. Це включає вимірювання впливу маніпуляцій, розробку захисних механізмів, баланс між доступністю інформації та захистом, а також етичні аспекти регулювання інформаційного простору.

Наукове завдання. Виходячи з виявлених протиріч у практичній та теоретичній площинах у дисертаційній роботі підлягає вирішенню нове наукове завдання щодо *створення моделі інформаційної захищеності особистості в умовах впливу результатів соціологічних досліджень*.

Зазначена модель повинна враховувати:

особисте апріорне (до ознайомлення з результатами соціології) ставлення особистості до певної події чи явища суспільного життя;

особисте апостеріорне (після ознайомлення з результатами соціології) ставлення особистості до певної події чи явища суспільного життя;

загальне публічне ставлення до певної події чи явища суспільного життя за результатами соціології;

ступінь незалежності мислення особистості;

рівень довіри до результатів соціології;

механізм управління надходженням соціологічної інформації до особистості;

критерій інформаційної захищеності особистості та його межі.

Мета дослідження – підвищення інформаційної захищеності особистості в умовах впливу результатів соціологічних досліджень.

Окремі завдання дослідження. Для досягнення мети роботи потребують вирішення окремі завдання дослідження, зокрема:

1. Проаналізувати проблематику та сучасні підходи до забезпечення інформаційної захищеності особистості.

2. Проаналізувати технології використання соціологічної інформації як інструмента інформаційного впливу на особистість.

3. Удосконалити модель поведінки особистості під впливом соціологічної інформації.

4. Розробити модель інформаційної захищеності особистості.

5. Адаптувати технології обробки результатів соціологічних досліджень для використання в моделях поведінки та інформаційної захищеності особистості.

6. Дослідити моделі та розробити рекомендації щодо їх впровадження.

Об'єкт дослідження – інформаційна захищеність особистості, як явище, яке полягає у забезпеченні її психічної стійкості, критичного мислення та здатності особистості протистояти інформаційним загрозам.

Предмет дослідження – моделі поведінки та інформаційної захищеності особистості в умовах впливу результатів соціологічних досліджень.

Також, необхідно надати пояснення деяким поняттям та термінам, які використовуються в дисертації. Зокрема, у темі роботи та впродовж всього тексту використовується поняття "*особистість*". З точки зору інформаційної безпеки, поняття "особистість" має специфічні відмінності від таких понять, як "людина", "громадянин", "суб'єкт" та "індивід". Кожне з цих понять має свої особливості та акценти у визначенні [64]:

Особистість – це комплекс соціально-психологічних характеристик людини, що включає її свідомість, характер, поведінкові моделі, цінності та самосвідомість. Інформаційна безпека особистості стосується захисту її особистих даних, індивідуальних інтересів, приватності та свободи висловлювань. Особистість враховує унікальні психологічні та соціальні

аспекти індивідуума, що може впливати на його взаємодію з інформаційними технологіями та системами.

Людина – це біологічна істота, що належить до виду Homo Sapiens. З точки зору інформаційної безпеки, захист людини може включати ширший контекст, такий як захист від фізичних загроз, що виникають через витік інформації. У той же час, для людини робиться менший акцент на індивідуальних психологічних характеристиках.

Громадянин – це людина, яка має правовий зв'язок з певною державою, наділена правами та обов'язками згідно з її законодавством. Інформаційна безпека громадянина зосереджена на правових аспектах, таких як захист персональних даних, право на приватність та дотримання законів про інформаційну безпеку. Особливий акцент, при цьому, робиться на правових механізмах захисту.

Суб'єкт – це активний діючий елемент, що має певні права і обов'язки в конкретних правових, соціальних чи економічних системах. Відмінність в контексті інформаційної безпеки: Захист суб'єкта може стосуватися не лише фізичних осіб, а й юридичних осіб або інших інституційних форм. Для суб'єкта зосередженість – на функціональних ролях та відповідальності в межах інформаційних систем.

Індивід – це окрема людина як носій певних біологічних, соціальних та психологічних характеристик. Інформаційна безпека індивіда може акцентувати увагу на базових аспектах захисту особистих даних та базових прав на приватність. Індивід – це більш загальне поняття, яке не враховує соціально-психологічних аспектів особистості.

Таким чином, ключова відмінність поняття "особистість" від інших термінів полягає в тому, що воно включає комплексні соціально-психологічні характеристики, що формують унікальну ідентичність людини. В контексті інформаційної безпеки це означає захист не лише базових прав і даних, але й унікальних інтересів та особистих аспектів

індивідуума. Інші терміни, такі як “людина”, “громадянин”, “суб’єкт” та “індивід”, акцентують увагу на біологічних, правових, функціональних або базових соціальних характеристиках, відповідно.

Висновки до розділу 1

1. В умовах сучасного інформаційного суспільства забезпечення інформаційної захищеності особистості набуває все більшої актуальності. Сьогодні людина постійно перебуває під дією інформаційних потоків, які можуть нести як корисну, так і шкідливу інформацію. Інформаційні загрози, такі як дезінформація, кібератаки, фішинг та маніпуляції в соціальних мережах, можуть серйозно впливати на приватне життя, здоров’я та безпеку особистості. Для забезпечення комплексної інформаційної захищеності особистості важливим є об’єднання технологічних та психологічних підходів на основі використання сучасних технологій кібербезпеки у поєднанні з розвитком критичного мислення, психологічної стійкості та інформаційної грамотності.

2. Соціологічні дослідження є потужним інструментом для розуміння соціальних процесів і ухвалення ефективних рішень у різних сферах життя. З іншого боку, результати соціології, які поширюються різноманітними медіа, є засобом впливу на свідомість та поведінку людини. Враховуючи схильність людської психіки до конформізму, сучасні медіа мають можливість керувати і навіть маніпулювати думками і поведінкою особистості, підштовхуючи її до певних рішень. Суперечливість різних поглядів на характер і ступінь впливовості медіа обумовлює необхідність теоретично та експериментально побудувати модель оцінки впливу соціологічної інформації на поведінку людини.

3. Питання формалізації процесів впливу результатів соціології на поведінку особистостей на теперішній час досліджені вкрай недостатньо. В існуючих моделях можна відзначити наступні недоліки, зокрема: емпіричні моделі можуть бути застосовані лише після завершення збору статистичних даних; соціально-когнітивні моделі не надають доступної формалізації для оцінки процесів впливу; евентуально-статистичні моделі переобтяжені внутрішнім психологічним аналізом особистості, який складно підлаштовується до методів соціології; підходи на основі багатомодельного мислення вимагають розробки додаткових механізмів переходу між моделями; моделі захисту в соціальних мережах не враховують ступінь конформізму особистості. Найбільш близькими для побудови моделі інформаційної захищеності є математичні моделі конформності та конформної поведінки, хоча і вони потребують удосконалення для можливості використання в них результатів соціології.

4. Існування у людини схильності до конформізму, як поведінки, яка відображає її прагнення слідувати груповим нормам, цінностям і звичаям, призводить до того, що майже будь-яка інформація, підкріплена результатами соціологічних досліджень, може стати тим тригером, що змінює поведінку особистості наперекір її вподобанням чи, навіть, здоровому глузду. Відтак, виникає протиріччя, яке пов’язане з конфліктом між необхідністю доступу до інформації та потребою захистити особистість від маніпуляцій і дезінформації. Виходячи з цього у дисертаційній роботі підлягає вирішенню нове наукове завдання щодо *створення моделі інформаційної захищеності особистості в умовах впливу результатів соціологічних досліджень*.

РОЗДІЛ 2
РОЗРОБЛЕННЯ МОДЕЛІ ІНФОРМАЦІЙНОЇ ЗАХИЩЕНОСТІ ОСОБИСТОСТІ ВІД ВПЛИВУ РЕЗУЛЬТАТІВ СОЦІОЛОГІЧНИХ ДОСЛІДЖЕНЬ

Інформаційна безпека особистості – це захищеність психіки й свідомості людини від небезпечних інформаційних впливів: маніпулювання свідомістю, дезінформування, спонукання до образ, самогубства тощо [65]. Розширюючи це поняття, можна констатувати, що інформаційна безпека особистості – це стан людини, у якому вона здійснює свою діяльність відповідно до своїх бажань, переконань та намірів. Порушенням інформаційної безпеки особистості можна вважати будь-який інформаційний вплив, який змінює лінію її поведінки, попередньо сформовану відповідно до її переконань. Тобто, у реальному житті при ухваленні рішень людина не завжди користується логікою або власними переконаннями, а часто діє всупереч своїм переконанням або власним інтересам.

Формування людини як особистості здійснюється під впливом численних факторів протягом тривалого часу, які і визначають зміст переконань, що керують її поведінкою. Разом з тим, на поведінку окремої особистості впливає також поточна інформація, яка надходить від її оточення (рідних, колег та друзів). І тому, у багатьох випадках особистість, навіть маючи власні переконання, в результаті діє “як усі”. Для пояснення цього явища, необхідно дослідити механізм, який лежить в основі такої поведінки. Підлаштування поведінки окремої особистості під діяльність більшості у науці носить назву “конформізм”. У цьому розділі розглядається математична модель такого механізму та робиться перевірка його адекватності на окремих прикладах.

2.1. Удосконалення моделі поведінки особистості під впливом соціологічної інформації

У роботі [23] автором пропонується модель поведінки людини, яка перебуває під впливом інших людей з її оточення. Модель враховує як власні переконання людини, а також ставлення до певних питань її оточення. Рішення приймаються індивідом з урахуванням думки колег. Таким чином, автор створює загальну модель конформізму, як специфічної характеристики людини, яка може мати як позитивну, так і негативну спрямованість. Запропонована модель враховує: початкові переконання особистості; ступінь незалежності її мислення та вплив оточення на особистість. Таким чином, зазначена модель може бути покладена в основу загальної моделі оцінки впливу соціології на поведінку особистості.

При розробці моделі конформної поведінки особистості у [23] в основу покладено спілкування її з іншими особистостями. Це виражається у застосуванні відповідних ймовірнісних показників впливу оточення на особистість та зворотного впливу особистості на оточення. На відміну від такого підходу, сприйняття особистістю результатів соціології має свої особливості, зокрема – особистість не впливає безпосередньо на соціологію. Крім того, особистість може сприймати вторинний вплив, коли результати соціології передаються особистості від інших суб’єктів її оточення. Таким чином, базова модель конформної поведінки особистості має бути удосконалена з урахуванням виявлених особливостей.

Зробимо спочатку загальний опис моделі поведінки особистості. Як і в базовій моделі, вважатимемо, що особистість, ухвалюючи рішення з того чи іншого питання, керується як своїми початковими переконаннями, так і ставленням до цього питання інших суб’єктів з її оточення. В рамках нашого розгляду, колективна думка включатиме як думку оточення, так і суспільну

думку, виражену у результатах соціологічних досліджень. Такі результати доступні особистості через численні медіа (інтернет-канали, соціальні мережі, телебачення, радіо тощо). Будемо розглядати події, які можуть бути подані у бінарному вигляді, типу “підтримую”, чи “не підтримую”. Наприклад, питаннями для ухвалення рішення можуть бути: чи підтримувати певного кандидата на виборах, чи брати участь у певному заході тощо. У таких випадках особистість має зробити вибір, чи перейти їй в інший стан, чи ні.

При такому підході можна розглядати множину альтернатив (теоретично – нескінченну), де кожна альтернатива може розглядатися як окремо, так і разом, у залежності від деталізації задачі. Такі альтернативи можуть бути сумісними або несумісними. Перехід до іншого стану у даному випадку, це лише теоретична абстракція і тому під станом може розумітися будь-яка, як завгодно складна конструкція.

В основу математичної моделі [23] покладені дві кількісні оцінки ставлення особистості до нового стану:

особисте апріорне ставлення до нового стану (переконання особистості), яке описується ймовірністю готовності особистості перейти у цей стан (α_j) – до спілкування особистості з колективом чи впливу на неї соціології;

особисте апостеріорне ставлення до нового стану, яке описується ймовірністю остаточного рішення перейти у новий стан (P_j) після спілкування з колективом чи ознайомлення з результатами соціологічних досліджень.

Ймовірності α_j і P_j описують саме інформаційну складову процесу переходу з початкового до фінального стану, оскільки обумовлені спілкуванням особистості з колективом та ознайомленням з результатами соціології. У випадку, коли особистість є незалежною в ухваленні рішень,

вона може не піддатися такому впливу і тоді, очевидно, її апостеріорне ставлення співпадатиме з апріорним $\alpha_j = P_j$.

Іншою характеристикою, яка врахована у моделі конформної поведінки і має бути врахована у подальшому, є ступінь незалежності особистості μ_j, яка визначається, як ймовірність того, що в конкретній ситуації особистість поводить себе як незалежна. Якщо $\mu_j = 1$, то рішення особистості не залежать від думок оточення, результатів соціології чи іншого інформаційного впливу. Якщо $\mu_j = 0$, то маємо абсолютну залежність, що означає майже миттєву зміну початкових переконань особистості під дією будь-якого інформаційного впливу.

На відміну від моделі конформної поведінки [23] у подальшому в роботі будемо розглядати лише зміну поведінки особистості під впливом повідомлень результатів соціології. Отже, як було зазначено у абсолютно незалежної особистості апостеріорна ймовірність P_j^1 збігається з апріорною $P_j^1 = \alpha_j$, тобто з її переконаннями. Апостеріорна ймовірність P_j^0 для абсолютно залежної особистості може бути визначена на основі наступних міркувань. Вважатимемо, що вплив кожного *i*-го повідомлення результатів соціології на дану *j*-ту особистість визначається числом $\lambda_{j,i}$ – ймовірністю того, що *j*-та особистість вчинить так, як слідує з *i*-го повідомлення результатів соціології. При цьому, також будемо вважати, що такий вплив *i*-го повідомлення результатів соціології на дану *j*-ту особистість не залежить від впливу інших альтернативних повідомлень. Це означає, що особистість перейде у новий стан із ймовірністю P_i. Тоді повна ймовірність переходу *j*-ї абсолютно залежної особистості в новий стан дорівнюватиме

$$P_j^0 = \sum_{i=1}^{N} \lambda_{j,i} P_i , \qquad (2.1)$$

де N – загальна кількість повідомлень (або джерел соціології); $\sum_{i=1}^{N}\lambda_{j,i}=1$ та всі $\lambda_{j,i}>0$, оскільки на абсолютно залежну особистість впливає будь-яке повідомлення результатів соціології.

Як бачимо, $\lambda_{j,i}$ виражає ступінь впливу соціології на особистість. З іншого боку, зважаючи на $\sum_{i=1}^{N}\lambda_{j,i}=1$, $\lambda_{j,i}$ може розглядатися також і як розподілений рівень довіри особистості до результатів соціології, оскільки, в будь-якому разі, хоча б одне джерело буде чинити вплив на особистість.

Апостеріорна ймовірність для довільно обраної j-ї особистості може бути отримана на основі формули повної ймовірності

$$P_j = P_j^1\mu_j + \left(1-\mu_j\right)P_j^0,\ j=\overline{1,N}, \tag{2.2}$$

або, у розгорнутому вигляді

$$P_j = \alpha_j\mu_j + \left(1-\mu_j\right)\sum_{i=1}^{N}\lambda_{j,i}P_i,\ j=\overline{1,N}. \tag{2.3}$$

Формули (2.2) та (2.3) і є моделлю поведінки особистості під впливом результатів соціологічних досліджень у загальному вигляді при тих спрощеннях, які було прийнято. На відміну від моделі конформної поведінки ця модель враховує рівень довіри до джерела соціологічної інформації та особливості інформаційного обміну між особистістю та джерелом соціології.

При заданих параметрах (α,μ,λ) з формули (2.3) можна визначити апостеріорні ймовірності (P), які у векторній формі матимуть вигляд

$$P = \mathrm{A}M + \left(E - M\right)\Lambda P, \tag{2.4}$$

де Λ – стохастична матриця ($\lambda_{j,i}$), M – діагональна матриця (μ_j), E – одинична матриця, А та P – вектори з компонентами α_j та P_j відповідно.

Проаналізуємо рівняння (2.3) і перевіримо, що $0 \le P_j \le 1$. Для цього перепишемо рівняння (2.4) у вигляді

$$\left(E - B\right)P = \mathrm{A}M\ , \tag{2.5}$$

де матриця $B = \left(E - M\right)\Lambda$.

Припустимо, що не всі $\mu_j = 0$ (випадок $\mu_j = 0$ необхідно буде дослідити окремо). Спочатку приймемо, що всі $\mu_j \ne 1$, тоді матриця B невід'ємна і нерозкладна, починаючи з $N > 2$, тому, що її квадрат строго більше 0. Така матриця (за теоремою Фробеніуса) завжди має позитивне характеристичне число r з максимальним модулем, яке є простим коренем характеристичного рівняння і задовольняє нерівності $s \le r \le S$, де s і S – мінімальна та максимальна суми елементів рядків матриці відповідно. Сувора рівність досягається лише за $s = S$ і тому, у нашому випадку, $r < 1$. Це гарантує існування та невід'ємність матриці, зворотної до ($E - B$). Таким чином, система (2.3) має єдине та невід'ємне рішення.

Доведемо, що це рішення за нормою не більше 1, тобто $\max P_j \le 1$. Для цього поділимо всі індекси j на дві групи: K і R. У групу K віднесемо всі індекси $j = k$, при яких $\mu_j = 0$, а в групу R – інші $j = r$. Тоді, з урахуванням наведеного поділу, систему рівнянь (2.3) можна подати у вигляді

$$P_r = \alpha_r \mu_r + (1-\mu_r)\sum_{i=1}^{N} \lambda_{r,i} P_i,\ r \in R, \tag{2.6}$$

$$P_k = \sum_{i=1}^{N} \lambda_{k,i} P_i,\ k \in K. \tag{2.7}$$

Всю множину індексів $j = m$, у яких реалізується $\max P_j = P_m$, позначимо через *M*. В групі індексів *R* міститься хоча б один індекс з *M*, інакше для всіх $m \in M$ мало б місце

$$P_m = \sum_{i=1}^{N} \lambda_{m,i} P_i, \tag{2.8}$$

а ця рівність можлива лише тоді, коли всі $P_i = P_m$, оскільки $\sum_{i=1}^{N} \lambda_{m,i} = 1$, всі $\lambda_{m,i} > 0$ і всі $P_i \geq 0$. Таким чином, множина *M* збігалася б з усією множиною індексів $j = 1,2,\ldots,N$, що призводить до суперечності з припущенням, що *R* не має жодного індексу з множини *M*. Відтак, група індексів *R* містить хоча б один індекс з множини *M*, але тоді при цьому індексі має місце рівність

$$\max P_j = \alpha_m \mu_m + (1-\mu_m)\sum_{i=1}^{N} \lambda_{m,i} P_i, \tag{2.9}$$

звідки випливає, що

$$\begin{gathered} \max P_j \leq \mu_m + (1-\mu_m)\sum_{i=1}^{N} \lambda_{m,i} \max P_j = \\ = \mu_m + (1-\mu_m)\max P_j = \mu_m (1 - \max P_j) + \max P_j \end{gathered} \tag{2.10}$$

а це призводить до нерівності: $\mu_m\left(\max P_j - 1\right) \le 0$. Оскільки $\mu_m > 0$, то виконано $\max P_j \le 1$, що і треба було довести.

Також розглянемо випадок, коли частина особистостей у колективі є абсолютно незалежною, тобто $\mu_s = 1$ для кожного з $s \in S \subseteq J$ (тут через J позначено всю множину індексів j). Початкова матриця B тепер стає розкладною, і це природно, так як в колективі з'являється незалежна група. Поведінка незалежної групи визначається як апріорне ($P_s = \alpha_s$), порядок системи зменшується, а нова матриця B^* як нерозкладний мінор матриці B зберігає всі необхідні властивості. Система (2.3) знову має єдине та невід'ємне рішення.

2.2. Дослідження моделі поведінки особистості під впливом соціологічної інформації

Для дослідження моделі поведінки особистості під впливом соціологічної інформації розглянемо абстрактний приклад щодо президентських виборів, запропонований у [23] і який більш детально було розглянуто у [30]. Як і в наведеному прикладі у якості елементарного суспільного осередку візьмемо середньостатистичну сім'ю з чотирьох осіб. До складу сім'ї включимо також джерело інформації – канал інформаційного впливу, під яким будемо розуміти усі медіа (Інтернет-видання, соціальні мережі, телебачення, радіо, та ін.), під дією яких перебувають члени сім'ї. Приймемо також, що такий канал інформаційного впливу має "власну думку".

Таким чином, в обраній умовній сім'ї є п'ять суб'єктів. Один з них, далі іменований як канал інформаційного впливу, має такі параметри: $\mu = 1$,

$P_0 = \alpha_0$. Тобто, канал інформаційного впливу цілком і повністю підтримує одного з лідерів президентської гонки. Для інших членів сім'ї встановимо: $P_j = P$, $\alpha_j = \alpha$, $\mu_j = \mu$. Скористаємось формулою (2.3), для якої отримаємо аналітичне рішення при $\lambda_{j,i} = \frac{1-\delta_{j,i}}{N-1}$:

$$P_j = \alpha_j \mu_j + \left(1-\mu_j\right)\frac{\sum_{i=1}^{N}\left(1-\delta_{j,i}\right)P_i}{N-1},\ j=\overline{1,N}. \tag{2.11}$$

Ця система має аналітичне рішення

$$P_j = \frac{N-1}{N-\mu_j}\alpha_j\mu_j + N\left(\frac{1-\mu_j}{N-\mu_j}\right)\frac{\sum_{i=1}^{N}\left(\frac{\alpha_i\mu_i}{N-\mu_i}\right)}{\sum_{i=1}^{N}\left(\frac{\mu_i}{N-\mu_i}\right)}, \tag{2.12}$$

$$\frac{M}{N} = \frac{\sum_{i=1}^{N}\left(\frac{\alpha_i\mu_i}{N-\mu_i}\right)}{\sum_{i=1}^{N}\left(\frac{\mu_i}{N-\mu_i}\right)}. \tag{2.13}$$

Тут $M = \sum_{i=1}^{N} P_i$ – математичне очікування числа членів сім'ї, які перейшли до даного стану.

Для зручності замінимо N на $N+1$, щоб відокремити канал інформаційного впливу від живих членів сім'ї. Формули (2.12, 2.13) після перетворень дають результат, який можна зазначити наступним чином:

$$P = \frac{M}{N} = \frac{N\alpha\mu + (1-\mu)\alpha_0}{1+(N-1)\mu}. \qquad (2.14)$$

При N = 4 отримуємо

$$P = \frac{M}{4} = \frac{4\alpha\mu + (1-\mu)\alpha_0}{1+3\mu}. \qquad (2.15)$$

Параметр μ встановимо рівним 0.5, розраховуючи на “середньо залежну” особистість, а параметр $\alpha_0 = 1$, так як канал інформаційного впливу повністю на стороні одного з кандидатів у президенти – лідерів гонки.

Як правило, виборчі кампанії проводяться у три етапи. Перший етап починається задовго до передвиборчої кампанії. На цьому етапі медіа заповнені щодо результатів соціологічних опитувань. У нашому прикладі канал інформаційного впливу переконує виборців про відсутність інших альтернатив, крім лідируючого кандидата. Другий етап, як правило, збігається з початком офіційної передвиборчої кампанії перед першим туром. На цьому етапі агітація через канал інформаційного впливу посилюється. Третій етап, у проміжку між першим і другим турами, характеризується ще більшим посиленням інформаційного тиску на виборців.

Проведемо дослідження на кожному з етапів, де використовуватимемо формулу (2.15). Причому, вважатимемо, що апостеріорна ймовірність P наприкінці попереднього етапу стає апріорною α на початку наступного. На всіх етапах канал інформаційного впливу має $\alpha_0 = 1$ і тому формулу (2.15) можна подати у вигляді

$$P^{(n)} = \frac{4P^{(n-1)} + 1}{5}, P^{(0)} = \alpha^{(1)}. \quad (2.16)$$

Як видно з (2.14), величина ймовірності P – це частка виборців, готових проголосувати за лідируючого кандидата. Такі рейтинги регулярно повідомляються каналами інформаційного впливу за результатами соціологічних опитувань населення.

Щоб дослідити роль каналу інформаційного впливу у виборчій кампанії за цією моделлю встановимо початковий рейтинг кандидата у президенти до початку першого етапу на рівні $P^{(0)} = \alpha^{(1)} = 0$. Тоді, за формулою (2.16), на кінець першого етапу перед офіційною передвиборчою кампанією канал інформаційного впливу створить кандидатові рейтинг $P^{(1)} = 0.2$, тобто 20% виборців готові віддати свій голос за цього кандидата. До кінця другого етапу, перед першим туром голосування, з (2.16) випливає, що за лідируючого кандидата будуть готові віддати свої голоси вже 36% населення, тобто $P^{(1)} = 0.36$. У статті [23] для такого прикладу показано, що при такому підході досягається розбіжність у результатах на рівні 0.72%, а відносна похибка складає 0.0223, тобто близько 2%.

На третьому етапі модель дає результат $P = 0.488$, тобто вже 48.80% виборців будуть готові віддати свої голоси за лідируючого кандидата. Як бачимо, всі ці показники досягнуті завдяки роботі каналу інформаційного впливу при $\mu_j = 0.5$ – середній залежності членів сім'ї від думок інших членів та самого каналу інформаційного впливу.

Алгоритм визначення залежності апостеріорної ймовірності впливу від стійкості особистості до інформаційного впливу. Розглянувши попередній приклад виникає питання, якою є залежність апостеріорної ймовірності P_j від початкової ймовірності α_j та стійкості особистості μ. Дослідження проведемо за наступним алгоритмом:

1. $n \leftarrow$ – введення числа ітерацій.

2. $\{\mu_j\}, j = \overline{1,m}$ – введення множини значень ступеня незалежності особистості.

3. $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ – формування одиничної матриці.

4. $\Lambda = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ – формування матриці інформаційного впливу.

5. $Do\left[j = \overline{1,m} \right]$ – цикл розрахунку за кількістю варіантів ступеня незалежності особистості.

6. $M = \begin{pmatrix} \mu_j & 0 \\ 0 & 1 \end{pmatrix}$ – формування матриці незалежності переконань.

7. $i = 1$ – встановлення початкового значення числа ітерацій.

8. $\mathrm{A} = (0,1)$ – введення початкового значення вектора апріорних переконань.

9. $P_{j,1} = \mathrm{A}$ – введення початкового значення вектора апостеріорних переконань.

10. $Do\left[i = \overline{1,n} \right]$ – цикл розрахунку за кількістю ітерацій.

11. $\mathrm{A} = \mathrm{A} \cdot M + (E - M) \cdot \Lambda \cdot \mathrm{A}^{\mathrm{T}}$ – визначення значення переконань для *i*-ї ітерації.

12. $P_{j,i+1} = (\alpha_1, \alpha_2)$ – запам’ятовування отриманого значення.

13. $i = i + 1$ – перехід до нової ітерації.

14. End $Do[n-1]$ – кінець циклу ітерацій.

15. End $Do[m]$ – кінець циклу за окремими варіантами ступеня незалежності особистості.

16. Print [$P_j, j = \overline{1,m}$] – виведення результатів.

Використовуючи розроблений алгоритм обчислимо значення ймовірності апостеріорних переконань P_j для різних значень ступеня незалежності особистості $\mu = \{0.5, 0.8, 0.9, 0.95, 0.99\}$, взявши за основу, що початкові переконання особистості $\alpha_{особ} = 0$, а каналу інформації $\alpha_{кан} = 1$. Обчислення будемо проводити для 50 ітерацій (стільки разів особистість прослуховує/переглядає канал впливу). В результаті обчислень (рис. 2.1) отримуємо, що при середніх і тим більше при низьких значеннях $\mu \le 0.5$ особистість достатньо швидко (вже після перших 5-7 сеансів перегляду інформації) схиляється до думки каналу інформаційного впливу і, з точки зору каналу інформаційного впливу, подальші раунди переконання такої особистості є практично зайвими.

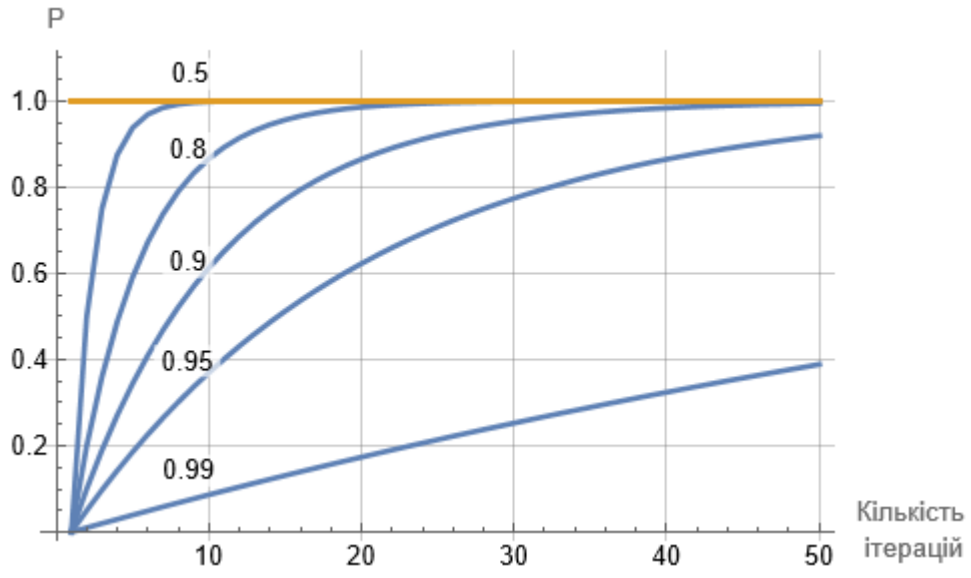


Рис. 2.1. Залежність апостеріорних переконань особистості від різних значень ступеня її незалежності $\mu_j, j = \overline{1,m}$

Картина суттєво змінюється при високих значеннях $\mu \ge 0.95$. У такому випадку особистість є досить “стійкою” відносно інформаційного впливу і зберігає здатність протидіяти йому. Навіть після 50 ітерацій ймовірність P_j

у такої особистості ще не досягає 1 і залишає особистості шанс на самостійне мислення.

Загальна залежність апостеріорного відношення особистості від ступеня незалежності, початкових переконань та різного впливу каналів інформації. У попередньому прикладі було досліджено випадок, коли особистість знаходиться під дією одного каналу інформаційного впливу. Разом з тим, сучасна людина отримує інформацію з багатьох джерел, які за своєю природою можуть мати різний ступінь довіри окремих особистостей. У такому випадку цікаво дослідити загальну залежність апостеріорного відношення від апріорного, ступеня незалежності та різної довіри особистостей до каналів інформації.

Припустимо, що особистість перебуває під дією 4-х джерел інформації з різним ступенем довіри до них (табл. 2.1). При цьому, як вже зазначалося, $\sum_{j=1}^{n} \lambda_{i,j} = 1$.

Таблиця 2.1

Значення довіри до каналів інформації

j / i	Значення $\lambda_{i,j}$			
	Джерело 1	Джерело 2	Джерело 3	Джерело 4
Варіант 1	0.7	0.1	0.1	0.1
Варіант 2	0.25	0.25	0.25	0.25
Варіант 3	0.01	0.01	0.01	0.97

Використовуючи формулу (2.6) та обравши у якості початкових значень апостеріорної ймовірності $P_j = \{1, 0.2, 0.7, 0.1\}$ отримаємо (рис. 2.2). Як видно з рис. 2.2 різне співвідношення між каналами інформаційного

впливу дає лише різний нахил площини, що описує апостеріорне відношення особистості до події P_j. Сам же характер залежності залишається сталим. При $\alpha_j \to 0$ і $\mu_j \to 1$ апостеріорне відношення особистості до події P_j прагне до 0, оскільки незалежна особистість навряд чи змінюватиме свої переконання під дією каналів інформаційного впливу. Ріст $\alpha_j \to 1$ при тому самому $\mu_j \to 1$ призводить до $P_j \to 1$, оскільки у цьому випадку особистість так само залишиться при своїх переконаннях. Якщо ж розглянути значення P_j при $\mu_j = 0$, то можна побачити, що вони зашишаються сталими на проміжку $0 \le \alpha_j \le 1$ і дорівнюють консолідованому значенню впливу 4-х джерел у різних їх комбінаціях.

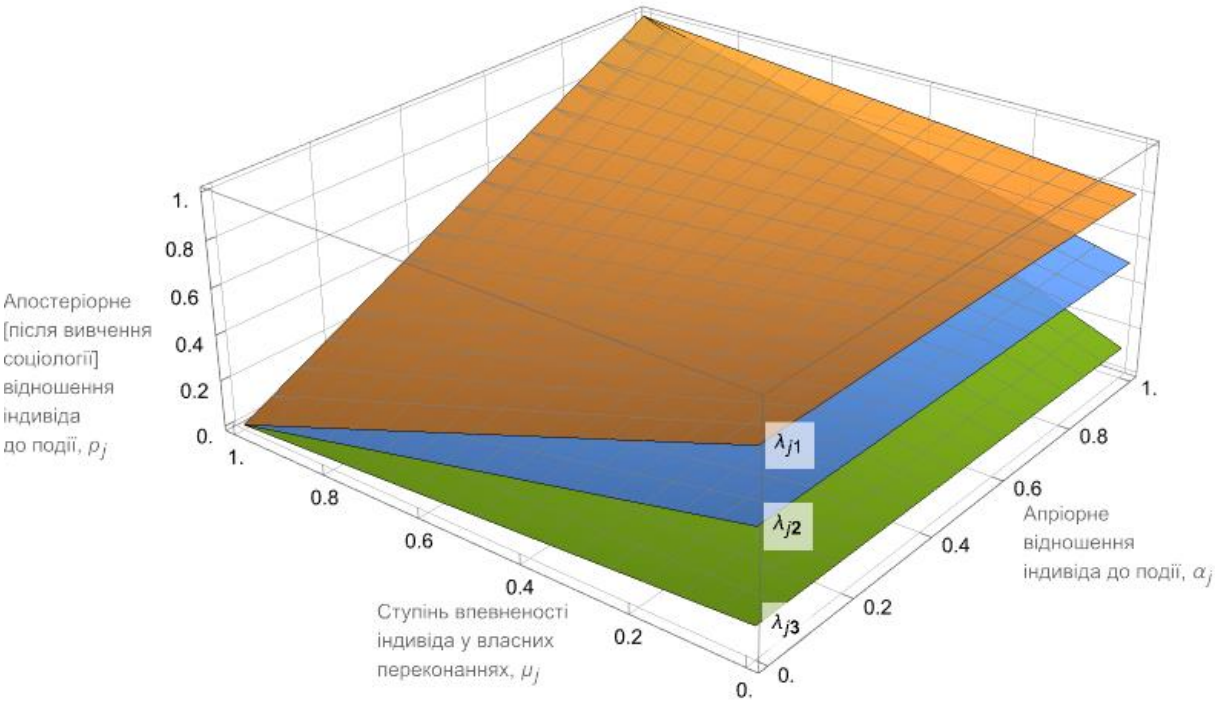


Рис. 2.2. Моделювання апостеріорного відношення особистості до події P_j у залежності від різних значень довіри до каналів інформації $\lambda_{i,j}$ та персональних параметрів μ_j та α_j

Таким чином, як бачимо, забезпечено адекватність удосконаленої моделі поведінки особистості під впливом соціологічної інформації, яка на відміну від моделі запропонованої у [23], дозволяє комплексно врахувати вплив на особистість каналів інформаційного впливу з результатами соціологічних досліджень.

2.3. Обґрунтування підходу щодо забезпечення інформаційної захищеності особистості під впливом соціологічної інформації

Якщо модель поведінки дає можливість оцінити зміну поведінки особистості під дією каналів інформаційного впливу, то виникає питання: чи можна у такому випадку використати такий підхід у зворотному напрямку – для забезпечення інформаційної захищеності особистості? У такому випадку, для забезпечення інформаційної захищеності особистості доцільно було б поставити за мету досягнення такого показника μ_j, який би при будь-яких зусиллях каналу інформаційного впливу ($\alpha = 1$) давав можливість забезпечити результуюче значення *P* не більше певного порогу. Встановимо такий поріг на рівні $P^* = 0.5$, виходячи з того, що ця величина не дасть змоги "перемогти" каналу інформаційного впливу за будь-якої кількості альтернатив вибору.

Для прикладу з виборами дослідимо тепер, як змінюватиметься величина *P* у залежності від кількості членів сім'ї та показника μ_j. На рис. 2.3 наведено залежність показника *P* для різної кількості членів сім'ї від 1 до 4. При цьому 0 означає, що канал інформаційного впливу "залишається один" протягом всієї виборчої кампанії і агітує за лідируючого кандидата. Відтак і *P* = 1.0. Якщо ж людину залишити сам на сам з каналом

інформаційного впливу, то показник P ймовірності того, що людина проголосує за лідируючого кандидата також наближається до 1. Лише збільшення кількості членів сім'ї (оточення особистості), у якій окремі особистості мають власну думку і незалежність мислення, зменшує ймовірність P (рис. 2.3).

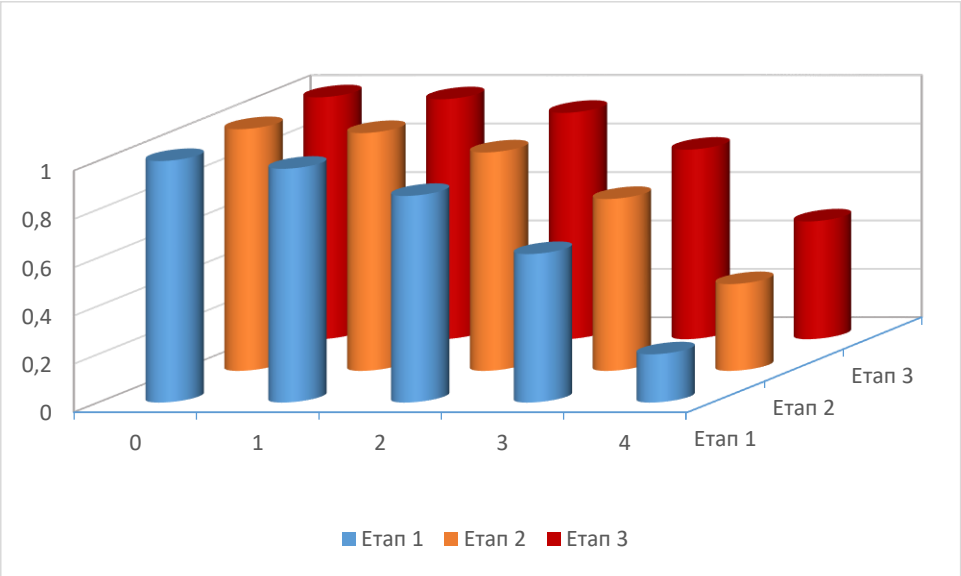


Рис. 2.3. Залежність P за етапами виборчої кампанії від кількості членів колективу ($\mu_j = 0.5$)

При збільшенні незалежності мислення членів сім'ї до $\mu_j = 0.8$ картина змінюється (рис. 2.4) і тепер вже навіть один член сім'ї, який залишився сам на сам з каналом інформаційного впливу протягом всієї виборчої кампанії, не має однозначної думки, хоча і у такому випадку говорити про інформаційну захищеність особистості ще немає підстав. Лише коли у сім'ї (колективі) є 2 та більше членів, у яких $\mu_j = 0.8$, можна говорити про забезпечення інформаційної захищеності членів сім'ї. У такому випадку "тиск" каналу інформаційного впливу на окрему особистість нівелюється поглядами інших членів сім'ї і значення P на кінець третього етапу становить менше 0.5.

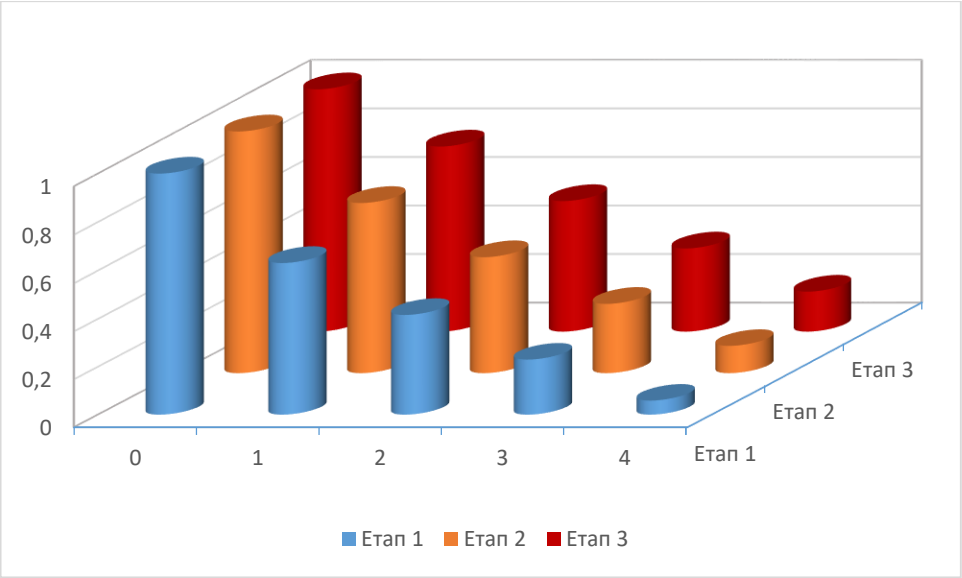


Рис. 2.4. Залежність P за етапами виборчої кампанії від кількості членів колективу ($\mu_j = 0.8$)

У протилежному випадку (рис. 2.5), коли члени сім'ї мають низький рівень незалежності поглядів ($\mu_j = 0.2$) свідчить про те, що навіть для сім'ї у повному складі інформаційна безпека для окремої особистості не забезпечується.

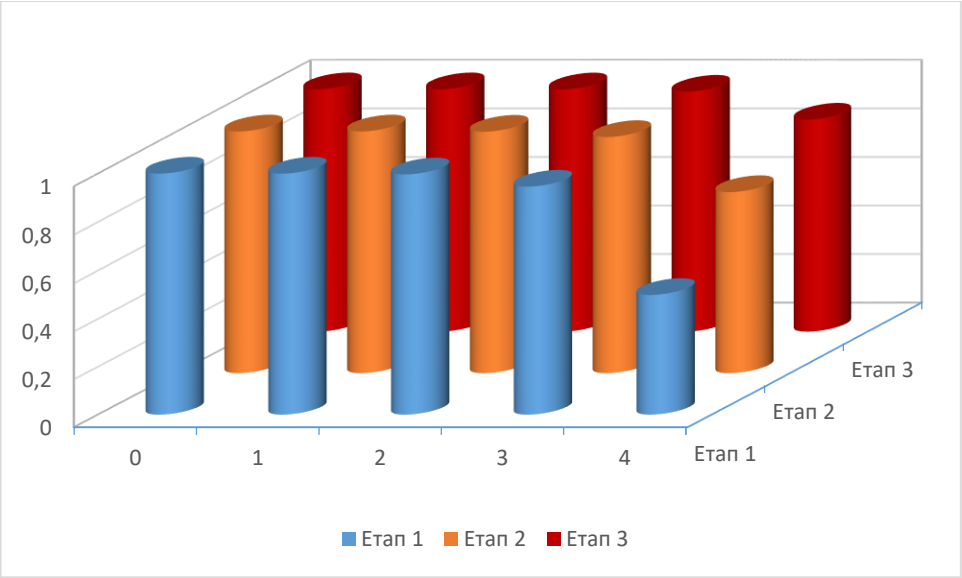


Рис. 2.5. Залежність P за етапами виборчої кампанії від кількості членів колективу $\mu_j = 0.2$

Як висновок, з проведеного розгляду випливає, що говорити про інформаційну захищеність особистості можна лише тоді, коли зазначена особистість володіє незалежністю думки $\mu_j \geq 0.8$ і перебуває в колективі, який складається з таких же незалежних однодумців.

2.4. Розробка моделі інформаційної захищеності особистості

Особистість постійно перебуває під дією каналів інформаційного впливу. Логічно припустити, що одні канали будуть схиляти особистість до одних рішень, інші канали, які мають альтернативну спрямованість – до альтернативних рішень. Таким чином, як видно з попереднього розгляду, значення P_j для кожної окремо взятої особистості під дією каналів інформаційного впливу буде коливатися від деякого максимального значення $P^{\max}$ до мінімального значення $P^{\min}$.

Враховуючи вищезазначені викладки, у загальному випадку модель інформаційної захищеності особистості може бути сформульована наступним чином

$$\begin{array}{c} \Delta P_j = P_j^{\max}(\tau) - P_j^{\min}(\tau) \leq \delta, \\ P_j^{\min}(\tau) \leq \alpha_j \leq P_j^{\max}(\tau). \end{array}, \qquad (2.17)$$

де: $P_j^{\max}(\tau)$, $P_j^{\min}(\tau)$ – відповідно максимальне та мінімальне значення P_j на протязі визначеного періоду часу τ; δ – деяке завчасно встановлене значення розкиду P_j.

Тобто, говорити про інформаційну захищеність особистості можна буде тоді, коли буде забезпечено умову (2.17), а саме: апостеріорна

ймовірність P_j переходу особистості до нового стану під дією інформації каналу інформаційного впливу буде залишатися у певних межах відносно її апріорної ймовірності α_j.

Для утримання P_j в заданих межах δ особистості, у залежності від початкових переконань α_j, ступеня незалежності μ_j та рівня довіри до каналу інформаційного впливу $\lambda_{j,i}$ необхідно мати власну стратегію "перемикання" каналів. Для спрощення розуміння будемо розглядати особистість, яка перебуває під впливом двох альтернативних каналів. Звісно, що у реальному житті таких каналів, які оточують і впливають на особистість, значно більше, але в багатьох випадках вся множина каналів може бути поділена на дві протилежні групи: "підтримую", "не підтримую"; "згоден", "не згоден"; "позитивно", "негативно" та ін.

При такому підході ключовою стратегією забезпечення інформаційної захищеності особистості буде стратегія "перемикання каналів" між двома альтернативами, яка задовольнятиме співвідношенню (2.17).

Стратегія перемикання каналів при суттєвому впливі (Стратегія-1). Дослідимо запропоновану модель на адекватність шляхом моделювання. Для цього скористаємося наступним алгоритмом [42].

Алгоритм 1.

1. $I \leftarrow$ введення кількості ітерацій;
2. $\alpha \leftarrow$ введення значення початкових переконань особистості;
3. $\mu \leftarrow$ введення значення незалежності особистості;
4. $\mathrm{A} = (\alpha, 1, 0)$ – формування вектора початкових переконань;
5. $M = \begin{pmatrix} \mu & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ – формування матриці незалежності;

6. $E = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ – формування одиничної матриці;

7. $\Lambda_1 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$; $\Lambda_2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ – формування матриць довіри до каналів інформаційного впливу;

8. $R = Table\left[\{0, \mathrm{A}_2, \mathrm{A}_3\}, \{I\}\right]$ – формування масиву результатів обчислень;

9. $C = Table\left[0, \{I-1\}\right]$ – формування масиву каналів інформаційного впливу;

10. $c_1 = 0; c_2 = 0$ – встановлення початкових значень лічильника каналів;

11. $i = 1$ – встановлення початкового значення лічильника ітерацій;

12. $Do\left[\, j = \overline{1, I-1}\right]$ – цикл розрахунку апостеріорної ймовірності;

13. $If\left[$ – перевірка на виконання умови суттєвого впливу;

14.
$$Abs\left[\left(\mathrm{A}\cdot M + \left(E-M\right)\cdot \Lambda_1 \cdot \mathrm{A}^{\mathrm{T}}\right)_1 - \alpha\right] \le$$
$$\le Abs\left[\left(\mathrm{A}\cdot M + \left(E-M\right)\cdot \Lambda_2 \cdot \mathrm{A}^{\mathrm{T}}\right)_1 - \alpha\right],$$
$$\mathrm{A} = \mathrm{A}\cdot M + \left(E-M\right)\cdot \Lambda_1 \cdot \mathrm{A}^{\mathrm{T}}; c_1 = c_1 + 1; C_i = 1,$$
$$\mathrm{A} = \mathrm{A}\cdot M + \left(E-M\right)\cdot \Lambda_2 \cdot \mathrm{A}^{\mathrm{T}}; c_2 = c_2 + 1; C_i = 2$$

15. $\left]$ – кінець умовного оператора;

16. $R_{i+1} = \mathrm{A}$ – запам’ятовування результату;

17. $i = i + 1$ – перехід до нової ітерації;

18. $\left]$ – кінець циклу;

19. $Plot\left[R\right]$ – виведення результатів.

Для початку оберемо стратегію “перемикання каналів при суттєвому впливі на особистість”. Відповідно до цієї стратегії особистість буде змінювати канал інформації на альтернативний лише тоді, коли така зміна

інформаційного потоку призведе до більшої зміни P_j (у протилежну сторону), ніж коли канали між інформаційними повідомленнями не будуть перемикатися.

Вхідні умови:

кількість ітерацій (сеансів впливу на особистість): 50;

початкове значення апріорних переконань особистості: $\alpha_j = 0.0$;

початкове значення ступеня незалежності особистості: $\mu_j = 0.0$;

крок зміни початкових переконань особистості (α_j): 0.1;

крок зміни ступеня незалежності особистості (μ_j): 0.1.

Змінні для визначення:

$P_j^{\max}(\tau)$ – максимальне значення апостеріорної ймовірності P_j протягом часу τ;

$P_j^{\min}(\tau)$ – мінімальне значення апостеріорної ймовірності P_j протягом часу τ;

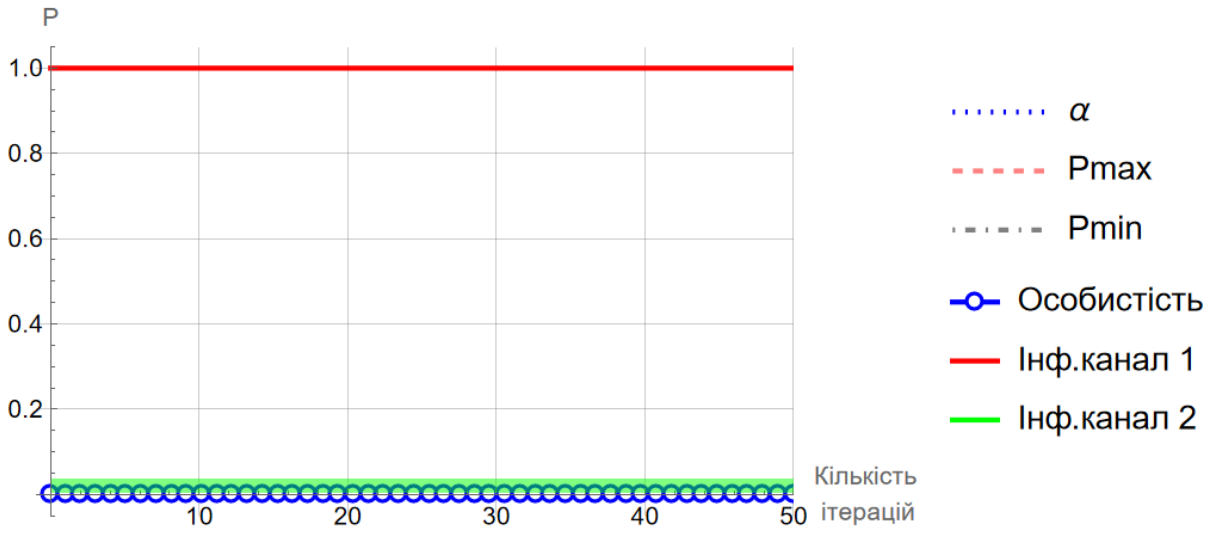
$\Delta P_j = P_j^{\max}(\tau) - P_j^{\min}(\tau)$ – динаміка зміни апостеріорної ймовірності P_j протягом часу τ;

$\text{Channel 1}, \text{Channel 2}$ – кількість перемикань каналів інформаційного впливу.

Наведемо окремі графіки та прокоментуємо можливі варіанти реалізації стратегії “перемикання каналів при суттєвому впливі на особистість”.

На рис. 2.6 показано, що при нульових значеннях ($\alpha_j = 0.0$, $\mu_j = 0.0$), коли особистість не володіє хоч якоюсь незалежністю в поглядах, її P_j при будь якому інформаційному впливі дорівнює 0 і жодні спроби вивести її з цього стану є марними, оскільки канал інформаційного впливу (Канал 2) у будь якому разі буде зводити всі зусилля нанівець. У такому випадку

$\Delta P_j = 0$ і тому навряд чи можна говорити про хоч якусь інформаційну захищеність такої особистості.



α = 0. μ = 0.

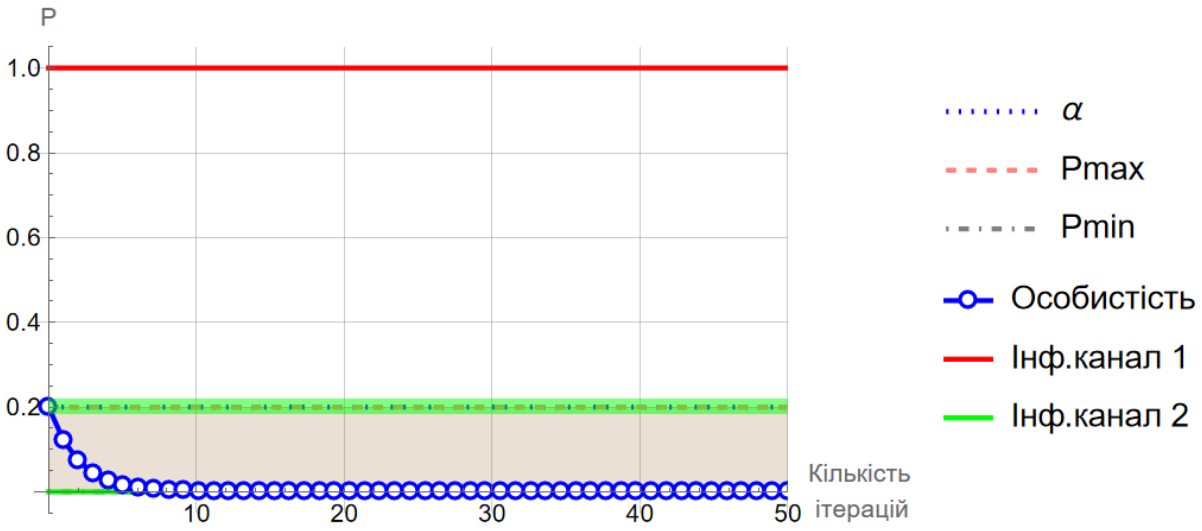
Channel 1 = 0 Channel 2 = 49

Pmax = 0. Pmin = 0.

Рис. 2.6. Результати моделювання при $\alpha_j = 0.0$, $\mu_j = 0.0$

Майже аналогічна картина спостерігається на рис. 2.7, ($\alpha_j = 0.2$, $\mu_j = 0.6$), де можна побачити, що навіть при достатньо суттєвому рівні незалежності особистості ($\mu_j = 0.6$) $P_j \to 0$ оскільки інформаційний вплив, який чинить Канал 2, є набагато сильнішим і жодні спроби перемикання каналу інформаційного впливу на Канал 1 не дають суттєвого результату. У такому випадку також не можна говорити про інформаційну захищеність особистості.

Зміну картини можна побачити при збільшенні ступеня незалежності особистості до 0.8 ($\alpha_j = 0.2$, $\mu_j = 0.8$), рис. 2.8.

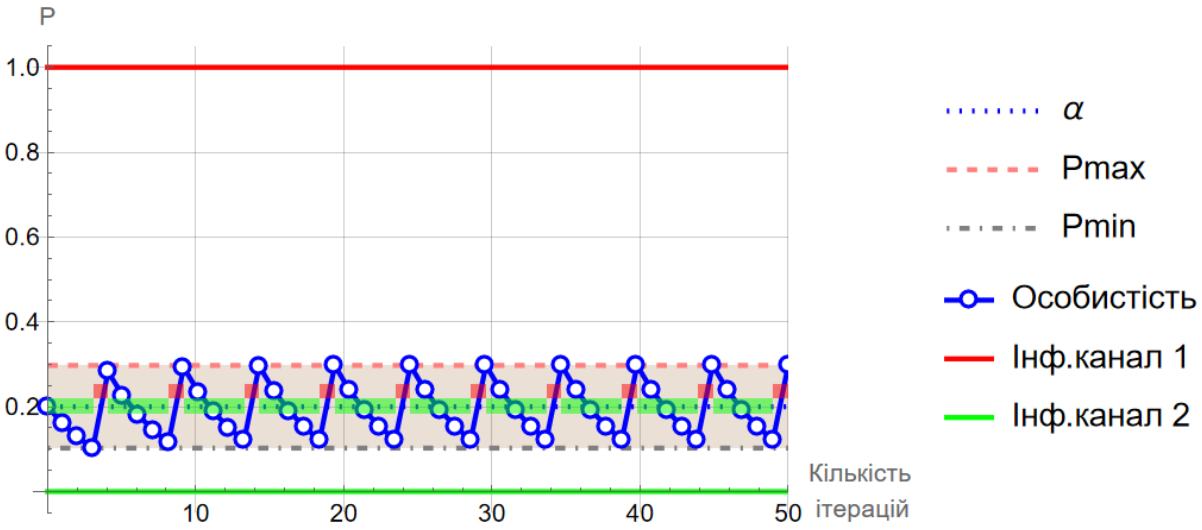


α = 0.2 μ = 0.6

Channel 1 = 0 Channel 2 = 49

Pmax = 0.2 Pmin = 2.7×10^{-12}

Рис. 2.7. Результати моделювання при $\alpha_j = 0.2$, $\mu_j = 0.6$



α = 0.2 μ = 0.8

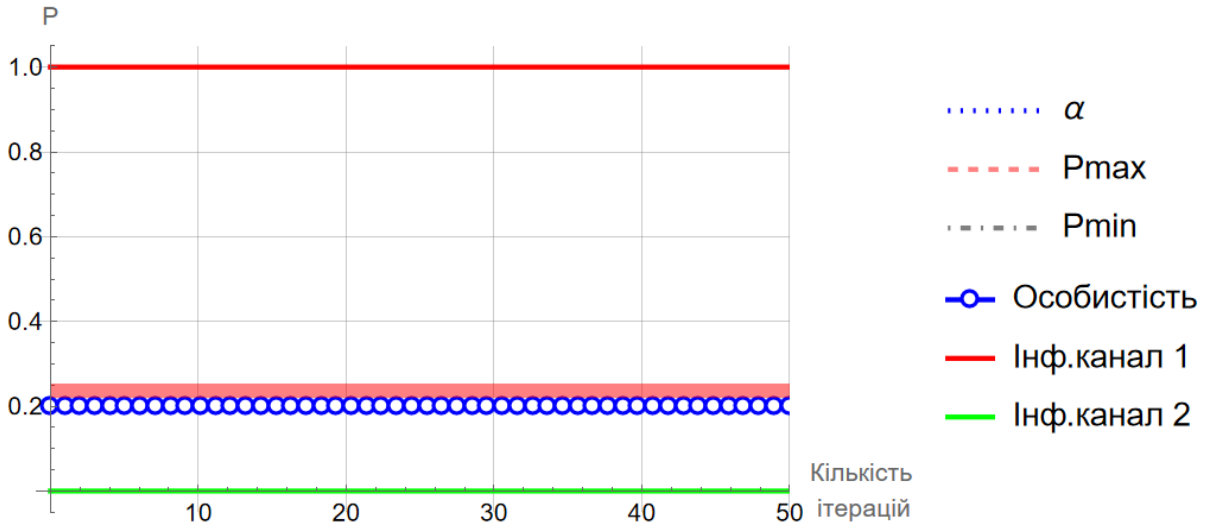
Channel 1 = 10 Channel 2 = 39

Pmax = 0.3 Pmin = 0.1

Рис. 2.8. Результати моделювання при $\alpha_j = 0.2$, $\mu_j = 0.8$

Як бачимо з рис. 2.8, у цьому випадку в особистості з'являється можливість перемикання каналів і таке перемикання стає ефективним, даючи можливість особистості змінити інформаційну картину. Як бачимо, всього Канал 1 було увімкнуто 10 разів, тоді як Канал 2 – 39 разів. Це означає, що для забезпечення інформаційної захищеності особистості було достатньо кожного 5-го разу перемикатися на альтернативне джерело інформації. У цьому випадку забезпечуються прийнятні показники $P_j^{\max}(\tau)$ та $P_j^{\min}(\tau)$, а загальне відхилення ймовірностей $\Delta P_j = 0.2$, що можна вважати досить непоганим результатом і що дає можливість говорити про інформаційну захищеність особистості.

Логічно припустити, що повна інформаційна захищеність буде забезпечена при $\mu_j \to 1.0$, оскільки у такому випадку будь-які перемикання каналів є зайвими, особистість ні в якому разі не змінить своїх поглядів, і тому $P_j^{\max}(\tau)$ буде дорівнювати $P_j^{\min}(\tau)$, а $\Delta P_j \to 0$ (рис. 2.9).



α = 0.2 μ = 1.

Channel 1 = 49 Channel 2 = 0

Pmax = 0.2 Pmin = 0.2

Рис. 2.9. Результати моделювання при $\alpha_j = 0.2$, $\mu_j = 1.0$

Більш складними є випадки, коли особистість має певні початкові переконання $0.2 \le \alpha_j \le 0.8$, достатньо далекі від офіційних $\{0.0,1.0\}$, які транслюються каналами інформаційного впливу, і, в той же час має різний ступінь незалежності $0.0 \le \mu_j \le 1.0$. У такому випадку, для того щоб забезпечити інформаційну захищеність особистості доведеться достатньо активно “маніпулювати” перемикачем каналів, постійно змінюючи їх контентну спрямованість.

На рис. 2.10 наведено варіант $\alpha_j = 0.4$, $\mu_j = 0.4$. Для утримання апостеріорної ймовірності P_j близько до апріорної α_j особистості необхідно постійно перемикати канали, змінюючи тим самим характер інформаційних потоків. Так, як бачимо, Канал 1 було увімкнуто 16 разів, Канал 2 – 33 рази. При цьому вдалося забезпечити $P_j^{\max}(\tau) = 0.66$ та $P_j^{\min}(\tau) = 0.1$, а $\Delta P_j = 0.56$.

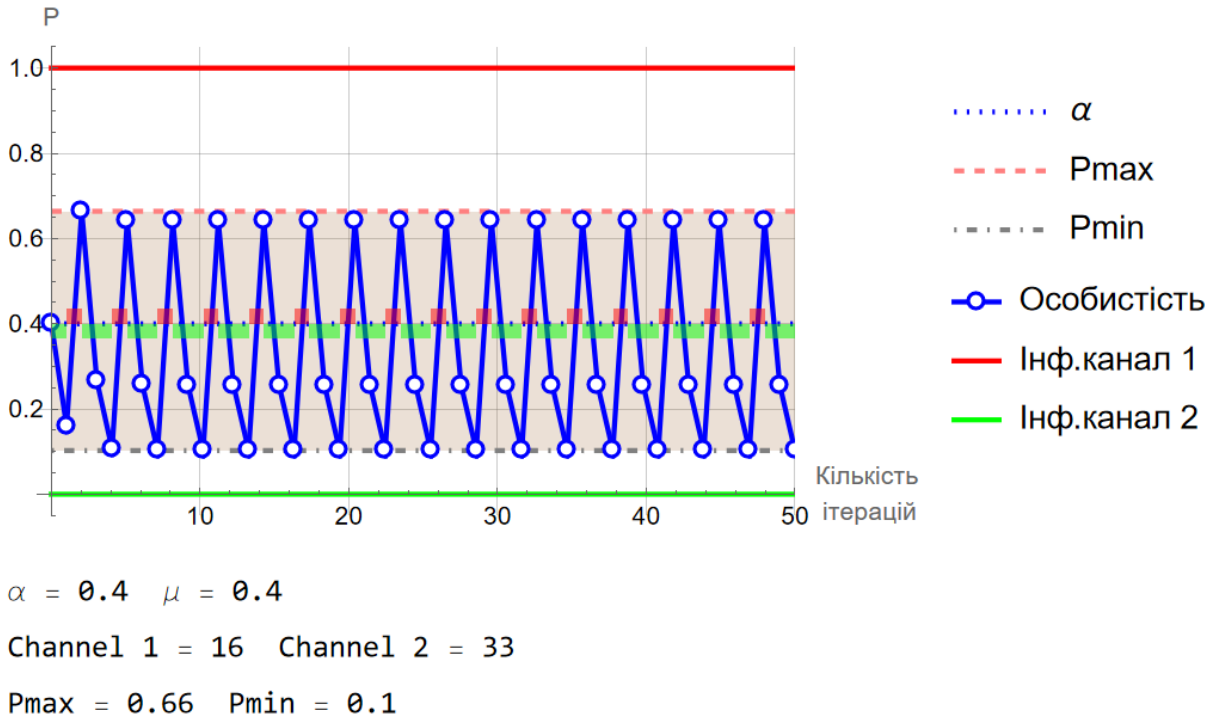


Рис. 2.10. Результати моделювання при $\alpha_j = 0.4$, $\mu_j = 0.4$

Значення $\Delta P_j = 0.56$ (рис. 2.10) свідчить про те, що особистість, хоча і залишається "при своїх поглядах", разом з тим достатньо сильно коливається у процесі збереження інформаційної захищеності. Звуження значення ΔP_j є можливим при збільшенні μ_j. Так, у випадку $\mu_j = 0.8$ цей параметр зменшується до $\Delta P_j = 0.18$ (рис. 2.11). При цьому особистість для збереження інформаційної захищеності потребуватиме більш рівномірного перемикання каналів: Канал 1 увімкнено 20 разів, Канал 2 – 29 разів.

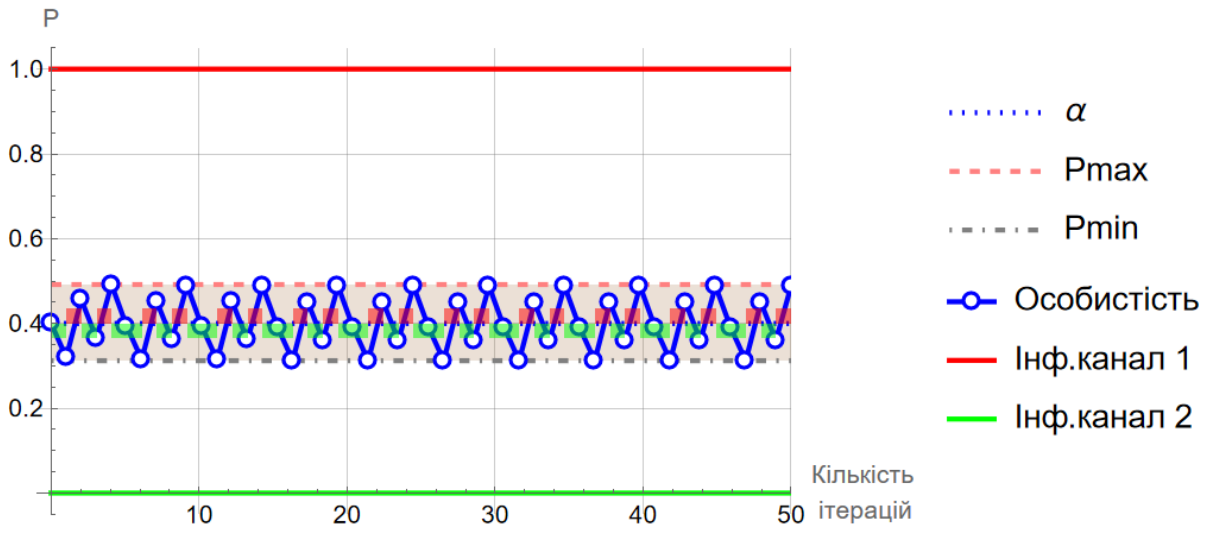
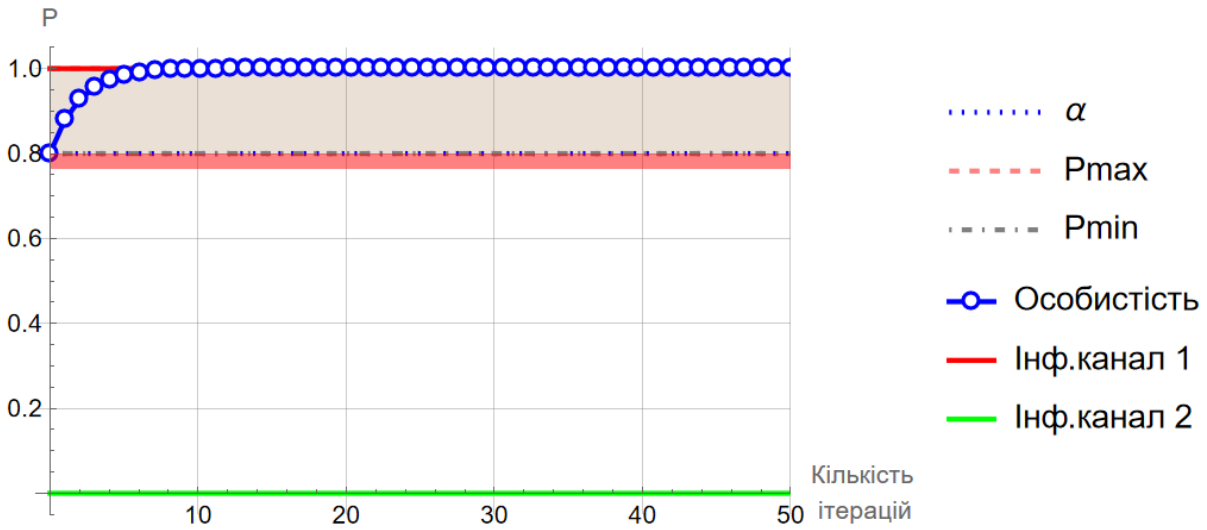


Рис. 2.11. Результати моделювання при $\alpha_j = 0.4$, $\mu_j = 0.8$

Як і раніше, при достатньо високих значеннях $\alpha_j \geq 0.8$ та недостатніх значеннях $\mu_j \leq 0.8$ спостерігається "звалювання" апостеріорної ймовірності P_j до крайнього значення (у даному випадку 1.0) через те, що жодне альтернативне джерело не здатне "перетягнути" особистість на свою сторону. Така ситуація зображена на рис. 2.12. При цьому Канал 1 залишається увімкненим протягом всього періоду τ.



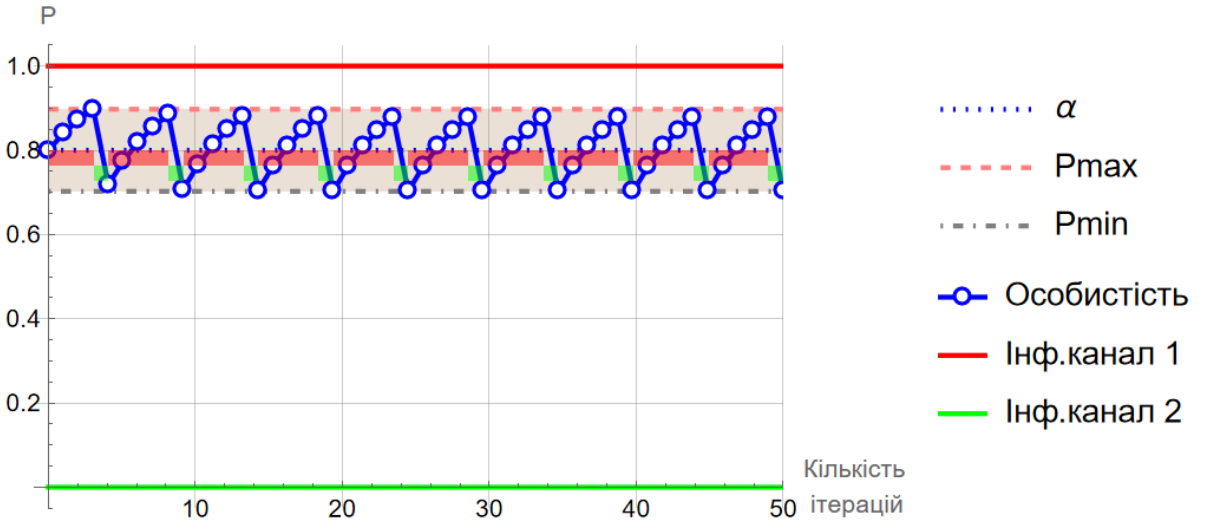
α = 0.8 μ = 0.6

Channel 1 = 49 Channel 2 = 0

Pmax = 1. Pmin = 0.8

Рис. 2.12. Результати моделювання при $\alpha_j = 0.8$, $\mu_j = 0.6$

Уникнути такої ситуації допомагає збільшення $\mu_j \geq 0.8$ (рис. 2.13), забезпечуючи при цьому $\Delta P_j = 0.2$.



α = 0.8 μ = 0.8

Channel 1 = 39 Channel 2 = 10

Pmax = 0.9 Pmin = 0.7

Рис. 2.13. Результати моделювання при $\alpha_j = 0.8$, $\mu_j = 0.8$

Узагальнені дані щодо дослідження моделі інформаційної захищеності особистості за Стратегією-1 наведено у таблиці 2.2.

Таблиця 2.2

Узагальнені дані щодо моделювання ΔP_j за Стратегією-1

у залежності від співвідношення α_j та μ_j

μ_j \ α_j	0.0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0
0.0	0.0	0.1	0.2	0.3	0.4	0.5	0.4	0.3	0.2	0.1	0.0
0.1	0.0	0.1	0.2	0.3	0.4	0.86	0.4	0.3	0.2	0.1	0.0
0.2	0.0	0.1	0.2	0.3	0.48	0.73	0.46	0.3	0.2	0.1	0.0
0.3	0.0	0.1	0.2	0.3	0.67	0.62	0.67	0.3	0.2	0.1	0.0
0.4	0.0	0.1	0.2	0.35	0.56	0.51	0.56	0.33	0.2	0.1	0.0
0.5	0.0	0.1	0.2	0.47	0.49	0.42	0.5	0.47	0.2	0.1	0.0
0.6	0.0	0.1	0.2	0.4	0.39	0.33	0.39	0.4	0.2	0.1	0.0
0.7	0.0	0.1	0.29	0.29	0.28	0.24	0.28	0.3	0.24	0.1	0.0
0.8	0.0	0.1	0.2	0.19	0.18	0.16	0.18	0.2	0.2	0.1	0.0
0.9	0.0	0.09	0.08	0.09	0.08	0.08	0.09	0.1	0.09	0.09	0.0
1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0

Як бачимо, у табл. 2.2 можна виділити декілька секторів, які описують інформаційну захищеність особистості (ΔP_j) у залежності від різного співвідношення її апріорних переконань α_j та ступеня незалежності суджень μ_j. Зелений сектор (високі значення $\mu_j \geq 0.8$ при будь-яких значеннях α_j) свідчить про те, що особистість з високим рівнем незалежності та при продуманій стратегії зміни каналів інформаційного

впливу здатна протистояти більшості інформаційних впливів і, тим самим, забезпечити власну інформаційну захищеність ($\Delta P_j \le 0.2$). Помаранчевий сектор визначає зону, в якій забезпечуються нижчі значення інформаційної захищеності особистості $0.2 < \Delta P_j \le 0.4$, обумовлені меншими значеннями μ_j. Різні відтінки рожевого кольору формують сектор, у якому забезпечення інформаційної захищеності є найбільш складним завданням через відсутність у особистості власних стійких переконань α_j та через низький рівень незалежності самої особистості μ_j.

Також, у табл. 2.2 присутні сектори жовтого кольору, які характеризуються достатньо низькими значеннями $\Delta P_j \le 0.2$. Такі ситуації також можуть свідчити про інформаційну захищеність особистості, але, разом з тим, характер інформаційної захищеності у даному випадку є іншим. У даному випадку особистість апріорі приймає одну з альтернативних точок зору і тому у подальшому, жодними маніпуляціями таку особистість неможливо переконати у зворотному. Таким чином, жовті сектори свідчать про інформаційну захищеність особистості “за замовчуванням”.

Стратегія перемикання каналів при найменшому впливі (Стратегія-2). Моделювання за стратегією перемикання каналів при суттєвому впливі підтверджує адекватність запропонованої моделі інформаційної захищеності особистості. Разом з тим, у даному модельному прикладі було розглянуто лише одну стратегію маніпулювання каналами інформаційного впливу. Є також і інші стратегії. Одна з них – “перемикання каналів при найменшому впливі”. Суть її полягає в тому, що особистість перемикає канали як тільки інформаційний вплив схиляє її в якусь зі сторін відносно її початкових переконань. Якщо при розгляді попередньої стратегії враховувався лише найбільш суттєвий вплив, який був здатен забезпечити зміну P_j на величину більшу, ніж був сумарний попередній вплив. То тепер,

особистість буде перемикати канали одразу ж після будь-якого впливу, що змінює погляди особистості.

Для реалізації такої моделі необхідно в Алгоритмі 1 замінити модуль перевірки умови (13 – 15) на інший:

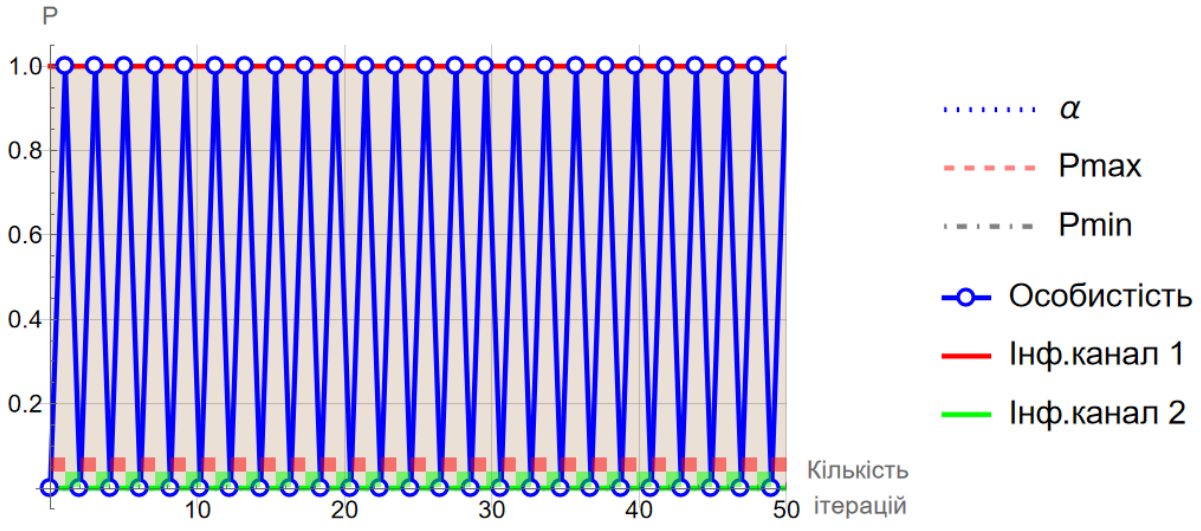
13. *If* [– перевірка на виконання умови найменшого впливу;

$$\mathrm{A}_1 > \alpha,$$

14. $$\mathrm{A} = \mathrm{A} \cdot M + (E - M) \cdot \Lambda_2 \cdot \mathrm{A}^{\mathrm{T}}; c_2 = c_2 + 1; C_i = 2,$$
$$\mathrm{A} = \mathrm{A} \cdot M + (E - M) \cdot \Lambda_1 \cdot \mathrm{A}^{\mathrm{T}}; c_1 = c_1 + 1; C_i = 1$$

15.] – кінець умовного оператора;

Відмінність цієї стратегії проявляється вже практично з перших кроків. Так, вже при $\alpha_j = 0.0$, $\mu_j = 0.0$ можна побачити (рис. 2.14), що особистість має перемикати канали практично одразу, не очікуючи будь-якого суттєвого впливу. При цьому $P_j^{\max}(\tau) = 1$, а $P_j^{\min}(\tau) = 0$, забезпечуючи при цьому $\Delta P_j = 1$.



α = 0. μ = 0.

Channel 1 = 25 Channel 2 = 24

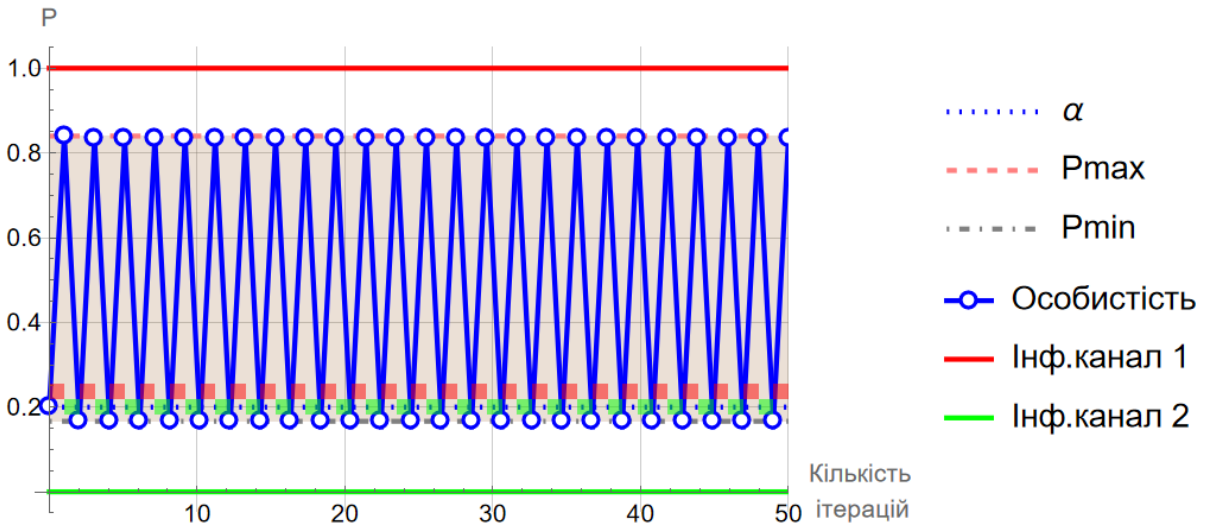
Pmax = 1. Pmin = 0.

ΔP = 1.

Рис. 2.14. Результати моделювання за Стратегією-2 при $\alpha_j = 0.0$, $\mu_j = 0.0$

Звісно, у такому випадку говорити про інформаційну захищеність неможливо, але загальна картина, у порівнянні з попередньою стратегією суттєво відрізняється і особистість не “звалюється” до однієї з полярних думок, а “блукає” в інформаційному просторі альтернатив.

Збільшення μ_j, як і при попередній стратегії, дає можливість звузити ΔP_j, забезпечуючи тим самим інформаційну захищеність особистості, починаючи з певних значень μ_j (рис. 2.15). Тут знову ж таки особистості доведеться маніпулювати каналами, але простір захищеності стає більш окресленим $\Delta P_j = 0.67$.



α = 0.2 μ = 0.2

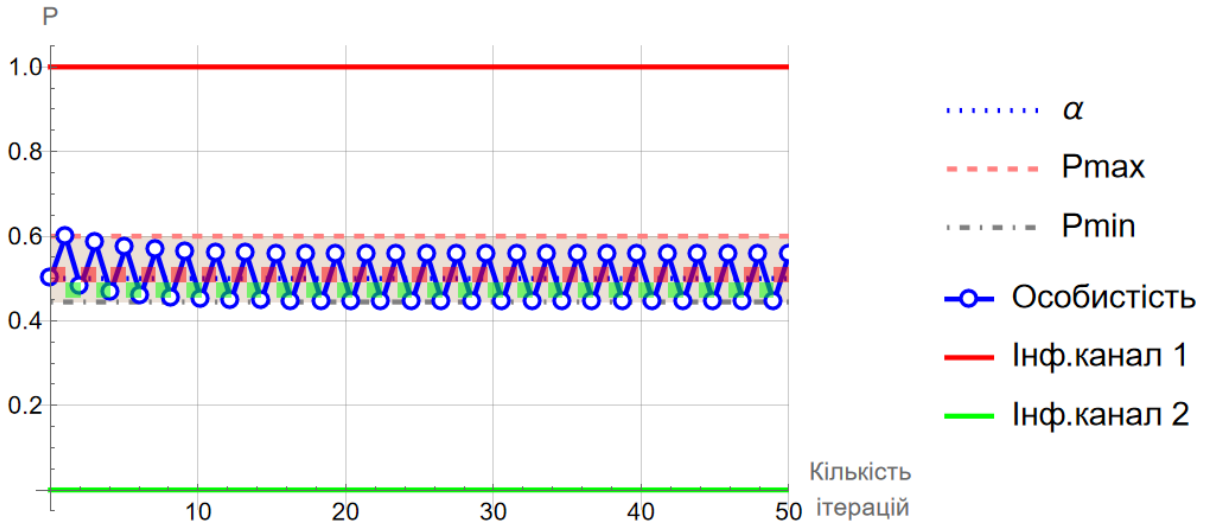
Channel 1 = 25 Channel 2 = 24

Pmax = 0.84 Pmin = 0.17

ΔP = 0.673333

Рис. 2.15. Результати моделювання за Стратегією-2 при $\alpha_j = 0.2$, $\mu_j = 0.2$

Подальше збільшення $\mu_j \geq 0.8$, практично незалежно від значень α_j, дозволяє говорити про наявність захищеності від інформаційного впливу, забезпечуючи при цьому $\Delta P_j \leq 0.2$ (рис. 2.16, 2.17).



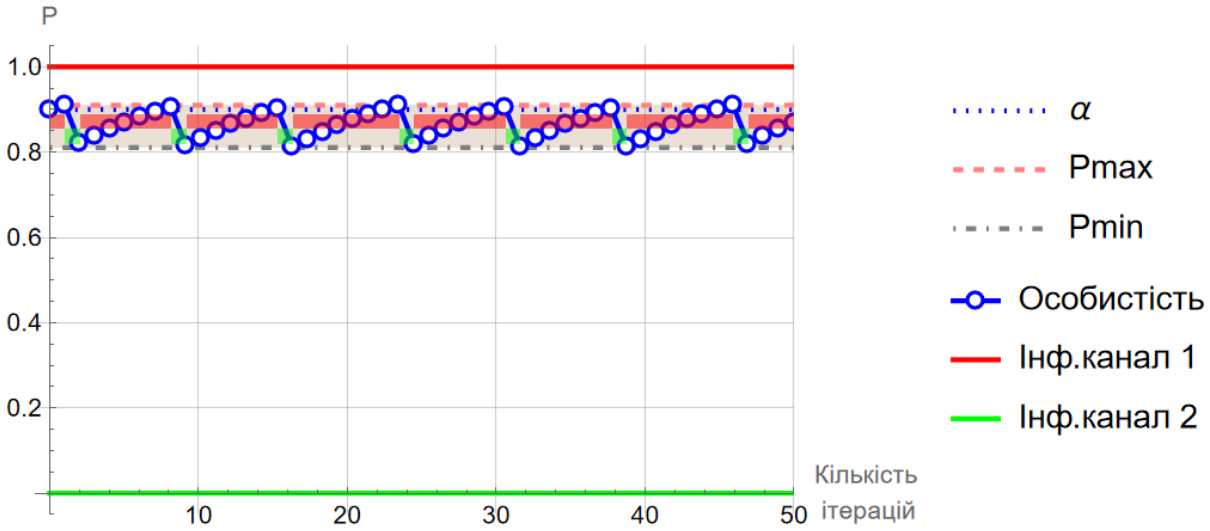
α = 0.5 μ = 0.8

Channel 1 = 25 Channel 2 = 24

Pmax = 0.6 Pmin = 0.44

△P = 0.155554

Рис. 2.16. Результати моделювання за Стратегією-2 при $\alpha_j = 0.5$, $\mu_j = 0.8$



α = 0.9 μ = 0.9

Channel 1 = 42 Channel 2 = 7

Pmax = 0.91 Pmin = 0.81

△P = 0.099342

Рис. 2.17. Результати моделювання за Стратегією-2 при $\alpha_j = 0.9$, $\mu_j = 0.9$

Як і при попередній стратегії, збільшення $\mu_j \to 1$ призводить до того, що апостеріорна ймовірність P_j наближається до апріорної α_j, а $\Delta P_j \to 0$. Таким чином, можна зробити тривіальний висновок, що незалежна особистість (яка має власне бачення на події і не сприймає інформацію, яка передається каналами інформаційного впливу), є інформаційно захищеною. Це ще раз підкреслює адекватність розробленої моделі та можливість її застосування для дослідження різноманітних процесів людського життя.

Узагальнені дані щодо дослідження моделі інформаційної захищеності особистості за Стратегією-2 наведено у таблиці 2.3. У цій таблиці, як і у табл. 2.2, також можна виділити декілька секторів. Зелений сектор (високі значення $\mu_j \geq 0.8$ при будь-яких значеннях α_j), як і раніше, свідчить про те, що особистість з високим рівнем незалежності та при заданій стратегії зміни каналів інформаційного впливу здатна протистояти більшості інформаційних впливів і, тим самим, забезпечити власну інформаційну захищеність $(\Delta P_j \leq 0.2)$. Помаранчевий сектор визначає зону, в якій забезпечуються нижчі значення інформаційної захищеності $0.2 < \Delta P_j \leq 0.4$, обумовлені меншими значеннями μ_j. Сектори рожевого кольору визначають значення ΔP_j, у якому забезпечення інформаційної захищеності є більш складним завданням через низький рівень μ_j.

Необхідно також звернути увагу на те, що у порівнянні з табл. 2.2 у табл. 2.3 немає секторів жовтого кольору. Це пояснюється іншим підходом до перемикання каналів, що забезпечує відсутність критичних зон у захищеності. А саме, перемикання каналів на альтернативний при найменшому впливі дозволяє особистості не бути упередженою навіть при безпосередній близькості до однієї з точок зору, яка транслюється джерелом інформації (звісно при наявності хоч якогось ступеня незалежності μ_j).

Таблиця 2.3

Узагальнені дані щодо моделювання ΔP_j за Стратегією-2

у залежності від співвідношення α_j та μ_j

μ_j \ α_j	0.0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0
0.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
0.1	0.9	0.82	0.83	0.84	0.85	0.86	0.87	0.88	0.89	0.9	0.9
0.2	0.8	0.79	0.67	0.69	0.71	0.73	0.75	0.77	0.79	0.77	0.8
0.3	0.7	0.67	0.7	0.56	0.59	0.62	0.65	0.68	0.66	0.69	0.7
0.4	0.6	0.6	0.58	0.43	0.47	0.51	0.55	0.59	0.56	0.6	0.6
0.5	0.5	0.48	0.46	0.49	0.37	0.42	0.47	0.5	0.47	0.48	0.5
0.6	0.4	0.36	0.34	0.4	0.27	0.33	0.39	0.33	0.39	0.4	0.4
0.7	0.3	0.28	0.29	0.29	0.3	0.24	0.3	0.25	0.3	0.29	0.3
0.8	0.2	0.19	0.19	0.18	0.19	0.16	0.2	0.17	0.18	0.19	0.2
0.9	0.1	0.1	0.1	0.07	0.1	0.08	0.1	0.1	0.1	0.1	0.1
1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0

Попередній розгляд та модельні приклади були наведені за умови, що параметри довіри особистості до офіційного та альтернативного каналів інформаційного впливу $\lambda_{j,i}$ дорівнював 1. Цей параметр входить до матриць впливу, які є складовою частиною моделі (2.4):

$$\Lambda_1 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}; \ \Lambda_2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Разом з тим, у реальному житті ступінь довіри до джерела інформації не завжди буває 100%-м. Більше того, на особистість, як правило, чинить вплив ціла низка каналів інформаційного впливу, які можуть бути як об’єднаними за тематичною спрямованістю, так і опозиційними один до одного. Відтак є необхідність розглядати дані соціологічних досліджень більш детально, встановлюючи у кожному окремому випадку для особистості ступінь довіри до конкретного каналу $\lambda_{j,i}$. Також, не слід забувати, що в цілому особистість, яка перебуває під дією декількох каналів, отримує деякий сумарний вплив і $\sum_{i=1}^{n} \lambda_{j,i} = 1$.

Висновки до розділу 2

1. Для формування загальної моделі інформаційної захищеності особистості від впливу результатів соціологічних досліджень найбільш доцільно взяти існуючу модель конформної поведінки людини з урахуванням її апріорних переконань, ступеня незалежності мислення та впливу оточення на особистість. Разом з тим, така модель має бути удосконалена з урахуванням особливостей сприйняття особистістю результатів соціології, зокрема, на відміну від поведінки в колективі, особистість не може безпосередньо впливати на результати соціології.

2. Удосконалена модель поведінки особистості під впливом соціологічної інформації, в основу якої покладено базову модель конформної поведінки людини з урахуванням її апріорних переконань та ступеня незалежності мислення, має бути розширена за рахунок використання коефіцієнтів впливу на особистість джерел соціологічної інформації, що дозволить враховувати рівень довіри особистості до джерела

соціологічної інформації та особливості сприйняття особистістю результатів соціологічних досліджень.

3. Основним підходом щодо забезпечення інформаційної захищеності особистості має бути вирішення оберненої задачі оцінки зміни поведінки особистості під дією каналів інформаційного впливу. У такому випадку, для забезпечення інформаційної захищеності особистості основною метою буде досягнення такого показника ступеня незалежності особистості μ_j, який би при будь-яких зусиллях каналу інформаційного впливу ($\alpha = 1$) давав можливість забезпечити результуюче значення апостеріорної ймовірності для особистості P не більше певного порогу. Іншим підходом щодо забезпечення заданого значення P є управління потоком інформації, що надходить до особистості від джерел соціології.

4. Вперше розроблена модель інформаційної захищеності особистості базується на концепції управління каналами інформаційного впливу на основі ймовірнісного контролю з використанням результатів моделювання поведінки особистості під впливом соціологічної інформації. Це дає можливість досліджувати різноманітні стратегії керування інформаційним впливом результатів соціології на особистість та обирати доцільну стратегію керування інформаційним потоком з метою забезпечення необхідного рівня інформаційної захищеності особистості.

5. Моделювання різних стратегій управління каналами інформаційного впливу підтверджує адекватність розробленої моделі і свідчить про те, що особистість з високим рівнем незалежності, при продуманій стратегії зміни каналів інформаційного впливу здатна протистояти більшості інформаційних впливів і, тим самим, забезпечити власну інформаційну захищеність на заданому рівні.

РОЗДІЛ 3
РОЗВИТОК ТЕХНОЛОГІЙ ОБРОБКИ РЕЗУЛЬТАТІВ СОЦІОЛОГІЧНИХ ДОСЛІДЖЕНЬ ДЛЯ ВИКОРИСТАННЯ В МОДЕЛІ ІНФОРМАЦІЙНОЇ ЗАХИЩЕНОСТІ ОСОБИСТОСТІ

Подання результатів соціологічних досліджень у медіа може мати різні форми, залежно від мети комунікації, цільової аудиторії та складності матеріалу. При цьому, можна виділити три основні групи форм подання результатів:

1) інтерактивні формати;
2) текстові повідомлення;
3) візуальні презентації.

Кожна група має свої характерні риси, які визначають особливості подання інформації і які потім будуть впливати на можливість застосування результатів соціологічних досліджень у моделі інформаційної захищеності особистості.

У даному розділі будуть розглянуті основні групи форм подання результатів та запропоновані рішення стосовно адаптації результатів кожної групи до моделі інформаційної захищеності особистості.

3.1. Технологія обробки соціологічної інформації в інтерактивних форматах

До інтерактивного формату подання результатів соціологічних досліджень належать: інтерактивні онлайн-платформи (Interactive Online Platforms) та соціальні мережі (Social Media Posts).

Інтерактивні платформи дозволяють користувачам взаємодіяти з даними дослідження, аналізувати їх та створювати власні висновки. Це можуть бути інтерактивні карти, графіки або навіть симулятори [66]. Короткі та доступні пости в соціальних мережах (Twitter, Facebook, Instagram) дозволяють швидко поширювати основні висновки дослідження. При цьому часто використовуються меми, короткі відеоролики та інфографіка. Пости можуть містити посилання на більш детальну інформацію [67].

Технологія адаптації результатів соціологічних досліджень в інтерактивних форматах до бінарних альтернативних оцінок. Інтерактивні формати є ефективним каналом для збору та поширення інформації, включаючи результати соціологічних досліджень. Подання таких результатів у вигляді бінарних альтернативних оцінок з ймовірностями дозволяє чітко і зрозуміло донести ключові висновки до аудиторії.

Процес подання результатів:

1. Збір даних і визначення ключових питань: Збираються результати соціологічного дослідження та визначаються ключові питання або аспекти, які можуть бути представлені як бінарні альтернативні оцінки.

2. Створення бінарних змінних: Дані перетворюються на бінарні альтернативи на основі чітких критеріїв для поділу на дві групи (наприклад, “підтримує/не підтримує”).

3. Розрахунок ймовірностей: Розраховуються ймовірності для кожної групи, базуючись на кількості респондентів у кожній категорії.

4. Створення контенту для соціальних мереж: Формуються повідомлення, що включають результати у вигляді бінарних альтернативних оцінок з ймовірностями, а також додаються візуальні матеріали (графіки, інфографіка).

5. Публікація в соціальних мережах: Публікується підготовлений контент у соціальних мережах, використовуючи відповідні формати і стилі.

Приклад. Розглянемо приклад соціологічного дослідження, яке вивчало ставлення населення до роботи місцевих органів влади. Результати будуть подані у вигляді бінарних альтернативних оцінок і опубліковані у соціальних мережах.

Припустимо, у нас є такі дані: 400 респондентів; 240 підтримують роботу місцевих органів влади; 160 не підтримують роботу місцевих органів влади.

Створення бінарних змінних і розрахунок ймовірностей. Бінарні альтернативи: “Підтримує” (1) – підтримує роботу місцевих органів влади. “Не підтримує” (0) – не підтримує роботу місцевих органів влади.

Розрахунок ймовірностей: Ймовірність підтримки: $P_{підтримує} = \frac{240}{400} = 0.6$;

Ймовірність непідтримки: $P_{не\ підтримує} = \frac{160}{400} = 0.4$.

Повідомлення у соціальних мережах може мати вигляд: “За результатами дослідження 60% населення підтримують роботу місцевих органів влади, тоді як 40% висловлюють свою непідтримку”.

Такий підхід дає можливість використовувати результати соціологічних досліджень, представлених в інтерактивних форматах, у моделі інформаційної захищеності особистості. Поширення таких результатів у соціальних мережах допомагає донести ключові висновки до широкої аудиторії зрозуміло і ефективно. Також, такий підхід полегшує сприйняття даних і стимулює активну взаємодію з контентом. Наявність бінарної класифікації з відповідними ймовірностями відповідає встановленим змінним моделі і дозволяє використовувати результати соціології напряму, без додаткових перетворень.

Якщо розглядати модель поведінки особистості під дією результатів соціологічних досліджень (2.4), то місце для ймовірностей бінарних альтернативних оцінок знаходиться у векторі

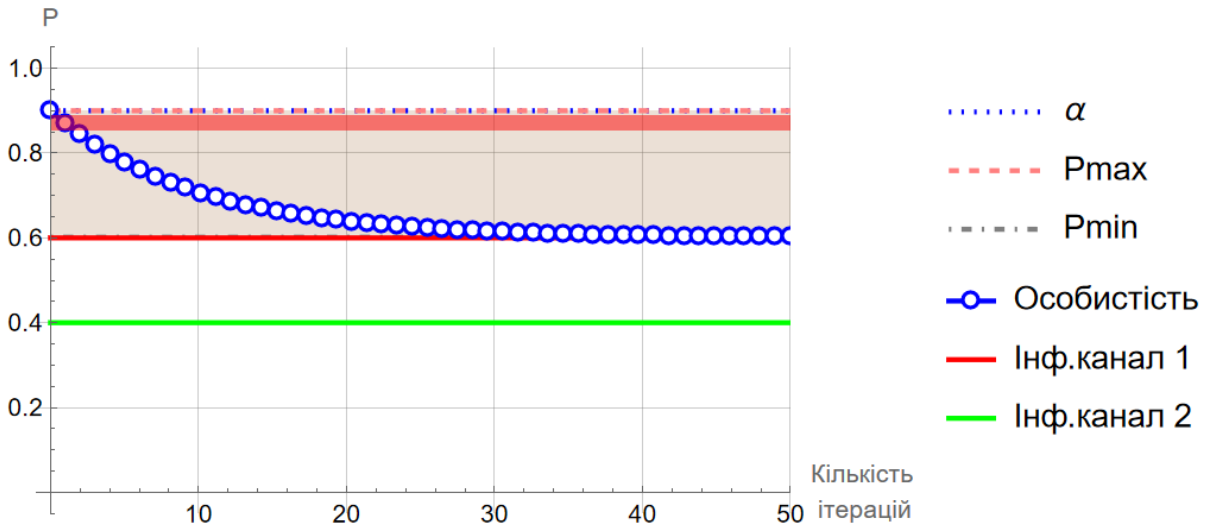
$$\begin{gathered} \mathrm{A} = \left(\alpha_j, \alpha^{+}_{соц}, \alpha^{-}_{соц} \right), \\ \alpha^{+}_{соц} + \alpha^{-}_{соц} = 1. \end{gathered} \tag{3.1}$$

де: $\alpha^{+}_{соц}, \alpha^{-}_{соц}$ – ймовірнісні характеристики альтернатив соціологічних досліджень. Як у раніше наведеному прикладі: “Підтримує” ($P_{підтримує}$); “Не підтримує” ($P_{не\ підтримує}$).

До цього часу ми розглядали модель інформаційної захищеності особистості, вважаючи, що соціологія несе лише полярні оцінки $\{0,1\}$. У реальному житті дані соціологічних досліджень є набагато складнішими і тому, урахування їх у ймовірнісному вигляді дозволяє зробити модель більш реалістичною.

Наприклад, для ситуації, наведеної на рис. 2.17 при $\alpha_j = 0.9$, $\mu_j = 0.9$ накладемо умову, коли $\alpha^{+}_{соц} = P_{підтримує} = 0.6$, а $\alpha^{-}_{соц} = P_{не\ підтримує} = 0.4$. Застосувавши модель отримаємо результат (рис. 3.1). Як бачимо, у разі коли переконання особистості є значно потужнішими $\alpha_j = 0.9$, ніж робота каналу інформаційного впливу $\alpha^{+}_{соц} = 0.6$, то зміна апостеріорної ймовірності відбувається значно плавніше, але, разом з тим, з часом канал “перемагає” і особистість набуває $P_j = \alpha^{+}_{соц} = 0.6$. Тобто, якщо апріорі особистість мала рівень підтримки роботи органів місцевої влади на рівні 0.9, то з часом, під дією каналу інформаційного впливу, що постійно транслює результати соціології на рівні 0.6, особистість і сама набуває апостеріорного рівня підтримки 0.6. Така ситуація цілком можлива у реальному житті, оскільки

медіа при тривалому впливі здатні “переконувати” навіть самих стійких адептів, які ними постійно користуються.



α = 0.9 μ = 0.9

Channel 1 = 49 Channel 2 = 0

Pmax = 0.9 Pmin = 0.6

ΔP = 0.298282

Рис. 3.1. Результати моделювання за Стратегією-2 при $\alpha_j = 0.9$, $\mu_j = 0.9$, $\alpha^{+}_{соц} = 0.6$, $\alpha^{-}_{соц} = 0.4$

Зважаючи на те, що розмах $\Delta P_j \approx 0.3$ і загальний характер переконань особистості співпадає з переконаннями каналу інформаційного впливу у цьому випадку також можна говорити про забезпечення інформаційної захищеності особистості, так як у будь якому разі особистість зберегла підтримку основної ідеї, яка і транслювалася через медіа. Для цього особистості знадобилося користуватися лише одним каналом інформаційного впливу, не перемикаючи на альтернативні канали. Достатньо високий рівень $\mu_j = 0.9$ призвів до того, що особистість повільно змінювала P_j, наближаючи її до рівня $\alpha^{+}_{соц}$.

Випадок, коли $\alpha_j << \alpha^{-}_{соц}$ є дзеркальним тому, який було щойно розглянуто, і тому всі логічні міркування є тотожними.

3.2. Технологія обробки соціологічної інформації у форматі текстових повідомлень

До групи текстових повідомлень відносяться: Аналітичні статті (Analytical Articles); Спеціалізовані новинні бюлетені (Specialized Newsletters); Інтерв'ю та коментарі (Interviews and Comments); Блоги та колонки (Blogs and Columns) та Прес-релізи (Press Releases).

Аналітичні статті дозволяють глибше розглянути результати дослідження, проаналізувати їх та представити можливі наслідки. Такі статті можуть бути опубліковані у спеціалізованих виданнях або на вебсайтах. Вони зазвичай містять [68]: огляд мети та методології дослідження; детальний аналіз основних висновків; коментарі експертів та інтерпретацію результатів; прогнози або рекомендації.

Спеціалізовані новинні бюлетені можуть бути розіслані журналістам та зацікавленим сторонам і містити детальну інформацію про результати дослідження. Це може бути корисно для аудиторії, яка шукає глибше розуміння теми [69].

Блоги та колонки. Публікація результатів у форматі блогів або колонок на відомих платформах дозволяє поділитися більш неформальними або особистими поглядами на результати дослідження. Це може зробити інформацію більш доступною та зрозумілою для широкого загалу [70].

Прес-релізи є одним з найпоширеніших способів представлення результатів досліджень для медіа. Вони містять ключову інформацію та основні висновки дослідження в стислому та доступному форматі. Прес-

релізи зазвичай включають [71]: заголовок, що привертає увагу; короткий вступ з найважливішими висновками; основну частину з детальнішим описом результатів і методології; контактну інформацію для подальших запитань.

Соціологічні дослідження у форматі текстових повідомлень містять, як правило, ключові результати та висновки. Це інформація, яка передається різноманітним медіа з метою інформування громадськості про основні висновки дослідження. Часто в таких релізах використовуються прості, зрозумілі формулювання, що роблять акцент на основних результатах.

Подання результатів у вигляді бінарних альтернативних оцінок. Для подання результатів соціологічних досліджень у вигляді бінарних альтернативних оцінок з встановленням їх ймовірностей можна дотримуватися наступних кроків:

1. Визначення ключових показників: Визначити основні аспекти або питання, які досліджувалися, і перетворити їх на бінарні оцінки.
2. Створення бінарних змінних: Визначити критерії для розподілу показників на дві категорії (наприклад, “задоволений/незадоволений”).
3. Розрахунок ймовірностей: Розрахувати ймовірності для кожної з бінарних груп на основі зібраних даних.
4. Формулювання текстового повідомлення: Створити прес-реліз з чітким, зрозумілим формулюванням, що включає бінарні оцінки і їх ймовірності.

Приклад. Розглянемо приклад соціологічного дослідження, яке досліджувало задоволення населення якістю послуг місцевого самоврядування. Ми перетворимо отримані дані на бінарні альтернативи та визначимо ймовірності для кожної з них.

Початкові дані. Опитування показало наступні результати: 300 осіб опитано; 180 осіб задоволені послугами; 120 осіб незадоволені послугами.

Створення бінарних змінних. Задоволеність послугами можна представити як бінарну змінну: “Задоволений” (1) – якщо задоволений. “Незадоволений” (0) – якщо незадоволений.

Розрахунок ймовірностей. Обчислимо ймовірності задоволеності та незадоволеності послугами. Ймовірність задоволеності послугами: $P_{задоволений} = \frac{180}{300} = 0.6$; Ймовірність незадоволеності послугами: $P_{незадоволений} = \frac{120}{300} = 0.4$.

Текстове повідомлення з результатами соціології може мати вигляд:

Більшість населення задоволені якістю послуг місцевого самоврядування. Згідно з останнім соціологічним опитуванням, проведеним серед 300 мешканців міста, 60% опитаних (180 осіб) задоволені якістю послуг, які надає місцеве самоврядування. Водночас, 40% респондентів (120 осіб) висловили своє незадоволення. “Це свідчить про те, що більшість мешканців міста схвально оцінюють діяльність місцевих органів влади, що підтверджується високим рівнем задоволеності” – зазначив представник соціологічної служби.

Отже, як і у випадку з інтерактивним форматом, результати соціології у форматі текстових повідомлень дозволяють ефективно і зрозуміло представити результати соціологічного дослідження у вигляді бінарних альтернативних оцінок, підкріплених точними ймовірностями. Це спрощує сприйняття інформації, допомагає краще розуміти настрої та уподобання громадськості та безпосередньо застосовувати такі результати у моделі інформаційної захищеності особистості. Урахування результатів соціологічних досліджень у форматі текстових повідомлень у моделі інформаційної захищеності особистості проводиться аналогічно (3.1).

3.3. Технологія обробки соціологічної інформації у форматі візуальних презентацій

До групи візуальних презентацій відносяться: Відео та мультимедійні презентації (Videos and Multimedia Presentations); Інтерв'ю та коментарі (Interviews and Comments); Брифінги та прес-конференції (Briefings and Press Conferences); Інфографіка (Infographics).

Відео та мультимедійні презентації використовуються для візуального представлення результатів. Вони можуть включати анімації, інтерв'ю з дослідниками та графічні зображення результатів. Такі презентації можуть бути розміщені на новинних сайтах, у соціальних мережах або на телебаченні [72].

Інтерв'ю та коментарі. Поширеним є також формат інтерв'ю з дослідниками або експертами, які можуть пояснити результати дослідження та їх значення. Коментарі можуть бути включені до новинних сюжетів або статей і забезпечують експертну думку [73].

Брифінги та прес-конференції. Організація брифінгів або прес-конференцій дозволяє представити результати досліджень безпосередньо журналістам і відповісти на їхні питання. Це забезпечує безпосередню комунікацію та дозволяє більш детально пояснити значення результатів [74].

Інфографіка дозволяє візуалізувати результати дослідження у формі графіків, діаграм та інших візуальних елементів. Це спрощує сприйняття інформації та робить її більш зрозумілою для широкої аудиторії. Інфографіка може включати [75]: графіки (стовпчикові, кругові, лінійні); діаграми та схеми; ілюстрації та значки; короткі текстові пояснення.

Разом з тим, за своєю структурою дані інфографіки дуже часто є множинними, що не дозволяє використовувати їх у запропонованій моделі

інформаційної захищеності особистості, запропонованій у розділі 2. Відтак, існує потреба приведення таких даних до бінарного вигляду, коли особистість буде перебувати у стані вибору одного з двох альтернативних варіантів: 1 або 0.

Технології приведення інфографіки з множинним вибором до бінарного вибору

Технологія приведення інфографіки з множинним вибором до бінарного вибору включає ряд методів і підходів, які дозволяють спростити представлення даних, зосередивши увагу на двох основних категоріях. Це може бути корисно для спрощення сприйняття інформації або підкреслення ключових аспектів даних. Розглянемо деякі з основних методів та технологій, які можна використовувати для цього завдання.

Групування варіантів (Option Grouping). Один із способів звести множинний вибір до бінарного – це об’єднати варіанти в дві категорії. Наприклад, якщо є декілька відповідей на запитання, їх можна згрупувати у дві основні категорії: позитивні та негативні, або згодні та незгодні [76].

Приклад: Якщо опитування містить варіанти “Дуже задоволений”, “Задоволений”, “Нейтральний”, “Незадоволений”, “Дуже незадоволений”, їх можна згрупувати як “Задоволений” (включає “Дуже задоволений” і “Задоволений”) та “Незадоволений” (включає “Нейтральний”, “Незадоволений” і “Дуже незадоволений”).

Після групування варіантів у дві категорії важливо оцінити ймовірності для кожної з отриманих бінарних груп. Це допомагає краще розуміти розподіл даних і приймати більш обґрунтовані рішення. Нижче наведено детальні кроки для визначення ймовірностей для кожної з отриманих бінарних груп:

Крок 1: Визначення груп. Спочатку потрібно чітко визначити, які варіанти будуть об’єднані в кожну з двох бінарних груп. Наприклад, при опитуванні задоволеності клієнтів можна об’єднати відповіді таким чином:

Група 1: Задоволений (включає “Дуже задоволений” і “Задоволений”).

Група 2: Незадоволений (включає “Нейтральний”, “Незадоволений” і “Дуже незадоволений”).

Крок 2: Підрахунок кількості відповідей для кожної групи. Необхідно підрахувати кількість відповідей, що належать до кожної з двох нових категорій. Це можна зробити за допомогою табличних редакторів або програмного забезпечення для аналізу даних.

Приклад: Припустимо, є такі дані: Дуже задоволений: 50 відповідей. Задоволений: 100 відповідей. Нейтральний: 30 відповідей. Незадоволений: 20 відповідей. Дуже незадоволений: 10 відповідей.

Тоді: Задоволений: 50 (Дуже задоволений) + 100 (Задоволений) = 150 відповідей. Незадоволений: 30 (Нейтральний) + 20 (Незадоволений) + 10 (Дуже незадоволений) = 60 відповідей.

Крок 3: Розрахунок ймовірностей. Ймовірність для кожної групи визначається як відношення кількості відповідей у цій групі до загальної кількості відповідей

$$P\left(Група\right)=\frac{n_{групи}}{N_{заг}}. \qquad (3.2)$$

Розрахунок: Ймовірність задоволення: $P\left(Задоволений\right)=\frac{150}{210}=0.714$.

Ймовірність незадоволення: $P\left(Незадоволений\right)=\frac{60}{210}=0.286$.

Після розрахунку ймовірностей важливо інтерпретувати результати в контексті дослідження. Наприклад, високий відсоток задоволених клієнтів може свідчити про ефективну роботу компанії, тоді як високий відсоток незадоволених може вказувати на необхідність поліпшення послуг.

Побудова дихотомічного показника (Construction of a Dichotomous Indicator). Цей підхід передбачає створення нового показника, який відображає, чи досягнуто певного критерію або ні [77]. Наприклад, можна задати порогове значення і категоризувати дані як “Вище порогу” або “Нижче порогу”.

Приклад: Якщо питання стосується рівня доходу, можна встановити пороговий рівень, наприклад, середній дохід, і розділити респондентів на дві групи: ті, хто має дохід вище середнього, та ті, хто має дохід нижче середнього.

Побудова дихотомічного показника (Construction of a Dichotomous Indicator) включає процес перетворення множинних виборів або континуальних змінних в дві категорії для спрощення аналізу та інтерпретації. Після цього важливо визначити ймовірності для кожної з отриманих бінарних груп, що дозволить оцінити розподіл даних та прийняти обґрунтовані рішення. Ось покроковий план, як це зробити:

Крок 1: Визначення критерію дихотомії. Спочатку необхідно визначити критерій або порогове значення, яке буде використано для поділу змінної на дві категорії. Це може бути середнє значення, медіана, певний поріг тощо.

Приклад: Припустимо, є дані про рівень доходу, і ми хочемо поділити їх на дві групи: “Високий дохід” і “Низький дохід”. В якості порогового значення можна взяти середній дохід.

Крок 2: Підрахунок кількості відповідей у кожній категорії. Після визначення критерію, потрібно підрахувати кількість відповідей, що належать до кожної з двох категорій.

Приклад: Високий дохід: кількість людей з доходом вище середнього.

Низький дохід: кількість людей з доходом нижче або рівним середньому.

Крок 3: Розрахунок ймовірностей. Ймовірності для кожної з бінарних груп визначаються як відношення кількості відповідей у кожній групі до загальної кількості відповідей, аналогічно формулі (3.2).

Крок 4: Приклад розрахунку. Дані: 300 осіб мають дохід вище середнього (високий дохід). 200 осіб мають дохід нижче або рівний середньому (низький дохід).

Загальна кількість відповідей: 300 (Високий дохід) + 200 (Низький дохід) = 500.

Ймовірності: Ймовірність високого доходу: $P_{високий\ дохід} = \frac{300}{500} = 0.6$.

Ймовірність низького доходу: $P_{низький\ дохід} = \frac{200}{500} = 0.4$.

Крок 5: Інтерпретація результатів. Після розрахунку ймовірностей їх потрібно інтерпретувати в контексті аналізу. Наприклад, якщо 60% людей мають високий дохід, це може вказувати на певні економічні тенденції або ефективність соціальної політики.

Крок 6: Візуалізація ймовірностей. Для візуалізації ймовірностей, щоб зробити їх більш наочними, використовуються графіки та діаграми.

Вибір найважливішого критерію (Selection of the Most Important Criterion). Цей метод полягає в ідентифікації одного або декількох ключових критеріїв серед множинних варіантів, які мають найбільше значення або частоту, і подальше їх використання для бінарного поділу [78].

Приклад: Якщо респондентам запропоновано вибрати кілька причин для купівлі продукту, можна зосередитися на одній або двох основних причинах і поділити вибір на “Важлива причина” або “Не важлива причина”.

Вибір найважливішого критерію є методом спрощення множинних виборів або змінних до двох основних категорій шляхом фокусування на ключовому показнику або критерію. Після цього необхідно визначити

ймовірності для кожної з отриманих бінарних груп, що допоможе краще зрозуміти розподіл даних та прийняти обґрунтовані рішення. Нижче наведено кроки для визначення ймовірностей для кожної з отриманих бінарних груп:

Крок 1: Визначення ключового критерію. Перший крок полягає у виборі найважливішого критерію, на основі якого будуть формуватися бінарні групи. Цей критерій може бути обраний на основі важливості для аналізу або впливу на результати.

Приклад: Припустимо, ми аналізуємо задоволеність клієнтів за різними критеріями: якість продукту, рівень обслуговування, ціна тощо. Визначаємо, що найважливішим критерієм для нашого аналізу є якість продукту.

Крок 2: Підрахунок кількості відповідей для кожної категорії на основі ключового критерію. Після вибору критерію необхідно розділити респондентів на дві групи на основі цього критерію.

Приклад:

Група 1: Ті, хто оцінює якість продукту високо (включає відповіді “Дуже добре” і “Добре”).

Група 2: Ті, хто оцінює якість продукту низько (включає відповіді “Посередньо”, “Погано”, “Дуже погано”).

Крок 3: Підрахунок кількості респондентів у кожній групі. Підраховується кількість респондентів, що належать до кожної з нових категорій на основі обраного критерію.

Приклад: Висока оцінка якості продукту: 150 респондентів. Низька оцінка якості продукту: 50 респондентів.

Крок 4: Розрахунок ймовірностей. Ймовірність для кожної групи визначається як відношення кількості респондентів у цій групі до загальної кількості респондентів, аналогічно до формули (3.2).

Крок 5: Розрахунок ймовірностей на прикладі. Загальна кількість респондентів: 150 (Висока оцінка) + 50 (Низька оцінка) = 200.

Ймовірності: Ймовірність високої оцінки: $P_{\text{висока оцінка}} = \frac{150}{200} = 0.75$;

Ймовірність низької оцінки: $P_{\text{низька оцінка}} = \frac{50}{200} = 0.25$.

Крок 6: Інтерпретація результатів. Після розрахунку ймовірностей їх потрібно інтерпретувати в контексті аналізу. Наприклад, якщо 75% респондентів оцінюють якість продукту високо, це може вказувати на позитивне сприйняття якості продукту серед споживачів.

Використання суми або середнього значення (Use of Sum or Average Value). Цей підхід включає підрахунок суми або середнього значення відповідей і класифікацію результату як “Високий” або “Низький” [79].

Приклад: Якщо є оцінка задоволеності за кількома критеріями, можна обчислити середній бал і визначити, чи задоволеність загалом висока або низька.

Використання суми або середнього значення для створення бінарних груп передбачає зведення складних даних або багатовимірних показників до однієї числової оцінки. Ця оцінка потім ділиться на дві категорії для полегшення аналізу. Далі потрібно визначити ймовірності для кожної з цих бінарних груп. Ось покроковий план, як це зробити:

Крок 1: Збір даних та обчислення суми або середнього значення. Спочатку необхідно зібрати дані та обчислити суму або середнє значення для кожного спостереження або респондента. Це дозволяє отримати єдину числову оцінку, яка буде використовуватися для поділу на бінарні групи.

Приклад: Припустимо, ми маємо дані опитування, де кожен респондент оцінює три аспекти задоволеності: якість обслуговування, швидкість обслуговування та загальне враження, кожен з яких оцінюється від 1 до 5.

1. Збір даних:

Респондент 1: [3, 4, 5]

Респондент 2: [2, 3, 4]

Респондент 3: [4, 4, 4]

...

2. Обчислення середнього значення:

Респондент 1: (3 + 4 + 5) / 3 = 4

Респондент 2: (2 + 3 + 4) / 3 = 3

Респондент 3: (4 + 4 + 4) / 3 = 4

...

Крок 2: Визначення порогового значення. Наступний крок – визначити порогове значення, яке буде використовуватися для поділу даних на дві групи. Це може бути середнє значення, медіана або інше значення, яке має сенс для вашого аналізу.

Приклад: Визначимо середнє значення усіх середніх оцінок: Середнє значення для всіх респондентів: (4 + 3 + 4 + ...) / N = 3.5

Крок 3: Поділ на бінарні групи. Поділити респондентів на дві групи на основі порогового значення:

Група 1: Респонденти з середнім значенням вище порогового (наприклад, > 3.5).

Група 2: Респонденти з середнім значенням рівним або нижчим порогового (≤ 3.5).

Приклад:

Група 1 (вище 3.5): Респондент 1 (4), Респондент 3 (4).

Група 2 (нижче або дорівнює 3.5): Респондент 2 (3).

Крок 4: Підрахунок кількості респондентів у кожній групі. Підрахувати кількість респондентів у кожній з двох груп.

Приклад:

Група 1: 2 респонденти

Група 2: 1 респондент

Крок 5: Розрахунок ймовірностей. Ймовірність для кожної групи визначається як відношення кількості респондентів у цій групі до загальної кількості респондентів, аналогічно до (3.2).

Крок 6: Приклад розрахунку

Загальна кількість респондентів: 2 (Група 1) + 1 (Група 2) = 3.

Ймовірності: Ймовірність високої оцінки: $P_{\text{група 1}} = \frac{2}{3} = 0.67$;

Ймовірність низької оцінки: $P_{\text{група 2}} = \frac{1}{3} = 0.33$.

Крок 7: Інтерпретація результатів. Після розрахунку ймовірностей важливо їх правильно інтерпретувати. Наприклад, якщо 67% респондентів оцінюють обслуговування високо (вище середнього), це може вказувати на позитивне сприйняття обслуговування.

Застосування методу використання суми або середнього значення для поділу даних на бінарні групи та розрахунок ймовірностей для кожної з груп дозволяє отримати зрозумілі результати та спрощує аналіз даних.

Дихотомізація за часовими показниками (Dichotomization by Temporal Metrics). Можна використовувати часові показники для поділу варіантів на “Досягнуто” або “Не досягнуто” певного часу або події [80].

Приклад: Якщо опитування стосується терміну виконання задач, респондентів можна поділити на дві групи: ті, хто виконав завдання вчасно, і ті, хто не виконав.

Дихотомізація за часовими показниками передбачає поділ даних на дві групи на основі часового критерію, такого як дата, період або тривалість події. Після поділу необхідно визначити ймовірності для кожної з отриманих бінарних груп. Ось покроковий план для цього:

Крок 1: Вибір часового показника. Спочатку необхідно визначити, який часовий показник буде використовуватися для дихотомізації. Це може бути дата, час події, тривалість перебування, період, тощо.

Приклад: Припустимо, ми аналізуємо дані про споживачів, які здійснили покупку. Часовий показник – дата покупки. Хочемо поділити дані на покупки, зроблені до певної дати, і покупки, зроблені після неї.

Крок 2: Визначення порогового значення. Необхідно вибрати порогове значення для часового показника, яке буде використовуватися для поділу даних. Це може бути конкретна дата, середнє значення або інше обґрунтоване значення.

Приклад: Визначаємо порогове значення – дата 1 січня 2024 року.

Крок 3: Поділ даних на дві групи. Розділити дані на дві групи на основі порогового значення.

Приклад: Група 1: Покупки, зроблені до 1 січня 2024 року. Група 2: Покупки, зроблені 1 січня 2024 року або після цієї дати.

Крок 4: Підрахунок кількості даних у кожній групі. Підрахувати кількість даних (наприклад, покупок або споживачів) у кожній з двох груп.

Приклад:

Група 1: 1200 покупок до 1 січня 2024 року.

Група 2: 800 покупок 1 січня 2024 року або після цієї дати.

Крок 5: Розрахунок ймовірностей. Ймовірність для кожної групи визначається як відношення кількості даних у цій групі до загальної кількості даних за формулою (3.2).

Загальна кількість даних: 1200 (Група 1) + 800 (Група 2) = 2000.

Ймовірності: Ймовірність для Групи 1: $P_{\text{група}\,1} = \frac{1200}{2000} = 0.6$. Ймовірність для Групи 2: $P_{\text{група}\,2} = \frac{800}{2000} = 0.4$.

Крок 7: Інтерпретація результатів. Після розрахунку ймовірностей важливо їх правильно інтерпретувати в контексті проведеного аналізу. Наприклад, якщо 60% покупок зроблено до 1 січня 2024 року, це може вказувати на певні тенденції у поведінці споживачів до і після цієї дати.

Конверсія множинних виборів у кілька бінарних варіантів (Conversion of Multiple Choices into Multiple Binary Options). Кожен можливий вибір може бути перетворений у окремий бінарний варіант, який відображає, чи був зроблений конкретний вибір [81].

Приклад: Замість об'єднання варіантів можна створити кілька бінарних змінних для кожного варіанту, наприклад, "Вибрано варіант А" або "Не вибрано варіант А".

Конверсія множинних виборів у кілька бінарних варіантів передбачає перетворення багатовимірних даних на серію дихотомічних (бінарних) змінних, де кожна змінна відповідає одному з можливих виборів або категорій. Кожна з цих бінарних змінних має два можливих значення: 0 (відсутність вибору) або 1 (наявність вибору). Це дозволяє аналізувати дані більш детально та отримувати ймовірності для кожного з бінарних варіантів.

Кроки для визначення ймовірностей для кожної з бінарних груп:

1. Вибір категорій для конверсії: Визначити всі можливі категорії або варіанти вибору, які будуть перетворені на бінарні змінні.
2. Перетворення даних на бінарні змінні: Створити нові бінарні змінні для кожної з категорій, де 1 означає вибір цієї категорії, а 0 означає, що ця категорія не була вибрана.
3. Підрахунок кількості одиниць (1) і нулів (0): Підрахувати кількість одиниць і нулів для кожної з бінарних змінних.
4. Розрахунок ймовірностей: Розрахувати ймовірність для кожної бінарної змінної як відношення кількості одиниць до загальної кількості спостережень.

Приклад. Припустимо, у нас є опитування, де респонденти могли вибрати кілька улюблених видів спорту: футбол, баскетбол, теніс і плавання. Кожен респондент міг вибрати один або кілька видів спорту:

Респондент	Вибір
1	Футбол, Баскетбол
2	Футбол, Теніс
3	Плавання, Футбол
4	Баскетбол
5	Плавання

Крок 1: Визначення категорій: Футбол. Баскетбол. Теніс. Плавання.

Крок 2: Перетворення даних на бінарні змінні:

Респондент	Футбол	Баскетбол	Теніс	Плавання
1	1	1	0	0
2	1	0	1	0
3	1	0	0	1
4	0	1	0	0
5	0	0	0	1

Крок 3: Підрахунок одиниць (1) і нулів (0):

Вибір	Кількість одиниць (1)	Кількість нулів (0)
Футбол	3	2
Баскетбол	2	3
Теніс	1	4
Плавання	2	3

Крок 4: Розрахунок ймовірностей:

Ймовірність для кожної категорії (бінарної змінної) розраховується як:

$$P\left(Група\right)=\frac{n_{(1)}}{N_{заг}}. \quad (3.3)$$

Ймовірність для Футболу: $P_{Футбол}=\frac{3}{5}=0.6$; решта видів спорту 0.4.

Ймовірність для Баскетболу: $P_{Баскетбол}=\frac{2}{5}=0.4$; решта видів спорту 0.6.

Ймовірність для Тенісу: $P_{Теніс}=\frac{1}{5}=0.2$; решта видів спорту 0.8.

Ймовірність для Плавання: $P_{Плавання}=\frac{2}{5}=0.4$; решта видів спорту 0.6.

Застосування методу конверсії множинних виборів у кілька бінарних варіантів для поділу даних на бінарні групи та розрахунок ймовірностей для кожної з груп дозволяє отримати детальні та зрозумілі результати, що спрощує аналіз складних даних.

Моделювання сценаріїв на основі множинних виборів (Scenario Modeling Based on Multiple Choices). Цей підхід використовує моделювання для створення ймовірнісних сценаріїв, що допомагає звести множинний вибір до двох основних сценаріїв або результатів [82].

Приклад: Можна моделювати можливі сценарії на основі множинних виборів і категоризувати їх у “Ймовірний позитивний результат” або “Ймовірний негативний результат”.

Моделювання сценаріїв на основі множинних виборів передбачає аналіз різних комбінацій виборів для оцінки ймовірностей різних результатів. Це дозволяє визначити ймовірності для кожної з отриманих бінарних груп (сценаріїв) та оцінити, як конкретні вибори або комбінації виборів впливають на результати.

Кроки для визначення ймовірностей для кожної з бінарних груп.

1. Вибір категорій для аналізу: Визначити всі можливі категорії або варіанти вибору, які будуть включені в моделювання сценаріїв.

2. Створення можливих комбінацій (сценаріїв): Визначити всі можливі комбінації виборів, які можуть формувати різні сценарії.

3. Перетворення даних на бінарні змінні: Для кожної комбінації (сценарію) створити бінарну змінну, де 1 означає, що сценарій реалізується, а 0 означає, що ні.

4. Підрахунок кількості реалізованих сценаріїв: Підрахувати кількість реалізованих сценаріїв (коли змінна дорівнює 1) для кожної комбінації.

5. Розрахунок ймовірностей: Розрахувати ймовірність для кожного сценарію як відношення кількості реалізованих сценаріїв до загальної кількості спостережень.

Приклад.

Розглянемо приклад, де опитувані вибирають свої улюблені види спорту з переліку: футбол, баскетбол, теніс, плавання. Ми хочемо змоделювати ймовірності для кожної комбінації виборів.

Початкові дані:

Респондент	Вибір
1	Футбол, Баскетбол
2	Теніс
3	Плавання, Футбол
4	Баскетбол, Теніс
5	Плавання

Крок 1: Вибір категорій: Футбол. Баскетбол. Теніс. Плавання.

Крок 2: Створення можливих комбінацій.

Можливі комбінації (сценарії) виборів включають: Футбол + Баскетбол. Футбол + Плавання. Баскетбол + Теніс. Плавання. Інші комбінації.

Крок 3: Перетворення даних на бінарні змінні:

Респондент	Футбол	Баскетбол	Теніс	Плавання	Футбол + Баскетбол	Футбол + Плавання	Баскетбол + Теніс	Інші
1	1	1	0	0	1	0	0	0
2	0	0	1	0	0	0	0	1
3	1	0	0	1	0	1	0	0
4	0	1	1	0	0	0	1	0
5	0	0	0	1	0	0	0	1

Крок 4: Підрахунок кількості реалізованих сценаріїв:

Сценарій	Кількість реалізованих сценаріїв
Футбол + Баскетбол	1
Футбол + Плавання	1
Баскетбол + Теніс	1
Інші	2

Крок 5: Розрахунок ймовірностей:

Ймовірність для кожного сценарію розраховується як:

$$P\left(Сценарій\right)=\frac{n_{(\text{реалізованих сценаріїв})}}{N_{(\text{загальна кількість спостережень})}}. \quad (3.4)$$

Ймовірність для Футбол + Баскетбол: $P_{Футбол+Баскетбол} = \frac{1}{5} = 0.2$; решта 0.8.

Ймовірність для Футбол + Плавання: $P_{Футбол+Плавання} = \frac{1}{5} = 0.2$; решта 0.8.

Ймовірність для Баскетбол + Теніс: $P_{Баскетбол+Теніс} = \frac{1}{5} = 0.2$; решта 0.8.

Ймовірність для Інші: $P_{Інші} = \frac{2}{5} = 0.4$; решта 0.6.

Моделювання сценаріїв на основі множинних виборів дозволяє оцінити ймовірності реалізації різних комбінацій виборів, що забезпечує детальний і точний аналіз даних.

Створення індексів (Index Creation). Можна створити композитний індекс на основі кількох варіантів і використовувати його для поділу даних на “Високий індекс” або “Низький індекс” [83].

Приклад: Різні фактори, що впливають на задоволеність життям, можуть бути об’єднані в індекс задоволеності, який потім розділяється на високий і низький рівні.

Створення індексів у соціологічних дослідженнях часто включає об’єднання декількох змінних в один комплексний показник, що відображає певну характеристику чи концепт. Після створення індексу виникає потреба визначити ймовірності для кожної з отриманих бінарних груп, що відповідають різним рівням цього індексу.

Кроки для визначення ймовірностей для кожної бінарної групи індексу:

1. Створення індексу: Об’єднати змінні, які входять до складу індексу, відповідно до заданої методології чи вагової схеми.

2. Бінаризація індексу: Після створення індексу визначити порогові значення чи категорії, за якими індекс можна бінаризувати. Це може бути, наприклад, розділення на “низький” і “високий” рівні за певним критерієм.

3. Визначення бінарних груп: Для кожного індексного рівня визначити бінарну змінну, де 1 відповідає наявності даного рівня, а 0 – відсутності.

4. Підрахунок кількості реалізованих сценаріїв: Підрахувати кількість спостережень (респондентів), які відповідають кожній з бінарних груп індексу.

5. Розрахунок ймовірностей: Розрахувати ймовірність для кожної бінарної групи як відношення кількості реалізованих сценаріїв до загальної кількості спостережень.

Приклад. Розглянемо приклад індексу задоволення життя, який складається з п’яти компонентів: фізичне здоров’я, емоційне благополуччя, соціальні відносини, освіта та матеріальне становище. Кожен компонент оцінюється за шкалою від 1 до 5, а індекс задоволення життя розраховується як середнє арифметичне цих п’яти компонентів.

Крок 1: Створення індексу: Індекс задоволення життя розраховується так:

$$\text{Індекс задоволення життя} = \big(\text{Фізичне здоров'я} + \text{Емоційне благополуччя} + \text{Соціальні відносини} + \text{Освіта} + \text{Матеріальне становище}\big) / 5$$

Крок 2: Бінаризація індексу. Бінаризація індексу здійснюється на дві групи: “Низький рівень” задоволення життя, якщо індекс ≤ 3. “Високий рівень” задоволення життя, якщо індекс > 3.

Крок 3: Визначення бінарних груп. Створимо бінарну змінну для кожної групи: “Низький рівень” задоволення життя: 1, якщо індекс ≤ 3; і 0, якщо індекс > 3. “Високий рівень” задоволення життя: 1, якщо індекс > 3; і 0, якщо індекс ≤ 3.

Крок 4: Підрахунок кількості реалізованих сценаріїв.

Нехай ми маємо такі дані (припустимо, що розподіл індексів у респондентів такий):

Респондент	Індекс задоволення життя
1	4.2
2	2.8
3	3.5
4	3.9
5	2.1

Крок 5: Розрахунок ймовірностей. Загальна кількість спостережень: 5. Ймовірність «Низький рівень» задоволення життя: $P_{Низький} = \frac{2}{5} = 0.4$.

Ймовірність «Високий рівень» задоволення життя: $P_{Високий} = \frac{3}{5} = 0.6$.

Результати. Індекс задоволення життя для кожного респондента обчислюється як середнє значення п’яти компонентів. Індекс дихотомізується на низький (≤ 3) і високий (> 3) рівень. Для кожної групи визначається ймовірність на основі кількості респондентів у групі. Цей підхід дозволяє легко оцінити ймовірності для кожної з бінарних груп, що значно полегшує аналіз даних у соціологічних дослідженнях.

3.4. Адаптація багатовимірних соціологічних даних до моделі інформаційної захищеності особистості на основі кластерного аналізу

В соціологічних дослідженнях число об’єктів дослідження може досягати кількох десятків чи навіть сотень; число ознак, що їх характеризують, також може обчислюватися десятками. Очевидно,

безпосередній (візуальний) аналіз матриці даних за великої кількості об’єктів і ознак практично малоефективний. Через це виникають завдання укрупнення, концентрації вихідних даних, аналізу структури об’єктів дослідження. Вирішення цих завдань може здійснюватися за допомогою сучасних методів багатовимірної класифікації [84].

Кластерний аналіз передбачає виділення компактних, віддалених один від одного груп об’єктів, відшукує “природне” розбиття сукупності на області скупчення об’єктів. Він використовується, коли вихідні дані подані у вигляді матриць близькості, або відстаней між об’єктами, або у вигляді точок у багатовимірному просторі. Найбільш поширені дані другого виду, для яких кластерний аналіз орієнтований на виділення деяких геометрично віддалених груп, всередині яких об’єкти близькі [84].

Вхідними даними у кластерному аналізі є, як правило, матриця вхідних даних

$$X = \begin{pmatrix} X_{1,1} & \cdots & X_{1,m} \\ \cdots & \cdots & \cdots \\ X_{n,1} & \cdots & X_{n,m} \end{pmatrix}, \qquad (3.5)$$

де n – об’єкти (рядки матриці); m – ознаки (стовпці матриці).

Формальна постановка задачі кластеризації виглядає наступним чином: нехай X – множина об’єктів, Y – множина імен кластерів. Задано функцію відстані між об’єктами $\rho(x, x')$. Сформовано навчальну вибірку об’єктів $X^m = x_1, \ldots, x_m \subset X$. Необхідно розбити вибірку на непересічні підмножини, які називають кластерами, так, щоб кожен кластер складався з об’єктів, близьких за метрикою ρ, а об’єкти різних кластерів істотно відрізнялися. Кожному об’єкту $x \in X^m$ приписується номер кластера Y_i.

Оскільки в навчальній вибірці об’єкти можуть характеризуватися ознаками, які вимірюються у різних одиницях, то для кластерного аналізу ознаки мають бути нормованими. Об’єднання схожих об’єктів у групи може бути здійснене різними способами. Виділяють певні групи методів кластерного аналізу: ієрархічні; ітеративні; факторні; на основі модальних значень щільності; на основі теорії графів.

Найбільш поширеними є ієрархічні методи, серед яких розрізняють агломеративний і дивізимний методи. Головна ідея агломеративного методу полягає в тому, що на першому кроці кожен об’єкт вважається окремим кластером. Два найбільш близьких об’єкта об’єднуються, і утворюється новий кластер. Процедура триває, доки всі об’єкти не будуть об’єднані в один кластер. Головна ідея дивізимного методу: спочатку всі об’єкти належать одному кластеру. Від цього кластера відокремлюються групи схожих між собою об’єктів. Так, на кожному кроці кількість кластерів зростає, а міра відстані між класами зменшується.

Серед ітеративних (ітераційних) методів кластеризації можна виділити методи: *К*-середніх; нечіткої кластеризації; метод пошуку згущень; метод дендритів; метод куль та ін.

Для прикладу адаптації багатовимірних соціологічних даних розглянемо задачу кластеризації кандидатів на пост Президента країни з використанням методу *К*-середніх. Застосування методу *К*-середніх для кластеризації кандидатів у Президенти дозволяє розділити їх на дві основні групи на основі різних характеристик, таких як політична ідеологія, стратегії виборчої кампанії, соціально-демографічні цільові групи та інші фактори.

Мета дослідження: визначити дві основні групи кандидатів у президенти на основі їхніх політичних та кампанійних характеристик, щоб краще розуміти їх стратегії та цільові аудиторії.

Збір даних. Дані можуть включати (табл. 3.1):

Таблиця 3.1

Вхідні дані для кластеризації кандидатів у Президенти

Кандидат	Політична ідеологія	Обіцянки	Фінансування (млн. грн)	Виборці	Активність у соц. мережах	Рейтинг підтримки	Географічний регіон
К-1	Л	З, СЗ	5	Сер., Ст.	3000	В	Пд, Сх
К-2	Ц	Р	3	М	2500	В	Ц, З, Пн
К-3	П	Р	8	М, Сер.	4000	С	Ц, З
К-4	П	Б	4	М, Сер.	1500	Н	Ц, Сх
К-5	Ц	З, Р	1	Сер., Ст.	2000	С	Пд, Сх
К-6	Л	СЗ	3	Сер., Ст.	1000	С	Ц, Пд
К-7	Л	СЗ	4	Сер., Ст.	2000	Н	Пд, Сх
К-8	Л	СЗ	2	Ст.	3000	С	Ц, Сх
К-9	П	Б, СЗ	6	Сер., Ст.	3000	В	З, Пн
К-10	Ц	Р, СЗ	5	М, Сер.	6000	В	Ц, З
К-11	Ц	З, Р	4	М, Сер.	4000	В	З, Пн
К-12	Л	СЗ	2	Ст.	2500	Н	Пд, Сх

політичну ідеологію (ліві [Л], центристські [Ц], праві [П]);

головні політичні платформи та обіцянки (реформи [Р], здоров’я [З], соцзахист [СЗ], безпека [Б]);

фінансування кампаній (витрати [млн. грн.]);

основні соціально-демографічні групи виборців, на які спрямовані кампанії (молодь [М], середній вік [Сер.], старший вік [Ст.]);

активність у соціальних мережах (кількість постів [шт.]);

рейтинги підтримки (високий [В], середній [С], низький [Н]);

географічні регіони, де проводяться кампанії (північ [Пн], південь [Пд], захід [З], схід [С], центр [Ц]).

Підготовка даних. Дані очищуються та нормалізуються для усунення будь-яких пропусків і забезпечення їх сумісності.

Застосування методу К-середніх. Вибір кількості кластерів (*k*): У цьому випадку ми заздалегідь знаємо, що хочемо розділити кандидатів на два кластери, тому *k* = 2.

Кластеризація: Метод *К*-середніх виконує кластеризацію даних, розподіляючи кандидатів на два кластери на основі схожості між даними:

Кластер 1: кандидати К-1, К-2, К-3, К-4, К-5, К-6, К-7, К-8, К-9, К-12;

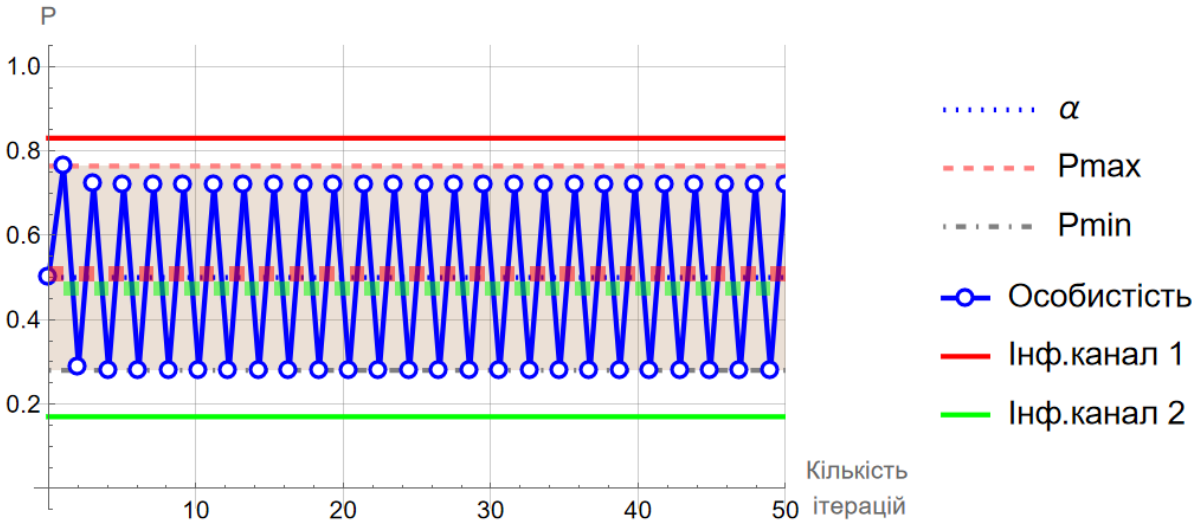
Кластер 2: кандидати К-10, К-11.

Визначення ймовірностей.

$$P_{Кластер1} = \frac{10}{12} = 0.83;\ P_{Кластер2} = \frac{2}{12} = 0.17.$$

У подальшому значення цих ймовірностей можуть бути прийняті як $\alpha^{+}_{соц}, \alpha^{-}_{соц}$, що дасть можливість оцінювати ступінь впливу результатів соціології на особистість.

Кожен з кластерів включає кандидатів з певною політичною ідеологією. Для звичайного виборця – особистості, яка розглядається у цій роботі, така інформація несе загальні тенденції виборчого процесу і спонукає його до прийняття ідеології тієї чи іншої групи у якості основної ключової ідеї виборів. Для забезпечення власної інформаційної захищеності особистість, у залежності від її α_j та μ_j, має сприймати інформацію про обидві групи (кластери) у певній пропорції. Підставивши значення $\alpha^{+}_{соц} = P_{Кластер1}, \alpha^{-}_{соц} = P_{Кластер2}$ у модель, отримуємо (рис. 3.2 – 3.5).



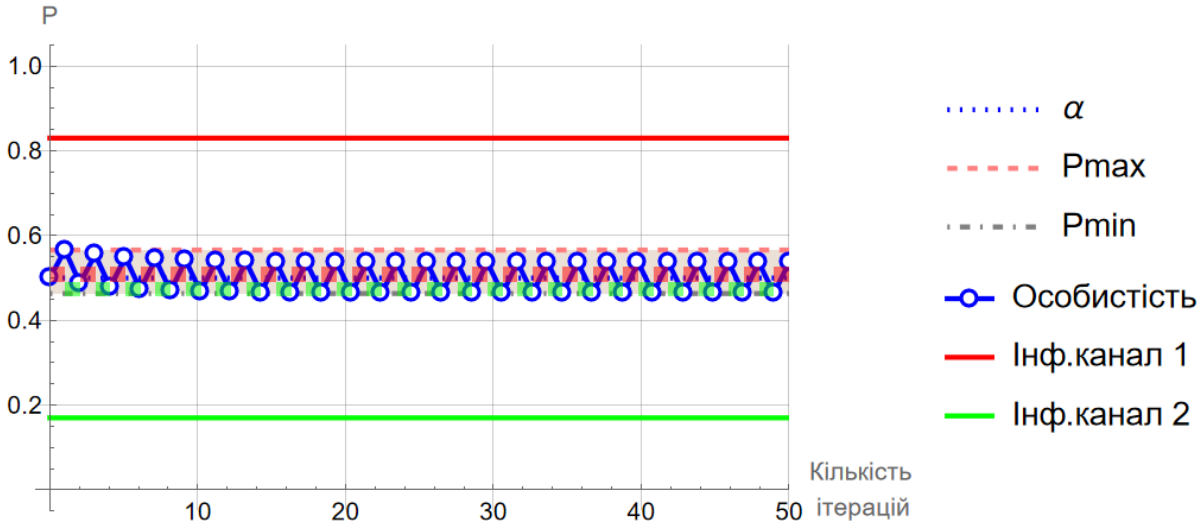
α = 0.5 μ = 0.2

Channel 1 = 25 Channel 2 = 24

Pmax = 0.76 Pmin = 0.28

△P = 0.484

Рис. 3.2. Результати моделювання при $\alpha_j = 0.5$, $\mu_j = 0.2$



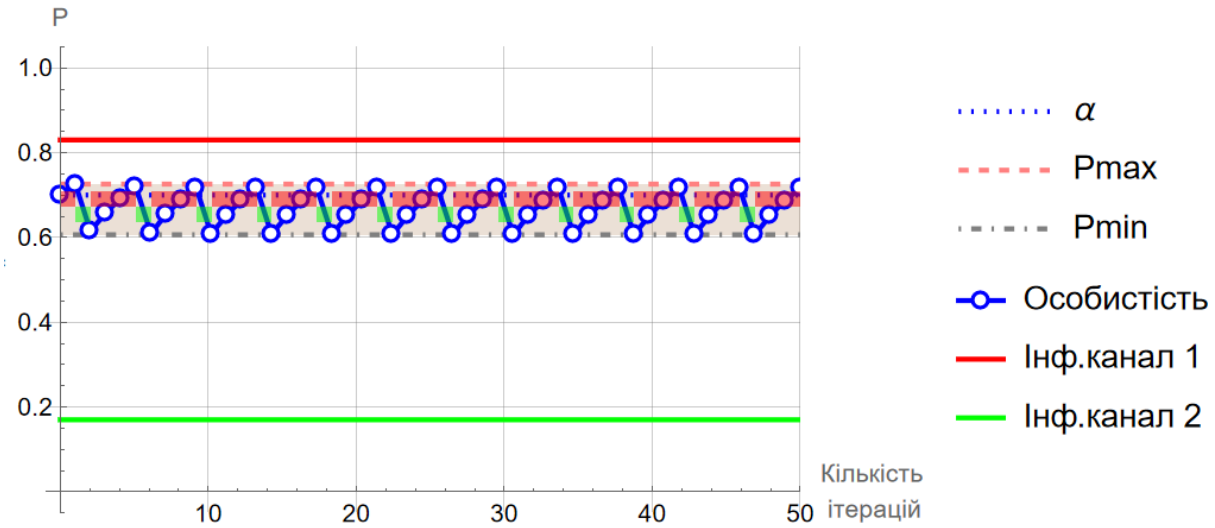
α = 0.5 μ = 0.8

Channel 1 = 25 Channel 2 = 24

Pmax = 0.57 Pmin = 0.46

△P = 0.102666

Рис. 3.3. Результати моделювання при $\alpha_j = 0.5$, $\mu_j = 0.8$



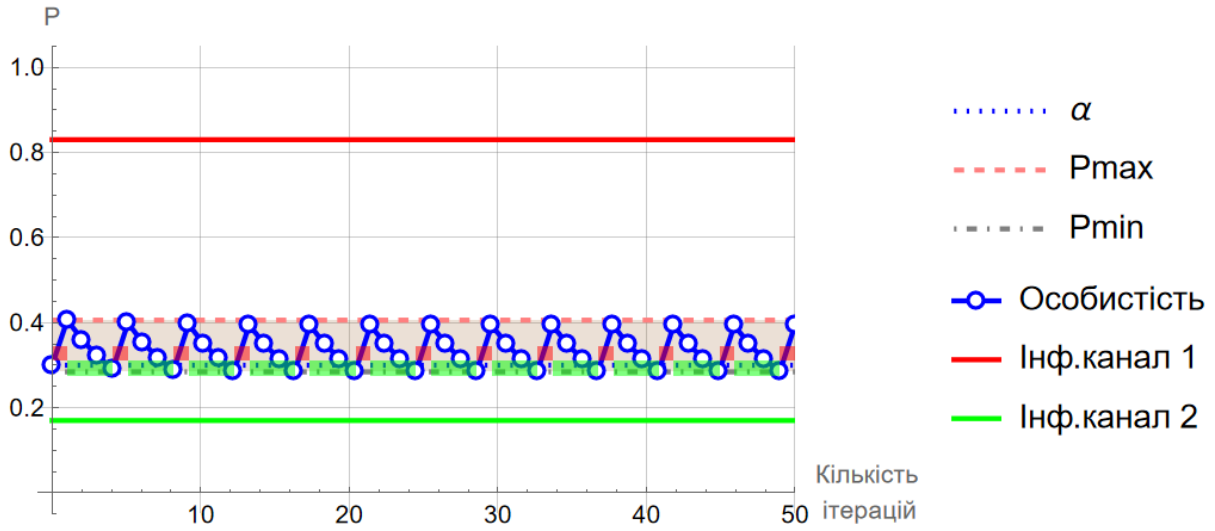
α = 0.7 μ = 0.8

Channel 1 = 37 Channel 2 = 12

Pmax = 0.73 Pmin = 0.61

ΔP = 0.119577

Рис. 3.4. Результати моделювання при $\alpha_j = 0.7$, $\mu_j = 0.8$



α = 0.3 μ = 0.8

Channel 1 = 13 Channel 2 = 36

Pmax = 0.41 Pmin = 0.28

ΔP = 0.121528

Рис. 3.5. Результати моделювання при $\alpha_j = 0.3$, $\mu_j = 0.8$

Як і раніше, з рис. 3.2 – 3.5 випливає, що інформаційна захищеність на рівні $\Delta P_j \le 0.2$ забезпечується при достатньо високих значеннях незалежності особистості $\mu_j \ge 0.8$. При цьому, для утримання ΔP_j в заданих межах особистості, яка не має чітко вираженої думки про групи кандидатів ($\alpha_j = 0.5$) необхідно регулярно змінювати канал інформаційного впливу, а саме: постійно перемикати джерело інформації з інформації про Кластер 1 на Кластер 2 і в зворотному напрямку.

У випадку, коли апріорна налаштованість особистості має спрямованість (наприклад $\alpha_j = 0.7$ на рис. 3.4) перемикання каналів інформаційного впливу матиме іншу тактику: на кожне перемикання "–" особистість, щоб залишатися у заданих межах ΔP_j має забезпечити три перемикання "+". Тобто, на практиці це може виглядати наступним чином: переглянувши одну новину про кандидатів з Кластера 2 необхідно потім переглянути 3 новини про кандидатів з Кластера 1. Така поведінка може здатися дивною з огляду на те, що особистість і так вже є прихильницею кандидатів з Кластера 1, разом з тим, вплив альтернативної новини є настільки потужним, що компенсувати його може лише втричі більша кількість новин з Кластера 1. Ситуація на рис. 3.5 є дзеркальною до ситуації на рис. 3.4 і тому не потребує окремого розгляду.

Отже, адаптація методів та технологій обробки соціологічної інофрмації має бути спрямована не стільки на джерела інформації, які можуть нести різну за своїм змістом інформацію, скільки на визначення основних концептів впливу (наративів), які можуть транслюватися різними медіа, разом з тим, підтримуючи якусь одну спільну ідею.

Висновки до розділу 3

1. Соціологічні дослідження проводяться, як правило, за різними методиками і у кінцевому вигляді їх результати надаються замовнику у вигляді таблиць, графіків, діаграм тощо. Подання результатів соціологічних досліджень у медіа може мати різні форми, залежно від мети комунікації, цільової аудиторії та складності матеріалу. В той же час, для використання результатів соціології в моделях поведінки та інформаційної захищеності особистості є необхідність приведення результатів соціології до бінарних класифікаторів з відповідними їм ймовірностями прояву. Отже, існує необхідність адаптації методів обробки соціологічної інформації для використання у моделях поведінки та інформаційної захищеності особистості.

2. Найбільш доцільним способом адаптації результатів соціологічних досліджень в інтерактивних форматах та у вигляді текстових повідомлень до бінарних альтернативних оцінок є перетворення даних на бінарні альтернативи на основі чітких критеріїв для поділу на дві групи. Наявність бінарної класифікації з відповідними ймовірностями відповідає встановленим змінним моделі інформаційної захищеності і дозволяє використовувати результати соціології напряму, без додаткових перетворень.

3. Для приведення інфографіки з множинним вибором до бінарного вибору доцільним є використання методів: групування варіантів; побудови дихотомічного показника; вибору найважливішого критерію; використання суми або середнього значення; дихотомізації за часовими показниками; конверсії множинних виборів у кілька бінарних варіантів; моделювання сценаріїв на основі множинних виборів; створення індексів.

4. Для адаптації багатовимірних соціологічних даних до моделі інформаційної захищеності особистості найбільш доцільними є методи кластерного аналізу. При цьому, об’єднання схожих об’єктів у групи може бути здійснене на основі груп методів кластерного аналізу: ієрархічних; ітеративних; факторних; на базі модальних значень щільності; з використанням теорії графів та ін. Визначення ймовірностей для кластерів підраховується за кількістю екземплярів у кластері.

5. Таким чином, набули подальшого розвитку методи обробки соціологічної інформації, які були адаптовані для використання у моделях поведінки та інформаційної захищеності особистості за рахунок бінаризації багатовимірних результатів досліджень з використанням методів кластерного аналізу та визначенням ймовірностей для бінарних кластерів. Застосування такого підходу дозволяє кількісно оцінювати вплив результатів соціології на особистість, обирати раціональну стратегію керування інформаційним впливом та забезпечувати необхідний рівень інформаційної захищеності особистості.

РОЗДІЛ 4
ДОСЛІДЖЕННЯ МОДЕЛЕЙ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЇХ ВПРОВАДЖЕННЯ

4.1. Дослідження моделі поведінки особистості

Не зважаючи на достатню спрощеність удосконаленої моделі поведінки особистості для перевірки її адекватності та ефективності необхідно дослідити її на простих прикладах. Розглянемо декілька ситуацій, коли модель повинна показати результати, близькі до реальних, які можна спостерігати в житті.

Неконтрольований натовп. Цю ситуацію будемо досліджувати взявши до уваги, що всі особистості (хоча, зважаючи на те, що натовп неконтрольований, більш доцільно було б назвати їх індивідами, суб'єктами, або членами стада) є абсолютно залежними і всі $\mu_j = 0$. У цьому випадку матриця $M = \begin{pmatrix} 0 & \cdots & 0 \\ \cdots & \cdots & \cdots \\ 0 & \cdots & 0 \end{pmatrix}$ і рівняння (2.4) набуває вигляду $(E - \Lambda)P = 0$. Суми елементів кожного з рядків матриці $(E - \Lambda)$ також дорівнюють 0. Відповідно, визначних матриці $(E - \Lambda)$ дорівнює 0, а це забезпечує існування рішення, яке не буде єдиним. Це пояснюється також тим, що у неконтрольованому натовпі, який складається з абсолютно залежних суб'єктів, немає суб'єкта з більш-менш визначеними прагненнями. Однак поведінка суб'єктів у натовпі не є хаотичною. Не зважаючи на невизначеність стану натовпу, всі суб'єкти поводять себе, у

деякому сенсі, як єдине ціле: всі P_j у всіх членів натовпу є рівними і суб'єкти діють як єдине ціле.

Дійсно, з (2.1) слідує, що $P_j = \sum_{i=1}^{N} \lambda_{j,i} P_i$. Якщо уявити, що не всі P_j є рівними між собою, то тоді серед них повинні бути суб'єкти з максимальними значеннями $P_j = P_{\max}$. Тоді відповідно, $P_{\max} = \sum_{i=1}^{N} \lambda_{\max,i} P_i$, а це, враховуючи властивості матриці Λ, можливо лише тоді, коли всі P_i є рівними між собою. Таким чином, суб'єкти поводять себе як єдине ціле.

Розглянемо приклад, коли вуличний натовп складається з 4-х осіб, які початково мають переконання $\mathrm{A} = (0.8, 0.3, 0.5, 0.2)$. Матриця незалежності для такого натовпу буде мати вигляд $M = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$. Матриця впливу, при припущенні, що кожен суб'єкт у натовпі слухає і довіряє іншим, але не слухає (і не довіряє) собі: $\Lambda = \begin{pmatrix} 0 & 1/3 & 1/3 & 1/3 \\ 1/3 & 0 & 1/3 & 1/3 \\ 1/3 & 1/3 & 0 & 1/3 \\ 1/3 & 1/3 & 1/3 & 0 \end{pmatrix}$.

Результат моделювання наведено на рис. 4.1. Як бачимо, ймовірності P_j для всіх учасників натовпу швидко сходяться до одного значення, що є результатом взаємного впливу та повної залежності від думок інших у окремих суб'єктів натовпу.

Неконтрольований натовп за своєю поведінкою нагадує стадо без вожака. Поведінка таких індивідів непередбачувана, хоча діють вони як єдине ціле, тобто можуть переходити з одного стану до іншого з загальною

для всіх ймовірністю P_j, значення якої є довільним. Однак, з цього аморфного стану натовп легко виводиться збуренням хоча б одного з параметрів μ_j: достатньо хоча б одному з суб'єктів зорієнтуватися і увесь натовп буде слідувати за лідером.

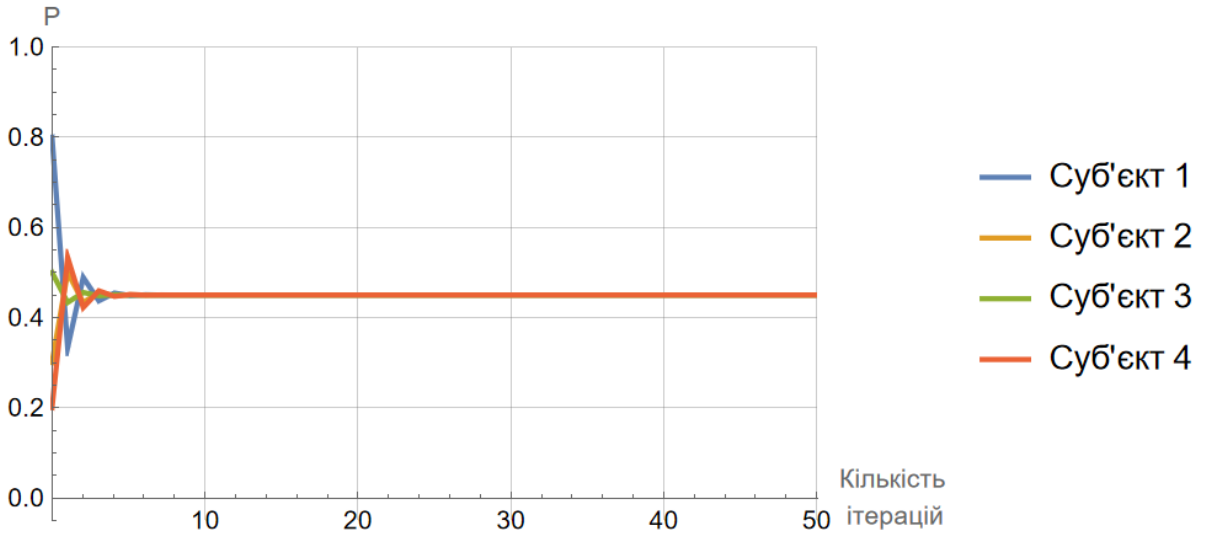


Рис. 4.1. Поведінка суб'єктів у неконтрольованому натовпі

Щоб побачити це, достатньо змінити один елемент у матриці $M = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$ і тоді лінії поведінки суб'єктів зміняться (рис. 4.2). Як бачимо, лінія P_1 залишається незмінною через $\mu_1 = 1$, в той час як лінії P_2, P_3, P_4 поступово наближаються до P_1.

Математично це пояснюється наступним чином: як тільки у натовпі з'явився лідер, у якого $\mu_k \neq 0$, то ситуація різко змінюється. Рішення рівняння стає єдиним, у всіх суб'єктів $P_j = \alpha_k$, де α_k – апріорна ймовірність k-го суб'єкта. Перевірити це можна підстановкою $P_j = \alpha_k$ в рівняння

системи (2.1). Таким чином, поведінку k-го суб'єкта (лідера) починають наслідувати решта учасників натовпу.

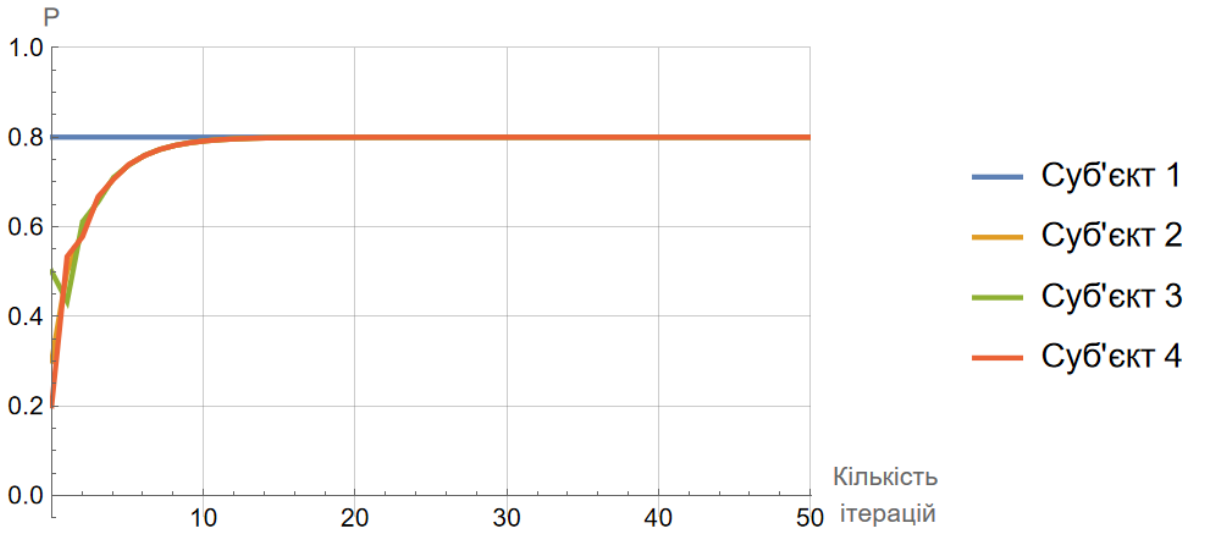


Рис. 4.2. Поведінка суб'єктів у натовпі з лідером

У цьому прикладі на початку було наведено варіант, коли, при абсолютній залежності $\mu_j = 0$, суб'єкти не надають якоїсь переваги окремим представникам натовпу. У такому натовпі для цього прикладу $\lambda_{j,i} = 1/3,\ j \neq i,\ i, j = \overline{1,3}$. Для будь якої довільної кількості учасників

$$\lambda_{j,i} = \begin{cases} \dfrac{1}{N-1}, j \neq i; \\ 0, j = i. \end{cases} \tag{4.1}$$

Вуличний мітинг. Розглянемо рівняння (2.3) більш детально, підставивши в нього (4.1).

$$P_j = \alpha_j \mu_j + \left(1 - \mu_j\right) \frac{\sum_{i=1}^{N} P_i}{N-1},\ j = \overline{1,N}, i \neq j\,. \tag{4.2}$$

Тут вираз $M = \frac{\sum_{i=1}^{N} P_i}{N-1}$ є математичним очікуванням частини суб'єктів, крім j-го, які перейшли до даного стану. Таким чином суб'єкт орієнтується на свій апріорний стан α_j і на частку решти колективу (групи, натовпу), які перейшли до цього стану. При цьому, персонально не важливо хто саме перейшов до даного стану. Система (4.2) по аналогії з (2.12) та (2.13) може бути вирішена аналітично, а при великих значеннях *N* записана у вигляді:

$$P_j = \alpha_j \mu_j + \left(1-\mu_j\right)\frac{\sum_{i=1}^{N}\alpha_i\mu_i}{\sum_{i=1}^{N}\mu_i},\ \frac{M}{N} = \frac{\sum_{i=1}^{N}\alpha_i\mu_i}{\sum_{i=1}^{N}\mu_i}. \qquad (4.3)$$

Для прикладу розглянемо вуличний мітинг, де виступають 2 лідери у яких $\alpha_1 = 1,\ \alpha_2 = 0$. Приймемо, що у натовпу $\mu_j = 0$, а $\alpha_j \in \{0;1\}$ – тобто, початкові переконання варіюються в широкому спектрі. З попереднього прикладу нам вже відомо, що початкові переконання для неконтрольованого натовпу не мають жодного значення, оскільки залежні суб'єкти легко відрікаються від власних переконань. Логічно, що такий натовп поділиться на дві частини у співвідношенні $\mu_1 \div \mu_2$, де за першим лідером піде частина $\frac{\mu_1}{\mu_1+\mu_2}$, за другим лідером $\frac{\mu_2}{\mu_1+\mu_2}$. Тобто, за більш незалежним лідером піде більша частина натовпу.

Наприклад, якщо на мітингу 2 лідери, у яких $\mu_1 = 1,\ \mu_2 = 0.8$, то у підсумку натовп поділиться у співвідношенні: $M_1 = \frac{1}{1+0.8} = 0.55$, $M_2 = \frac{0.8}{1+0.8} = 0.45$.

Перемовини. У попередньому прикладі лідери впливали на абсолютно залежних суб'єктів у натовпі. Але модель дозволяє досліджувати також вплив двох лідерів один на одного під час перемовин з якогось складного питання, на яких кожен буде відстоювати власну точку зору. Приймемо, що Лідер 1 апріорі "за", тобто $\alpha_1 = 1$ і його $\mu = \mu_1$; Лідер 2 апріорі "проти", його $\alpha_2 = 0$ і його $\mu = \mu_2$. Перемовини ведуться протягом багатьох турів тому, логічно припустити, що апостеріорна ймовірність після кожного *n*-го туру у кожного лідера стає апріорною ймовірністю для наступного *n*+1 туру: $P_1^{(n)} = \alpha_1^{(n+1)}$, $P_2^{(n)} = \alpha_2^{(n+1)}$.

Припустимо, що різниця між незалежністю лідерів не надто значна і $\mu_1 = 1$, $\mu_2 = 0.9$. У такому випадку Лідер 1 залишиться "на своїх позиціях", а Лідер 2 поступово тур за туром буде наближатися до позиції Лідера 1 (рис. 4.3). Дещо інша ситуація буде тоді, коли і Лідер 1 і Лідер 2 матимуть значення $0 < \mu < 1$. У такому випадку (рис. 4.4) позиції лідерів тур за туром будуть зближуватися одна до одної, фіксуючись на деякому проміжному значенні, що і буде реалістичним зображенням поняття "Перемовини".

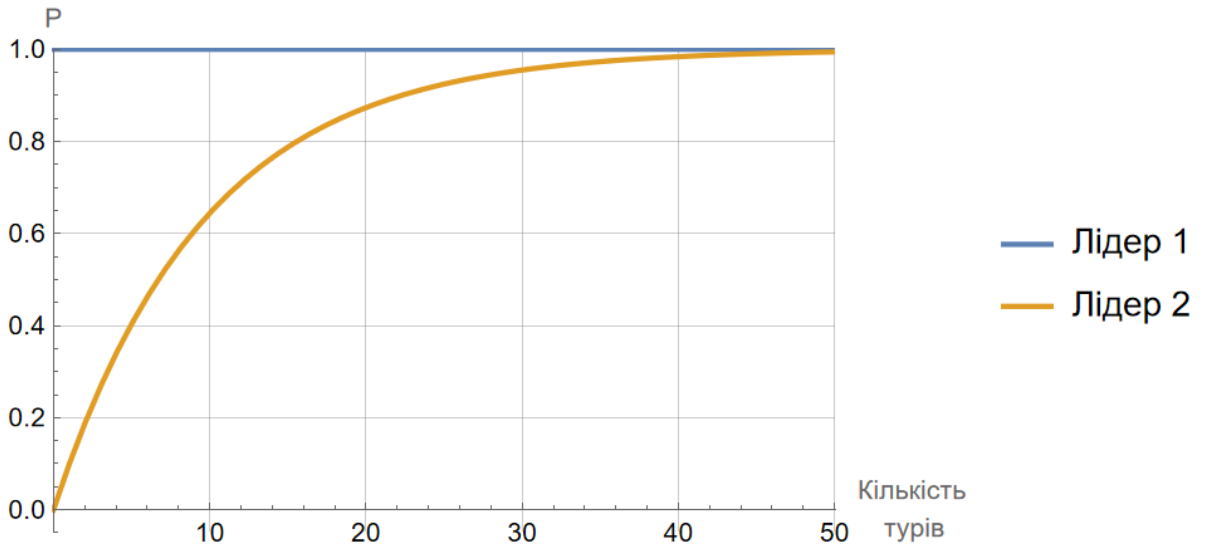


Рис. 4.3. Ілюстрація сценарію "Перемовини" при $\mu_1 = 1$, $\mu_2 = 0.9$

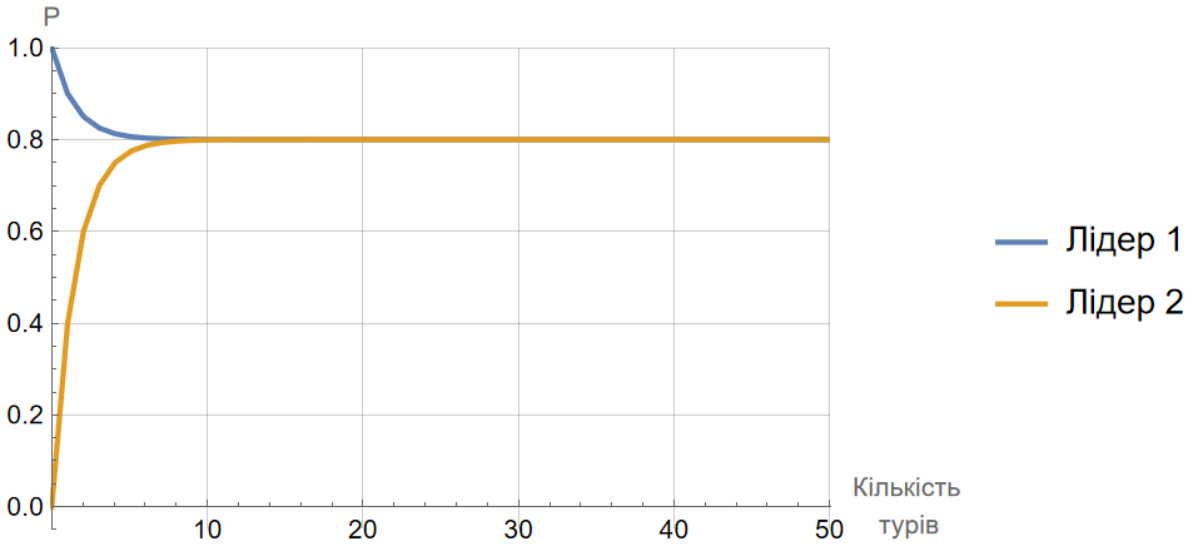


Рис. 4.4. Ілюстрація сценарію “Перемовини” при $\mu_1 = 0.9$, $\mu_2 = 0.6$

Колектив організації. Модель поведінки особистості дає можливість дослідити також деякі чисельні характеристики, які не випливають прямо з самої моделі. Розглянемо, наприклад, колектив працівників на чолі з керівником, у якого $\alpha_1 = 1$, $\mu_1 = 1$. У решти членів колективу всі $\alpha_j = \alpha$, $\mu_j = \mu$ (рис. 4.5). На цьому рисунку можна побачити, що такий колектив не є керованим, оскільки кожен з його членів має власне значення $\mu_j = \mu$.

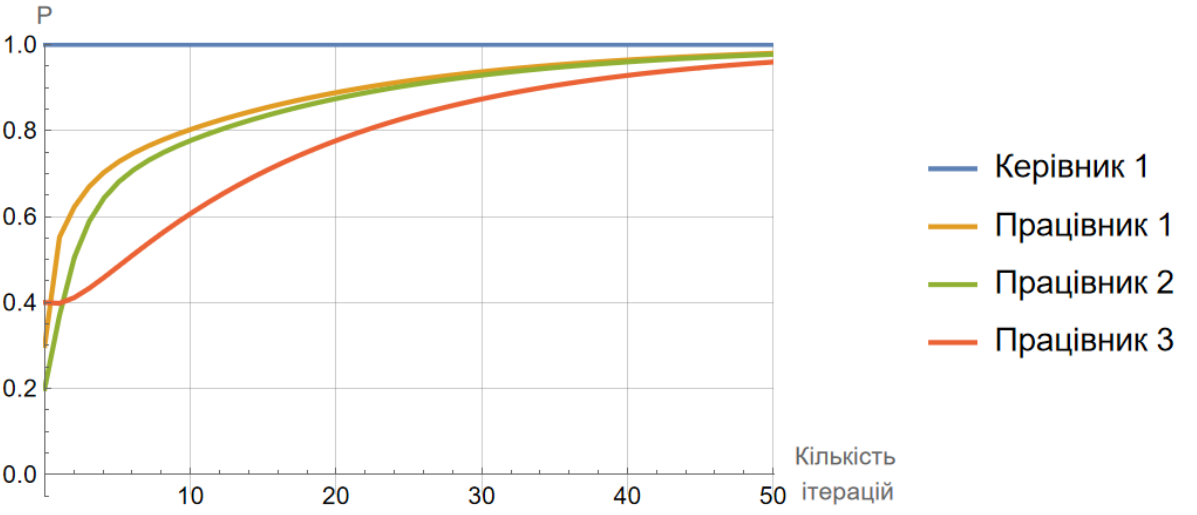


Рис. 4.5. Поведінка членів колективу при $\mu_1 = 1$, $\mu_2 = 0.1$, $\mu_3 = 0.5$, $\mu_4 = 0.9$

З формул (2.12) та (2.13) можна отримати точне рішення для

$$\frac{M}{N} = \frac{N - \mu + \alpha\mu\left(N-1\right)^2}{N - \mu + \mu\left(N-1\right)^2}. \qquad (4.4)$$

З формули (4.4) видно, що при $N \to \infty, \frac{N}{M} \to \alpha$, тобто колектив стає некерованим, оскільки взаємний вплив членів колективу один на одного нівелює вплив керівника. Відтак, виникає задача щодо визначення раціональної співвідношення членів колективу $\frac{M}{N}$, щоб частка членів колективу, які будуть виконувати вказівки керівника, була не менше деякого значення *Q*. Показник *Q* по суті справи є показником продуктивності колективу, оскільки виражає відносну кількість працівників, які будуть сумлінно працювати відносно загальної кількості працівників *N*. То скільки ж тоді потрібно мати працівників у колективі *N*, щоб забезпечити необхідний рівень продуктивності *Q*?

Промоделюємо рівняння (4.4) для різних значень α_j (рис. 4.6).

Як видно з рис. 4.6 при середніх значеннях працівників $\mu_j = 0.5$ і $\alpha_j = 0.5$ щоб вплив керівника забезпечував задану продуктивність $Q = 0.6$ у колективі має бути 9 працівників (разом з керівником), а для забезпечення $Q = 0.8$ необхідно щоб колектив складався з 3 працівників. У даному випадку мова йде саме про ефективність комунікації між керівником та працівниками у залежності від їх апріорної налаштованості α_j та незалежності μ_j. Зменшення продуктивності *Q* призводить до неефективного використання трудових ресурсів.

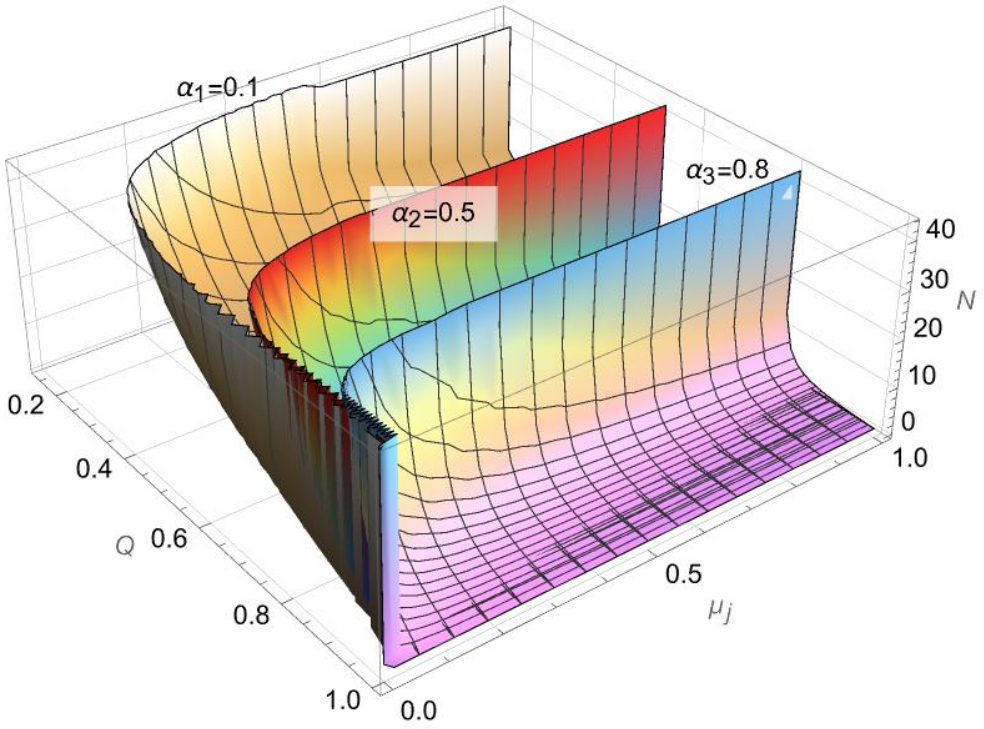


Рис. 4.6. Залежність загального числа працівників N від заданого рівня продуктивності Q, ступеня незалежності працівника μ_j та його початкового ставлення до роботи α_j

4.2. Дослідження моделі інформаційної захищеності особистості

Інформаційний портрет середньостатистичного українця. Для дослідження моделі інформаційної захищеності особистості необхідно спочатку створити інформаційний портрет середньостатистичного українця, з яким потім порівняти громадянина, який самостійно керує інформаційним впливом на нього. За даними [85] найпопулярнішим джерелом інформації для українців є соціальні мережі – 77.9% опитаних. На другому місці – телебачення з 62.5%, на третьому – інтернет (без урахування соціальних мереж) – 57.7%. Менш популярними є радіо (33.7%) та

друковані медіа (17.8%). Помітні відмінності у споживанні новин спостерігаються в розрізі вікових категорій (табл. 4.1) [85].

Таблиця 4.1

Розподіл джерел інформації за віковими категоріями

Вік респондентів	18–29 років	30–39 років	40–49 років	50–59 років	60–69 років	70+ років	**Сер. знач.**
Соціальні мережі	95.8%	90.3%	87.0%	79.8%	66.6%	36.5%	**77.9%**
Телебачення	40.5%	50.8%	58.2%	72.2%	78.0%	83.7%	**62.5%**
Інтернет-ресурси	73.8%	64.2%	62.5%	58.7%	51.6%	22.5%	**57.7%**
Радіо	23.6%	34.6%	29.1%	32.5%	40.7%	43.6%	**33.7%**
Друковані медіа	10.5%	13.7%	16.8%	23.1%	26.4%	31.3%	**17.8%**

Географічно, у різних регіонах України популярність соціальних мереж та інтернету майже не відрізняється. Найчастіше слухають радіо (40%) та читають друковані медіа (24.1%) на Заході України. Телебачення дещо частіше дивляться на Заході (65.6%) та в Центрі (64.9%), ніж на Півдні (57.9%) та Сході (58.4%). Також, на відміну від інших регіонів, мешканці Сходу та Півдня майже однаково часто споживають новини з телевізора й інтернету (без урахування соцмереж).

Телебачення та соціальні мережі мають практично однаковий рівень довіри українців. З незначним відривом лідерство зберігає телебачення (61.1%), а соціальним мережам довіряють лише на 1.1% менше опитаних. Довіра до інтернету без соціальних мереж є дещо меншою (45.1%), до радіо – 41%, до друкованих медіа – 30.3%. Не довіряють жодному з джерел майже 8% респондентів [85].

Розмір Інтернет аудиторії у лютому 2024 року склав 26.2 млн Real Users. Середній час проведений інтернет-користувачем (ATS) = 18 год 6 хв.

Найбільше українці використовували для виходу в глобальну мережу Смартфони (24.1 млн Real Users та ATS = 8 год 29 хв) та ПК (14.3 млн Real Users та ATS = 8 год 29 хв). Планшетна аудиторія становить 2.3 млн Real Users, а ATS =15 хв. Аудиторія десктопів та смартфонів – 12.3 млн Real Users з урахуванням перетину аудиторії між цими платформами.

На платформах ПК+Телефони у лютому, лідерами по охопленню є наступні медіа. На першій позиції знаходиться сервіс Google (88.9%), на другій – YouTube (54.4%), а на третьому місці – соціальна мережа Facebook (53.4%), потім вільна онлайн бібліотека Wikipedia (45.2%), за нею маркетплейс Rozetka (38.8%) та новинний портал UNIAN (36.6%). На сьомому місці – портал UKR.net (36.5%). Далі – Instagram (35.3%). А закриває Топ-10 – сайт новин TSN (34.4%) та маркетплейс PROM.ua (33.9%). Найдовший середній проведений час на сайті незмінно у Google, а за ним маркетплейс OLX та YouTube [86].

Соціологічні дослідження є частиною новинного простору українських медіа, забезпечуючи журналістів, аналітиків та громадськість достовірною та актуальною інформацією про суспільні настрої, думки та тенденції. Ось кілька ключових аспектів цієї ролі:

Інформування громадськості. Соціологічні дослідження надають медіа інформацію про те, що турбує громадян, їхні пріоритети та настрої. Це допомагає формувати новинний порядок денний, орієнтуючи журналістів на теми, які є найбільш актуальними для суспільства.

Аналіз політичних настроїв. Соціологічні опитування часто використовуються для аналізу політичних настроїв та рейтингів політичних партій і лідерів. Це важливо під час виборчих кампаній та в періоди політичної нестабільності.

Оцінка ефективності політик і реформ. Медіа використовують результати соціологічних досліджень для оцінки ефективності державних

політик і реформ, а також для розуміння того, як ці політики сприймаються громадянами.

Виявлення соціальних проблем. Соціологічні дослідження допомагають виявити соціальні проблеми, які можуть бути недостатньо висвітлені в медіа. Наприклад, питання безробіття, корупції, охорони здоров'я та освіти часто стають предметом досліджень і, відповідно, новинних сюжетів.

Підвищення довіри до медіа. Використання результатів науково обґрунтованих соціологічних досліджень підвищує довіру до медіа. Громадяни бачать, що новини базуються на реальних даних, а не лише на думках чи припущеннях.

Глибинний аналіз та експертні коментарі. Медіа часто залучають соціологів для експертних коментарів і глибинного аналізу подій та тенденцій. Це додає новинам професійного виміру та дозволяє глибше розуміти причини і наслідки тих чи інших явищ.

Моніторинг громадської думки. Регулярні соціологічні опитування дозволяють медіа моніторити зміни у громадській думці протягом часу. Це важливо для відстеження довготривалих тенденцій і швидких змін у настроях населення. Приклади використання соціологічних досліджень у медіа:

Рейтинги політичних партій перед виборами. Опитування про соціальні настрої щодо актуальних питань, таких як війна, економіка чи пандемія.

Аналіз ефективності державних заходів і громадських реакцій на них. Виявлення та висвітлення соціальних проблем, які потребують уваги громадськості та влади.

Соціологічні дослідження є невід'ємною частиною якісного журналістського контенту, що сприяє кращому розумінню суспільства та інформуванню громадян. При цьому, розподіл присутності результатів соціології в різних медіа є досить неоднорідним. Так, станом на 2024 рік

можна визначити наступну присутність результатів соціології в джерелах інформації (табл. 4.2.)

Таблиця 4.2

Вплив соціологічної інформації на середньостатистичного українця

Медіа	Розподіл використання джерел інформації середньостатистичним українцем	Розподіл повідомлень соціології за джерелами інформації	Частка загальної кількості повідомлень соціології, яку сприймає середньостатистичний українець
Інтернет	0.23	0.25	**0.0575**
Телебачення	0.25	0.20	**0.05**
Соціальні мережі	0.31	0.10	**0.031**
Журнали	0.03	0.30	**0.009**
Газети	0.04	0.10	**0.004**
Радіо	0.14	0.05	**0.007**
Всього	**1.0**	**1.0**	**0.1585**

Отже, з кожних 100 повідомлень, які висвітлюють результати соціології, лише 16 доходить до середньостатистичного українця через різні канали інформаційного впливу. Разом з тим, зважаючи на цінність і вагу інформації, яка висвітлюється у таких повідомленнях, результуючий загальний вплив на особистість може бути достатньо суттєвим.

Офіційні повідомлення результатів соціології в українських офіційних медіа, висвітлюють, як правило, основні наративи держави та її влади. Разом з тим, в численних медіа присутні також альтернативні погляди на різноманітні суспільні процеси, які також підкріплюються результатами соціології. В Україні працює не більше десяти авторитетних служб, спроможних провести якісне та достовірне всеукраїнське опитування

громадської думки. Коли правдиві результати політиків не влаштовують, вони через спеціальні псевдосоціологічні служби оприлюднюють вигідні для себе результати. Це потрібно для того, наприклад, щоб набрати додаткові голоси на виборах. За даними [87] активність псевдосоціологів різко збільшується у часи значних соціальних потрясінь в суспільстві, таких як вибори, різноманітні кризові явища, в т.ч. війна та ін. Крім того, український та доступний світовий медіапростір не позбавлені також явно ворожих втручань, агресивної ворожої пропаганди та прихованого впливу.

Присутність альтернативного (проросійського) контенту у різних джерелах інформації в Україні може варіюватися залежно від конкретного джерела, регіону та інших факторів. У табл. 4.3 наведено оцінки кількості інформаційних повідомлень з різних джерел інформації та розподілу частки альтернативного контенту у різних медіа за добу станом на 2024 рік.

Таблиця 4.3

Добова активність та кількість повідомлень, які сприймає середньостатистичний українець

Медіа	Кількість сприйнятих повідомлень за добу	Час використання ресурсу (годин за добу)	Частка альтернативного (проросійського) контенту (%)	Кількість альтернативних (проросійських) повідомлень
Інтернет	42	3	19%	7.98
Телебачення	15	2	8%	1.2
Соціальні мережі	25	1.5	24%	6
Радіо	7	1	7%	0.49
Газети	5	0.5	3%	0.15
Журнали	2	0.25	2%	0.04
Всього	**96**	**7.5**		**15.86**

Навіть на третій рік повномасштабної війни частка альтернативного (проросійського) контенту в українському інформаційному просторі залишається досить високою. За даними [88] майже 8% респондентів користуються російськими медіа. Частка тих, хто користується російськими медіа в оточенні респондентів, становить до 16%. Головна причина використання російських медіа – дізнатися, що вони говорять про Україну (рис. 4.7).

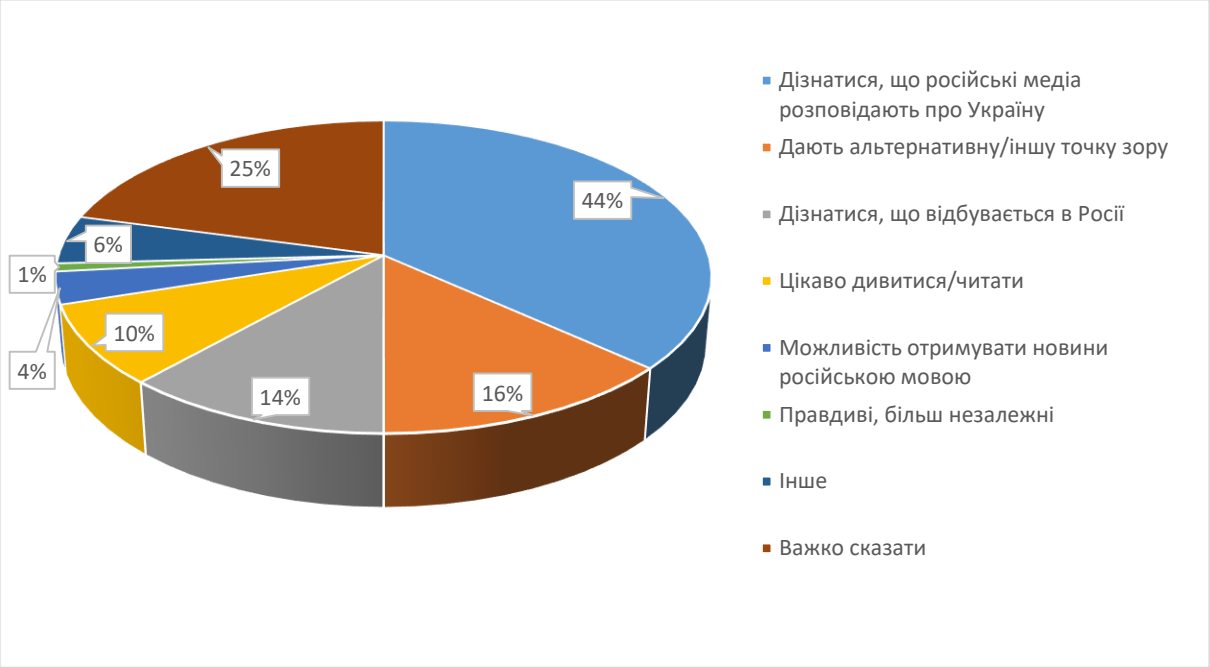


Рис. 4.7. Статистика використання російських медіа в інфопросторі України [88]

Відповідно до табл. 4.3, якщо перерахувати кількість повідомлень альтернативного (проросійського) контенту, яку сприймає середньостатистичний українець (15.86), до загальної кількості повідомлень з усіх медіа (96), то можна побачити, що 16.5% є альтернативною. Тобто, кожне шосте повідомлення відноситься до альтернативних (на теперішній час, переважно проросійських). Відтак, для особистості, яка не керує

інформаційним потоком самостійно, саме це співвідношення і буде визначати її рівень інформаційної захищеності.

Дослідження моделі. Тепер проведемо дослідження моделі інформаційної захищеності особистості, базуючись на тих даних, які були отримані під час попереднього розгляду. Для такого дослідження скористаємось сценарієм “Рейтинг президента”. Суть цього сценарію полягає в тому, що офіційні медіа періодично публікують результати соціологічних досліджень щодо рейтингів ключових інституцій держави та окремих політиків. Серед них рейтинг Президента України відображає загальні тенденції підтримки населенням політики та курсу, який реалізується у державі на поточний момент. Крім того, таке дослідження достатньо легко провести, оскільки в руках дослідників є велика кількість інформації та власні спостереження, що дає змогу оцінювати результати з точки зору їх адекватності та точності. Крім офіційних даних, які зібрані відомими соціологічними компаніями, у медіа часто публікуються/висвітлюються дані альтернативних джерел, які, через свою доступність, також є каналами інформаційного впливу на особистість. Достатньо важко оцінювати неупередженість таких джерел, але, маючи модель інформаційної захищеності можна кількісно оцінити той вплив, який чинять такі джерела на особистість і як, в решті решт, впливають на її інформаційну захищеність.

Отже, соціологічна служба Центру Разумкова з 21 по 27 березня 2024 року провела опитування у 22-х областях та місті Києві (у Запорізькій, Миколаївській, Харківській, Херсонській областях – лише на тих територіях, що контролюються урядом України та на яких не ведуться бойові дії). Опитування проводилося за стратифікованою багатоступеневою вибіркою із застосуванням випадкового відбору на перших етапах формування вибірки та квотного методу відбору респондентів на заключному етапі. Структура вибіркової сукупності відтворює

демографічну структуру дорослого населення територій, на яких проводилося опитування, станом на початок 2022 року (за віком, статтю, типом поселення). Всього було опитано 2020 респондентів віком від 18 років. Теоретична похибка вибірки не перевищує 2.3% [89].

Також, 16 – 22 травня 2024 року Київський міжнародний інститут соціології (КМІС) провів власне всеукраїнське опитування громадської думки "Омнібус", до якого на замовлення громадської організації Центр стратегічних комунікацій "Форум" були додані запитання щодо 5-річчя Президента В. Зеленського. Методом телефонних інтерв'ю на основі випадкової вибірки мобільних телефонних номерів було опитано 1002 респонденти, що мешкають у всіх регіонах України (підконтрольна Уряду України територія). Опитування проводилося з дорослими (у віці 18 років і старше) громадянами України, які на момент опитування проживали на території України, яка контролювалася Урядом України. До вибірки не включалися жителі територій, які тимчасово не контролюються владою України, а також опитування не проводилося з громадянами, які виїхали за кордон після 24 лютого 2022 року [90].

Станом на травень 2024 року довіру до Президента України висловили 59% опитаних громадян. Формально за звичайних обставин статистична похибка такої вибірки (з імовірністю 0.95 і з врахуванням дизайн-ефекту 1.1) не перевищувала 3.4% для показників, близьких до 50%, 3.0% для показників, близьких до 25%, 2.1% - для показників, близьких до 10%, 1.5% – для показників, близьких до 5% [90].

Тобто, як бачимо дві потужні соціологічні організації з різницею у 2 місяці дали однаковий результат щодо рейтингу Президента України – 59%.

У цей же період альтернативні медіа, переважно через Телеграм канали та інші медіа, які є доступними в Україні і список яких періодично публікується на сайті СБУ [91, 92], опублікували власні дані також з

посиланнями на результати соціологічних досліджень, згідно з якими рейтинг Президента України склав лише 25%.

Отже, для застосування в моделі інформаційної захищеності маємо у якості початкових даних: $\alpha_1 = 0.59$, $\alpha_2 = 0.25$. Оскільки достатньо складно визначити реальний рівень довіри до таких джерел інформації, візьмемо найбільш складну ситуацію, коли такий рівень довіри в обох випадках дорівнює 1, тобто, $\lambda_1 = 1$, $\lambda_2 = 1$. Основним змінним параметром при моделюванні буде кількість сприйнятої інформації, яка визначатиметься співвідношенням кількості офіційних та альтернативних інформаційних повідомлень. Як було встановлено раніше, таке співвідношення для середньостатистичного українця, який не дбає про власну інформаційну безпеку а сприймає інформацію з українського медіа сегменту, складає 5:1. Для особистості, яка власноруч керує інформаційною захищеністю, таке співвідношення буде залежати від стратегії перемикання каналів інформаційного впливу, які і будуть аналізуватися пізніше.

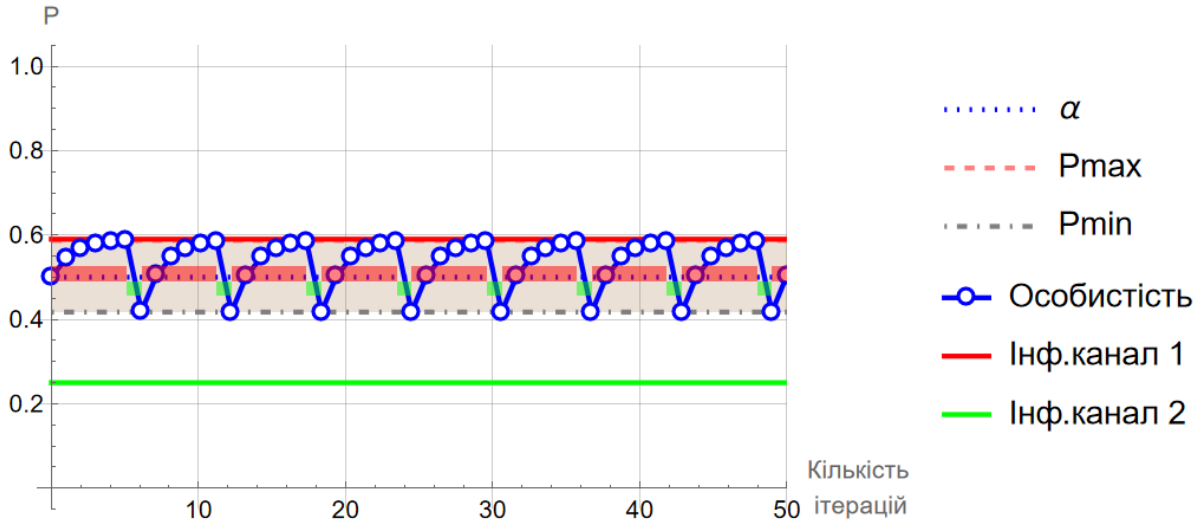
У якості основного параметра інформаційної захищеності досліджуватиметься ΔP_j, який показує "розкид" ймовірності того, що особистість у якийсь довільний момент часу може прийняти рішення на користь однієї з альтернативних точок зору. Дослідимо та порівняємо зміну ΔP_j при різних значеннях початкових переконань особистості α_j, її незалежності μ_j для кожного з варіантів:

1) особистість під впливом медіа в українському інформаційному середовищі (без керування власною інформаційною захищеністю);

2) особистість самостійно керує власною інформаційною захищеністю перемикаючи канали інформаційного впливу при найменшому впливі;

3) особистість самостійно керує власною інформаційною захищеністю перемикаючи канали інформаційного впливу при суттєвому впливі.

Наведемо приклад для особистості, яка не має початкових уподобань щодо підтримки чи не підтримки президента $\alpha_j = 0.5$ та є посередньо незалежною $\mu_j = 0.5$. Як бачимо з рис. 4.8 для особистості, яка не керує інформаційним впливом (сприймає інформацію у тій кількості та у тих пропорціях, яку надають медіа) $\Delta P_j = 0.17$. Перемикання каналів впливу за стратегією найменшого впливу дає такій особистості перевагу, оскільки тепер її $\Delta P_j = 0.15$ (рис. 4.9). Зміна стратегії перемикання каналів на перемикання при суттєвому впливі за даного співвідношення $\alpha_j = 0.5$ та $\mu_j = 0.5$ не дає суттєвої переваги і $\Delta P_j = 0.17$ (рис. 4.10).



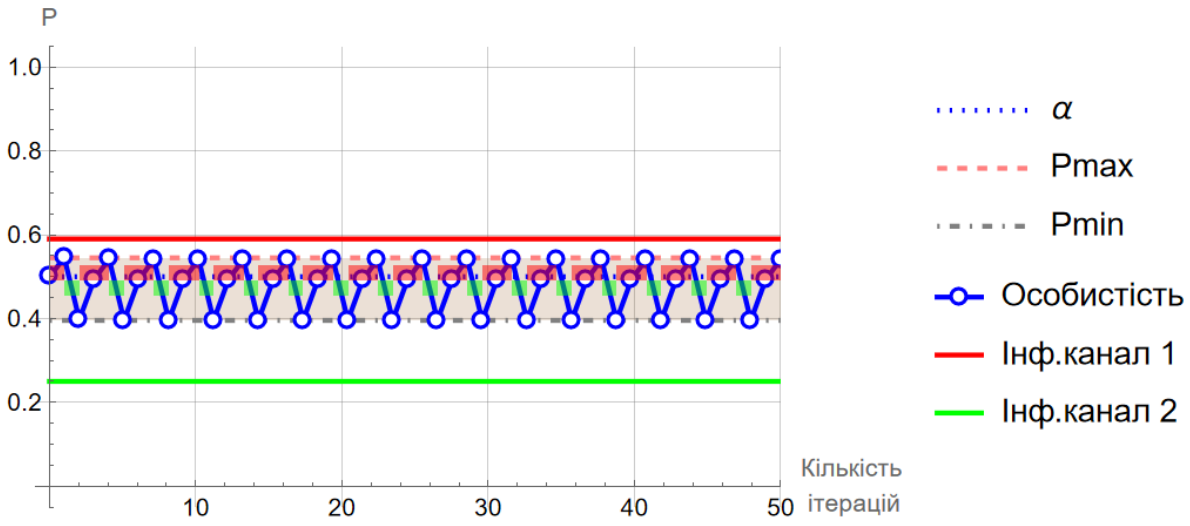
α = 0.5 μ = 0.5

Channel 1 = 41 Channel 2 = 8

Pmax = 0.59 Pmin = 0.42

△P = 0.169886

Рис. 4.8. Моделювання інформаційної захищеності для особистості без керування інформаційним впливом



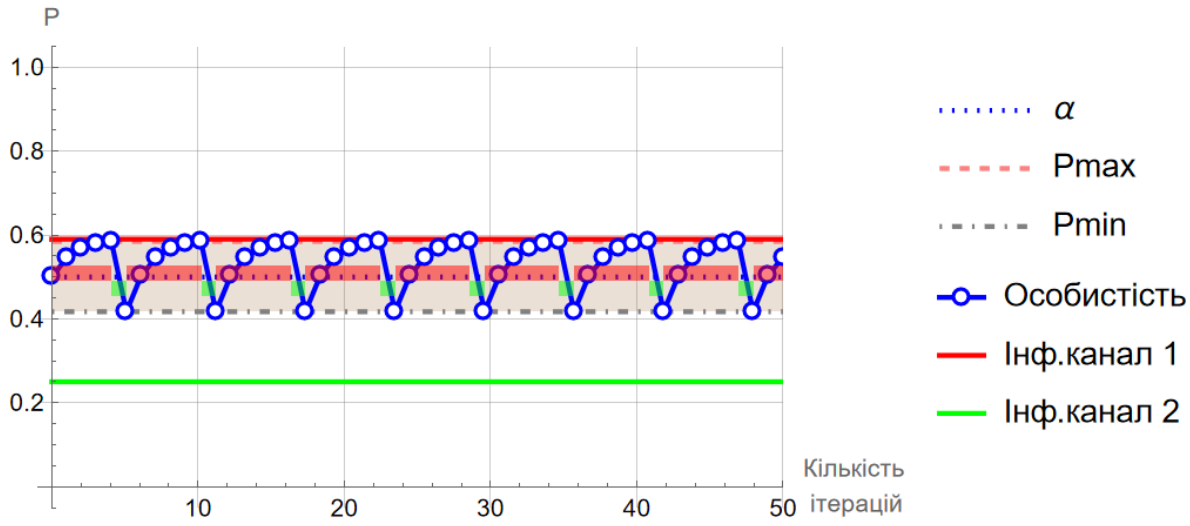
α = 0.5 μ = 0.5

Channel 1 = 33 Channel 2 = 16

Pmax = 0.54 Pmin = 0.4

ΔP = 0.149286

Рис. 4.9. Моделювання інформаційної захищеності для особистості з перемиканням за найменшим інформаційним впливом



α = 0.5 μ = 0.5

Channel 1 = 41 Channel 2 = 8

Pmax = 0.58 Pmin = 0.42

ΔP = 0.167416

Рис. 4.10. Моделювання інформаційної захищеності для особистості з перемиканням за суттєвим інформаційним впливом

Промоделюємо для різних значень α_j та μ_j. При цьому α_j будемо брати в діапазоні від 0.25, що означає підтримку альтернативної соціології щодо рівня довіри президентові, до 0.59, що означає підтримку офіційного рівня довіри президентові (табл. 4.4 – 4.6).

Таблиця 4.4

Значення ΔP_j для середньостатистичного українця в типовому інформаційному просторі

μ_j \ α_j	0.25	0.3	0.4	0.5	0.59
0.0	0.34	0.34	0.34	0.34	0.34
0.1	0.34	0.31	0.31	0.31	0.31
0.2	0.34	0.29	0.27	0.27	0.27
0.3	0.34	0.29	0.24	0.24	0.24
0.4	0.34	0.29	0.20	0.20	0.20
0.5	0.33	0.28	0.18	0.17	0.17
0.6	0.33	0.28	0.18	0.14	0.14
0.7	0.32	0.27	0.17	0.11	0.12
0.8	0.31	0.26	0.16	0.10	0.9
0.9	0.30	0.25	0.15	0.05	0.07
1.0	0.0	0.0	0.0	0.0	0.0

Аналіз таблиць 4.4 – 4.6 показує явну перевагу сприйняття даних соціології за однією зі стратегій перемикання каналів інформаційного впливу над поведінкою середньостатистичної особистості, яка перебуває у звичайному інформаційному просторі.

Таблиця 4.5

Значення ΔP_j для особистості з перемиканням каналів при найменшому впливі

μ_j \ α_j	0.25	0.3	0.4	0.5	0.59
0.0	0	0.34	0.34	0.34	0
0.1	0	0.28	0.29	0.30	0
0.2	0	0.27	0.24	0.27	0
0.3	0	0.23	0.20	0.23	0
0.4	0	0.19	0.17	0.20	0
0.5	0	0.15	0.13	0.15	0
0.6	0	0.13	0.10	0.12	0
0.7	0	0.09	0.07	0.09	0
0.8	0	0.07	0.07	0.07	0
0.9	0	0.03	0.03	0.03	0
1.0	0.0	0.0	0.0	0.0	0.0

Щоб оцінити це покращення кількісно, необхідно знайти відсоток зменшення ΔP_j для кожної зі стратегій відносно ΔP_j захищеності середньостатистичної особистості в типовому інформаційному просторі. Особливо чітко це проглядається на краях таблиць, де вдається забезпечити $\Delta P_j = 0$ через те, що у таких випадках при $\alpha_j = 0.25$ або $\alpha_j = 0.59$ переконання особистості збігаються з офіційною або альтернативною соціологією.

Результати обчислень приросту ефективності (зменшення ΔP_j) наведені в табл. 4.7 – 4.8.

Таблиця 4.6

Значення ΔP_j для особистості з перемиканням каналів при суттєвому впливі

μ_j \ α_j	0.25	0.3	0.4	0.5	0.59
0.0	0	0.05	0.15	0.09	0
0.1	0	0.05	0.15	0.09	0
0.2	0	0.05	0.25	0.09	0
0.3	0	0.05	0.22	0.09	0
0.4	0	0.05	0.18	0.09	0
0.5	0	0.05	0.15	0.17	0
0.6	0	0.05	0.12	0.12	0
0.7	0	0.05	0.10	0.09	0
0.8	0	0.07	0.07	0.06	0
0.9	0	0.03	0.03	0.03	0
1.0	0.0	0.0	0.0	0.0	0.0

Як бачимо, в табл. 4.7 та в табл. 4.8 при $\alpha_j = \{0.25, 0.59\}$ значення зменшення ΔP_j сягає 100%. Ця обставина обумовлена самою суттю процедури перемикання каналів. А саме, перед тим як особистість намагається перемкнути канал, вона спочатку аналізує ступінь отриманого впливу та ступінь впливу, який потенційно може бути отримано після перемикання. Значення $\alpha_j = \{0.25, 0.59\}$ в даній задачі є крайовими і тому модель не пропонує користувачу навіть пробувати перемикати канал впливу, оскільки це не призведе до суттєвої зміни апостеріорної ймовірності P_j відносно апріорної ймовірності α_j.

Таблиця 4.7

Зменшення ΔP_j для особистості з перемиканням каналів при найменшому впливі

μ_j \ α_j	0.25	0.3	0.4	0.5	0.59
0.0	100.0%	0.0%	0.0%	0.0%	100.0%
0.1	100.0%	9.7%	6.5%	3.2%	100.0%
0.2	100.0%	6.9%	11.1%	0.0%	100.0%
0.3	100.0%	20.7%	16.7%	4.2%	100.0%
0.4	100.0%	34.5%	15.0%	0.0%	100.0%
0.5	100.0%	46.4%	27.8%	11.8%	100.0%
0.6	100.0%	53.6%	44.4%	14.3%	100.0%
0.7	100.0%	66.7%	58.8%	18.2%	100.0%
0.8	100.0%	73.1%	56.3%	30.0%	100.0%
0.9	100.0%	88.0%	80.0%	40.0%	100.0%
1.0	–	–	–	–	–

Тобто, якщо апріорне переконання особистості повністю співпадає з апріорною ймовірністю джерела соціологічної інформації, то в такому разі немає сенсу застосовувати альтернативний інформаційний вплив – він жодним чином не вплине на апостеріорну ймовірність прийняття рішення особистістю. Ці випадки є прикладом 100% інформаційної захищеності, оскільки у даному випадку думка особистості на 100% співпадає з соціологією (хоч офіційною, хоч альтернативною).

Таблиця 4.8

Зменшення ΔP_j для особистості з перемиканням каналів при суттєвому впливі

μ_j \ α_j	0.25	0.3	0.4	0.5	0.59
0.0	100.0%	85.3%	55.9%	73.5%	100.0%
0.1	100.0%	83.9%	51.6%	71.0%	100.0%
0.2	100.0%	82.8%	7.4%	66.7%	100.0%
0.3	100.0%	82.8%	8.3%	62.5%	100.0%
0.4	100.0%	82.8%	10.0%	55.0%	100.0%
0.5	100.0%	82.1%	16.7%	0.0%	100.0%
0.6	100.0%	82.1%	33.3%	14.3%	100.0%
0.7	100.0%	81.5%	41.2%	18.2%	100.0%
0.8	100.0%	73.1%	56.3%	40.0%	100.0%
0.9	100.0%	88.0%	80.0%	40.0%	100.0%
1.0	–	–	–	–	–

Якщо в табл. 4.7 – 4.8 розглядати середнє покращення інформаційної захищеності особистості, то, відкинувши крайові значення та взявши середнє значення по таблиці у проміжку $0.25 < \alpha_j < 0.59$ та $0 \le \mu_j < 1$, можна обчислити:

середнє значення покращення для стратегії перемикання каналів при найменшому впливі складає 27.9%;

середнє значення покращення для стратегії перемикання каналів при суттєвому впливі складає 54.2%.

Такий висновок свідчить про перевагу ручного керування інформаційною захищеністю у порівнянні споживання особистістю контенту у тому вигляді і у тій кількості, яку пропонує український медіасегмент.

Дослідження точності моделі. Оскільки модель інформаційної захищеності особистості (2.17) побудована на результатах соціологічних досліджень, то цілком логічно припустити, що точність моделювання буде залежати від вхідних даних – а саме, результатів соціології. Не зважаючи на всю складність соціологічної науки, у багатьох випадках результати таких досліджень залежать від розміру вибірки (частки населення, яке підлягає опитуванню).

Визначення необхідної кількості вибірки для соціологічних досліджень при заданій похибці результатів та заданій ймовірності (рівні довіри) можна здійснити за допомогою формули для обчислення розміру вибірки [93]. Для цього введемо деякі поняття:

Рівень довіри (confidence level) – зазвичай 95% або 99%. Відповідає значенню Z у стандартному нормальному розподілі.

Похибка (margin of error, E) – максимальна допустима похибка результату.

Пропорція (p) – очікувана частка населення, яка має певну характеристику. Якщо невідома, часто використовують 0.5 для максимальної невизначеності.

Розмір популяції (N) – загальна кількість населення регіону, території, держави. Якщо популяція дуже велика ($N > 30\,000$) або нескінченна, використовується спрощена формула:

$$n = \frac{Z^2 p(1-p)}{E^2}.$$

Якщо розмір популяції відомий і менший, використовується коригована формула:

$$n = \frac{Z^2 p(1-p)}{E^2} \cdot \frac{N}{N + Z^2 p(1-p) - 1}.$$

Для різних рівнів довіри Z буде мати різні значення:

для 90% рівня довіри, $Z \approx 1.645$;

для 95% рівня довіри, $Z \approx 1.96$;

для 99% рівня довіри, $Z \approx 2.576$.

Приклад обчислення. Припустимо, що треба визначити необхідну кількість вибірки для дослідження з такими параметрами:

рівень довіри: 95% ($Z = 1.96$);

похибка: 5% ($E = 0.05$);

пропорція: 0.5 ($p = 0.5$ – максимальна невизначеність);

розмір популяції: 10 000 осіб.

Обчислення за спрощеною формулою дає результат $n = 384.16$. Обчислення за коригованою формулою (для 10 000 осіб) дає $n = 369.21$. Отже, для популяції розміром 10 000 необхідно опитати приблизно 370 осіб, щоб досягти 95% рівня довіри з похибкою 5%.

На графіку (рис. 4.11) показана залежність величини похибки від кількості опитаних осіб для вибірки з розміром популяції 10 000 осіб при рівні довіри 95%. Тут синя крива показує, як зменшується похибка зі збільшенням кількості опитаних осіб. Червона пунктирна лінія показує рівень похибки 5%. Як видно з графіку, для досягнення похибки менше 5% необхідно опитати приблизно 370 осіб, що і відповідає нашим попереднім розрахункам.

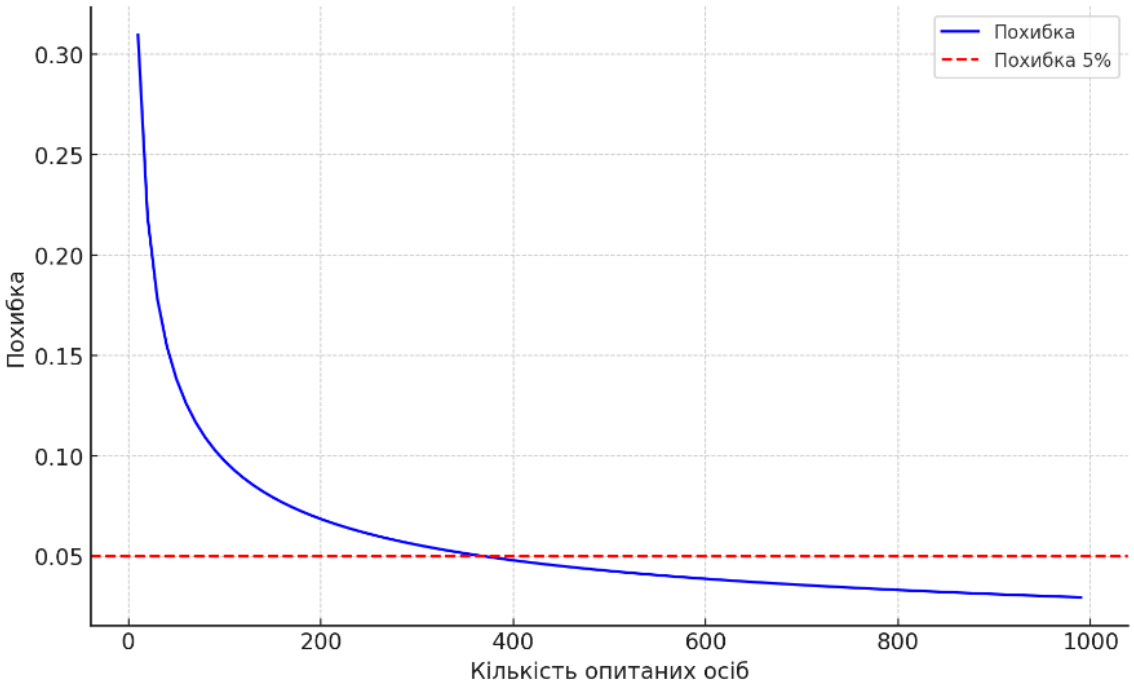


Рис. 4.11. Залежність похибки від розміру вибірки (кількості опитаних осіб)

Методика розрахунку необхідної кількості вибірки для соціологічних досліджень, яка використовує рівень довіри та похибку, є стандартним підходом у статистиці. Вона базується на теорії ймовірності та нормальному розподілі, зокрема на використанні формули для довірчого інтервалу. Для визначення необхідної кількості вибірки потрібно врахувати рівень довіри, допустиму похибку, очікувану пропорцію та розмір популяції. Використовуючи наведені формули, можна розрахувати необхідний розмір вибірки для конкретних умов дослідження.

Як вже зазначалося у прикладі з соціологічним дослідженням, проведеним Центром Разумкова та КМІС щодо довіри до Президента України, статистична похибка (з імовірністю 0.95) склала від 2.3% (Центр Разумкова) до 3.4% (КМІС), що може вважатися цілком прийнятним результатом для точності розробленої моделі [90].

4.3. Розробка рекомендацій щодо застосування моделі інформаційної захищеності особистості

У попередніх розділах роботи було розроблено математичні моделі, які, при їх сумісному застосуванні, дають можливість кількісно оцінювати інформаційний вплив, який чинять на особистість повідомлення результатів соціологічних досліджень. Ці моделі враховують початкові переконання особистості щодо певного проблемного питання в суспільстві, ступінь незалежності її мислення, результати соціологічних досліджень та рівень довіри особистості до джерел соціологічної інформації. Метою застосування моделей для окремо взятої особистості може бути оцінювання поточного інформаційного впливу та відпрацювання стратегії її поведінки в інформаційному полі задля збереження рівня початкових переконань та недопущення нав'язування думки "більшості" через соціологію. Відтак, необхідно розробити рекомендації щодо застосування запропонованих моделей. Зміст таких рекомендацій буде зводитись до послідовності етапів застосування моделей з метою забезпечення заданого рівня інформаційної захищеності особистості:

I. Локалізація предмету впливу в інформаційному полі.
II. Вибір каналів інформаційного впливу.
III. Визначення апріорних ймовірностей інформаційного впливу.
IV. Визначення рівня довіри до каналів інформаційного впливу.
V. Встановлення початкового рівня переконаності особистості.
VI. Встановлення рівня незалежності особистості.
VII. Визначення співвідношення між кількістю офіційних та альтернативних впливів в медіа.
VIII. Моделювання розкиду апостеріорної ймовірності.

IX. Визначення найкращої стратегії перемикання каналів інформаційного впливу.

І. Локалізація предмету впливу в інформаційному полі. Перш ніж розробляти заходи з підвищення інформаційної захищеності особистості необхідно спочатку визначитись: відносно якої події, факту або інформаційного приводу необхідно забезпечити захищеність особистості. Людину щодня оточують сотні інформаційних повідомлень з різних джерел і тому не можна говорити про інформаційну захищеність взагалі, адже кожне повідомлення, новина, інформаційний вкид є тим тригером, який може спричинити зміну лінії поведінки особистості або її відношення до поточних подій. Таким чином, є необхідність локалізації інформаційних приводів, які впливають на конкретну особистість.

Оскільки предметом розгляду у дисертаційній роботі є саме існування особистості в інформаційному полі соціологічних досліджень, то найбільш очевидним у цьому аспекті є звуження інформаційного простору саме до результатів соціології. Результати соціології періодично публікуються та висвітлюються у медіа, що дає можливість окреслити інформаційні приводи та звузити поле досліджень. Ось лише декілька таких прикладів, взятих з офіційного сайту Українського центру економічних і політичних досліджень імені Олександра Разумкова [94]:

1) оцінка ситуації в країні, довіра до соціальних інститутів, політиків, посадовців та громадських діячів, ставлення до виборів, віра в перемогу (червень 2024 р.);

2) чи потрібна мілітаризація українського суспільства: ставлення громадян (березень 2024 р.);

3) оцінка впливу зовнішньополітичних чинників на Україну. Ставлення до іноземних держав та окремих ініціатив їх лідерів. Оцінка громадянами України легітимності правління Путіна (березень 2024 р.).

Або, аналогічно, з сайту Київського міжнародного інституту соціології [95]:

1) динаміка готовності до територіальних поступок та ставлення до окремих пакетів мирних домовленостей (липень 2024 р.);

2) якими українці бачать відносини України і Росії та які асоціації у українців викликають Росія та прості росіяни (липень 2024 р.);

3) сприйняття українцями безпекових угод (липень 2024 р.).

Як бачимо, соціологічні агенції дають можливість достатньо просто локалізувати інформаційне поле, у якому має бути забезпечена інформаційна захищеність особистості. Разом з тим, вивчення офіційних повідомлень соціологічних служб не є єдиним засобом такої локалізації. Адже сам процес досліджень потребує часу і тому, результати дослідження можуть з'явитись з деякою затримкою, хоча сама подія вже відбулася і набула певного суспільного резонансу. Відтак, постійний моніторинг інформаційного простору, оцінка кожної резонансної події через призму власного сприйняття є також одним зі способів звуження інформаційного поля.

II. Вибір каналів інформаційного впливу. Відповідно до розробленої концепції в структурі моделі інформаційної захищеності особистості мають бути присутні 2 канали інформаційного впливу: офіційний та альтернативний.

Офіційний канал не потребує детальних пояснень, оскільки представляє офіційну (державну) точку зору на події, транслюється через офіційні та всім доступні медіа і майже не обмежується цензурою. Під каналом інформаційного впливу, як вже було зазначено, ми розуміємо цілий комплекс організаційних та технічних заходів, що здатні впливати на особистість. Сюди включаються: джерело інформації та засоби її розповсюдження – все те, що забезпечує доставку офіційної точки зору до кінцевого споживача (особистості). Офіційний канал інформаційного

впливу є найбільш доступним і практично не потребує жодних специфічних дій щодо його вибору.

Більш складна ситуація з вибором альтернативного каналу. Його наявність та доступність не завжди очевидна. В умовах політичної та військової цензури пошук альтернативного джерела інформації пов'язується, як правило, з необхідністю залучення додаткових зусиль та ресурсів. Основна вимога – альтернативний канал повинен надавати інформацію не обов'язково ворожого чи провокативного змісту, але в тій області і з тих самих питань, які висвітлює офіційний канал інформаційного впливу. Тобто, якщо офіційний канал обговорює ставлення населення до владних інституцій, то і альтернативний канал має обиратися у розрізі тих самих питань, надаючи власне бачення ситуації зі ставленням населення до владних інституцій.

Такий підхід вимагає від особистості не бути пасивним споживачем інформації, а особисто керувати процесами інформаційного впливу, що і визначає суть інформаційної захищеності особистості.

III. Визначення апріорних ймовірностей інформаційного впливу. До складу моделі поведінки особистості (2.4) та моделі інформаційної захищеності особистості (розділ 2.4) входить вектор $\mathrm{A} = \left(\alpha_j, \alpha_{оф}, \alpha_{альт}\right)$, який поєднує початкові переконання особистості α_j та ймовірності $\alpha_{оф}, \alpha_{альт}$, які представляють собою початкову налаштованість каналів впливу (офіційного та альтернативного) відносно події, яка розглядається. Заради справедливості відмітимо, що запропоновані у розділі 2 моделі не враховують зворотного впливу особистості на канали інформаційного впливу, а також те, що ймовірності $\alpha_{оф}, \alpha_{альт}$ можуть змінюватися в процесі інформаційної кампанії і тому будемо приймати ці ймовірності у вигляді констант.

Значення $\alpha_{оф}, \alpha_{альт}$ обираються за результатами соціологічних досліджень. Соціологічні служби, як правило, дають їх у своїх медіарелізах у прямих чисельних значеннях (в більшості випадків у відсотках) – для бінарних подій (рівень довіри до конкретної посадової особи, рівень підтримки дій влади та ін.). Для більш складних подій з множинними оцінками, такі оцінки потребують бінаризації та, в окремих випадках, нормалізації за методиками, наведеними у розділі 3. В будь якому випадку, дослідник на виході має отримати 2 бінарні оцінки (офіційну та альтернативну) стосовно одного й того ж предмету впливу в інформаційному полі.

Наприклад, при оцінюванні інформаційного впливу щодо питання “Чи потрібна мілітаризація українського суспільства?” (Центр Разумкова, березень 2024 року) у якості офіційної точки зору можна взяти результати дослідження, які показали, що 67% опитаних позитивно ставляться до можливості зміни на довгостроковий період пріоритетів державного бюджету на користь посилення сектору безпеки і оборони [96], тобто $\alpha_{оф} = 0.67$. У той же час, у якості альтернативної точки зору, за даними того ж проросійського Телеграм-каналу “Легітимний” (включений до списку СБУ [97], але доступний для Української аудиторії) підтримка громадянами України курсу на продовження війни та подальшу мілітаризацію суспільства становить не більше 20%, тобто $\alpha_{альт} = 0.20$. Така розбіжність у офіційній та альтернативний позиції, взята лише для наочності, показує, як може бути застосована модель навіть для самих актуальних і неоднозначних подій.

IV. Визначення рівня довіри до каналів інформаційного впливу. Визначення рівня довіри до джерела соціологічної інформації (каналу інформаційного впливу) можна здійснити за допомогою низки критеріїв.

Кожен з них можна оцінити окремо, а потім об’єднати ці оцінки в загальну шкалу від 0 до 1. Ось деякі з критеріїв, які можна врахувати:

1. Репутація джерела: Чи є джерело відомим і визнаним у наукових колах? Оцінка: від 0 (невідоме джерело) до 1 (визнане і авторитетне джерело).

2. Методологія збору даних: Чи прозорі методи, які використовувались для збору даних? Чи відповідають вони стандартам соціологічних досліджень? Оцінка: від 0 (непрозора або сумнівна методологія) до 1 (чітка і визнана методологія).

3. Час і актуальність даних: Наскільки свіжі дані? Чи відповідають вони актуальним реаліям? Оцінка: від 0 (застарілі дані) до 1 (свіжі і актуальні дані).

4. Обсяг вибірки та її репрезентативність: Наскільки велика вибірка? Чи є вона репрезентативною для цільової аудиторії? Оцінка: від 0 (мала та нерепрезентативна вибірка) до 1 (велика та репрезентативна вибірка).

5. Незалежність джерела: Чи не має джерело конфлікту інтересів? Чи не фінансується воно зацікавленими сторонами? Оцінка: від 0 (явний конфлікт інтересів) до 1 (повна незалежність).

6. Публікація в рецензованих журналах: Чи публікувались результати досліджень у рецензованих наукових журналах? Оцінка: від 0 (відсутність публікацій) до 1 (наявність публікацій у високорейтингових журналах).

Для кожного критерію, методом експертних оцінок можна визначити оцінку від 0 до 1, потім обчислити середнє значення цих оцінок.

Приклад розрахунку: репутація джерела: 0.8; методологія збору даних: 0.9; час і актуальність даних: 0.7; обсяг вибірки та її репрезентативність: 0.6; незалежність джерела: 0.9; публікація в рецензованих журналах: 0.8. Середня оцінка: (0.8 + 0.9 + 0.7 + 0.6 + 0.9 + 0.8)/6 = 0.78. Таким чином, рівень довіри до джерела соціологічної інформації буде 0.78. У моделях

рівень довіри до джерел інформації враховується через показники $\lambda_{i,j}$, де $i = 1,2$, а $\sum_{j=1}^{2} \lambda_{i,j} = 1$.

V. Встановлення початкового рівня переконаності особистості. Визначення початкового рівня власних переконань особистості щодо певної суспільної події α_j у вигляді ймовірності її сприйняття або несприйняття відповідно до офіційної точки зору можна здійснити через системний підхід. У такому випадку доцільною буде реалізація деяких основних кроків:

1. Саморефлексія та аналіз власних переконань: необхідно задати собі питання: “Як я зараз ставлюсь до цієї події?” та “Чи підтримую я офіційну точку зору?”. Також, необхідно спробувати оцінити свою позицію у відсотках, наприклад, 70% підтримки та 30% несприйняття.

2. Інформаційне середовище: на цьому кроці необхідно визначити, звідки особистість отримує інформацію про подію (ЗМІ, соціальні мережі, експерти, офіційні заяви). Необхідно оцінити рівень довіри до цих джерел інформації. Ці питання вже розглядалися на попередньому етапі рекомендацій, де оцінювався рівень довіри до джерел соціологічної інформації ще до початку реалізації інформаційного впливу на особистість. Але, тим не менше довіра до інформаційного середовища впливає також і на початкові переконання особистості, тому потребує врахування при визначенні α_j.

3. Аналіз аргументів та доказів: необхідно зібрати аргументи “за” та “проти” офіційної точки зору. Треба визначити, які аргументи для особистості виглядають переконливішими та оцінити їх вплив на погляди особистості.

4. Соціальні впливи: необхідно визначити, як впливають на погляди особистості переконання близьких їй людей, колег, соціальних груп. Також,

треба оцінити, чи є у особистості схильність приймати думку авторитетних для неї осіб? Питання схильності приймати думку авторитетних/сторонніх осіб, так само як і результатів соціології, будуть розглянуті на наступному етапі рекомендацій.

5. Психологічні фактори: потрібно визначити, як попередні переконання особистості, її цінності та досвід впливають на сприйняття події. Наприклад, якщо особистість схильна довіряти офіційним органам, ваша ймовірність підтримки офіційної точки зору може бути вищою.

6. Балансування оцінок: на цьому кроці треба сформулювати початкову оцінку у вигляді ймовірності. Наприклад, особистість може вважати, що з ймовірністю 0.6 (60%) підтримує офіційну точку зору та з ймовірністю 0.4 (40%) – ні.

Для точнішого визначення початкового рівня переконань можна скористатись шкалою оцінок та опитувальником, який включатиме різні аспекти сприйняття особистості. Наприклад:

1. Довіра до офіційних джерел інформації (0 – не довіряю, 1 – повністю довіряю): 0.7.

2. Значущість події для вас особисто (0 – незначуща, 1 – дуже значуща): 0.8.

3. Підтримка думки оточуючих (0 – не підтримую, 1 – повністю підтримую): 0.6.

4. Вплив попередніх переконань (0 – не впливають, 1 – сильно впливають): 0.5.

5. Сприйняття аргументів офіційної точки зору (0 – не переконливі, 1 – дуже переконливі): 0.7.

Середня оцінка: (0.7 + 0.8 + 0.6 + 0.5 + 0.7)/5 = 0.66.

Отже, початковий рівень переконань особистості щодо підтримки офіційної точки зору можна оцінити як 0.66.

VI. Встановлення рівня незалежності особистості. Визначення рівня незалежності особистості від думок та поглядів оточуючих і інформації медіа (ступінь конформізму) у шкалі від 0 до 1 можна здійснити через оцінку різних аспектів поведінки та переконань особистості. Ось кілька кроків, які можуть допомогти в цьому процесі:

1. Саморефлексія та самооцінка: необхідно оцінити, наскільки часто особа погоджується з думками оточуючих, навіть якщо вони не співпадають з її внутрішніми переконаннями. Також, можна оцінити як часто особистість змінює свою думку під впливом медіа.

2. Аналіз поведінки у соціальних ситуаціях: проаналізувати часто особистість висловлює свою власну думку, навіть якщо вона відрізняється від думок інших. Оцінити, наскільки особистість впевнена в своїх поглядах і як реагує на тиск з боку оточуючих.

3. Вплив інформаційного середовища: визначити як часто особистість перевіряє інформацію з різних джерел перед тим, як скласти власну думку. Оцінити, наскільки особистість схильна довіряти першому джерелу інформації, яку зустрічає.

4. Психологічні фактори: оцінити рівень самостійності особистості в прийнятті рішень. Як часто вона приймає рішення, спираючись на власні переконання, а не на думку оточуючих?

5. Поведінкові тести та анкети: можна використати анкети або тести для оцінки рівня конформізму, наприклад, шкала соціальної конформності.

Приклад анкети для оцінки рівня незалежності (ступеня конформізму). Оцініть кожне з тверджень за шкалою від 0 до 1, де 0 означає “повністю не згоден”, а 1 – “повністю згоден”:

1. Я часто погоджуюсь з думками оточуючих, навіть якщо не згоден з ними. (Зворотне твердження): 0.3 (1 – 0.7).

2. Моя думка легко змінюється під впливом нової інформації з медіа. (Зворотне твердження): 0.4 (1 – 0.6).

3. Я уникаю висловлювати свою власну думку, якщо вона відрізняється від думок інших. (Зворотне твердження): 0.2 (1 – 0.8).

4. Я часто перевіряю інформацію з різних джерел, перш ніж скласти власну думку: 0.7.

5. Я впевнений у своїх поглядах і не змінюю їх під тиском оточуючих: 0.8.

6. Я приймаю рішення самостійно, спираючись на власні переконання: 0.6.

Розрахунок загальної оцінки: середнє значення: (0.3 + 0.4 + 0.2 + 0.7 + 0.8 + 0.6)/6 = 0.5.

Це значення від 0 до 1 може інтерпретуватись як рівень незалежності. В даному прикладі, 0.5 означає середній рівень незалежності. Чим ближче значення до 1, тим більше особистість є незалежною в своїх поглядах та рішеннях, і навпаки, чим ближче до 0, тим більше особистість залежить від думок оточуючих та інформації медіа.

VII. Визначення співвідношення між кількістю офіційних та альтернативних впливів в медіа. В сучасному світі кожна людина, дотична до інформації різноманітних медіа, може власноруч підрахувати кількість повідомлень з визначеної тематики (як офіційних так і альтернативних), які вона отримує протягом певного періоду часу. Разом з тим, у багатьох випадках таке завдання може стати достатньо складним і потребуватиме комплексного підходу та використання спеціальних інструментів і методів аналізу даних. Тобто, якщо робити це на професійній основі орієнтуючись на великі групи людей, то необхідно дотримуватись певної послідовності кроків:

1. Визначення джерел даних соціології (каналів інформаційного впливу): Інтернет-медіа (новинні сайти, блоги, онлайн журнали); телебачення (новинні канали, ток-шоу); соціальні мережі (Facebook, Twitter,

Instagram, YouTube); радіо (новинні програми, ток-шоу); газети та журнали (друковані видання, онлайн версії друкованих видань).

2. Збір даних, для чого використовуються спеціалізовані сервіси та інструменти: сервіси моніторингу медіа (наприклад, Meltwater, Cision, Mention, Brandwatch) дозволяють відстежувати згадки у різних медіа та соціальних мережах; аналіз соціальних мереж за допомогою інструментів типу Socialbakers, Hootsuite, Sprout Social; сервіси збирання та аналізу новин (Google News, Media Cloud), що дозволяють зібрати новини з різних джерел.

3. Аналіз даних – автоматичне збирання та категоризація повідомлень: Веб-скрапінг з використанням бібліотек (наприклад, BeautifulSoup, Scrapy) для автоматичного збирання даних з вебсайтів; API доступ до соціальних мереж з використанням API соціальних мереж (наприклад, Twitter API, Facebook Graph API) для збирання даних; текстовий аналіз та машинне навчання – аналіз тональності (Sentiment Analysis) для визначення, чи є повідомлення провладним чи опозиційним; класифікація тексту – використання моделей машинного навчання (наприклад, BERT, LSTM) для автоматичної класифікації повідомлень.

4. Ручний аналіз та верифікація – вибіркова перевірка: ручна перевірка та аналіз вибіркових повідомлень для підтвердження правильності автоматичної класифікації; аналіз контексту та змісту повідомлень для визначення їх провладності чи опозиційності.

5. Підрахунок та візуалізація даних – статистичний аналіз: підрахунок кількості повідомлень у кожній категорії; побудова графіків та діаграм для візуалізації даних.

В результаті такого дослідження для моделі інформаційної захищеності особистості необхідно отримати співвідношення між кількістю офіційних повідомлень з певного питання до кількості альтернативних (опозиційних) повідомлень. Це дозволить визначити показник ΔP_j для особистості, яка не керує інформаційним впливом і сприймає інформацію у тій кількості та у

тих пропорціях, яку надають медіа. Саме це співвідношення і буде визначати рівень інформаційної захищеності особистості.

VIII. Моделювання розкиду апостеріорної ймовірності. Маючи необхідні вхідні дані α_j, μ_j, $\lambda_{j,i}$ відповідно до умови (2.17) можна визначити параметри P_j та ΔP_j на певному часовому проміжку і встановити на скільки є захищеною особистість, яка не керує інформаційним впливом. Тобто, говорити про інформаційну захищеність особистості можна буде тоді, коли буде забезпечено умову (2.17), а саме: апостеріорна ймовірність P_j переходу особистості до нового стану під дією інформації каналу інформаційного впливу буде залишатися у певних межах відносно її апріорної ймовірності α_j.

Як вже було зазначено у розділі 2, такий розгляд доцільно здійснити як для особистості, яка не керує інформаційним впливом (не перемикає канали впливу), так і для різних стратегій перемикання каналів. У варіанті без перемикання каналів спочатку необхідно встановити співвідношення офіційних та альтернативних повідомлень, яке визначатиме періодичність зміни каналів впливу, обумовлену лише структурою інформаційного простору.

Таким чином, в результаті моделювання буде отримано оцінки для декількох варіантів поведінки особистості:

1) без перемикання каналів впливу;

2) з перемиканням за стратегією суттєвого впливу;

3) з перемиканням за стратегією найменшого впливу.

Порівняння цих варіантів і дасть можливість визначити необхідність зміни поведінки та чисельне значення покращення інформаційної захищеності особистості у випадку зміни варіанта.

IX. Визначення найкращої стратегії перемикання каналів інформаційного впливу. З розглянутих варіантів поведінки особистості в

інформаційному просторі можна побачити, що вони, хоч і описують основні можливі лінії поведінки, разом з тим, не є вичерпними. Адже у реальній дійсності може бути велика кількість підходів щодо комбінування можливих варіантів, або відпрацювання нових, більш просунутих.

Зокрема, у даній роботі не розглядався варіант, коли особистість суттєво змінює інтенсивність інформаційних потоків (офіційного або альтернативного), включаючи ситуації зменшення такого потоку повідомлень до 0, або його збільшення до нескінченності. Такі варіанти також можливі, але, скоріш за все, теоретично. Адже складно уявити собі сучасну людину, яка може створити собі такі умови, коли вона зовсім не дотикається до інформації або її не сприймає. Також, майже теоретичною виглядає ситуація, коли людина завалена інформацією і не сприймає її через надто велику кількість. Всі такі ситуації можуть бути предметом подальших досліджень у даному напрямку.

Також, у подальшому можуть бути досліджені комбіновані варіанти впливу. Зокрема, вплив джерел соціології в їх поєднанні з вторинним впливом інших людей з оточення конкретної особистості. Так, окрема особистість може сказати, що не користується медіа для формування власних уподобань, а лише довіряє своїм колегам, друзям або членам сім'ї. Разом з тим, ніхто не застрахований від того, що це оточення не перебуває під суттєвим впливом джерел соціології і, відтак, цей вплив буде розповсюджуватись і на саму особистість.

Висновки до розділу 4

1. Дослідження удосконаленої моделі поведінки особистості на простих прикладах (неконтрольований натовп, вуличний мітинг,

перемовини, колектив організації) показують результати, близькі до реальних. Поведінка особистостей у даних прикладах є схожою на реальну поведінку людей в наведених обставинах, що свідчить про адекватність та можливість практичного застосування такої моделі.

2. Для дослідження моделі інформаційної захищеності особистості необхідно спочатку створити інформаційний портрет середньостатистичного українця. Зокрема, необхідно визначити з яких джерел та в якій кількості споживає інформацію пересічний українець. Також, в цьому інформаційному портреті необхідно виділити частку інформації, яку займають повідомлення результатів соціологічних досліджень, та визначити співвідношення між офіційними та альтернативними (псевдосоціологія, проросійський контент) каналами інформаційного впливу. Моделювання впливу за вказаними параметрами дасть зміну апостеріорної ймовірності для особистості, яка не керує таким впливом, а споживає інформацію з доступних медіа.

3. Зміна стратегії керування впливом (шляхом перемикання каналів) дає змогу досліджувати інформаційну захищеність особистості в різних умовах такого впливу. Дослідження ефективності розробленої моделі інформаційної захищеності особистості дає змогу зробити висновок, що, у порівнянні зі споживанням особистістю контенту у тому вигляді і у тій кількості, яку пропонує український медіасегмент, середнє значення покращення для стратегії перемикання каналів при найменшому впливі складає 27.9%; а для стратегії перемикання каналів при суттєвому впливі – 54.2%. Такий результат свідчить про перевагу ручного керування інформаційною захищеністю у порівнянні споживання особистістю контенту у тому вигляді і у тій кількості, яку пропонує український медіасегмент.

4. Точність результату щодо забезпечення інформаційної захищеності особистості в умовах впливу результатів соціологічних досліджень

визначається достовірністю соціології і залежить від кількості та репрезентативності вибірки, рівня довіри, допустимої похибки, та загального розміру популяції. Для прикладів, які було розглянуто, статистична похибка (з імовірністю 0.95) склала від 2.3% до 3.4%, що може вважатися цілком прийнятним результатом для точності розробленої моделі.

5. Розробка математичних моделей для кількісної оцінки інформаційного впливу, який чинять на особистість результати соціологічних досліджень, є достатньо складним завданням. Як видно з попереднього розгляду, такі моделі повинні враховувати початкові переконання особистості щодо певного проблемного питання в суспільстві, ступінь незалежності її мислення, результати соціологічних досліджень та рівень довіри особистості до джерел соціологічної інформації. Результатом застосування моделей для окремо взятої особистості може бути оцінювання поточного інформаційного впливу та відпрацювання стратегії її поведінки в інформаційному полі задля збереження рівня початкових переконань та недопущення нав’язування думки “більшості” через соціологію.

ВИСНОВКИ

У результаті дисертаційних досліджень, виконаних автором, вирішено важливе наукове завдання щодо створення моделі інформаційної захищеності особистості в умовах впливу результатів соціологічних досліджень, яке має суттєве значення для теорії та практики інформаційної безпеки держави, суспільства та окремої особистості. Відсутність аналогічних рішень у нашій країні та за кордоном робить результати досліджень пріоритетними.

У дисертації одержані такі основні результати:

1. На основі проведеного аналізу проблематики та сучасних підходів до забезпечення інформаційної захищеності особистості було виявлено, що в умовах, коли сучасні медіа мають можливість керувати і маніпулювати поведінкою особистості, підштовхуючи її до певних рішень, існує протиріччя між необхідністю доступу особистості до інформації та потребою захистити її від маніпуляцій і дезінформації. Питання формалізації процесів впливу результатів соціології на поведінку особистості на теперішній час досліджені вкрай недостатньо, а з існуючих моделей та методів найбільш адекватними є математичні моделі конформної поведінки, хоча і вони потребують удосконалення для можливості використання в них результатів соціології. Зазначені обставини підтверджують актуальність поставленого наукового завдання.

2. Удосконалено модель поведінки особистості під впливом соціологічної інформації, в основу якої покладено базову модель конформної поведінки людини з урахуванням її апріорних переконань та ступеня незалежності мислення, і яку було розширено за рахунок використання коефіцієнтів впливу на особистість джерел соціологічної інформації, що дозволяє враховувати рівень довіри особистості до джерела

соціологічної інформації та особливості сприйняття особистістю результатів соціологічних досліджень.

3. Вперше розроблено модель інформаційної захищеності особистості яка базується на концепції управління на основі ймовірнісного контролю з використанням результатів моделювання поведінки особистості під впливом соціологічної інформації, що дає можливість досліджувати різноманітні стратегії керування інформаційним впливом результатів соціології на особистість та обирати доцільну стратегію керування інформаційним потоком з метою забезпечення необхідного рівня інформаційної захищеності особистості.

4. Набули подальшого розвитку методи обробки соціологічної інформації, які були адаптовані для використання у моделях поведінки та інформаційної захищеності особистості за рахунок бінаризації багатовимірних результатів досліджень з використанням методів кластерного аналізу та визначенням ймовірностей для бінарних кластерів. Застосування такого підходу дозволяє кількісно оцінювати вплив результатів соціології на особистість, обирати раціональну стратегію керування інформаційним впливом та забезпечувати необхідний рівень інформаційної захищеності особистості.

5. Розроблені у дисертаційній роботі моделі інформаційного впливу та захищеності особистості дають можливість кількісно оцінювати вплив результатів соціологічних досліджень на особистість та визначати раціональну стратегію керування впливом, чим підвищують ефективність інформаційного захисту особистості. На базі них розроблено рекомендації для психологів, психотерапевтів, соціальних психологів, фахівців з медіаграмотності, фахівців з комунікацій та PR, юристів з питань захисту особистих прав з покращення інформаційної захищеності особистості в умовах впливу соціології. Середнє значення покращення інформаційної захищеності особистості: для стратегії перемикання каналів при

найменшому впливі складає 27.9%, для стратегії перемикання каналів при суттєвому впливі складає 54.2%.

6. Достовірність отриманих наукових результатів забезпечується використанням апробованого математичного апарату та збіжністю теоретичних результатів з результатами моделювання на реальних прикладах соціологічних досліджень, проведених провідними українськими соціологічними організаціями. При цьому, статистична похибка результату (з імовірністю 0.95) складає від 2.3% до 3.4%.

7. Мета досліджень щодо підвищення інформаційної захищеності особистості в умовах впливу результатів соціологічних досліджень досягнута і всі поставлені окремі завдання виконані повністю. Наукові результати досліджень є внеском у розвиток теоретичних основ інформаційної безпеки держави, суспільства та окремої особистості в умовах впливу результатів соціологічних досліджень.

8. Перспективними напрямками подальших досліджень може бути широке коло питань розвитку запропонованих моделей, дослідження впливу різноманітної інформації на особистість з урахуванням її персональних особливостей, розробки технічних та програмних засобів керування інформаційним впливом на особистість.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Lippmann, W. (1922). Public opinion / Walter Lippmann; with a new introduction by Michael Curtis. NewYork: Macmillan, 427 p. https://monoskop.org/images/b/bf/Lippman_Walter_Public_Opinion.pdf (дата звернення: 03.02.2024).

2. Merton, R. K. (1948). The Self-Fulfilling Prophecy. The Antioch Review, 8(2), 193–210. https://doi.org/10.2307/4609267.

3. Ajzen, I., & Fishbein, M. (1977). Attitude-behavior relations: A theoretical analysis and review of empirical research. Psychological Bulletin, 84, 888–918. https://doi.org/10.1037/0033-2909.84.5.888.

4. Noelle-Neumann, E. (1984). The Spiral of Silence: Public Opinion – Our Social Skin. Chicago, IL: The University of Chicago Press, ISBN 0-226-58932-3.

5. Zaller, J. R. (1992). The Nature and Origins of Mass Opinion. Cambridge: Cambridge University Press, 367 p. ISBN 978-0-521-40786-1.

6. Bishop, G. F. (2008). Rational public opinion or its manufacture? Reply to page. Critical Review, 20(1–2), 141–157. https://doi.org/10.1080/08913810802316399.

7. Пейдж, С. (2020). Модельне мислення. Як аналізувати складні явища за допомогою математичних моделей: перекл. з англ. Н. Яцюк; [наук. ред. І. Красіков, О. Мінько]. Видавництво: Манн, Іванов і Фербер. 528 с. ISBN 978-5-00146-867-7.

8. Разуваєва, О. О. (2005). Моделі впливу засобів масової інформації на масову політичну свідомість. Наукові записки Інституту журналістики, 18, 35–40. http://journlib.univ.kiev.ua/index.php?act=article&article=1659 (дата звернення: 08.02.2024).

9. Брайант, Д., & Томпсон С. (2004). Основи впливу ЗМІ: перекл. з англ. М.: Видавничий дім “Вільямс”. 432 с. ISBN 5-8459-0597-4.

10. Савченко, В. А., Ахрамович, В. М., & Акулінічева, М. В. (2020). Оцінювання параметрів безпеки персональних даних у степеневих соціальних мережах на основі їх топології. Сучасний захист інформації, 3(43), 6–13. https://doi.org/0.31673/2409-7292.2020.030613.

11. Савченко, В. А., Ахрамович, В. М., Дзюба, Т. М., Лаптєв, С. О., & Матвієнко, М. В. (2021). Метод розрахунку захисту інформації від взаємовпливу користувачів в соціальних мережах. Сучасний захист інформації, 1(45), 6–13. https://doi.org/10.31673/2409-7292.2021.010613.

12. Shchypanskyi, P., Savchenko, V., Akhramovych, V., Muzshanova, T., Lehominova, S., & Chegrenets, V. (2020). The Model of Secure Social Networks Activity Based on Graph Theory. International Journal of Innovative Technology and Exploring Engineering (IJITEE), 9(4), 1803–1810. http://www.ijitee.org/wp-content/uploads/papers/v9i4/D1768029420.pdf (дата звернення: 03.02.2024).

13. Савченко, В. А. (2024). Дослідження потенційного впливу соціальної інженерії на процеси цифрової трансформації. Зв’язок, 3(169), 12–17. https://doi.org/10.31673/2412-9070.2024.031217.

14. Laptiev, O., Savchenko, V., Kotenko, A., Akhramovych, V., Samosyuk, V., Shuklin, G., & Biehun, A. (2021). Method of Determining Trust and Protection of Personal Data in Social Networks. International Journal of Communication Networks and Information Security (IJCNIS), 13(1), 15–21. https://www.ijcnis.org/index.php/ijcnis/article/view/4882 (дата звернення: 23.02.2024).

15. Savchenko, V., Akhramovych, V., Matsko, O., & Havryliuk, I. (2021, September 13−19). Method of Calculation of Information Protection from Clusterization Ratio in Social Networks. Міжнародна науково-практична конференція “Інформаційна безпека та інформаційні технології”. Forum “DIGITAL REALITY”, Odesa, Ukraine, Proceedings, 32–38.

16. Savchenko, V., Akhramovych, V., Dzyuba, T., Lukova-Chuiko, N., & Laptiev, O. (2021). Methodology for calculating information protection from parameters of its distribution in social networks. IEEE 3rd International Conference on Advanced Trends in Information Theory, ATIT-2021, Proceedings, 99–105.

17. Гайдур, Г. І., Гахов, С. О., Марченко, В. В., & Гайдур, К. В. (2024). Концептуальна модель виявлення фішингових атак на основі використання методів опорних векторів. Сучасний захист інформації, 2(58), 24–33. https://doi.org/10.31673/2409-7292.2024.020003.

18. Наконечний, В. С., Лаптєв, О. А., Погасій, С. С., Лазаренко, С. В., & Мартинюк, Г. В. (2021). Відбір джерел з неправдивою інформацію методом бджолиної колонії. Наукоємні технології, 4(52), 330–337. https://doi.org/10.18372/2310-5461.52.16379.

19. Лаптєв, О. (2020). Контрпропаганда як дієвий засіб боротьби в інформаційній війні Росії проти України. Індивідуальність у психологічних вимірах спільнот та професій: збірник наукових праць / за заг. ред. Л. В. Помиткіної, О. М. Іванської. К.: ТОВ «Альфа-ПІК», 203-206. https://er.nau.edu.ua/handle/NAU/49272 (дата звернення: 01.03.2024).

20. Molodetska, K. (2024). Analysis of Modern Approaches to the Transformation of Social Systems in Postmodern Society. In: Štarchoň, P., Fedushko, S., Gubíniová, K. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, 208. Springer, Cham. https://doi.org/10.1007/978-3-031-59131-0_4.

21. Fedushko, S., Molodetska, K., & Syerov, Y. (2023). Decision-making approaches in the antagonistic digital communication of the online communities users. Social Network Analysis and Mining, 13:18. https://doi.org/10.1007/s13278-022-01021-4.

22. Бреєр, В. В. (2014). Моделі конформної поведінки. Ч. 1. Від філософії до математичних моделей. Проблеми управління, 1, 2–13.

https://econpapers.repec.org/article/scn00953/14508003.htm (дата звернення: 27.02.2024).

23. Краснощоков, П. С. (1998). Найпростіша математична модель поведінки. Психологія конформізму. Математичне моделювання, 10(7), 76–92.

24. Про інформацію : Закон України від 02.10.1992 р. № 2658-XII : станом на 14.03.2024. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 14.03.2024).

25. Про медіа : Закон України від 13.12.2022 р. № 2849-IX : станом на 14.03.2024. URL: https://zakon.rada.gov.ua/laws/show/2849-20#Text (дата звернення: 14.03.2024).

26. Про національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII: станом на 14.03.2024. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 14.03.2024).

27. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI: станом на 14.03.2024. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 14.03.2024).

28. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII: станом на 14.03.2024. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 14.03.2024).

29. Стратегія інформаційної безпеки України : Указ Президента України від 28.12.2021 р. № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення: 14.03.2024).

30. Ветлицька, О. С., & Дзюба, Т. М. (2022). Модель оцінки впливу соціологічної інформації на поведінку людини в контексті її інформаційної

безпеки. Телекомунікаційні та інформаційні технології, 4(77), 35–45. https://doi.org/10.31673/2412-4338.2022.043545.

31. Ветлицька, О. С., & Мужанова, Т. М. (2023). Математична модель інформаційної безпеки особистості під впливом медіаінформації. Сучасний захист інформації, 2(54), 6–12. https://doi.org/10.31673/2409-7292.2023.020001.

32. Ветлицька, О. С., & Треньов, М. Г. (2024). Проблеми кіберстійкості ІКТ-систем в умовах цифрової трансформації. Телекомунікаційні та інформаційні технології, 1(82), 64–72. https://doi.org/10.31673/2412-4338.2024.016472.

33. Ветлицька, О. С., & Треньова, К. О. (2024). Виявлення атак умережах Інтернету речей методами машинного навчання. Сучасний захист інформації, 1(57), 39–49. https://doi.org/10.31673/2409-7292.2024.010005.

34. Ветлицька, О. С., & Треньова, К. О. (2024, лютий 22). Проблеми кіберстійкості ІКТ-систем в умовах цифрової трансформації. Стратегії кіберстійкості: управління ризиками та безперервність бізнесу: матеріали IV Всеукр. наук.-практ. конф., м. Київ, 71–73. URL: https://duikt.edu.ua/uploads/p_2661_62255520.pdf

35. Ветлицька, О. С. (2022, жовтень 27). Сучасні методи виявлення автоматизованих аккаунтів у соціальних мережах. Актуальні проблеми кібербезпеки: матеріали всеукр. наук.-практ. конф., м. Київ, 186–187. URL: https://dut.edu.ua/uploads/p_2121_20358827.pdf

36. Ветлицька, О. С. (2023, квітень 27). Соціологічна концептуалізація інформаційної безпеки. Цифрова трансформація кібербезпеки: матеріали всеукр. наук.-практ. конф., м. Київ, 14–16. URL: https://dut.edu.ua/uploads/p_2626_12162422.pdf

37. Ветлицька, О. С. (2023, травень 16). Методика виявлення вразливостей, пов’язаних з параметрами нейронної мережі, в алгоритмах на основі машинного навчання. Сучасні інтелектуальні інформаційні

технології в науці та освіті: матеріали всеукр. наук-практ. конф., м. Київ, 45–46. URL: https://duikt.edu.ua/uploads/n_11208_13331372.pdf

38. Ветлицька, О. С. (2024, квітень 26). Вплив цифрових технологій на стійкість ланцюгів поставок. Цифрова трансформація кібербезпеки: матеріали всеукр. наук.-практ. конф., м. Київ, 19–22. URL: https://duikt.edu.ua/uploads/n_12581_11703414.pdf

39. Ветлицька, О. С. (2024, квітень 18). Виявлення атак у мережах інтернету речей методами машинного навчання. Сучасний стан та перспективи розвитку IoT: матеріали V Наук.-техніч. конф., м. Київ, 165–167. URL: https://duikt.edu.ua/uploads/p_2661_70423010.pdf

40. Ветлицька, О. С. (2023). Інформаційна безпека: соціологічна концептуалізація. Сучасний захист інформації, 3(55), 52–56. URL: https://doi.org/10.31673/2409-7292.2023.030007.

41. Ветлицька, О. С. (2024). Модель інформаційної захищеності особистості від впливу соціологічної інформації. Сучасний захист інформації, 3(59), 29–41. https://doi.org/10.31673/2409-7292.2024.030003.

42. Почепцов, Г. Г. (2016). Сучасні інформаційні війни. Вид. 2-е, допов., Київ: Києво-Могилянська академія, 504 с. ISBN 966-518-704-2.

43. Золотар, О. О. (2018). Інформаційна безпека людини: теорія і практика: монографія. К.: ТОВ «Видавничий дім «АртЕк», 446 с. ISBN 978-617-7264-79-7.

44. Алещенко, В. (2022). Інформаційно-психологічна безпека особистості в умовах гібридної війни. Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки, 1(49), 13–21. https://doi.org/10.17721/1728-2217.2022.49.13-21.

45. Ліпатов, І. І., Дробаха, Г. А., Гунбін, К. Ю., Воробйова, І. В., Мацегора, Я. В., Приходько, І. І., Тімченко, О. В., Товма, М. І., Пасічник, В. І., & Ліпатова, С. Л. (2015). Протидія негативному інформаційно-психологічному впливу на особовий склад Національної гвардії України в

умовах масових заворушень: монографія. Х.: Нац. акад. НГ України. 229 с. https://books.ndcnangu.co.ua/knigi/Monografija_protidija_vujs'k_aspekt_nezakon2015.pdf (дата звернення: 12.05.2024).

46. Арістова, І. В., & Сулацький, Д. В. (2013). Інформаційна безпека людини як споживача телекомунікаційних послуг: монографія. К.: Ред. журн. «Право України»; Х.: Право, 184 с. https://ippi.org.ua/informatsiina-bezpeka-lyudini-yak-spozhivacha-telekomunikatsiinikh-poslug (дата звернення: 12.05.2024).

47. Наконечний, В. С., Хлевна, Ю. Л., Половінкін, І. М., & Кузьменко, М. Д. (2024). Метод оцінки розповсюдження неправдивої інформації за допомогою спеціальних програм та технологій на базі середовища Інтернет. Сучасний захист інформації, 2(58), 84–90. https://doi.org/10.31673/2409-7292.2024.020010.

48. Мащак, С. О., & Вихор, М. Б. (2023). Особливості впливу стресу на психічне здоров’я військовослужбовців. Науковий вісник Ужгородського національного університету. Серія: Психологія, (3), 18–22. https://doi.org/10.32782/psy-visnyk/2023.3.3.

49. Чекмарьова, І. М. (2024). Шахрайство в Інтернеті як один із видів шахрайства. Аналітично-порівняльне правознавство, 2. https://doi.org/10.24144/2788-6018.2024.02.106.

50. Рудик, М. (2020). Вплив соціальних медіа на формування громадської думки. Вісник Львівського університету. Серія Журналістика, 48, 198–206. http://dx.doi.org/10.30970/vjo.2020.48.10560.

51. Шемчук, В. В. (2020). Загрози інформаційній безпеці: проблеми визначення та подолання. Експерт: парадигми юридичних наук і державного управління, 1(7), 285–296. https://doi.org/10.32689/2617-9660-2020-1(7)-285-296.

52. Котляров, В. (2023). Проблеми інформаційної боротьби у контексті забезпечення національних інтересів. Наукові інновації та

передові технології, 1 (15), 499–511. https://doi.org/10.52058/2786-5274-2023-1(15)-499-511.

53. Деркаченко, Я. А. (2016). Соціальні мережі, як середовище для технологій маніпулятивного впливу. Сучасний захист інформації, 1, 51–59. https://journals.dut.edu.ua/index.php/dataprotect/article/view/531/493 (дата звернення: 24.05.2024).

54. Мельничук, В. В., & Горохова, Л. В. (2022). Критичне мислення як складова інформаційної безпеки. Вісник Львівського університету. Серія філософські науки, 29, 7–13. https://doi.org/10.30970/PHS.2022.29.1.

55. Єсімов, С. С. (2013). Психолого-правові особливості забезпечення інформаційно-психологічної безпеки особистості працівника міліції. Науковий вісник Львівського державного університету внутрішніх справ (серія психологічна), 2, 255–261. http://nbuv.gov.ua/UJRN/Nvldu_2013_2_28 (дата звернення: 27.05.2024).

56. Котляров, В. (2024). Аналіз сучасного стану інформаційної безпеки в Україні. Mechanism of an economic regulation, 2(104), 101–104. https://doi.org/10.32782/mer.2024.104.16.

57. Кузіна, Є. І. (2023). Психологічні механізми інформаційного впливу на особистість дорослої людини: дисертація на здобуття ступеня доктора філософії за спеціальністю 19.00.07 “Вікова та педагогічна психологія” (053 Психологія) / наук. керівник – канд. психол. наук, доц. І. М. Шаповал; Криворізький державний педагогічний університет. Кривий Ріг, 200 с. http://elibrary.kdpu.edu.ua/xmlui/handle/123456789/7441 (дата звернення: 13.06.2024).

58. Корнелюк, І. (2018). Нормативно-правове закріплення результатів соціологічних досліджень в Україні. Вісник Прикарпатського університету. Політологія, 1(18), 107–113. https://journals.pnu.edu.ua/index.php/politics/article/view/4225 (дата звернення: 26.06.2024).

59. Котеленець, К., & Хобта, С. (2023). Проектування польового етапу соціологічного дослідження: аналіз існуючих соціологічних організацій. Науково-теоретичний альманах Грані, 26(6), 104–108. https://doi.org/10.15421/1723137.

60. Худолій, А. О. (2022). Інформаційна війна 2014–2022 рр.: монографія. Острог: Видавництво Національного університету “Острозька академія”, 208 с. ISBN 978-617-8041-16-8. https://doi.org/10.25264/978-617-8041-16-8.

61. Петросян, Д. С. (2022). Евристичні математичні моделі поведінки людини як економічного агента. У кн. Інституційна економіка: управління формуванням і розвитком соціально-економічних інститутів. Видавництво: Інфра-М, 279 с. ISBN 978-5-16-006778-0. https://doi.org/10.12737/970.

62. Kahneman, D. (2012). Thinking, Fast and Slow. London: Penguin, 499 p. ISBN 978-0141033570.

63. Kahneman, D., & Tversky, A. (1984). Choices, values, and frames. American Psychologist, 39(4), 341–350. https://doi.org/10.1037/0003-066X.39.4.341.

64. Філософський енциклопедичний словник / НАН України, Ін-т філософії імені Г. С. Сковороди; [редкол.: В. І. Шинкарук (голова) та ін.]. К.: Абрис, 2002, VI, 742 с. ISBN 966-531-128-X.

65. Рогова, Є. (2020). Теоретичні основи правового забезпечення інформаційної безпеки. Актуальні проблеми держави і права, 86, 190–196. https://doi.org/10.32837/apdp.v0i86.2436.

66. Baltar, F. & Brunet, I. (2012). Social research 2.0: virtual snowball sampling method using Facebook. Internet Research, 22(1), 57–74. https://doi.org/10.1108/10662241211199960.

67. Wilson, S. (2022). Social Media as Social Science Data. Cambridge University Press. https://doi.org/10.1017/9781108677561.

68. Borup, M., Brown, N., Konrad, K., & Van Lente, H. (2006). The sociology of expectations in science and technology. Technology Analysis & Strategic Management, 18(3–4), 285–298. https://doi.org/10.1080/09537320600777002.

69. Knott, E., Rao, A.H., Summers, K. et al. (2022). Interviews in the social sciences. Nat Rev Methods Primers 2, 73. https://doi.org/10.1038/s43586-022-00150-6.

70. Dergach, D. (2020). Research variations of blog analysis: genre or format? Opera in linguistica Ukrainiana, 291–299. https://doi.org/10.18524/2414-0627.2020.27.206554.

71. El Arabi, B., & Zahi, F. (2023). Sociology & Digital Technology: The Mutation of Sociological Research. SHS Web of Conferences, 175. https://doi.org/10.1051/shsconf/202317501054.

72. Блажко, В. (2024). Мультимедійні презентації як засіб формування кліпового мислення студентів. Педагогічна інноватика: сучасність та перспективи, 55-59. https://doi.org/10.32782/ped-uzhnu/2024-3-9.

73. Thunberg, S., & Arnell, L. (2021). Pioneering the use of technologies in qualitative research – A research review of the use of digital interviews. International Journal of Social Research Methodology, 25. https://doi.org/10.1080/13645579.2021.1935565.

74. Olariu, I., & Bogdan, N. (2015). A conceptual approach on press conference. studies and scientific researches. Economics edition, 21. https://doi.org/10.29358/sceco.v0i21.317.

75. Santos, C., & Pereira Neto, M., & Neves, M. (2019). The Influence of Infographics in Accessing Information: Multidimensionality in Visual Representation and Configuration of Different Media. Advances in Ergonomics in Design, 777. ISBN : 978-3-319-94705-1. https://doi.org/10.1007/978-3-319-94706-8_53.

76. Goy, S., Coors, V., Finn, D. (2021). Grouping techniques for building stock analysis: A comparative case study. Energy and Buildings, 236, 110754. https://doi.org/10.1016/j.enbuild.2021.110754.

77. Ogunkunle, A. T. J. (2021). Solving the mystery of the construction and elucidating the structural and functionality attributes of dichotomous key, a widely used tool for plant identification. African Journal of Plant Science, 15(2), 49–58. https://doi.org/10.5897/AJPS2020.2021.

78. Popović, M., Popovic, G., & Karabasevic, D. (2021). Determination of the importance of evaluation criteria during the process of recruitment and selection of personnel based on the application of the SWARA method. Ekonomika, 67, 1–9. https://doi.org/10.5937/ekonomika2104001P.

79. Dubey, S., Kumar, A., & Upadhyay, V. (2018). The Average Sum Method for the Unbalanced Assignment Problems. International Journal of Mathematics Trends and Technology, 55, 89–100. https://doi.org/10.14445/22315373/IJMTT-V55P512.

80. MacCallum, R., Zhang, S., Preacher, K., & Rucker, D. (2002). On the Practice of Dichotomizing Quantitative Variables. Psychological methods, 7, 19–40. https://doi.org/10.1037/1082-989X.7.1.19.

81. Ma, W., Sorrel, M., Zhai, X., & Ge, Y. (2024). A Dual-Purpose Model for Binary Data: Estimating Ability and Misconceptions. Journal of Educational Measurement, 61. https://doi.org/10.1111/jedm.12383.

82. Oliveira Dionisio, A., Gomes, C. F., Clarkson, C., Sanseverino, A., Barcelos, M., Costa, I., & Santos, M. (2021). Multiple Criteria Decision Making and Prospective Scenarios Model for Selection of Companies to Be Incubated. Algorithms, 14, 111. https://doi.org/10.3390/a14040111.

83. Banadka, A. (2020). Indexing and Reviewing: Concept and Its Practice. Smart Moves Journal IJELLH, 8, 99. https://doi.org/10.24113/ijellh.v8i5.10586.

84. Клебанова, Т. С., Гур'янова, Л. С., Чаговець, Л. О., Панасенко, О. В., Сергієнко, О. А., & Яценко, Р. М. (2018). Бізнес-аналітика

багатовимірних процесів. Харків: ХНЕУ ім. С. Кузнеця, 272 с. http://ebooks.git-elt.hneu.edu.ua/babap/index.html

85. Медіаспоживання українців: другий рік повномасштабної війни. Опитування ОПОРИ, (2023). https://www.oporaua.org/polit_ad/mediaspozhivannia-ukrayintsiv-drugii-rik-povnomasshtabnoyi-viini-24796 (дата звернення: 08.07.2024).

86. Інтернет та використання медіа в Україні – лютий 2024. Дані дослідження gemiusAudience за лютий 2024 року, (2024). https://gemius.com/ua/%D0%B1%D0%BB%D0%BE%D0%B3/internet-and-media-in-ukraine-february-2024-report/ (дата звернення: 08.07.2024).

87. Продавці рейтингів. База псевдосоціологів та прихованих піарників. https://texty.org.ua/d/socio/ (дата звернення: 08.07.2024).

88. Нановська, В. (2023). Медіаспоживання українців 2023 року: що та де читають і кому довіряють. https://mediamaker.me/yak-zminylos-mediaspozhyvannya-ukrayincziv-2023-roku-opytuvannya-usaid-internews-5628/ (дата звернення: 19.07.2024).

89. Баранівська, М. (2024). Опитування Центру Разумкова: у лютому 2024 року довіру до Президента України висловили 64% респондентів, у березні – 59%. https://detector.media/infospace/article/225324/2024-04-11-opytuvannya-tsentru-razumkova-u-lyutomu-2024-roku-doviru-do-prezydenta-ukrainy-vyslovyly-64-respondentiv-u-berezni-59/ (дата звернення: 19.07.2024).

90. Грушецький, А. (2024). 5-річчя президентства Володимира Зеленського: як змінювалася довіра президенту в 2019-2024 роках та оцінка діяльності його партії. https://kiis.com.ua/?lang=ukr&cat=reports&id=1413&page=1 (дата звернення: 20.07.2024).

91. СБУ викрила агентурну мережу спецслужб РФ, яка дестабілізувала ситуацію в Україні через Telegram-канали. Офіційний сайт Служби безпеки України. https://ssu.gov.ua/novyny/sbu-vykryla-ahenturnu-

merezhu-spetssluzhb-rf-yaka-destabilizuvala-sytuatsiiu-v-ukraini-cherez-telegramkanaly (дата звернення: 22.07.2024).

92. Реєстр заблокованих сайтів. https://uablocklist.com/ (дата звернення: 22.07.2024).

93. Cochran, W. G. (1977). Sampling Techniques. Third Edition. New York: John Wiley & Sons, 442 p.

94. Соціологічні дослідження Центру Разумкова, (2024). https://razumkov.org.ua/napriamky/sotsiologichni-doslidzhennia (дата звернення: 02.08.2024).

95. Київський міжнародний інститут соціології. Опитування, (2024). https://kiis.com.ua/?lang=ukr&cat=soc-pol (дата звернення: 02.08.2024).

96. Чи потрібна мілітаризація українського суспільства: ставлення громадян (березень 2024р.). https://razumkov.org.ua/napriamky/sotsiologichni-doslidzhennia/chy-potribna-militaryzatsiia-ukrainskogo-suspilstva-stavlennia-gromadian-berezen-2024r (дата звернення: 02.08.2024).

97. Facebook-сторінка Служби безпеки України. https://www.facebook.com/SecurSerUkraine/posts/308791978014386 (дата звернення: 02.08.2024).

ДОДАТКИ

IT specialist

ТОВ «IT Спеціаліст», 03124, Україна, м.Київ
бул. Вацлава Гавела, 6, корпус 3
ЄДРПОУ 39230764, +38 044 390 81 90

АКТ

впровадження результатів дисертаційного дослідження **Ветлицької Олени Сергіївни**, поданих на здобуття наукового ступеня доктора філософії за спеціальністю 125 Кібербезпека та захист інформації в галузі знань 12 Інформаційні технології

Комісія у складі:
голови комісії – Керівник департаменту, Дегтяр Лілія Анатоліївна;

членів комісії:
Провідний фахівець з тестування систем захисту інформації, Рабчун, Д.І.;

Керівник департаменту «Аудит та сертифікація платіжних та банківських систем», Журавльов, А.О.

склала цей акт про те, що:

1. Результати здобувача наукового ступеня Ветлицької О.С., одержані в дисертаційній роботі на тему «Модель інформаційної захищеності особистості в умовах впливу результатів соціологічних досліджень», впроваджені у практичній діяльності ТОВ «IT Спеціаліст» за напрямком оцінки захищеності інформаційних систем методом тестування на проникнення:

1.1. Удосконалена модель поведінки особистості під впливом соціологічної інформації – у процесах тестування захищеності соціальним каналом для розробки достовірних та дієвих сценаріїв фішингових атак на працівників.

1.2. Вперше розроблена модель інформаційної захищеності особистості – на етапі аналізу та оцінювання результатів тестування методом соціальної інженерії для визначення проблем безпеки та розробки рекомендацій щодо підвищення кіберобізнаності працівників.

1.3. Методи обробки соціологічної інформації, які набули подальшого розвитку, – у модулі аналізу ризиків для кожного працівника з можливістю візуалізації у реальному часі, що дає змогу миттєво реагувати на будь-які зміни у рівні знань або поведінки працівників.

IT specialist

ТОВ «IT Спеціаліст», 03124, Україна, м.Київ
бул. Вацлава Гавела, 6, корпус 3
ЄДРПОУ 39230764, +38 044 390 81 90

2. Наукові результати Ветлицької О.С. реалізовані у формі технічних вимог та методології виконання завдань із тестування методом соціальної інженерії та підвищення рівня обізнаності з питань кібербезпеки співробітників компанії на основі автоматизації процесу навчання та покращення навичок. Завдяки індивідуальному підходу до кожного співробітника, тестування методом соціальної інженерії надає можливість оцінити загальний рівень кіберобізнаності, мінімізує ризики, пов'язані з людським фактором, та покращує загальну кіберстійкість організації.

Голова комісії:

Керівник департаменту

Л.А., Дегтяр

Члени комісії:

Провідний фахівець з тестування систем захисту інформації

Д.І., Рабчун

Керівник департаменту «Аудит та сертифікація платіжних та банківських систем», Журавльов, А.О.

А.О., Журавльов

Директор
ТОВ “IT СПЕЦІАЛІСТ” **Олексій Морозов**

«IT СПЕЦІАЛІСТ» Ідентифікаційний код 39230764

ЗАТВЕРДЖУЮ

Перший проректор Державного університету інформаційно-комунікаційних технологій

Член-кореспондент НАН України, доктор технічних наук, професор, лауреат Державної премії України в галузі науки і техніки, Заслужений діяч науки і техніки України

_____Олександр КОРЧЕНКО

«30» жовтня 2024 р.

АКТ

впровадження в освітній процес Державного університету інформаційно-комунікаційних технологій наукових результатів **Ветлицької Олени Сергіївни**, одержаних під час проведення дисертаційного дослідження на здобуття наукового ступеня доктора філософії за спеціальністю 125 Кібербезпека та захист інформації, галузі знань 12 Інформаційні технології

Комісія у складі:

голови комісії – завідувача кафедри Управління кібербезпекою та захистом інформації Навчально-наукового інституту кібербезпеки захисту інформації, д.е.н., професора Легомінової С.В.;

членів комісії:

доцента кафедри Управління кібербезпекою та захистом інформації, к.е.н., доцента Капелюшної Т.В.;

доцента кафедри Управління кібербезпекою та захистом інформації, к.т.н., доцента Щавінського Ю.В.;

доцента кафедри Управління кібербезпекою та захистом інформації, к.військ.н., доцента Якименка Ю.М.,

провела роботу щодо визначення фактичного впровадження результатів наукового дослідження здобувача наукового ступеня доктора філософії Ветлицької О.С. в освітній процес Державного університету інформаційно-комунікаційних технологій.

У результаті проведеної роботи комісія встановила:

1. Нові наукові результати, одержані Ветлицькою О.С., використовуються при підготовці здобувачів освіти освітніх рівнів Бакалавр та Магістр за спеціальністю 125 Кібербезпека та захист інформації, освітня програма «Управління інформаційною та кібернетичною безпекою:

1.1. Удосконалена модель поведінки особистості під впливом соціологічної інформації, в основу якої покладено базову модель конформної поведінки людини з урахуванням її апріорних переконань та ступеня незалежності мислення, і яку було розширено за рахунок використання коефіцієнтів впливу на особистість джерел соціологічної інформації – під час проведення лекційних та практичних занять з дисциплін «Основи національної безпеки», «Інформаційна безпека держави».

1.2. Вперше розроблена модель інформаційної захищеності особистості яка базується на концепції управління на основі ймовірнісного контролю з використанням результатів моделювання поведінки особистості під впливом соціологічної інформації – під час проведення лекційних та практичних занять з дисциплін «Система менеджменту інформаційної безпеки», «Системний аналіз інформаційної безпеки», «Стратегічні комунікації».

1.3. Методи обробки соціологічної інформації, які набули подальшого розвитку, і які були адаптовані для використання у моделях поведінки та інформаційної захищеності особистості за рахунок бінаризації багатовимірних результатів досліджень з використанням методів кластерного аналізу та визначенням ймовірностей для бінарних кластерів – під час проведення лекційних та практичних занять з дисциплін «Управління ризиками інформаційної безпеки», «Системи управління інформаційною безпекою».

2. Зазначені наукові результати Ветлицької О.С. представлені у формі окремих навчальних питань та включені до методичних матеріалів для лекційних та практичних занять.

Голова комісії:

Завідувач кафедри Управління кібербезпекою та захистом інформації
д.е.н., професор Світлана ЛЕГОМІНОВА

Члени комісії:

Доцент кафедри Управління кібербезпекою та захистом інформації
к.е.н., доцент Тетяна КАПЕЛЮШНА

Доцент кафедри Управління кібербезпекою та захистом інформації
к.т.н., доцент Юрій ЩАВІНСЬКИЙ

Доцент кафедри Управління кібербезпекою та захистом інформації
к.військ.н., доцент Юрій ЯКИМЕНКО