МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Кваліфікаційна наукова праця
на правах рукопису

ГРІГА ВЛАДИСЛАВ СЕРГІЙОВИЧ

УДК 004.738.5:159.923

ДИСЕРТАЦІЯ
МЕТОДИ ТА МОДЕЛІ УПРАВЛІННЯ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИМ ВПЛИВОМ У СОЦІАЛЬНИХ МЕРЕЖАХ

122 «Комп’ютерні науки»
12 «Інформаційні технології»
Подається на здобуття ступеня доктора філософії

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

_____В.С.Гріга

Науковий керівник:
Гізун Андрій Іванович
кандидат технічних наук,
доцент

Київ – 2023

АНОТАЦІЯ

Гріга В. С. Методи та моделі управління інформаційно-психологічним впливом у соціальних мережах. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії з галузі знань 12 «Інформаційні технології» за спеціальністю 12 «Комп'ютерні науки». – Національний авіаційний університет, м. Київ, 2023 рік.

Дисертаційна робота присвячена дослідженню інформаційного протиборства, виявленню та ідентифікації видів інформаційно-психологічного впливу, оцінюванню критичності дописів у соціальних мережах, розгляду засобів протидії негативним тенденціям, а також розробці власної системи управління інформаційно-психологічним впливом у соціальних мережах.

Інформаційний вплив стає дедалі більш важливим у сучасному світі. Даному процесу сприяє глобалізація та перехід до інформаційного суспільства. Саме цей чинник впливає на більш широке застосування інформаційних засобів впливу задля отримання власної вигоди. Найпоширенішими сферами їхнього застосування є військова, політична та економічна. Під час військових дій важливими аспектами є позитивна підтримка населенням дій військовослужбовців, погіршення морально-психологічного стану противника, його дезорганізація, у політичній – це створення підтримки населенням влади, насадження ідеології, а в економічній – отримання переваги над конкуруючою компанією чи державою в цілому. Одним із методів досягнення цього є інформаційно-психологічний вплив.

Інформаційно-психологічний вплив (ІПВ) – це вплив на свідомість особи і населення з метою внесення змін у їх поведінку та (або) світогляд. Звідси виникає потреба у забезпеченні інформаційно-психологічної безпеки. Інформаційно-психологічна безпека особи (у вузькому розумінні) – це стан захищеності психіки людини від негативного впливу, який здійснюється шляхом упровадження деструктивної інформації у свідомість і (або) у

підсвідомість людини, що призводить до неадекватного сприйняття нею дійсності.

Особливої актуальності забезпечення інформаційно-психологічної безпеки в Україні набуло у зв’язку з агресією росії проти України, коли гостро постало питання щодо формування підтримки частиною населення територіальної цілісності України, підтримання на високому рівні морального бойового духу військовослужбовців Збройних Сил України. Застосування інформаційно-психологічного впливу та забезпечення інформаційно-психологічної безпеки неможливе без детального розгляду його теорії та методів реалізації.

Тому дисертаційне дослідження має вагому наукову і пратичну цінність, адже його результати допоможуть краще захищати та орієнтуватися в інформаційних потоках особам, які відповідають за даний напрям на підприємствах чи державі.

У вступі наведено мету та завдання дисертаційного дослідження, а також обґрунтовано актуальність даної теми. Також визначено наукову новизну, серед яких 2 нових наукових методи, сформульовано практичне значення отриманих результатів. Продемонстровано зв’язок дослідження з науковими темами. Крім того, надано інформацію про 22 наукових публікацій автора, серед яких 7 статей, а також апробацію результатів роботи на 12-ти науково-технічних конференціях.

В першому розділі проведено аналіз сучасних теоретичних підходів та засад, виявлення, ідентифікації та оцінювання інформаційно-психологічного впливу. Встановлено, що розроблені наразі методи мають як свої переваги, так і недоліки. Проведено дослідження сучасних систем аналізу ефективності публічних сторінок у соціальних мережах. Також проведено аналіз сучасних методів дослідження соціальних мереж.

У другому розділі розроблено функціональну та інтегровані моделі інформаційно-психологічного впливу, які характеризують інформаційне

протиборство в соціальних мережах. Ключовими елементами даних моделей є множини ідентифікуючих параметрів та оціночних парметрів. Розроблено еталони ідентифікуючих параметрів та евристичні правила ідентифікації інформаційно-психологічного впливу. Вперше розроблено метод виявлення та ідентифікації інформаційно-психологічного впливу, який базується на теоретичних засадах нечіткої логіки та дозволяє виконувати свої дії у слабоформалізованому нечіткому середовищі й має можливість аналізувати контент соціальних мереж у режимі реального часу.

У третьому розділі розроблено метод оцінювання критичності інформаційно-психологічного впливу в соціальних мережах, відповідно до оціночних параметрів. Враховано усі виявлені в результаті аналізу недоліки існуючих систем оцінки. Визначено найбільш універсальні оціночні параметри, розроблено їх еталони. Даний метод ґрунтується на кількісних методах експертної оцінки, що дає переваги у відсутності необхідності збору великих кількостей статистичних даних та чіткої формалізації поточної ситуації та елементах нечіткої логіки.

У четвертому розділі розроблено систему управління інформаційно-психологічним впливом. Розроблена система включає в себе підсистеми моніторингу, виявлення, ідентифікації та оцінювання критичності інформаційно-психологічних впливів. Розглянуто та запропоновано заходи протидії деструктивному інформаційно-психологічних впливів в соціальних мережах з точки зору самих інформаційних майданчиків, а також особи, яка відповідає за інформаційну безпеку держави або підприємства.

Запропоновано власний механізм маркування джерел інформації, який побудовано на основі визначення різниць тональностей інформаційних повідомлень. Таким чином оператори систем управління інформаційно-психологічним впливом мають можливість одразу розуміти, яке джерело поширило інформацію та більш належно формувати аналітичні матеріали щодо цього.

Також у цьому ж розділі розроблено програмно-апаратний комплекс на основі системи управління інформаційно-психологічного впливу. У якості середовища розробки програмних засобів на основі системи обрано технологічну платформу Microfocus IDOL. MicroFocus IDOL (Intelligent Data Operating Layer) – це програмний продукт, який призначений для аналізу та обробки надмірної кількості даних різних типів, включаючи текст, зображення, аудіо та відео. IDOL володіє розширеними функціональними можливостями, які дозволяють витягувати інформацію з навіть найскладніших та неструктурованих даних. Завдяки використанню модуля NiagaraFiles платформа дозволяє налаштовувати свою роботу, а завдяки використанню в ньому штучного інтелекту вдалося автоматизувати та замінити роботу експертів з управління інформаційно-психологічним впливом. Роботу програмно-апаратного комплексу досліджено шляхом проведення експериментів. Експериментальні дослідження полягали в аналізі дописів конкретних публічних сторінок у соціальних мережах, аналізі пулу інформаційних повідомлень та оцінюванні конкретного допису за ключовими словами. Під час експериментів комплекс виконав усі поставлені до нього вимоги.

Ключові слова: інформаційно-психологічний вплив, інформаційне протиборство, інформаційна війна, соціальні мережі, інформаційно-комунікаційні системи, інформаційно-телекомунікаційні системи, експертні системи, нечітка логіка, нейронні мережі, штучний інтелект, системи оцінювання, системи прийняття рішень, інформаційний простір, критичність впливу.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті проіндексовано в наукометричній базі Scopus:

1. Gizun, A., Hriha, V., Roshchuk, M., Yevchenko, Y., & Hu, Z. (2019). Method of informational and psychological influence evaluation in social networks based on fuzzy logic Control. *Optimisation and Analytical Processing of Social Networks: Proceedings of the 1st International Workshop (Lviv, May 16–17, 2019)*. pp. 10–11.

2. Zahran, B., Al-Azzeh, J., Gizun, A., Griga, V., & Bystrova, B. (2019). Developing an expert system for assessment of information-psychological influence. *Indonesian Journal of Electrical Engineering and Computer Science*, 15(3), pp. 1571-1577.

3. Gizun, A., Pisarchuk, A., Hriha, V., Buriachok, V., & Berdibayev, R. (2019). Incidents Correlation Mechanism for Assessing Average and Total Criticality Level of Situation in the Infosphere. *In Proceedings of the International Workshop on Cyber Hygiene (CybHyg-2019)*, Vol. 2654, pp. 654-664.

4. Pysarchuk, O., Gizun, A., Dudnik, A., Griga, V., Domkiv, T., & Gnatyuk, S. (2019). Bifurcation Prediction Method for the Emergence and Development Dynamics of Information Conflicts in Cybernetic Space. *In Proceedings of the International Workshop on Cyber Hygiene (CybHyg-2019),* Vol. 2654, pp. 692-709.

5. Gizun, A., Avkurova, Z., Hriha, V., Monashnenko, A., Akatayev, N., & Aleksander, M. (2021). Method for the Criticality Level Assessment for Crisis Situations with Parameters Fuzzification. *In Advances in Computer Science for Engineering and Education IV,* pp. 147-161.

Статті у фахових виданнях:

6. Грига, В., Гнатюк, С., & Гизун, А. (2015). Информационно-психологическая безопасность общества, как средство сохранения народа. *Безпека інформації*, 21(2), С. 179-190.

7. Гізун, А., & Гріга, В. (2016). Аналіз сучасних теорій інформаційно-психологічних впливів в аспекті інформаційного протиборства. *Безпека інформації*, 22(3), С. 272-282.

Розділи колективних монографій:

8. Hriha, V., Gizun, A., & Shchudlyck, I., (2017) Information psychological impact detection and identification system. *Projekt interdyscyplinarny projektem XXI wieku TOM 2: Monografia: VII Miedzynarodowa Konferencja Studentow oraz Doktorantow*, pp. 131-149.

9. Hriha, V., Bystrova, B, Kadanova, V., Blidar, A.,& Roshchuk, M. (2018) Method of evaluation of informational and psychological influence. *Projekt interdyscyplinarny projektem XXI wieku TOM 2: Monografia: VIII Miedzynarodowa Konferencja Studentow oraz Doktorantow*, pp. 91-105.

10. Hriha, V., Blidar, A., Roshchuk, M., & Derkach, S. (2019). Insider attacks system identification. *Projekt interdyscyplinarny projektem XXI wieku TOM 2: Monografia: IX Miedzynarodowa Konferencja Studentow oraz Doktorantow*, pp. 155-166.

Тези доповідей на конференціях:

11. Гріга, В. С., Гізун, А. І., & Іванченко, І. С., (2016). Характеристика базових складових інформаційного протиборства. *Матеріали Другої всеукраїнської науково-практичної конференції «Перспективні напрями захисту інформації»,* С. 22-25.

12. Гріга, В. С., Каданова, В. О., & Гізун, А. І. (2017). Архітектура системи виявлення та ідентифікації інформаційно-психологічного впливу. *Матеріали Третьої всеукраїнської науково-практичної конференції «Перспективні напрями захисту інформації»,* С. 26-28.

13. Гріга, В. (2017). Цільова та функціональна моделі інформаційно-психологічного впливу. *Збірник тез X Всеукраїнської студентської науково-технічної конференції „Природничі та гуманітарні науки. Актуальні питання“,* С. 49-50.

14. Griga, V., Gizun, A., & Lanovyi, I. (2017). Formation of identifying parameters reference values of information and psychological impact. *Міжнародний Молодіжний Науковий Форум "Litteris Et Artibus"*, С. 404-408.

15. Гріга, В.С., Щудлик, І.А. (2018) Формування множини параметрів оцінки інформауійнопсихологічного впливу. *Стан та удосконалення безпеки інформаційнотелекомунікаційних систем (SITS'2018): тези доп. X Всеукр. наук.практ. конф. (Миколаїв-Коблево, 21-23 червня 2018 р.)*, С. 21-23.

16. Грига, В. С., & Кобильнык, Б. Ю. (2018). Функциональная и целевая модели информационнопсихологического воздействия. *Современные средства связи: тезисы доклада XXIII междунар. науч.-тех. конф.(г. Минск, 18-19 октября 2018 г.),* С. 32 -36.

17. Hriha, V. (2018). Information psychological impact detection and identification as a basis for counteracting information aggression. *Aviation in the XXI-st century. Safety in Aviation and Space Technologies: proceedings of the VIII world congress (October 23-25, 2018),* Рз. 3.1.16-3.1.18.

18. В., Гріга, & А., Гізун (2019). Експериментальне дослідження методу виявлення та ідентифікації інформаційно-психологічного впливу. *ITSec: Безпека інформаційних технологій: IX міжнародна науково-технічна конференція, 22-27 березня 2019 р.*, С. 30-31.

19. Hriha, V., Blidar, A., & Zakharchuk, O. (2019). Information interference of Russia in the election process in Ukraine in 2019. *9th International Youth Science Forum "Litteris et Artibus" & 14th International Conference «Young Scientists Towards The Challenges Of Modern Technology» (Lviv, November 21–23, 2019),* pp. 65-74.

20. А., Гізун, & В., Гріга (2020). Модель інформаційного впливу Російської Федерації на виборчий процес в Україні в 2019 році. *Матеріали Шостої всеукраїнської науково-практичної конференції «Перспективні напрями захисту інформації»*, С. 60-64.

21. Гріга, В. С., & Гізун, А. І. (2023). Інформаційно-психологічний вплив як чинник військового протиборства. *Інтегровані інтелектуальні*

робототехнічні комплекси (ІПРТК-2023). Шістнадцята міжнародна науково-практична конференція 23-24 травня 2023 р., Київ, Україна, С. 316-317.

22. А. Гізун, & В. Гріга (2023). Визначення базових параметрів для оцінювання інформаційно-психологічного впливу. *Захист інформації і безпека інформаційних систем: матеріали IX Міжнар. наук.-техн. конф.,* С. 23-24.

ЗМІСТ

ВСТУП

Інформаційний вплив стає дедалі більш важливим у сучасному світі. Даному процесу сприяє глобалізація та перехід до інформаційного суспільства. Саме цей чинник впливає на більш широке застосування інформаційних засобів впливу задля отримання власної вигоди. Найпоширенішими сферами їхнього застосування є військова, політична та економічна. Під час військових дій важливими аспектами є позитивна підтримка населенням дій військовослужбовців, погіршення морально-психологічного стану противника, його дезорганізація, у політичній – це створення підтримки населенням влади, насадження ідеології, а в економічній – отримання переваги над конкуруючою компанією чи державою в цілому. Одним із методів досягнення цього є інформаційно-психологічний вплив [56].

Інформаційно-психологічний вплив (ІПВ) – це вплив на свідомість особи і населення з метою внесення змін у їх поведінку та (або) світогляд [56]. Звідси виникає потреба у забезпеченні інформаційно-психологічної безпеки. Інформаційно-психологічна безпека особи (у вузькому розумінні) – це стан захищеності психіки людини від негативного впливу, який здійснюється шляхом упровадження деструктивної інформації у свідомість і (або) у підсвідомість людини, що призводить до неадекватного сприйняття нею дійсності [56].

Особливої актуальності забезпечення інформаційно-психологічної безпеки в Україні набуло у зв’язку з агресією росії проти України, коли гостро постало питання щодо формування підтримки частиною населення територіальної цілісності України, підтримання на високому рівні морального бойового духу військовослужбовців Збройних Сил України. Застосування інформаційно-психологічного впливу та забезпечення інформаційно-психологічної безпеки неможливе без детального розгляду його теорії та методів реалізації.

На сьогодні існує певна кількість робіт у напрямку вивчення виявлення та ідентифікації інформаційно-психологічного впливу, серед яких: Молодецька-

Гринчук К. В., Грищук Р. С., Дудатьєв А. В., Левченко О. В., Горбулін В. П., Ланде Д. В., Залкін С. В., Опірський І. Р., Козловський В. В., Сидоренко В. М. та ін. [3-8].

Теоретична база вивчення виявлення та ідентифікації інформаційно-психологічного впливу розкрита на достатньому рівні. Проте, розробки щодо їх практичної реалізації в умовах сьогодення майже відсутні. Тому актуальною є необхідність розкриття практичних шляхів швидкого виявлення та ідентифікації інформаційно-психологінчого впливу задля оцінювання та впровадження ефективних контрзаходів.

Мета і завдання дослідження.

Метою дисертаційної роботи є забезпечення процесів виявлення, ідентифікації та оцінювання інформаційно-психологічних впливів за рахунок розробки методів, а на їх основі автоматизованої системи управління інформаційно-психологічного впливу, що здатні функціонувати в слабоформалізованому нечіткому середовищі, якими є соціальні мережі.

Для цього сформульовано комплекс наступних науково – технічних задач:

1. Провести аналіз наявних теоретичних підходів та засад виявлення, ідентифікації та оцінювання інформаційно-психологічного впливу, розглянути сучасні засоби аналізу контенту соціальних мереж.
2. Розробити моделі відображення інофрмаційно-психологічних впливів в інформаційному просторі, зокрема в соцмережах.
3. Розробити метод виявлення та ідентифікації інформаційно-психологічного впливу, який буде ефективним під час аналізу каскаду інформаційних повідомлень у різних соціальних мережах, зважаючи на їх характеристики, а також зможе встановити конкретний вид такого впливу.
4. Розробити метод оцінювання критичності інформаційно-психологічного впливу та конкретного допису в соціальних мережах задля точного встановлення загрози інформаційному простору, іміджу та вибору адекватних засобів реагування.

5. Розробити систему управління інформаційно-психологічним впливом, яка буде включати в себе підсистеми моніторингу, виявлення, ідентифікації та оцінювання критичності таких впливів, а також формувати набори рекомендацій щодо контрзаходів по нейтралізації впливу.
6. Розробити програмно-апаратний комплекс на основі системи управління інформаційно-психологічним впливом для забзепечення процесів управління ним в інформаційному просторі та дослідити його роботу через проведення симуляційних експериментів.

Об'єкт дослідження – процеси виявлення, ідентифікації та оцінювання інформаційно-психологічного впливу в соціальних мережах.
Предмет дослідження – моделі та методи виявлення, ідентифікації та оцінювання інформаційно-психологічного впливу в соціальних мережах.

Наукова новизна отриманих результатів полягає в тому, що:

1. **Отримали подальшого розвитку** процеси моделювання інформаційно-психологічних впливів за рахунок їх представлення у вигляді цільової, що включає такі елементи як вид інформаційного простору, мета та час дії інформаційно-психологічного впливу і набір контрзаходів, та інтегрованої, що включає ідентифікатор інформаційно-психологічного впливу, підмножин можливих ідентифікуючих та оціночних параметрів, множин евристичних правил, моделей, які дозволяють однозначно їх описати та керувати ними, зокрема здійснювати процеси виявлення та оцінювання критичності інформаційних впливів в певному виді інформаційного простору, зокрема у соціальних мережах.

2. **Вперше** розроблено метод виявлення та ідентифікації інформаційно-психологічних впливів, що за рахунок обробки нечітких ідентифікуючих параметрів та застосування запропонованої інтегрованої моделі

інформаційно-психологічного впливу, дозволяє виявити і однозначно ідентифікувати інформаційно-психологічний вплив в нечіткому слабоформалізованому середовищі, в тому числі і в соціальних мережах.

3. **Отримали подальший розвиток** підходи та методи оцінювання інформаційно-психологічних впливів за рахунок розробки методу оцінювання інформаційно-психологічних впливів, що заснований на обробці нечітких оціночних параметрів та застосуванні запропонованої інтегрованої моделі інформаційно-психологічного впливу, який дозволяє оцінити дію інформаційних впливів на інформаційне середовище відповідно до рівня їх критичності.

4. **Отримали подальший розвиток** структурні рішення систем управління інформаційно-психологічним впливом, які за рахунок поєднання підсистеми моніторингу соціальних мереж, підсистеми виявлення та ідентифікації інформаційно-психологічного впливу і підсистеми оцінювання інформаційно-психологічного впливу в єдину систему та використання методів нечіткої логіки, дозволяють забезпечити автоматизацію процесів управління інформаційно-психологічним впливом (від його виявлення до підбору контрзаходів) в інфомраційному середовищі, зокрема соціальних мережах.

Практичне значення одержаних результатів. Практично вагомими вважаються такі результати:

1. Запропоновані моделі, методи та систему можна використовувати при дослідженні інформаційно-психологічного впливу в соціальних мережах на особу та суспільство, а також для їх виявлення, ідентифікації, оцінювання та нейтралізації.
2. На основі запропонованих методів та системи управління інформаційно-психологічного впливу розроблено програмно-апаратних комплекс на базі Microfocus IDOL, який має модульну структуру та дозволяє використовувати нейронні мережі для аналізу інформаційних потоків.

3. Розроблений програмно-апаратний комплекс може використовуватися під час оцінювання впливу на аудиторію окремої сторінки в соціальних мережах, каскаду інформаційних повідомлень, а також окремо взятого допису (без встановлення виду інформаційно-психологічного впливу).
4. Розроблена система управління інформаційно-психологічного впливу є достатньо гнучкою для зміни та перерахунку ідентифікуючих та оціночних параметрів, тому завдяки використанню технологій штучного інтелекту може змінюватися та удосконалюватися самостійно.
5. Використання цільової та інтегрованої моделей при розробці спеціального ПЗ для виявлення та оцінювання ІПВ дозволило забезпечити високу ефективність та підвищити рівень автоматизації процесів управління ІПВ, що підтверджується актами впровадження у діяльність Центру психологічного, фізичного та мовленнєвого розвитку дитини «Динаміка» (акт впровадження від 04.09.2023 №03/0923).
6. Теоретичні результати дисертації та результати експериментальних досліджень виокристовуються в навчальному процесі підготовки фахівців спеціальності 121 «Інженерія програмного забезпечення» у дисциплінах «Групова динаміка і комунікації» і «Основи технологій R&D» на кафедрі інженерії програмного забезпечення Національного авіаційного університету (акт впровадження від 27.09.2023 р.).

Зв'язок з науковими темами

Зв'язок роботи з науковими програмами, планами, темами. Одержані результати дисертаційної роботи відображені у звітах кафедральній науководослідній роботі кафедри інженерії програмного забезпечення Національного авіаційного університету НДР 58/09.01.02 «Методологія підвищення ефективності процесів життєвого циклу розробки програмного забезпечення у гнучких підходах його розробки».

Апробація результатів дисертації. Основні результати дисертаційної роботи були представлені та обговорені на дванадцяти міжнародних науково-технічних та науково-практичних конференціях:

1. Стан та удосконалення безпеки інформаційно-телекомунікаційних систем (SITS'2018): Всеукр. наук.практ. конф. (Миколаїв-Коблево, 21-23 червня 2018 р.). Миколаїв, 2018.
2. VIII Miedzynarodowa Konferencja Studentow oraz Doktorantow December 5-8, 2018, Bielsko-Biala, Poland.
3. Aviation in the XXI-st century. Safety in Aviation and Space Technologies. October 23-25, 2018, Kyiv, Ukraine.
4. ITSec: Безпека інформаційних технологій: IX міжнародна науково-технічна конференція, 22-27 березня 2019 р., Київ, Україна.
5. 1st International Workshop, Lviv, May 16–17, 2019.
6. 14th International Conference «Young Scientists Towards The Challenges Of Modern Technology», Lviv, November 21–23, 2019.
7. IX Miedzynarodowa Konferencja Studentow oraz Doktorantow December 6-9, 2019, Bielsko-Biala, Poland.
8. International Workshop on Cyber Hygiene (CybHyg-2019), November 29-30 2019, Kyiv, Ukraine.
9. Шоста всеукраїнська науково-практична конференція «Перспективні напрями захисту інформації», 3-8 вересня 2020 року, Одеса.
10. Захист інформації і безпека інформаційних систем: IX Міжнар. наук.-техн. Конф., 23-26 травня 2023 року, Львів.
11. Інтегровані інтелектуальні робототехнічні комплекси (ІІРТК-2023). Шістнадцята міжнародна науково-практична конференція 23-24 травня 2023 р., Київ, Україна.
12. VIII-rth International Conference Cognitive Science - Approaches and Results towards Artificial Intelligence, September 25-27 2023, Sofia, Bulgaria.

Публікації. Основні результати дисертаційного дослідження були опубліковані в 22 наукових працях. Зокрема 7 статей в наукових журналах, 5 з яких проіндексовані міжнародними наукометричними базами даних. Також отримані результати були представлені в 3 розділах колективних монографій та в 12 публікаціях у матеріалах міжнародних науково-технічних та науково-практичних конференцій.

Структура та обсяг дисертації. Дисертація складається з анотації, змісту, вступу, чотирьох розділів, висновку, списку використаних джерел та додатків. Повний обсяг роботи становить 178 сторінок друкованого тексту, з них анотація – на 4 стор., зміст – на 2 стор., основний текст – на 167 стор., список із 110 використаних джерел – на 13 стор., додатки – на 10 стор. Дисертація містить 32 рисунки та 36 таблиць.

РОЗДІЛ 1. СУЧАСНІ МЕТОДИ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ВПЛИВУ

1.1. Поняття інформаційно-психологічного впливу та аналіз методів і технологій інформаційно-психологічного впливу в соціальних мережах

Керування інформаційними потоками внаслідок інформатизації та технічного розвитку суспільства має у наші дні досить велике значення. Важливість інформаційного протиборства доводив китайський воєначальник Сунь-Цзи у своєму Трактаті «Мистецтво війни» ще у IV ст. до н. е., але повністю світова спільнота усвідомила це в 2010-их рр., коли воно почало вноситися у військові доктрини багатьох держав світу. Першим документально засвідченим дослідженням з теорії інформаційного протиборства є робота М. Лібікі «Що таке інформаційна війна?», (серпень 1995 року, Національний інститут оборони США). У ній автор намагався розкрити суть інформаційного протиборства та війни, а також визначив її форми. Однак ще раніше термін «інформаційна війна» увів в обіг китайський теоретик Шень Веньгуань [56]. Значних успіхів досягли американські дослідники Дж. Стейн і Р. Шафранскі, російський С. Расторгуєв, українські Я. Жарков, В. Петрик, М. Присяжнюк.

В теорії інформаційних протиборств основне місце займає інформаційний вплив – організований та цілеспрямований вплив за допомогою інформаційних технологій на свідомість особистості, соціальних груп, суспільства та народу, інформаційну інфраструктуру, що поділяється на інформаційно-психологічний та інформаційно-технічний вплив. Інформаційно-психологічний вплив – це вплив на свідомість та підсвідомість людини та суспільства з метою внесення змін в їх поведінку [82]. Інформаційно-технічний вплив – це вплив на інформаційну інфраструктуру з метою внесення змін в її роботу. Реалізація названих впливів породжує інформаційне протиборство Формами інформаційного протиборства є інформаційні війни, спеціальні інформаційні операції (СІО) та акції інформаційного впливу (АІВ). Інформаційна війна – це

форма ведення інформаційного протиборства між різними суб'єктами, що передбачає здійснення комплексу заходів із завдання шкоди інформаційній сфері конфронтуючої сторони й захисту власної інформаційної безпеки. Інформаційні війни складаються з СІО та АІВ.

Акція інформаційного впливу – це одноразова акція інформаційно-психологічного та інформаційно-технічного впливу, яка передбачає спланований впливу на свідомість і поведінку людей [95]. Основними ознаками їх є сенсаційність, лавино подібність розгортання подій, короткостроковість. АІВ тривають один-три дні. Основними суб'єктами АІВ виступають ЗМІ, неурядові організації, Інтернет-ресурси. Об'єктами АІВ є свідомість і підсвідомість суспільства, певної групи людей. Головним інструментом АІВ є «інформаційний вкид», який надалі різними методами використовується задля досягнення певних цілей. «Інформаційний вкид» - це інформаційна новина, здебільшого не правдивого характеру, яка з'являється в інформаційному просторі та за достовірність і джерело якої ніхто не несе відповідальність. Основними методами проведення АІВ є дезінформування та поширення чуток.

Дезінформування – це метод, який передбачає обман чи уведення об'єкта впливу в оману щодо справжності намірів для спонукання його до запрограмованих дій [78]. Найчастіше у світовій практиці застосовуються такі форми дезінформування: тенденційне викладення фактів; дезінформування «від зворотного»; «термінологічне «мінування»; «сіре» та «чорне» дезінформування. У загальному вигляді акції дезінформування можуть проводитися шляхом створення видимості випадкового витоку закритої інформації, успіхів розвідки іноземних партнерів, використання засобів масової інформації (власні інформаційні агентства, теле-, радіокомпанії, друковані видання, «кишенькові» журналісти й т. ін.) [56].

Поширення чуток – це діяльність щодо поширення переважно неправдивої інформації серед широких верств населення здебільшого неофіційними каналами з метою дезорганізації суспільства та держави або їхніх установ чи організацій [56]. За одним із визначень, чутки – це циркулююча

форма комунікації, за допомогою якої люди, котрі перебувають у неоднозначній ситуації, об'єднуються, утворюючи зрозумілу їм інтерпретацію цієї ситуації, спільно використовуючи власні інтелектуальні можливості. Чутки можна класифікувати за експресивною характеристикою на чутки-бажання, чутки-залякування й роз'єднувальні агресивні чутки, за інформаційною характеристикою – на абсолютно недостовірні, недостовірні, недостовірні з елементами правдоподібності та правдоподібні [56,78]. Чутки самопоширювані. Позитивний чинник використання цієї форми АІВ полягає ще й у тому, що практично немає ефективних засобів протидії чуткам. На офіційному рівні зупинити їх неможливо: офіційні заходи протидії викликають прямо протилежний ефект: для людей, яких безпосередньо цікавлять чутки, це є підтвердженням правдивості останніх [95].

Середня вартість проведення однієї АІВ складає порядку 1 тис. Євро. Цілями проведення АІВ є порушення стабільного стану інформаційного простору держави, «розігрів» аудиторії різноплановою інформацією задля підтримки нестабільності інформаційного простору та створення певної аудиторії. Основним результатом проведення АІВ є створення інформаційного приводу для можливого подальшого проведення СІО та зацікавлення певною аудиторією новиною, «інформаційним вкидом» [74]. Прикладом АІВ є випуск новин на телеканалі «Россия24», згідно яких українські бійці у зоні АТО катували хлопчика у м. Слов'янськ Донецької області.

Спеціальна інформаційна операція – це сплановані дії, спрямовані на аудиторію з метою схилення до прийняття певних рішень або (та) вчинення певних дій, вигідних для суб'єкта інформаційного впливу. Перед здійсненням операції може відбутися кілька АІВ. Існує класичний алгоритм проведення СІО: 1) Інформаційний етап; 2) «Розкручування» інформаційного приводу; 3) Загострення напруження; 4) Вихід із операції або етап закріплення. Основними ознаками проведення СІО є збільшення повідомлень негативного змісту з певної тематики, зростання емоційності, зростання тенденційності, збільшення сенсаційності, лавиноподібність розгортання подій, взаємоузгодження дій

суб'єктами операції. СІО проводяться за час від одного тижня до двох місяців. Основними суб'єктами СІО виступають керівництва іноземних держав, ЗМІ, неурядові організації, спецслужби іноземних держав, Інтернет ресурси, агентура впливу іноземних держав. Об'єктами СІО є свідомість і підсвідомість «людини, що приймає рішення», населення країни.

СІО передбачає досягнення різних цілей залежно від стадії інформаційного протиборства (див. таблицю 1) [56]. Основними методами проведення СІО є пропаганда, диверсифікація громадської думки, психологічний тиск.

Пропаганда – це спосіб поширення інформаційних повідомлень для впровадження в громадському соціумі певних наративів, активізації використання їх в повсякденному діяльності більшої кількості населення. Пропаганда включає у себе й повідомлення, які націлені на зміну громадської думки, викликання емоцій чи зміну ставлення до чогось людей. Диверсифікація громадської думки – це зміна ставлення до чогось критично важливої маси людей, яка призводить до корегування відповідних дій владних еліт. Розрізняють кілька форм диверсифікації громадської думки: дестабілізація обстановки в державі чи окремих її регіонах; активізація кампаній проти політичного курсу панівної еліти та окремих її лідерів різними міжнародними установами; ініціювання антидемпінгових кампаній й іншого роду скандальних судових процесів, застосування міжнародних санкцій з інших причин [82]. Психологічний тиск – це вплив на психіку людини шляхом залякування, погроз із метою її спонукання до запланованої моделі поведінки. Форми психологічного тиску: доведення до об'єкта впливу відомостей про реальні чи неіснуючі загрози та небезпеки; прогнози щодо репресій, переслідувань, убивств тощо; шантажування; здійснення вибухів, підпалів, масових отруєнь, захоплень заручників, інших терористичних акцій [82].

Середня вартість однієї СІО складає порядку 100 тис. Євро. Результатом проведення СІО є зміни в поведінці та (або) світогляді певної групи людей або суспільства. Прикладом проведення СІО є підготовка Росією до анексії

Автономної республіки Крим, згідно якої населення півострова переконували у їхній приналежності до російського народу та т. з. «історичну помилку» передачі у 1954 р. республіки Україні.

Проведемо аналіз відомих публікацій в сфері інформаційно-психологічного впливу, виділимо ключові особливості відомих методів, моделей та теорій інформаційно-психологічного впливу.

Базові положення концепції інформаційного протиборства та війни були закладені в основному в роботах закордонних вчених, в першу чергу з США та Китаю, проте суттєвий внесок був внесений і вітчизняними науковцями. Зокрема, активно методами захисту від негативного інформаційно-психологічного впливу займається український вчений Шиян А. А. Він, з метою використання інформаційного середовища для підвищення захищеності людини та соціальної групи від негативного інформаційно-психологічного впливу розглядає кортеж, який описує результат інформаційного простору:

$$IS =< DB, G, d_1, d_{1u}, d_{1d}, d_2, C_1, ..., C_8 >,$$

де DB – база даних, яка описує задачу; G – характеристика мети діяльності; d_1, d_{1u}, d_{1d}, d_2 – оператори дихотомічного поділу; $C_1, ..., C_8$ – вісім компонентів інформаційного простору [105]. Згідно даного дослідження інформаційно-психологічний вплив може бути здійснено щодо кожного елементу вищенаведеного кортежу або на певну його сукупність, а його здійснення на довільний елемент – можна описати оператором А:

$$A: IS_k \to IS_k^a .$$

У вищенаведеній формулі індексом «а» позначено один із елементів кортежу, що змінився.

Важливим із точки зору теорії інформаційно-психологічного впливу є розгляд науковцем двох випадків:

$$\exists is_j (is_j \in IS_k : is_j \notin IS_k^a) .$$

Перший випадок відповідає ситуації, під час якої через зовнішній інформаційно-психологічний вплив із елементу кортежу інформаційного середовища вилучається одна із його «правильних» складових. Внаслідок цього інформаційний простір стає неповним. У другому випадку – внаслідок зовнішнього інформаційно-психологічного впливу до елементу кортежу додається нова «неправильна» складова. Внаслідок цього інформаційний простір перестає відповідати задачі. Випадок, коли одна «правильна» складова елементу кортежу замінюється на «неправильну» зводиться до послідовного застосування вищенаведених операцій [106].

Шиян А. А. запропонував метод протидії інформаційно-психологічному впливу, згідно якого певні дії можна взагалі ідентифікувати саме як процес інформаційно-психологічного впливу. Метод базується на формуванні адекватної цілі діяльності інформаційного простору, який можна представити у вигляді кількох етапів:

Етап 1. Створюється база даних еталонних інформаційних просторів $IS_e(G,SA)$, які відповідають цілі діяльності G та предметним областям діяльності SA.

Етап 2. Здійснюється визначення поточних станів інформаційного простору із часом, у результаті якого будується інформаційний простір задачі $IS(t)$ в момент часу t.

Етап 3. Здійснюється порівняння по компонентам кортежу еталонного інформаційного простору IS_e із $IS(t)$.

Якщо в результаті порівняння отримана рівність $IS(t)_k - IS_e = \varnothing$ то акт негативного інформаційно-психологічного впливу не мав місця. У даному випадку рівень захищеності суб'єкту інформаційної безпеки є достатнім.

Якщо ж має місце таке співвідношення $IS(t)_k - IS_e = \Delta IS(t) \neq \varnothing$ то це означає, що потрібно приступати до захисту інформаційного простору [105].

Значних успіхів у дослідженні інформаційного протиборства досяг український науковець Руслан Грищук. Згідно його дослідження, суб'єктами інформаційного протиборства є вище політичне та військове керівництво держави, органи місцевого самоврядування та власне населення [6]. Виходячи з цього, вплив зловмисників направлений на дестабілізацію обстановки всередині країни. Також вони відзначили, що методи інформаційного протиборства ґрунтуються на психічних процесах людини. Науковці розглядають ознакову класифікацію методів інформаційного протиборства. Вона має п'ять характеристик: за типом протиборства, за метою, за характером впливу, за джерелом розповсюдження, за цільовою аудиторією. Згідно з цією класифікацією, за типом протиборства (ТС) суб'єктами захисту (або впливу) при інформаційно-психологічному протиборстві є:

– системи прийняття політичних рішень;

– системи формування громадської думки;

– системи формування суспільної свідомості (книги, фільми, телевізійні програми, друковані ЗМІ);

– психологічний вплив на психіку осіб, що приймають рішення (дискредитація лідерів) тощо [71].

За метою (АЕ) розрізняють методи пропаганди та контрпропаганди [71]. Пропаганда направлена на те, щоб поширити у свідомості визначеної групи людей необхідну інформацію. Контрпропаганда направлена на припинення поширення в інформаційному просторі повідомлення.

За джерелами розповсюдження (SD) різниця методів проявляється в способах їх реалізації [6]. Визначальна роль належить засобам масової інформації (ЗМІ): телерадіомовлення та друковані видання. В останнє десятиліття відбувається небувалий розвиток Інтернет-ресурсів. Проте, більш традиційні ЗМІ мають ряд переваг. Передусім це аудиторія: частка населення, яке дивиться телебачення значно більша, ніж та, яка читає електронні ЗМІ.

Іншою перевагою є те, що телебачення сильніше у фоновому та наведеному інформаційних впливах.

За цільовою аудиторією (РА) при виборі методів, способів та прийомів інформаційного впливу обов'язково необхідно враховувати характер цільової аудиторії [70]. Передусім, необхідно враховувати такі характеристики як вік аудиторії, соціальний статус та рівень обізнаності.

Дослідники представили схему «Технологічні аспекти інформаційного протиборства на сучасному етапі», де детально наведено кожний аспект та зв'язок між ними (рис. 1.1) [71].

Південноафриканські науковці Брет Ван Нікерк та Манодж Махарадж дали визначення інформаційній війні як комплекс наступальних і оборонних операцій із використання інформаційних ресурсів. Ван Нікерк та Махарадж визначили, що вона проводиться через зростаючу цінність інформації для людей. Наступальні операції направлені на збільшення цього значення. Оборонні – на потенційні втрати.

Із вищевказаного визначення вони зробили висновок, що використання інформаційної війни є спробою отримати перевагу над конкурентом або противником завдяки використанню власних або блокування інших інформаційних ресурсів. Вони довели, що інформаційна війна може вестися у фізичній, інформаційній і когнітивній області – це показує, що інформаційне протиборство може включати як традиційне фізичне знищення інформаційних ресурсів противника, так і виконання дій, направлених на людський розум.

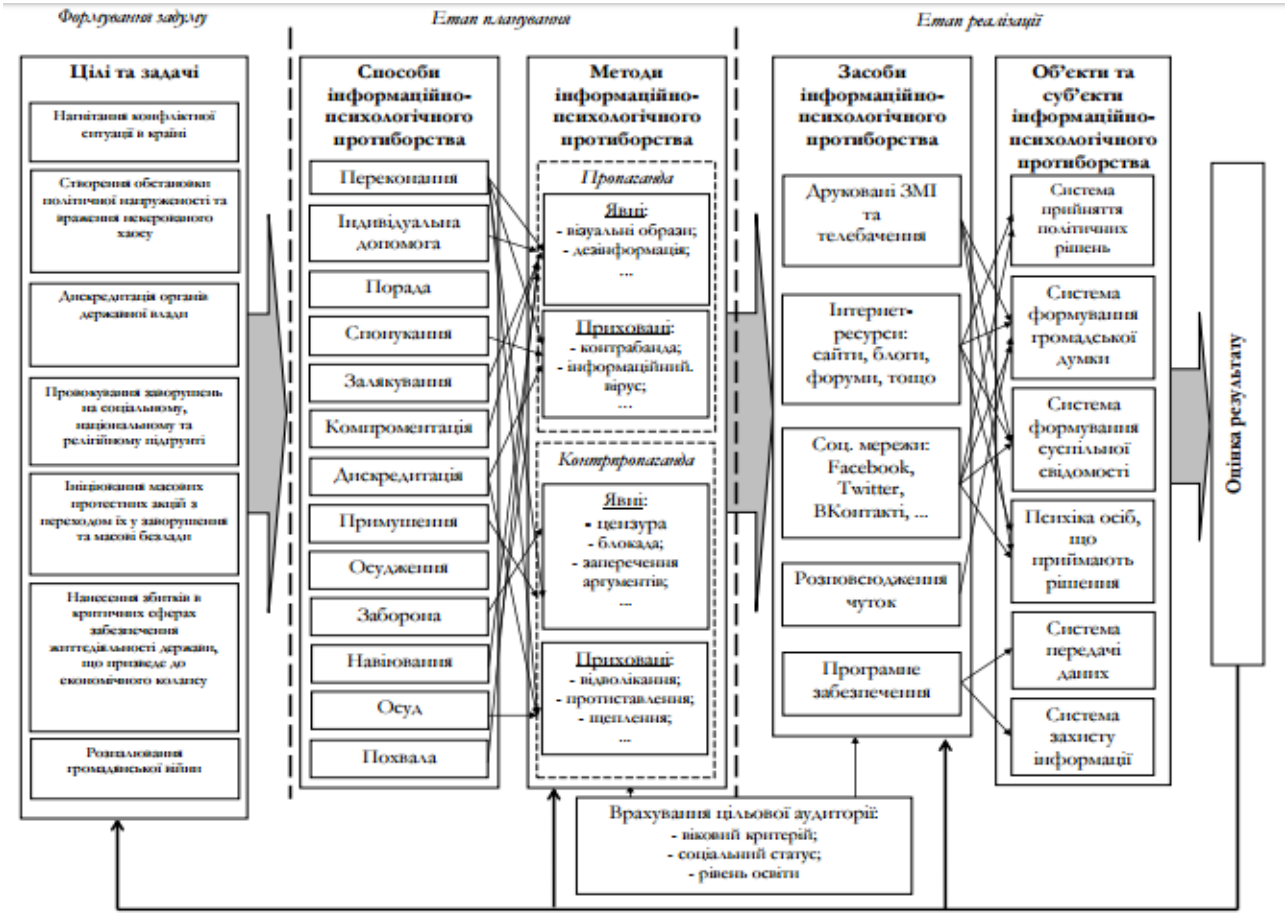


Рис. 1.1. Технологічні аспекти інформаційного протиборства на сучасному етапі

Ван Нікерк та Махарадж зазначають, що інформаційна війна ведеться проти трьох основних характеристик інформації: цілісності, доступності та конфіденційності. Виходячи з цього ставляться задачі щодо проведення дій:

– порушити та погіршити доступ до інформації, або знищити інформацію;

– перехоплення інформації;

– погіршення інформації шляхом зміни змісту, вставка додаткової «брехливої» інформації, зміна контексту, у якому проглядається інформація і зміна сприйняття її людьми [56].

Дослідники визначають, що інформаційно-психологічний вплив здійснюється під час психологічної війни та розглядають модель Л. Кокса (рис. 1.2) [56].

Рис. 1.2. Модель Л. Кокса

Дана модель приймає форму потоку повідомлень. Вона побудована таким чином, що надає стимул для цільової аудиторії щодо дій. Відправник доставляє повідомлення за допомогою інструментів ЗМІ, що забезпечує певну реакцію аудиторії і можливість спостерігати за нею. Так, цільові спільноти реагують на повідомлення своєю підтримкою або байдужістю до нього, відправник потім повторно його оцінює на цій основі.

Південноафриканськими науковцями було запропоновано модель життєвого циклу інформаційного протиборства. Ними було розроблено дворівневий цикл. Цикл високого рівня містить основні блоки циклу (контекст, напад і захист, наслідки, реакції, відновлення і впливу на контекст). Це поєднується з більш детальним циклом, який показує застосування кількох понять високого рівня, наприклад, планування операцій буде виконуватися із урахуванням контексту і може проводитися до початку нападу або контрдій. Блок «АТАКА» містить кілька детальних інструкцій. Блок «ЗАХИСТ» має захисні методи та інструменти. Блок «СУСПІЛЬСТВО» має 4 концепції на високому рівні [56].

Дослідження Національної дослідницької ради США вказує на те, що роль інформаційно-психологічного впливу є дуже вагомим під час сучасних конфліктів. Вони вбачають, що вплив, який направлений на соціальні процеси противника, базується лише на психології і розглядають 4 напрями: математичні моделі формування переконання у відповідь на передачу повідомлень, переконання мереж, моделі обробки соціальної мережі та транзактивна пам'ять.

Більша частина соціальної роботи по формуванню психології переконань фокусується на тому, як повідомлення впливає на переконання. Розроблено важливі теоретичні поняття щодо цього: теорія підкріплення та теорія обробки інформації. На відміну від них, моделі соціальної мережі переконань зосереджені на тому, що положення індивіда в соціальній мережі та переконання інших членів групи впливають на переконання індивіда. Дані моделі називають моделями соціального впливу [56].

Багаточисельні емпіричні дослідження показали, що установлені переконання важче змінити. Крім цього доведено, що переконання, що засновані на малій кількості інформації менш стійкі до змін. Таким чином давно установлені переконання будуть стійкі до змін у тому ступені, у якому людина має найбільше аргументів для їх підтримання (вірить у них через факти пов’язані із переконанням). Таким чином, дані твердження доводять ідею, що існує від’ємна кореляція між здвигом віри і теперішнього переконання незалежно від змісту повідомлення [56].

Дослідники виявили, що одним із найбільш перспективних підходів до розуміння інформаційної війни на локальному рівні є гібридні моделі, які використовують моделі визначеного інформаційного простору та моделі соціальної мережі. Дана гібридна модель включає в себе організаційні та когнітивні моделі. У даній моделі інформація зменшується і перетворюється у вузлах та із затримкою через обмеження зв’язку між вузлами. Така модель може об’єднати аналіз соціальних мереж для оцінки аспектів комунікації та ієрархії із переконанням мереж для оцінки аспектів індивідуальної обробки інформації. Тобто в них використовують соціальні мережі, для того, щоб зробити переконання мережі динамічними.

Соціальна обробка інформації передбачає введення у дію моделей структурних процесів, які впливають на переконання. Сучасні моделі зазвичай стимулюють процес, за допомогою якого люди взаємодіють з невеликою групою інших. Типова модель виглядає наступним чином:

$$T = Y + AWY + XB + E \ ,$$

де: Y – представляє собою вектор власної особистості і відношення до друга або віра у певний момент; X – представляє собою матрицю із екзогенних факторів; W – вагова матриця, яка взаємодіє або проводить/спричиняє вплив, є постійною; B – представляє собою вектор розвитку певного інформаційного середовища; E – вектор (вектори) помилок [56].

Більш конкретно моделі вагомо відрізняються тим, як вони будують матрицю W.

Одне з ключових понять у даній моделі є транзактивна пам'ять, що полягає у здатності груп мати систему пам’яті. Ідея заключається у тому, що знання зберігаються стільки, скільки перебувають у динамічному використанні. Модель Вегнера транзактивної пам’яті заснована на представлені людської пам’яті у вигляді комп’ютерної системи.

У Європейському союзі було утворено проект СЕРА задля виявлення інформаційно-психологічного впливу, контролю, збору, аналізу, даванню відсічі і виведенні на чисту воду російських пропагандистів у країнах Центральної та Східної Європи. Програма об’єднує провідних журналістів, активістів і аналітиків ЗМІ із держав Європи та використовує свій досвід для розробки аналітичного інструменту для ефективного рішення проблем із російською дезінформації на інституціальному, стратегічному і концептуальному рівнях [56]. Програма включає семінари, регулярний моніторинг програм російського змісту для конкретних країн і методів пропаганди.

Фінські науковці Йорма Йормакка та Ярмо Молса розглядають інформаційне протиборство та інформаційно-психологічний вплив зі сторони теорії ігор. Вчені доводять, що теорія ігор є однією з можливих шляхів вивчення математичних моделей інформаційної війни та інформаційно-психологічного впливу. У дослідженні також розглянуто мета стратегії, метою яких є зміни затрат на «гру». Такого роду управління громадською думкою тісно пов'язані з петлями спостереження (петлі Бойда, OODA) – кібернетичний самостійний і

саморегулюючий цикл, що має в своїй структурі 4 процеси: спостереження, орієнтація, рішення і дія. Моделювання інформаційного протиборства та інформаційно-психологічного впливу як гри передбачає наявність двох гравців: злодія та захисника [56]. Всі гравці, як очікується, будуть раціональними. Виграш для зловмисника – це втрати жертви. Можливі чотири сценарії для моделювання:

1. Напад противника на командування, управління та системи зв'язку і намагання відключити їх.

2. Група нападників здійснює масовану атаку проти критичних інформаційних ресурсів.

3. Здійснення цільових добре спланованих та скоординованих атак за допомогою кіберзброї, таких як нові віруси, хробаки та DoS інструменти.

4. Група нападників проводить довгострокову інформаційна війну, щоб викликати економічні втрати і сповільнити технічний розвиток.

Розглядається кілька стратегій. Однією з них є «терористичні ігри». Терористична гра є статичною грою для двох гравців, де обидва гравці раціональні. Терористи (T) захопили заручників і загрожують їх підірвати, якщо вимоги терористів не приймаються. Уряд (G) пропонує, що терористи повинні здатися і сісти до в'язниці. Обидва гравці мають дві стратегії p_1 і p_2 Стратегія p_1 означає прийняття умов одного з гравців у повному обсязі: терористи віддають заручників або уряд приймає вимоги (наприклад, платить викуп). Стратегія p_2 означає, що виконується лише одна умова, і гравець повністю відкидає інші [56]. Виграшем є наступні ситуації:

– якщо обидва гравці грають p_1 , то вони разом отримують -1: G приймає вимоги, T здається і йде до в'язниці, але отримує вигоду згідно допустимих вимог;

– якщо обидва гравці грають p_2 обидва гравці, то отримують -10; G відкидає вимоги, T вбивають заручників і отримують вигоду сам;

– якщо один з гравців обере стратегію p_1, то він отримує 0: Т грає p_1, а інший гравець грає p_2, то T отримує -5 і G відкидає умови, T здається та йде до в'язниці [56].

Припустимо, що G відіграє p_2. Тоді G говорить, що він не буде вести переговори з T, T може не вірити, що G так зіграє і може спробувати стратегію p_2 скінченим числом раз, але якщо G грає p_2, врешті-решт, і T доведеться почати грати p_1 для того, щоб звести до мінімуму втрати. Дану гру можна так проаналізувати якщо T приймає, що G завжди відіграє p_2 і буде приймати рішення або в підірвати заручників або прийняти вимоги уряду [56]. Потім раціональний гравець T завжди повинен грати p_1. Сміливий раціональний гравець виграє завжди над менш сміливим раціональним гравцем в довгостроковій перспективі, коли терористична гра повторюється.

Австралійські науковці Біл Хатчисон та Мет Уорен визначили та дослідили тактики проведення інформаційного протиборства, одним із інструментів здійснення якого є інформаційно-психологічний вплив. Дослідження окреслює можливі режими інформації атаки, використовуючи модель життєздатності системи інформаційного протиборства як структуру для їх проведення. Це спроба використовувати засіб системного аналізу вразливостей інформаційної інфраструктури в усіх організаціях. Його акцент робиться на процес атаки, а не на контрнаступ.

Є кілька способів як інформація або інформаційні системи можуть бути використані для проведення інформаційного протиборства.. Нижче перераховані деякі агресивні тактики, які є авторськими розробками дослідників:

– інформацією можна маніпулювати або дезінформувати. На одному рівні це може розглядатися як реклама, а на іншому як навмисний обман;

– інформація може бути перехоплена, таким чином даючи перехоплювачу уявлення про сильні чи слабкі сторони противнику;

– інформаційні потоки в цільовій аудиторії можуть бути порушені, або зупинитися, тим самим виробляючи перевагу для нападника;

– цільовій аудиторії може бути «залита» інформація, яка сповільнить переробку або аналіз вхідних даних;

– інформація може бути недоступною або блокованою для аудиторії;

– порушення інформації або інформаційних потоків призводить до зниження достовірності інформаційної системи;

– розголошення конфіденційної та таємної інформації призводить до незручного становища органів влади [56].

Мотивацією для атак можуть бути певні організаційні цілі або зловмисні. Напади можуть здійснюватися організацією або окремими особами. Деннінг виділив п'ять класів ресурсів, задіяних у інформаційній війні. Це:

– контейнери, наприклад комп'ютери і людські спогади;

– транспортери, наприклад люди, телекомунікаційні системи.

– датчики, наприклад, сканери, камери, мікрофони, людські почуття.

– реєстратори, наприклад принтери, людські процеси, що показують характеристики інформаційного середовища.

– процесори, наприклад мікропроцесори, люди, програмне забезпечення [56].

Кожен з цих елементів, або їх компоненти, можуть бути середовищем атак. Таким чином, коло об'єктів може варіюватися від громадської думки до мікрохвильового посилання. Дослідники описують життєздатну модель інформаційного протиборства (VSM) Стафорда Біра [56].

Модель складається з п'яти підсистеми, які мають такі функції [56]:

1. Реалізація ($S1$): ця функція складається з напівавтономних одиниць, які виконують оперативні завдання у системі. Це функції, які є основою для

існування системи. Вони взаємодіють з їх місцевим середовищем і один з одним. Кожен блок має своє власне локальне управління, яке підключається до ширшого управління вертикальних інформаційних потоків. Ця функція є частиною «роботи» організації.

2. Координація (*S2*): ця функція координує *S1* для того, щоб кожна одиниця *S1* діяла в інтересах всієї системи, а не своєї власної. Це може бути представлено як простий графік, або мораль серед працівників.

3. Внутрішній контроль (*S3*): ця функція обробляє інформацію політики з «вищої» функції (*S4*) і «нижчої» функції. Даний процес є функцією, яка контролює оперативний рівень. Його роль полягає в тому, щоб не створювати політику, але реалізувати її.

4. Розвідка та розробка (*S4*): ця функція діє як фільтр інформації від S3 і зовнішнього середовища.

5. Стратегія і політика (*S5*): ця функція є відповідальною за напрямок всієї системи. Вона повинна збалансувати внутрішні і зовнішні чинники.

Дослідники розглядають атаки на кожні функції більш детально:

Атака на основні діючі енергоблоки (S1)

Діючі енергоблоки можуть бути порушені:

– припинення їх експлуатації у локальному середовищі;

– відключення їх з іншими підрозділами *S1*;

– відділення їх від функції управління.

Інформація може бути використана для дезінформації локального середовища. Після цього окремі одиниці починають погано взаємодіяти одне з одним і значно погіршується управління ними. Дані напади мають на меті знизити ефективність організації порушуючи функції оперативного реагування.

Атаки на координаційну функцію (S2)

Мета атак на функцію узгодження ($S2$) полягає у знищенні згуртованості діючих енергоблоків. Метою, яку переслідують нападники є маніпулювання, заміна або заперечення інформації для того, щоб зробити функцію узгодження неефективною. Таким чином, діяльність $S1$ одиниць була б неузгодженою і працювали один проти одного до точки повного зриву під час успішної атаки. Прикладом може бути поширення неправдивої інформації задля дезінформування, що може призвести до втрати морального духу противником. Під час цих атак широко використовується інформаційно-психологічний вплив, який допомагає частково змінити характеристики середовища проведення операції [56].

Атаки на контролюючі функції ($S3$)

Головним для атак на функції контролю є використання інформації щодо порушення сприйняття політики. Таким чином, інструкції, що передаються з $S1$ будуть пропорційними з намірами політики, створені у $S5$. Зміна інформації в $S3$ і $S1$ впливає на зміни характеристик $S4$. На даному етапі формується вплив на політику, внаслідок якого вона буде змінена або деформована.

Атаки на $S3$ повинні порушити або знищити ефективне співробітництво між плануванням політики інформаційного середовища і її виконанням. Тому основною метою є зменшення ефективності взаємодії усіх ланок інформаційного середовища [56].

Знищення «мозку» і почуття організації ($S4$ / $S5$)

Метою $S4$ є динамічний зв'язок між зовнішнім і внутрішнім середовищем шляхом обробки і об’єднання інформації $S5$ і $S3$. $S5$ виробляє політику з даних, які надсилаються з $S4$. Ці дві функції можуть розглядатися як «мозок» середовища. Таким чином, метою атаки є створення хибних уявлень внутрішнього і зовнішнього середовищ, тобто створення такої політики та стратегії, які не підходять середовищу. Кінцева мета передбачає знищення визначеного інформаційного середовища. $S4$ також може бути переповнений неправдивою інформацією, яка викликає плутанину та недовіру до неї. Згідно

дослідження основними завданнями інтелектуальних систем (*S4*) є збір, обробка, аналіз та поширення інформації.

Класифікується рівень «Інформація» як:

– дані (вимірювання і спостереження);

– інформація (контекст, проіндексовані і організовані дані);

– знання (розуміння інформації);

– мудрість (знання ефективно застосовані).

Таким чином, завдання атак є порушення, маніпуляції з інформацією задля зміни цілі визначеного середовища Після отримання цільовою аудиторією інформації, нападники нею маніпулюють у раніше визначеному контексті. Класичним прикладом цього є кампанія з дезінформації німецьких військ британською владою до висадки військ союзників у Нормандії в 1944 році. На більш пізніх стадіях зловмисник має заперечувати ефективне застосування знань мети.

Американський дослідник Скот Джонсон визначає, що інформаційне протиборство відбувається власне інформаційною атакою, комп'ютерною атакою та психологічною операцією. При чому усі компоненти часто взаємодіють між собою. Ці форми як правило використовуються на тактичному рівні, і вони потребують знання технічних характеристик мішені та експлуатаційних процедур. За нормальних умов вони є незалежними та ізольованими. Науковець розробив трирівневу цільову модель інформаційного протиборства. Вона складається з таких рівнів [56]:

– рівень інформаційної системи – фізичні елементи, які генерують, передають або зберігають інформацію. Атаки на інформаційні системи створюють технічні ефекти;

– рівень управління інформацією – процеси для обробки і розповсюдження інформації. На даному рівні атаки створюють функціональний ефект;

– рівень прийняття рішення – інтелектуальні процеси для інтерпретації та використання інформації. На даному рівні атаки створюють експлуатаційні ефекти.

Горбулін В. П., Додонов О. Г., Ланде Д. В. розглянули різні методи виявлення інформаційно-психологічного впливу. Серед них – метод DFA (Detrended fluctuation analysus), який часто використовується для виявлення статистичної самоподібності сигналів [90].

Цей метод є варіантом дисперсійного аналізу одномірних випадкових блукань і дає змогу досліджувати ефекти тривалих кореляцій у рядах, що розглядаються. У рамках алгоритму DFA аналізується середньоквадратична помилка лінійної апроксимації залежно від розміру ділянки апроксимації (вікна спостереження) [90]. Нехай є ряд вимірів $x_t, t \in 1, \dots, N$. Позначимо середнє значення цього ряду вимірів:

$$\langle x \rangle = \frac{1}{N} \sum_{k=1}^{t} x_k$$

З вихідного ряду будується ряд накопичення:

$$\langle x \rangle = \frac{1}{N} \sum_{k=1}^{t} (x_k - \langle x \rangle)$$

Потім ряд X_t розділяється на часові вікна довжиною L, будується лінійна апроксимація (L_j,L) за значеннями X_{kjL} з X_{jL} усередині кожного вікна (у свою чергу, X_{jL} - підмножина $X_{t,j}$ = 1,...,J, J = N/L - кількість вікон спостереження) і розраховується відхилення точок ряду накопичення від лінійної апроксимації:

$$E(j,L) = \sqrt{\frac{1}{L} \sum_{k=1}^{L} (X_{k,j,L} - X_{k,j,L})^2} = \sqrt{\frac{1}{L} \sum_{k=1}^{L} \left|\Delta_{k,j,L}\right|^2}$$

де $L_{k,j,L}$ – значення локальної лінійної апроксимації в точці t = (j – 1)L + k. Тут $\left|\Delta_{k,j,L}\right|^2$ - абсолютне відхилення елемента $X_{k,j,L}$ від локальної лінійної апроксимації [90]. Далі обчислюється середнє значення: після чого, у випадку $F(L) \propto L^{\alpha}$, де α деяка константа, робляться висновки щодо наявності статистичної самоподібності та характеру поведінки ряду вимірів, який досліджується [90].

С. Джонсон представив використання моделі для атаки під час інформаційного протиборства:

Рівень інформаційної системи. Передусім атаки здійснюється на інформаційну систему. У багатьох, але не у всіх випадках, ця система є початковою метою атаки, і технічні ефекти призначені задля перевантаження приймача, порушення цілісності даних, виключення комп'ютера, стирання даних, фізичного знищення носіїв інформації, і так далі [56].

Рівень управління інформацією. Управління інформацією означає передачу інформації, поширення, зберігання, злиття і перетворення. Ці функції виконуються інформаційними системами, і вони являють собою логічний рівень, накладеного на фізичному рівні інформаційних систем. Прикладами функціональних ефектів є зміна потужності передачі інформації, затримки продуктивності і перевантаження інформацією. Відбувається поширення дезінформації або розкручення певними фактами задля підривання довіри до органів влади, збройних сил. Ще більш серйозною проблемою є військова неправдива інформація. Ця проблема має ще й мережеву вразливість. Це викликано мінливими вимогами для проведення спільних операцій, в поєднанні з величезним збільшенням кількості систем зв'язку і передачі даних, які мають жорсткі вимоги до сумісності. Традиційні УКВ голосові радіостанції , що працюють на стандартних каналах можуть бути використані ким-небудь; інші передавачі можуть бути використані тільки якщо одержувач має сумісне обладнання. Противник може використовувати цю проблему шляхом виявлення і орієнтації критичних вузлів, де виконується перетворення даних, або

скориставшись плутаниною або проведенням атак. Якщо інформаційні управлінці звикли бачити нечитабельні дані, вони можуть не визнати той факт, що деякі дані були зіпсованими або пошкоджені, приписуючи проблеми до недоліків самої системи. Таким чином, планувальник атак повинен розуміти процеси управління інформацією ворога [56].

Процес прийняття рішення. Кінцевою метою інформаційної атаки є процес прийняття рішень. Дані ефекти можуть бути непрямими, для маскування та більш пізнього виявлення та прийняття контрдій противником. (табл. 1.1) [56].

Таблиця 1.1

Інформаційні атаки

Вид атаки	***Цільовий рівень***	***Технічний ефект***	***Функціональний ефект***	***Операційний ефект (приклади)***
Глушіння систем звязку	Інформаційні системи	Блокування сигналу	Втрата інформації	Затримка або помилкове вирішення
Вторгнення у системи звязку	Управління інформацією	Лінії звязку перестають працювати	Втрата інформації, самогенеруючі перевантаження	Затримка
Компютерні віруси	Інформаційні системи	Параліч системи	Втрата даних, втрата функціональних властивостей	Затримка або помилкове вирішення
Мережеві черви	Управління інформацією	Лінії звязку перестають працювати	Затримка або перевантаження, що спричиняють втрату даних	Затримка вирішення, навмисне згортання вузлів
Інформаційно-психологічний вплив	Процес вирішення	Немає	Немає	Вирішення впливу
Інформаційно-психологічний вплив під час бойових дій	Процес вирішення	Немає	Немає	Сприйняття маніпуляції

Джонсон визначає основні елементи інформаційного протиборства. Елементи ІВ виходять за рамки методів і можливостей для традиційних форм

інформаційної атаки. Беручи буквальне уявлення терміну «війна,» необхідними елементами для інформаційного протиборства є: первинна: атака і обороноздатність.

Підтримка: збір розвідки для таргетингу інформації – розташування (яке, для інформаційного протиборства, може бути фізичним або логічним), сильні і слабкі сторони.

Підтримка: збір розвідки для оцінки збитку битви (BDA).

Підтримка: збір розвідки для свідчень атаки і попередження (I & W).

Шведські дослідники Іда Маністо та Ніклас Нільсен реалізували кардинально інший підхід до дослідження інформаційного протиборства, що ґрунтується на теорії фреймів. Свою теорію вони експериментально довели на основі подій впливу США на Ірак у 2001 р. та Росії на АР Крим в 2014 р.

Багато дисциплін в області соціальної науки були зацікавлені в використанні фреймів як аналітичного інструменту; психологія, засоби масової інформації і комунікація, політологія та соціології є всього лише кількома прикладами. Концепції і способи застосування розрізняються між різними дисциплінами і різні дослідники використовували різні шляхи аналізу фреймів. Фрейми як правило складаються з 4 компонентів: фрейми визначають активи, що знаходяться під загрозою, і агенти, що беруть участь, у діагностуванні активів шляхом виявлення причин загроз і їх походження, оцінки залучених компонентів і структур за допомогою моральних суджень і пропонують дії, щоб впоратися з проблемою та виконати запропоновані рішення. Не визначено, що всі чотири компоненти завжди повинні існувати одночасно, фрейм, який з'являється в тексті, може або не може включати в себе всі чотири компоненти [56].

Зведена інформація про розглянуті моделі представлено у таблиці 1.2.

Таблиця 1.2

Узагальнення результатів аналітичного дослідження

Назва	**Особливості**
Модель протидії інформаційно-психологічному впливу *(автор – А. Шиян)*	Виявлення інформаційно-психологічного впливу через зміну однієї із характеристик або всього інформаційного простору
Технологічні аспекти інформаційного протиборства *(автор – Р. Грищук)*	Розгляд ознакової класифікації методів інформаційного протиборства. Вона має п’ять характеристик: за типом протиборства, за метою, за характером впливу, за джерелом розповсюдження, за цільовою аудиторією.
Модель життєвого циклу інформаційного протиборства (*автори – Б. Ван Нікерк, М. Махарадж*)	Дворівневий цикл: «АТАКА» і «ЗАХИСТ» із власним набором методів.
Моделі інформаційно-психологічного впливу НДР США	Розгляд чотирьох складових: математичні моделі формування віри у відповідь на передачу повідомлень, переконання мереж, моделі обробки соціальної інформації та транзактивна пам’ять
Інформаційне протиборство зі сторони теорії ігор *(автори – Й. Йормакка, Я. Молса)*	Передбачається, що інформаційне протиборство – це гра з двома раціональними гравцями, для яких можливі кілька сценаріїв. Суть гри полягає у виборі кращого сценарію.
Модель інформаційної атаки *(автор – С. Джонсон)*	Визначення, що атаки може відбуватися як в цілому на інформаційне середовище, так і на окремі його рівні.
Проект CEPA	Аналіз інформаційного середовища по ключовим словам, виявлення та ідентифікації інформаційно-психологічного впливу по контексту.
Тактики проведення інформаційного протиборства *(автори – Б. Хатчисон, М. Уорен)*	Представлення інформаційного простору як 5 підсистем: реалізація, координація, внутрішній контроль, розвідка та обробка, політика і стратегія, побудова тактик атак та захисту на них.
Математичні моделі інформаційного протиборства *(автор – Д. Ланде)*	Розроблено формули проведення інформаційних операцій, визначення критичних активів та виявлення негативного інформаційного впливу
Теорія фреймів під час дослідження інформаційного протиборства *(автори – І. Маністо, Н. Нільсен)*	Розбір інформаційного протиборства на фрейми, що дозволить краще визначати їх джерело та впроваджувати контрзаходи

1.2. Поняття соціальних мереж та моделі поширення інформації в них

Соціальна мережа – це певне соціальне об’єднання, яке утворене індивідами за певними зв’язками, взаємовідносинами. соціальна структура, утворена індивідами або організаціями. Вперше термін було запропоновано в 1954 році Дж. А. Барнесом. З початку 2000-их рр. в мережі Інтернет з’явилися ресурси, які дозволяють обмінюватися повідомленнями, переглядати різні види контенту, створювати різноманітні спільноти за інтересами. З кожним роком популярність таких ресурів збільшується і вони перетворюються на великі майданчики поширення інформації з надзвичайно низькою «точкою входу» (будь-хто може створити інформаційну сторінку та поширювати власний контент або інформацію з власною інтерпретацією), поступово витісняючи з джерел отримання інформації традиційні, такі як телебачення, газети тощо.

Першим інтернет-ресурсом, який мав набір функцій соціальних мереж став сайт classmates.com, який було створено в 1995 році. Наступним став сайт SixDegrees.com, створений у 1997 році. З 2001 року такі розпочали широко застосовувати технологію «коло друзів» для залучення нових користувачів та об’єднання їх у соціальні спільноти. Найбільш популярним ресурсом, який одним із перших використовував таку технологію став Friendster. У 2004 році була створена найбільша соціальна мережа за кількістю користувачів у світі – Facebook. У 2022 році кількість щоденних користувачів мережі досягла понад 2 млрд. За цей час Facebook перетворився з соціальної мережі на велику платформу для поширення інформації, пропагування ідей, а її засновник та власник Марк Цукерберг на одного із найвпливовіших людей сучасного світу. Її вплив важко переоцінити, оскільки через дану соціальну мережу розвивалися та координувалися революційні події під час «Арабської весни» в 2011 році, її механізми таргетування інформації широко використовуються під час різних виборчих процесів, а апогеєм стали президентські вибори в США в 2016 році.

Після цих подій компанія неодноразово змінювала правила модерації та поширення контенту.

У 2004 році було створено найбільш популярну соціальну мережу сьогодення – Facebook. Після цього у тому ж році Google запустив свій аналог, але він так і не набув значного поширення. 2004 рік можна вважати початком буму створення соціальних мереж, адже у період 2004-2005 рр. зявилися Yahoo! 360° та MySpace. Згодом почали виникати і спеціалізовані, наприклад такі як LinkedIn.

Абсолютна більшість соціальних мереж є публічним і у них зареєструватися може будь-хто. Єдиною умовою є лише наявність мобільного телефонного номера або електронної пошти.

Повномасштабне вторгнення рф в Україну призвело до різкого зростання використання соціальних мереж як джерела новин. Серед 76,6% громадян України, які використовують соціальні мережі як джерело інформації, 66% обирають Telegram, 61% - YouTube, 58% - Facebook.

Індійські науковці В. Анантхасвамі та Б. Сітхалакшмі представляють поширення інформації в соціальних мережах через математичні моделі поширення інфекційних захворювань. Вони запропонували модель S-SEIR, яка враховує цінність інформації та поведінку користувачів через аналіз режиму поширення інформації у різних соціальних мережах [3]. Відповідно до цієї моделі науковці визначають взаємодію користувачів у соціальних мережах як взаємодію між вузлами. Такі вузли класифікуються на чотири категорії відповідно до поширення: вузол публікації, комунікаційний вузол, імунний вузол та «неінфікований» вузол. Комунікаційний вузол отримує повідомлення від сусідніх вузлів і має здатність поширювати інформацію на веб-сайті або за його межами. Імунний вузол отримує повідомлення від сусідів, але без поширення інформації. «Інфікований вузол» не отримує та не переглядає інформацію від свого сусіда тимчасово, але має можливість отримати повідомлення [3].

Модель поширення інформації в соціальних мережах S-SEIR представлена на рис. 1.3 [3].

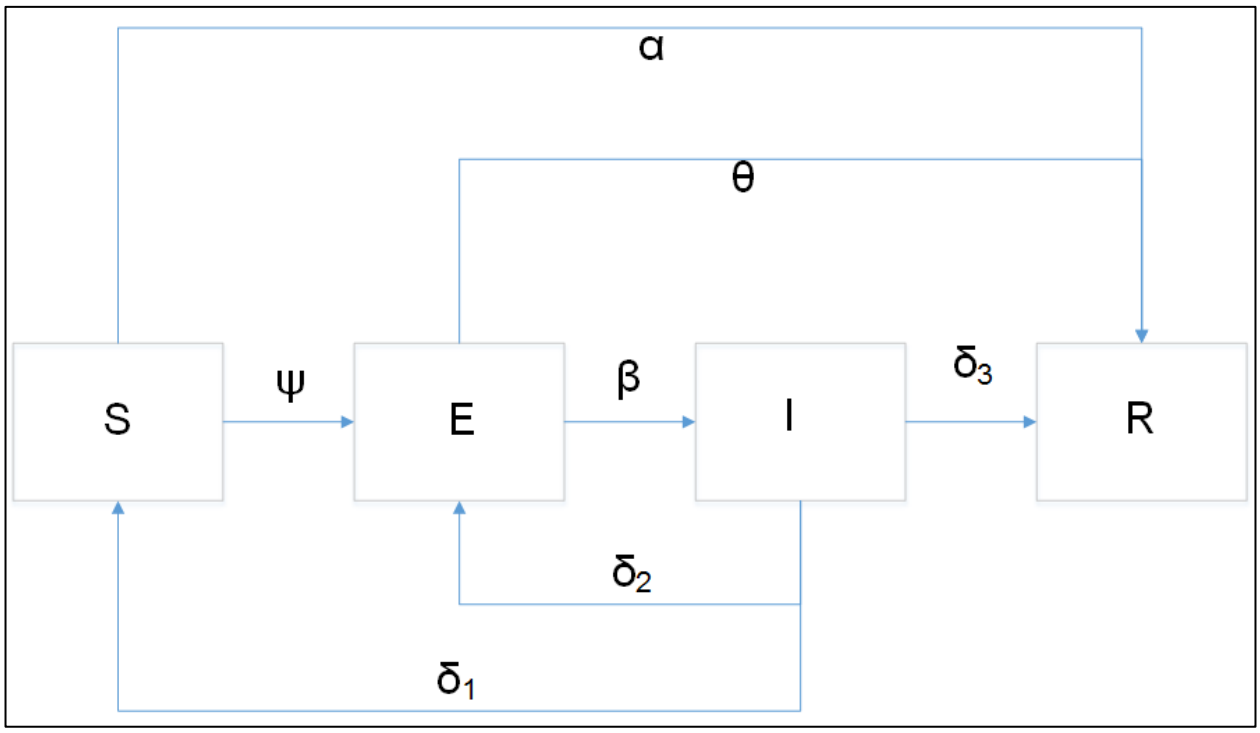


Рис. 1.3. Модель поширення інформації в соціальних мережах S-SEIR

Китайські дослідники Джиан Донг, Бін Чен, Хуан Ай та Фанг Жанг пропонують зображувати процес поширення інформації в соціальних мережах як неоднорідну стохастичну епідемічну модель SVFR [8]. У даній модель кожен користувач може перебувати в чотирьох станах, включаючи сприйнятливий (S), перегляд (V), вперед (F) та ізоляція (R) [8]. Перехід станів можна зобразити на рисунку 1.4. Процес розповсюдження інформації можна описати наступним чином:

1) на кроці $t = 0$ вузол вибирається як початковий (джерело інформації) та встановлюється в стан F, поки інші вузли встановлюються в стан S;

2) на будь-якому наступному кроці t кожен вузол у стані S має імовірність λ для перегляду інформації та стан вузла стає V на кроці t+1, якщо він має сусіда в стані F. Крім того, кожен вузол у стані V має імовірність θ для пересилання інформації і стає у стан F на кроці t+1. Кожен вузол у стані S має

ймовірність 1- λ для ігнорування інформації та кожен вузол у стані V має імовірність 1 - θ для не передавання інформації [8].

3) кожен вузол у стані F буде перетворений у стан R в залежності від часу. У цьому процесі усі зв'язки перегляду та пересилання інформації будуть записані. Починаючи з інформації джерела, увесь інформаційний каскад може бути побудований відповідно до відносин [8].

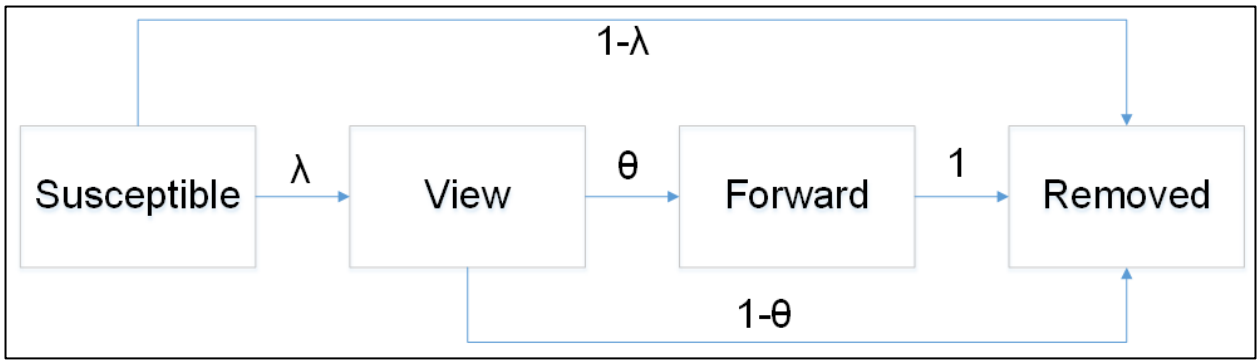


Рис. 1.4. Перехід станів моделі SVFR

Розподіл ступенів $P(d)$ безмасштабна мережа має степеневий розподіл $P(d) \sim D^{-\phi}$, де $d-$ ступінь вузла, а ϕ - експонента масштабування. Науковці розглядають безмасштабну мережу як основною моделлю поширення інформації в соціальній мережі [8].

У загальному в моделі SIR припускається, що кожен користувач може перебувати в одному з трьох станів:

S (Susceptible) - особа, яка ще не отримала інформацію, але може вразитися нею.

I (Infected) - особа, яка вже отримала інформацію та поширює її серед інших.

R (Recovered) - особа, яка отримала інформацію і більше не бере участі в процесі розповсюдження [8].

Динаміка поширення моделі SIR може бути описана наступними диференціальними рівняннями:

Рівняння Susceptible (S):

$\frac{dS}{dt} = -\beta * S * I$, де

β - коефіцієнта передачі інформації, S - кількість осіб, які ще не отримали інформацію, а I - кількість осіб, які отримали інформацію.

Рівняння Infected (I):

$\frac{dI}{dt} = \beta * S * I - \gamma * I$, де

γ - коефіцієнт відновлення (залежить від часу, який особа залишається в стані I [8].

Рівняння Recovered (R):

$\frac{dR}{dt} = \gamma * I$

Ці рівняння описують, як кількість осіб в станах S, I і R змінюється з часом. Зазвичай модель починається з початкового числа осіб, які отримали інформацію, а потім відстежується, як інформація розповсюджується серед інших користувачів з часом [8].

Ця модель може бути розширена для врахування більш складних факторів, таких як контакт між користувачами, вплив впливових осіб та інші. Але базова модель SIR надає загальний каркас для вивчення розповсюдження інформації в соціальних мережах [8].

Модель Вірусного Поширення (SIR) та її різні варіації мають кілька переваг при вивченні розповсюдження інформації в соціальних мережах:

- Модель SIR має просту математичну структуру і легко зрозуміти. Це робить її доступною для використання та інтерпретації навіть людям без глибоких знань в області математики та статистики.

- Модель SIR може бути використана для передбачення того, як швидко інформація поширюватиметься в мережі, і для визначення того, чи виникає

епідемія (в даному випадку - поширення інформації) в мережі. Це корисно для розробки стратегій контролю та оптимізації поширення інформації.

- Модель SIR може допомогти визначити, які інтервенції або заходи можуть бути ефективними для зменшення поширення інформації в мережі. Наприклад, вона може вказати, наскільки ефективно буде обмеження доступу до інформації для певних користувачів або вплив на впливових осіб.

- Модель SIR дозволяє ідентифікувати впливових користувачів, які можуть відігравати ключову роль у розповсюдженні інформації в мережі. Це важливо для маркетингових кампаній та стратегій впливу.

- За допомогою моделі SIR можна аналізувати різні сценарії розповсюдження інформації, включаючи варіанти зміни параметрів, такі як коефіцієнти передачі та відновлення, для прогнозування можливого впливу на розповсюдження [10].

Модель вірусного поширення (SIR) та її варіації мають кілька недоліків та обмежень, які важливо враховувати при їхньому використанні:

- модель SIR базується на спрощених припущеннях про розповсюдження інформації та не враховує багато складних аспектів реальних соціальних мереж, таких як взаємодія між користувачами, різноманітність інформаційних вмістів та інші фактори.

- Модель SIR припускає, що кожен користувач має однакову імовірність інфікування, що не відповідає реальній ситуації, де деякі користувачі можуть бути більш впливовими або активними в поширенні інформації.

- Для використання моделі SIR потрібні точні дані про початковий стан мережі та параметри моделі, такі як коефіцієнти передачі та відновлення. Отримання цих даних може бути важким завданням, особливо в реальних соціальних мережах.

- Модель SIR припускає сталий коефіцієнт відновлення для інфікованих осіб, що не завжди відповідає реальності, де тривалість інфікованості може змінюватися з часом.

- Модель SIR не враховує можливих змін у мережі з часом, таких як з'явлення нових користувачів, зміна зв'язків або зникнення користувачів.

- Модель SIR не враховує індивідуальні особливості користувачів та їхню поведінку, що може суттєво впливати на розповсюдження інформації.

- У складних соціальних мережах з великою кількістю взаємодій модель SIR може бути недостатньою для точного моделювання розповсюдження інформації [12].

З урахуванням цих обмежень, модель SIR корисна як базовий інструмент для вивчення розповсюдження інформації в соціальних мережах, але для більш точних та реалістичних результатів часто використовують більш складні моделі та аналізують додаткові фактори.

Іншою моделлю поширення інформації в соціальних мережах є *Independent Cascade* - стохастична модель для моделювання розповсюдження інформації в соціальних мережах. У цій моделі припускається, що поширення інформації залежить від ймовірностей активації кожного зв'язку між користувачами. Основна ідея полягає в тому, що інформація може бути передана від одного користувача до іншого з певною ймовірністю, і цей процес відбувається стохастично [2].

У моделі Independent Cascade ми маємо граф соціальної мережі, представлений вузлами (користувачами) і ребрами (зв'язками між користувачами). Кожен зв'язок має власну ймовірність передачі інформації від одного користувача до іншого. Коли користувач активуєся (наприклад, через отримання інформації від іншого активованого користувача), він може спробувати активувати своїх сусідів згідно з відповідними ймовірностями [2].

Ймовірність активації зв'язку (ребра) між користувачами позначається наступним чином:

$$\rho_{u \to v}$$

Дана імовірність позначає наскільки ймовірно користувач u активує користувача v [2].

Для початку моделі ми визначаємо початковий стан графу, де певні користувачі активовані (знають інформацію), інші - ні. Далі процес розповсюдження відбувається в декілька ітерацій:

1) користувач u намагається активувати користувача v з імовірністю

$$\rho_{u \to v};$$

2) якщо спроба активації вдається і користувач u активував користувача v, то він стає активованим;

3) процес продовжується для всіх активованих користувачів, які можуть спробувати активувати своїх сусідів [2].

У моделі Independent Cascade можна використовувати різні стратегії активації користувачів і вивчати розповсюдження інформації через граф соціальної мережі в стохастичних умовах [2].

Модель Independent Cascade має кілька переваг і важливих застосувань у вивченні та моделюванні розповсюдження інформації в соціальних мережах:

- модель Independent Cascade дозволяє враховувати стохастичний характер розповсюдження інформації. Вона враховує той факт, що активація користувачів та поширення інформації можуть бути випадковими та варіювати з ітерації в ітерацію.
- Модель Independent Cascade має просту структуру, що робить її легкою для розуміння і інтерпретації. Вона може бути використана як введення для вивчення процесів розповсюдження інформації в соціальних мережах.

- Модель Independent Cascade враховує вплив зв'язків між користувачами (інтеракції між ними). Вона враховує ймовірність передачі інформації через конкретні зв'язки, що важливо для аналізу та передбачення поширення інформації.

- Модель Independent Cascade може бути застосована для вивчення поширення не лише інформації, але і вірусів, ідей, рекламних кампаній та інших елементів в соціальних мережах. Це корисно для маркетингу та реклами.

- За допомогою моделі Independent Cascade можна аналізувати різні стратегії активації користувачів для максимізації поширення інформації або інших елементів.

- Модель Independent Cascade може допомогти ідентифікувати впливових користувачів, які можуть відігравати ключову роль у розповсюдженні інформації в соціальній мережі [2].

Загалом, модель Independent Cascade є важливим інструментом для дослідження розповсюдження інформації та впливу в соціальних мережах, особливо коли важливо враховувати випадковий та стохастичний характер таких процесів [2].

Модель Independent Cascade, хоча і корисна для дослідження розповсюдження інформації в соціальних мережах, також має свої недоліки і обмеження:

- модель Independent Cascade припускає, що поширення інформації відбувається лише через безпосередні зв'язки між користувачами та випадково. В реальних соціальних мережах інформація може поширюватися більш складними шляхами, враховуючи вплив впливових користувачів і глобальні фактори.

- Для точного моделювання розповсюдження інформації через модель Independent Cascade потрібні точні дані про зв'язки між користувачами та їхній характер. Отримання таких даних може бути важким завданням.

- Ефективність моделі Independent Cascade значно залежить від правильного визначення параметрів, таких як ймовірності активації зв'язків між користувачами. Недостатньо точні параметри можуть призвести до неточних результатів.

- Модель не враховує можливі зміни в структурі соціальної мережі з часом, такі як поява нових користувачів або зміни в зв'язках між користувачами.

- Модель не враховує індивідуальні особливості користувачів та їхню поведінку, що може важливо впливати на розповсюдження інформації.

- Модель Independent Cascade не дозволяє в моделюванні різноманітних сценаріїв інтервенцій або зміни стратегій активації користувачів [2].

Модель широкого поширення (Wide-Spread Model), також відома як модель масового поширення або модель гомогенного поширення, є простою і спрощеною моделлю для дослідження розповсюдження інформації в соціальних мережах. У цій моделі передбачається, що інформація, що поширюється, досягає всіх користувачів, які знаходяться в безпосередній близькості до того, хто почав поширення [5].

У цій моделі граф може бути представлений у вигляді матриці суміжності. Матриця суміжності для моделі Wide-Spread (модель масового поширення) буде мати специфічну структуру, оскільки вона припускає, що інформація поширюється від одного користувача до всіх його безпосередніх сусідів [5]. У такому випадку, матриця суміжності буде мати тільки ненульові значення на діагоналі та у рядках і стовпцях, що відповідають безпосереднім сусідам кожного користувача.

Розглянемо приклад графа з трьома користувачами (вузлами) і зв'язками між ними. Припустимо, що ми маємо користувачів A, B і C, і їх зв'язки представлені так:

користувач A з'єднаний з користувачем B і C.

користувач B з'єднаний з користувачем A і C.

користувач С з'єднаний з користувачем А і В.

Модель розпочинається з початкового користувача, який знає інформацію (ініціатора поширення), інші користувачі не мають інформації.

У цій моделі припускається, що інформація передається з одного користувача до всіх його безпосередніх сусідів. Інформація широко поширюється від початкового користувача на всіх його безпосередніх сусідів у кожному кроці [5].

Модель завершується, коли всі користувачі, які можуть бути активовані, вже знають інформацію, і більше немає нових активованих користувачів.

Модель Wide-Spread дуже спрощена і не враховує багато аспектів реального розповсюдження інформації, такі як вплив впливових користувачів або випадковість процесу [5].

1.3. Системи аналізу ефективності публічних сторінок у соціальних мережах

Наразі, у відкритому доступі відсутні інструменти, які одночасно ідентифікують інформаційну кампанію проти особи/компанії/держави, визначають методи впливу та оцінюють її. Проте із розвитком соціальних мереж з’явилися початки такого підходу. Більшість таких засобів спрямовано на SMM співробітників та покликані покращити їхню роботу і комунікаційну діяльність вцілому.

Варто виділити наступні системи, які допоможуть здійснити аналіз ефективності сторінок у соціальних мережах:

Klear – інструмент, алгоритми якого можуть визначити блогерів, які найкраще відповідають цільовій аудиторії. Він аналізує близько двох десятків показників, серед яких профіль користувачів, теми дописів. У системи наявна власна система оцінок, яка виставляє їх відповідно до популярності тої, чи

іншої сторінки. Засіб застосовує технологію штучного інтелекту FakeSpot для виявлення у блогерів фейкових підписників. Програма може аналізувати контент та рекламні кампанії. Працює виключно в Instagram, YouTybe та TikTok.

Social Mention – це інструмент для моніторингу згадок бренду, ключових слів, та публікацій у соціальних мережах, блогах, форумах і інших джерелах в Інтернеті. Mention дозволяє підприємствам та особам відстежувати та аналізувати інформацію, яка стосується їхнього бренду, продуктів чи послуг, а також слідкувати за трендами та спостерігати за конкурентами. Засіб збирає інформацію з соціальних мереж, новин, блогів, форумів та інших джерел Інтернету для слідкування за згадками бренду або ключових слів.

Інструмент надає звіти та аналітику щодо кількості згадок, їхнього поширення, аналіз настроїв (негативні, позитивні, нейтральні) та інші показники, що допомагають зрозуміти, як бренд сприймається в Інтернеті.

Mention дозволяє об'єднувати команди для спільного моніторингу та аналізу згадок. Користувач може призначити завдання та вести діалоги з командою безпосередньо в інтерфейсі інструмента. Засіб інтегрується з різними соціальними платформами, такими як Facebook, Twitter, Instagram, і дозволяє реагувати на коментарі та повідомлення безпосередньо з інтерфейсу.

Засіб Mention використовується для виявлення і аналізу згадок бренду, забезпечення реакції на відгуки користувачів, а також для розробки більш ефективних маркетингових стратегій на основі даних, отриманих з соціальних мереж та Інтернету загалом.

Talkwalker – це платформа для моніторингу та аналізу соціальних мереж і онлайн-засобів масової інформації. Цей інструмент допомагає підприємствам і маркетологам відстежувати та аналізувати активність в Інтернеті, щоб зрозуміти публічну думку, тренди та споживчі попити.

Платформа надає інструменти для аналізу настроїв - негативних, позитивних та нейтральних коментарів. Є можливість відстежувати, як

змінюється публічна думка щодо бренду чи продукту. Talkwalker дозволяє відстежувати активність конкурентів в соціальних мережах і в Інтернеті загалом, аналізувати їхні стратегії та взаємодію з аудиторією. Talkwalker допомагає відстежувати вірусні публікації та виявляти важливі суспільні події, які можуть вплинути на бренд.

Засіб Talkwalker є потужним інструментом для моніторингу та аналізу соціальних мереж і онлайн-активності, який допомагає компаніям виявляти можливості та ризики, а також покращувати свою стратегію в інтернет-просторі.

Awario – це інструмент для моніторингу веб-згадок, який дозволяє відстежувати і аналізувати активність в Інтернеті стосовно бренду, ключових слів чи певних тем. Цей інструмент допомагає підприємствам та особам слідкувати за публічною думкою, виявляти тренди та взаємодіяти з аудиторією. Інструмент моніторить згадки не лише у соціальних мережах, але й у блогах, форумах, новинах та інших онлайн-джерелах. Це дозволяє отримати повну картину публічної думки. Awario надає інформацію про настрої у згадках - негативні, позитивні та нейтральні.

Socialbakers – це комплексний інструмент для управління соціальними мережами та аналізу даних у соціальних медіа. Ця платформа допомагає підприємствам та маркетологам краще розуміти та оптимізувати свою присутність в соціальних мережах, а також слідкувати за конкурентами та аналізувати результати своїх маркетингових кампаній.

Socialbakers дозволяє відстежувати активність сторінки в різних соціальних мережах, таких як Facebook, Instagram, Twitter, YouTube і багатьох інших. Користувачам надається можливість слідкувати за згадками, коментарями, лайками та іншими показниками в соціальних мережах. Інструмент надає детальну аналітику стосовно аудиторії, включаючи вікову групу, географічний розподіл, інтереси і звички користувачів. Платформа надає засоби для вимірювання ефективності маркетингових кампаній в соціальних

мережах. Засіб формує звіти про взаємодію аудиторії, конверсію та інші метрики успіху.

Socialbakers – це потужний інструмент для аналізу та управління соціальними мережами, який допомагає підприємствам покращити свою стратегію в соціальних мережах і досягти більшого успіху в онлайн-середовищі.

Brandwatch – це інструмент для моніторингу соціальних мереж та аналізу веб-згадок, який допомагає підприємствам і маркетологам відстежувати і аналізувати публічну думку, тренди та взаємодію аудиторії в Інтернеті. Засіб дозволяє відстежувати згадки бренду, продуктів чи ключових слів в соціальних мережах, новинах, блогах, форумах та інших джерелах Інтернету.

Інструмент аналізує коментарі та згадки та визначає настрої аудиторії - негативні, позитивні чи нейтральні. Платформа надає засоби для вимірювання ефективності маркетингових кампаній та взаємодії з аудиторією в соціальних мережах.

Brandwatch – це потужний інструмент для моніторингу та аналізу соціальних мереж і веб-згадок, який допомагає покращити стратегію маркетингу, слідкувати за публічною думкою та взаємодіяти з аудиторією в Інтернеті.

Sprout Social – це комплексний інструмент для управління соціальними мережами та аналізу результатів маркетингових кампаній в соціальних медіа. Ця платформа допомагає підприємствам та маркетологам ефективно керувати своєю присутністю в соціальних мережах, взаємодіяти з аудиторією та вимірювати результати своїх зусиль. Sprout Social надає інструменти для моніторингу активності бренду в різних соціальних мережах, таких як Facebook, Twitter, Instagram, LinkedIn та інші через відстеження згадок, коментарів, лайків та інших інтеракції.

Платформа надає моджливість створювати, планувати та публікувати контент в соціальних мережах безпосередньо з інтерфейсу Sprout Social.

Платформа надає детальну аналітику стосовно ефективності соціальних кампаній. Існує можливість вимірювати ключові показники, такі як зростання аудиторії, взаємодія з публікаціями, конверсія та інші метрики. Засіб дозволяє відповідати на коментарі, повідомлення та звернення аудиторії зі свого централізованого інтерфейсу.

Buffer – це інструмент для планування та управління контентом в соціальних мережах. Засіб дозволяє планувати та розкладати публікації на різних соціальних мережах.

Платформа надає можливість додавати і керувати декількома обліковими записами в соціальних мережах, такими як Facebook, Twitter, Instagram, LinkedIn та інші, з одного облікового запису Buffer. Засіб надає базову аналітику, включаючи кількість лайків, репостів та коментарів.

Hootsuite – це інструмент для управління соціальними мережами, призначений для планування та виконання маркетингових кампаній в різних соціальних медіа. Hootsuite дозволяє планувати і публікувати контент на багатьох платформах, включаючи Facebook, Twitter, Instagram, LinkedIn та інші. Платформа надає розширену аналітику, яка допомагає вимірювати ефективність стратегії в соціальних мережах.

Hootsuite дозволяє відстежувати згадки вашого бренду в соціальних мережах та слідкувати за трендами у ваших галузях.

Наведемо порівняльний аналіз перелічених засобів у табл. 1.3:

Таблиця 1.3

Порівняльний аналіз систем аналізу соціальних мереж

Назва	**Підтримка багатьох соціальних мереж**	**Виявлення згадок про сторінку**	**Виявлення трендів**	**Оцінювання дописів**	**Ідентифікація інформаційної кампанії**	**Оцінювання кампанії**
Klear	-	+	+	+	-	-
Mention	+	+	+	+	-	-
Talkwalker	+	+	+	+	-	-
Awario	-	+	-	+	-	-
Socialbakers	+	+	+	+	-	-
Brandwatch	+	+	-	+	-	-
Sprout Social	+	+	+	+	-	-
Buffer	-	+	-	+	-	-
Hootsuite	-	+	-	+	-	-

1.4. Висновки

1. Дослідники у багатьох країнах світу широко описали процеси та створили моделі інформаційно-психологічного впливу. Враховуючи, сучасну ситуацію із інформаційного протиборства актуальність даних досліджень буде лише зростати.

Під час дослідження було проаналізовано теорію інформаційного протиборства з точки зору різних підходів: теорії ігор, теорії фреймів, різних математичних представлень, моделі атаки та захисту, виявлення та протидії. Це дозволило виділити переваги та недоліки кожного з підходів, а також сформувати власний щодо проблеми математичного аналізу та опису інформаційного протиборства.

У результаті було обрано логіко-математичний апарат нечіткої логіки для забезпечення процесів виявлення, ідентифікації, оцінювання та підбору контрзаходів. Методи нечіткої логіки дозволяють виконувати вищевказані процеси у слабоформалізованому нечіткому середовищі, чого не можуть робити інші підходи.

2. Проаналізовано моделі поширення інформації в соціальних мережах. Виявлено, що дана тема не є поширеною серед науковців.

Проте виділяють наступні моделі поширення інформації в соціальних мережах: модель вірусного поширення (SIR); модель SEIR; модель Independent Cascade; модель широкого поширення (Wide-Spread).

Даний аналіз допоміг краще зрозуміти природу поширення інформації у соціальних мережах. У подальшому це допоможе під час розроблення методу оцінювання критичності інформаційно-психологічного впливу в соціальних мережах.

3. Проведено порівняльний аналіз сучасних систем аналізу ефективності публічних сторінок у соціальних мережах. Можемо зробити висновок із табл. 1.3 про те, що більшість систем аналізу соціальних мереж націлені на аналіз рекламних кампаній та пошук згадок про бренд, проте не дозволяють зробити висновок про детальний стан справ в інформаційному просторі. Також у них відсутні будь які рекомендації щодо подальших дій власнику сторінки чи бренду, а значить не забезпечують процеси управління.

Відповідно до цього були поставлені завдання щодо розробки методів виявлення, ідентифікації та оцінювання інформаційно-психологічного впливу, системи управління інформаційно-психологічним впливом у соціальних мережах, розгляду заходів протидії його негативного прояву.

РОЗДІЛ 2. МЕТОД ВИЯВЛЕННЯ ТА ІДЕНТИФІКАЦІЇ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИМ ВПЛИВОМ У СОЦІАЛЬНИХ МЕРЕЖАХ

2.1. Узагальнена класифікація та моделі представлення інформаційно-психологічного впливу у соціальних мережах

Інформаційно-психологічні впливи займають важливе місце в сучасному світі. Передусім це спричинено процесами глобалізації та інформатизації, що інтегрували в одне ціле усі інформаційні простори планети. Інформаційно-психологічний вплив застосовується для вирішення певних задач з найменшими витратами.

Модель інформаційно-психологічного впливу представлено на рис. 2.1.

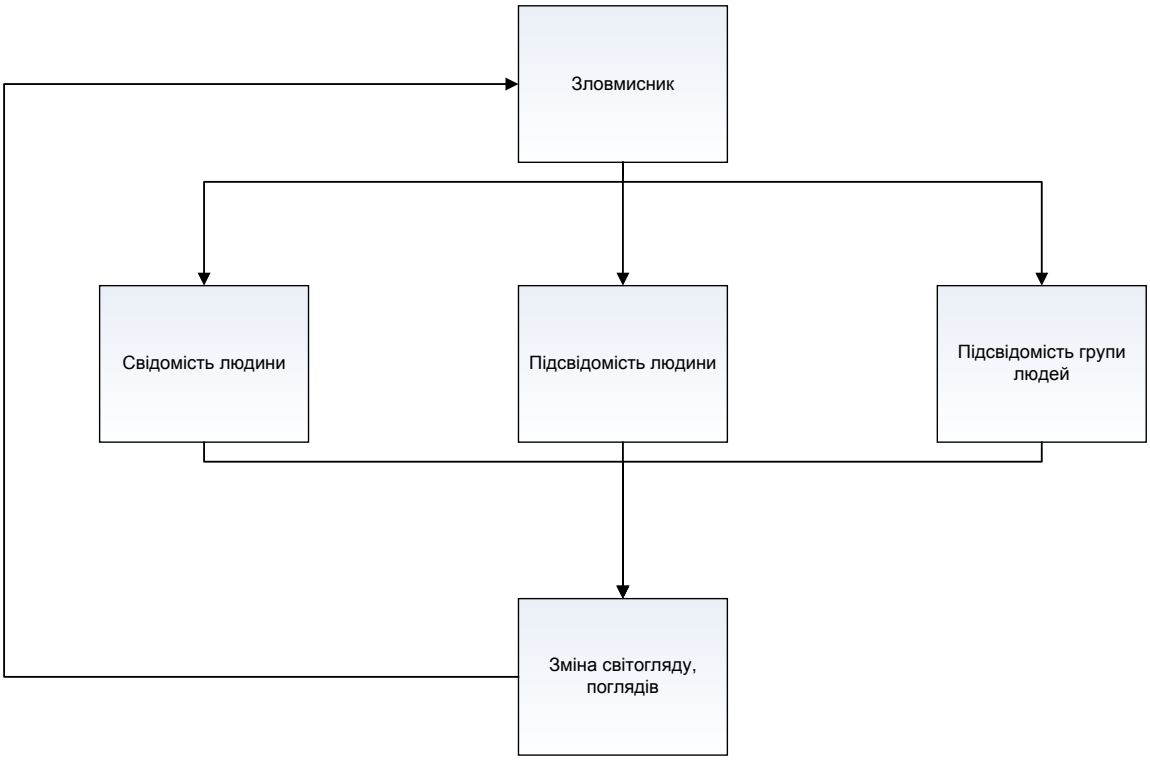


Рис. 2.1. Модель інформаційно-психологічного впливу

Із рис. 2.1, бачимо, що зловмисник діє на підсвідомість та свідомість людини. Потім відбувається перевірка реакції людей і виправлення та доопрацювання дій.

Запропонуємо визначення, що інформаційно-психологічний вплив – це дія на свідомість та підсвідомість людини, групи людей, суспільства з метою внесення змін у їх поведінку шляхом використання психологічних методів впливу, що застосовуються інформаційним шляхом. Тобто, засобами здійснення якого є ЗМІ, листівки тощо. У загальному, інформаційно-психологічний вплив – це атака на свідомість та підсвідомість.

Будь-які інформаційно-психологічні впливи можуть існувати і реалізовуватися лише в інформаційному просторі. Інформаційний простір можна представити у вигляді кортежу кортеж (1):

$$Information\,Space = < Users, Infrastructure, Informationflow, Is > \qquad (1)$$

де $Users$ – це усі члени інформаційного простору;

$Infrastructure$ – інформаційна інфраструктура;

$Informationflow$ – інформаційні потоки;

Is – показник інформаційного простору.

Вищенаведені компоненти повинні широко взаємодіяти між собою, оскільки інформаційні потоки стали б менш поширені. Інформаційна інфраструктура – це засоби передачі інформації до населення, організація взаємодії інформаційних ресурсів. Серед неї транслятори радіо, ТВ-передавачі, ТВ-приймачі тощо.

Інформаційний потік – це рух інформації від її джерела до отримувача, що визначається функціональними зв’язками між ними.

Кортеж (1) показує, що у разі зміни усіх або хоча б однієї з характеристик, можна зробити висновок, що відбувся чи відбувається дія інформаційно-психологічного впливу. Визначити чи продовжується, чи вже завершилася дія можна завдяки кільком перевіркам із певним проміжком часу.

За даним пунктом відбувається процес ідентифікації інформаційно-психологічного впливу: відбувається порівняння інформаційного простору у даний момент часу з еталонним.

$$Is_1 \neq Is \qquad (2)$$

Еталонні значенні інформаційного простору задаються шляхом визначення середніх значень властивостей інформаційного простору протягом певного періоду часу, що розвивався до даного моменту часу. Тобто еталонні значення ґрунтуються на статистиці.

Будемо вважати, що відбувається інформаційно-психологічний вплив, коли під час порівняння (2) немає рівності. Із даних формул, можна зробити висновок, що при умові зміни інформаційного простору, або хоча б однієї його характеристики відбувається інформаційно-психологічний вплив.

Виходячи з цього та цілей, що ставлять перед собою джерела ІПВ, запропонуємо цільову модель інформаційно-психологічного впливу, згідно з якою ІПВ можна описати завдяки кортежу:

$$IPI =< Idp, Is, T, Q, R > \qquad (3)$$

Вищенаведені параметри кортежу формують цільову модель і визначаються ознаками інформаційно-психологічного впливу.

Idp – методи інформаційно-психологічного впливу. Із цих методів виключено найбільш небезпечні види інформаційної зброї, що не дозволить надійно контролювати рівень збитку, що завдається.

Is – простір, щодо якого здійснюється інформаційно-психологічний вплив. Важливим є обмеження розмірів простору, об'єктів інформаційної інфраструктури та соціальних груп, які піддаються враженню ІПВ (агресія зачіпає не весь інформаційно-психологічний простір держави-жертви, а тільки його частину). Зміна цього простору свідчить про наявність в ньому ІПВ.

T – час впливу. Тривалість застосування методів інформаційно-психологічного впливу щодо певного інформаційного-простору.

Q – мета впливу. Мета є локальною або частковою метою, як правило, агресія припиняється після повного досягнення агресором усіх поставлених конкретних цілей і рідко приймає затяжний характер.

R – набір контрзаходів, які покликані протидіяти інформаційно-психологічному впливу.

Наприклад, представимо пропаганду у випуску «кто против?» на телеканалі «россия1» в ефірі від 22 лютого 2022 року за допомогою цільової моделі ІПВ:

$$IPI =< P_5, \begin{Bmatrix} телебачення, \\ новинні\ платформи, \\ соціальні\ мережі, \\ радіо \end{Bmatrix}, 24год, примус, блокування >$$

Функціональну модель інформаційно-психологічного впливу можна представити як:

$$IPI =< Id, Pi, < \mathbf{Po}, KB >, ER >, \qquad (4)$$

де Id – це набір методів інформаційно-психологічного впливу. Під час одної дії з інформаційно-психологічного впливу може використовуватися кілька методів одночасно.

Pi – набір (множина) ідентифікуючих параметрів інформаційно-психологічного впливу. Ідентифікуючі параметри інформаційного простору можна представити кортежом

$$Pi =< Pi_1, Pi_2, ...Pi_n > .$$

Ідентифікуючими параметрами виступають такі показники інформаційного простору як: «лавиноподібність» - PM; «зростання емоційності» - IF; «зростання тенденційності» - EL; «збільшення сенсаційності» - PP; «тональність» - PN; «взаємоузгодження дій суб'єктів здійснення» - CG; «час проведення» - LT.

Po – набір (множина) оціночних параметрів інформаційно-психологічного впливу. Оціночні параметри інформаційного простору можна представити кортежом

$$Po =< Po_1, Po_2, ...Po_m > .$$

Оціночними параметрами виступають такі показники інформаційного простору як: CSA – «Повнота і сила аргументації», CGN – «Узгодженість з нормами загальносуспільної думки», PR – «Реакція громадськості», GAF –

«Зростання фактора тривожності», VD – «Швидкість розповсюдження», NAT – «Кількість уражених цілей», DR – «Тривалість».

ER – набір (множина) евристичних правил, за якими здійснюється ідентифікація виявлених ІПВ, що є по суті логіко-лінгвістичною звязкою комбінації ідентифікуючих параметрів та відповідного їй конкретному типу ІПВ в інформпросторі.

Представимо пропаганду у випуску «кто против?» на телеканалі «россия1» в ефірі від 22 лютого 2022 року за допомогою функціональної моделі ІПВ:

$$IPI =< P_5, \{\text{LT}, \text{PP}, \text{CG}\}, \{\mathbf{Po}, < 0,292; 0,176; 0,155; 0,110; 0,078; 0,065; 0,054 >, \text{Правило } 28 >$$

Розглянемо більш детально методи інформаційно-психологічного впливу як перший елемент кортежу (4) – Id. Під час сучасних протиборств можна зробити таку їхню класифікацію:

1) методи, що направлені на людей, які критично сприймають інформацію:

- зміна поглядів шляхом переконання;
- психологічна ізоляція об’єкту;
- примус.

2) методи, що направлені на людей, які некритично сприймають інформацію:

- дезінформація;
- пропаганда;
- зміна поглядів шляхом навіювання;
- зараження;
- маніпуляції;
- рефреймінг.

Як бачимо, існує певний дисбаланс серед методів, які у більшості випадків направлені на людей, що некритично сприймають інформацію. Дана ситуація викликана тим, що значно легше досягти результату, провести атаку,

якщо дії нападника направлені на некритичне мислення, адже вони будуть обходити певний «психологічний щит» людини.

В залежності від критичності сприйняття особою інформації, що подається разом з впливами виділяють два способи зміни поглядів: переконання та навіювання.

Розпочнемо розгляд методів із групи тих, що націлені на критичне мислення. Першим та найбільш поширеним із них є переконання. Воно забезпечує включення нових фактів у свідомість людини, яка аналізує й оцінює інформацію, що надходить до неї. Одним із головних чинників, від якого залежить ефективність даного методу є майстерність відправника повідомлення та власне сама якість повідомлення. Найбільш сприятливими умовами для переконання є дискусія, групова полеміка, суперечка, оскільки сформована під час вищенаведених форм думка набагато глибша, ніж та, що виникла за пасивного сприймання інформації. Розрізняють пряме та непряме переконання. Особливістю прямого є те, що особа або группа осіб зацікавлені в інформації, використовується логічні, правдиві, очевидні аргументи. За непрямого переконання на перше місце виходять випадкові чинники, наприклад, авторитет комунікатора [85]. Сила і глибина переконання залежать від переконуючої комунікації – сукупності заходів, спрямованих на підвищення ефективності мовного впливу. Це є основою для експериментальної риторики.

У випадку критичного сприйняття особою інформації, що цілеспрямовано подається їй для зміни поглядів матимемо справу з таким видом інформаційно-психологічного впливу як навіювання – процесс впливу на психічну сферу людини, пов'язаний з істотним зниженням її критичності до інформації, що надходить, відсутністю прагнення перевірити її достовірність, необмеженою довірою до її джерел [81].

Основним засобом навіювання є довіра до джерела інформації. Ним виступати може практично будь хто: від друзів до постів випадкових людей у соціальних мережах. Навіювання звертається не до критичного мислення особи, а до емпатійного сприйняття, підсвідомого утвердження наративів. Під час

застосування даного методу велике значення мають якості безпосерднього інливіду: самостійний досвід, емоційний стан, набуті переконання, знання тощо [99]. Важливе значення, яке впливає на ефективність навіювання є подача інформації від джерела, його авторитет, статус тощо.

Психологічна ізоляція об'єкту відбувається у трьох галузях: політична, економічна, військова [99]. Заходи щодо психологічної ізоляції у політичній галузі зводяться до дипломатичного впливу на керівництво держави. Яскравим прикладом цього є ситуація напередодні вводу військ Варшавського договору до Чехословаччини 1968 року. Тоді, 23 березня 1968 року у відповідь на «Празьку весну» було скликано засідання керівників країн-членів Варшавського договору, на якому відбулося різке засудження політики чехословацького лідера А. Дубчека. ЗМІ підхопили тему і видали як загальне невдоволення його політикою сусідніми країнами. Результатом стало введення військ СРСР, Польщі, Угорщини та Болгарії до Чехословаччини 21 серпня 1968 року.

Примус характеризується психологічним тиском на особистість чи групу людей. Психологічний тиск – це представницький, сильний, вказівний, інтенсивний вплив на психіку людини з метою внесення змін у поведінку або спонукання до дії людини [99].

Дезінформацію у нашому досліджені виділено в окремий метод інформаційно-психологічного впливу, адже вона, під час останніх інформаційних протиборств, застосовується окремо від пропаганди та наносить значний вплив на аудиторію. Даний метод застосовується для найкоротшого переконання групи людей у певній доцільності дій, вирішення проблеми. Дезінформування розділяють на термінологічне «мінування», «сіре» дезінформування, «чорне» дезінформування, тенденційне викладення фактів, дезінформування «від зворотного» [99].

Одним із найбільш ефективних методів інформаційно-психологічного впливу є пропаганда, яка використовується у даному випадку для коректування наявних думок. Власне сама пропаганда – це поширення політичних, філософських, наукових та ін. Ідей задля утвердження їх у громадській думці

населення [99]. Яскравим прикладом є утвердження ідей нацизму у Німеччині після приходу до влади А. Гітлера під керівництвом Й. Геббельса.

Зараження – це метод інформаційно-психологічного впливу, під час якого особі передаються наративи та повідомлення через настрої, емпатійну складову.

Під час зараження передається емоційний стан від джерела впливу до конкректного індивіда. Сфера свідомості за таких умов різко звужується, майже зникає критичність до подій, інформації, що надходить з різних джерел [99].

Маніпулювання – це процес систематичного та умисного впливу на інформаційне середовище з метою вплинути на громадську думку, перекрутити факти, створити спотворені образи або навіть викликати розпалення суспільно-політичних конфліктів. Цей вид маніпуляцій використовує інформацію та засоби масової комунікації для досягнення певних політичних, економічних або стратегічних цілей.

Маніпуляції в інформаційній війні можуть включати в себе розповсюдження фейкових новин, кібератаки, створення фальшивих профілів у соціальних мережах, маніпулювання алгоритмами пошуку і багато інших технік. Метою таких дій може бути підрив авторитету держави чи політичного лідера, спровокування соціальних розбіжностей, дестабілізація суспільства або навіть вплив на результати виборів.

Маніпуляції можуть бути здійснювані як державними акторами, так і нестандартними суб'єктами, такими як кіберзлочинці, хакери та групи впливу.

Рефреймінг - це процес зміни визначення або сприйняття певної ситуації, проблеми, ідеї чи поняття, зазвичай з метою вплинути на спосіб, яким люди їх розуміють і реагують на них. Цей процес передбачає переформулювання питань, аргументів або інформації з метою створення нового ракурсу або контексту для розгляду справи. Рефреймінг може бути використаний для зміни точки зору, підвищення рівня підтримки чи впливу на прийняття рішень.

Рефреймінг важливий в багатьох контекстах, включаючи комунікації, політику, медіа, маркетинг та конфліктологію. Виходячи з вищевикладеного, можна зробити висновок, що завдяки цільової моделі відбувається процес виявлення інформаційно-психологічного впливу та в подальшому реагування на нього, а завдяки функціональній – ідентифікація його видів шляхом встановлення відповідного евристичного правила, яке було активоване. Точна ідентифікація виду ІПВ допоможе якнайшвидше підібрати потрібні методи та / або заходи контрзаходів.

2.2. Формування еталонних значень ідентифікуючих параметрів

Запропоновано модель еталонів лінгвістичних змінних, яка орієнтована на побудову систем виявлення, ідентифікації та оцінювання інформаційно-психологічного впливу, що засновані на ідентифікації аномального стану в інформаційному просторі.

Розглянемо метод лінгвістичних термів з використанням статистичних даних (МЛТС) [59], де в якості міри належності елемента множині приймається оцінка частоти використання поняття, яке задається нечіткою множиною для характеристики елемента. Для цього на універсальній шкалі [0;1] розміщуються значення лінгвістичної змінної (ЛЗ) $X=\{x1, x2, \ldots, xn\}$.

Основою даного методу є те, що кожен проміжок шкали вимірювань зараховується визначена постійна кількість експериментів, проте під час практичного застосування цього досягти практично неможливо. У такому випадку складається таблиця вимірювань, у якій експерименти нерівномірно розподіляються відповідно до інтервалів. Деякі можуть бути взагалі не використані, тому отримані дані обробляються із застосуванням матриці підказок [86]. Наведемо приклад, під час якого виникла потреба в оцінюванні значення лінгвістичних змінних відхилення параметра $\Delta B \in [0, B]$ (B - максимально можливе відхилення), яке характеризує поточні виміри. Далі для $n = 5$ визначимо значення ЛЗ $\{x1, x2, x3, x4, x5\}$ [86]. Інтервал [0, B] і $\Delta B/B$

(оцінюване відношення) розділені на k відрізків, по якими збирається статистика, що характеризує частоту використання експертом значення лінгвістичної змінної для відображення своїх висновків. Під час наступного етапу отримані дані записують до таблиці та обробляються таким чином, щоб зменшити похибки: реквізити таблиці видаляються по праву та ліву сторону від яких у рядку стоять нульові значення. Сама ж матриця підказок інтерпретується як рядок, елементи якої розраховуються відповідно до формули:

$$k_j = \sum_{i=1}^{n} b_{ij}$$

Далі в отриманому рядку матриці вибирається максимальний елемент $k_{max} = max_{kj}$, і потім всі елементи таблиці перетворюються за виразом $c_{ij} = b_{ij}k_{max}/k_j$ [87].

Для стовпців, де $k_j = 0$ застосовується лінійна апроксимація $c_{ij} = (c_{ij-1} + c_{ij+1})/2$. Далі обчислюється значення функції приналежності за формулою $m_{ij} = c_{ij}/c_{max}$ [87].

Аналіз понять і класифікацій щодо інформаційно-психологічного впливу показав, що на сьогодні відсутня єдина класифікація, що охоплювала б усі аспекти і характеристики його здійснення під час інформаційного протиборства.

В процесі дослідження були виділені наступні ідентифікуючі параментри ІПВ:

- «лавиноподібність» - PM,

- «зростання емоційності» - IF,

- «зростання тенденційності» - EL;

- «збільшення сенсаційності» - PP;

- «тональність» - PN;

- «взаємоузгодження дій суб’єктів здійснення» - CG;

- «час проведення» - LT.

Для параметру LT характерні такі лінгвістичні оцінки: {короткотривала (К), середньотривала (С), довготривала (Д)}. Інтервали для визначення еталонних значень = {[0-25], [26-50], [51-75]} проміжків часу. Сформуємо узагальнену таблицю оцінок і базову матрицю частот, що представлена у вигляді таблиці 2.1.

Таблиця 2.1

Узагальнена таблиця оцінок параметру LT

	0-25	26-50	51-75
К	24	9	5
С	14	29	21
Д	12	19	30

$v = |50;57;56|$

$Max = 57$

Обрахуємо похідну матрицю частот:

$$\begin{vmatrix} 27,36;9;5,09 \\ 15,96;29;21,38 \\ 13,68;19;30,54 \end{vmatrix}$$

та вектор максимумів = ||27,36 29 30,54||

Обрахуємо матрицю належностей та супорти еталону для параметра

$$\begin{vmatrix} 1;0,3;0,1 \\ 0,6;1;0,7 \\ 0,5;0,7;1 \end{vmatrix}$$

Супорти: $T_{log11} = T_{log21} = T_{log31} = 25 / 100 = 0,25$, $T_{log12} = T_{log22} = T_{log32} = 50 / 100 = 0,5$, $T_{log13} = T_{log23} = T_{log33} = 75 / 100 = 0,75$ [30]. Здійснивши перетворення отримаємо набір еталонів параметра LT = T_{log} = {короткотривала (К), середньотривала (С), довготривала (Д)} і терми лінгвістичних змінних для цього параметра:

К = {0/0,25; 1/0,25, 0,3/0,5; 0,1/0,75; 0/0,75},

С = {0/0,25; 0,6/0,25; 1/0,5; 0,7/0,75; 0/0,75},

Д= {0/0,25; 0,5/0,25; 0,7/0,5; 1/0,75; 0/0,75}.

Графік функції належності термів лінгвістичної змінної Час проведення показаний на рис. 2.2:

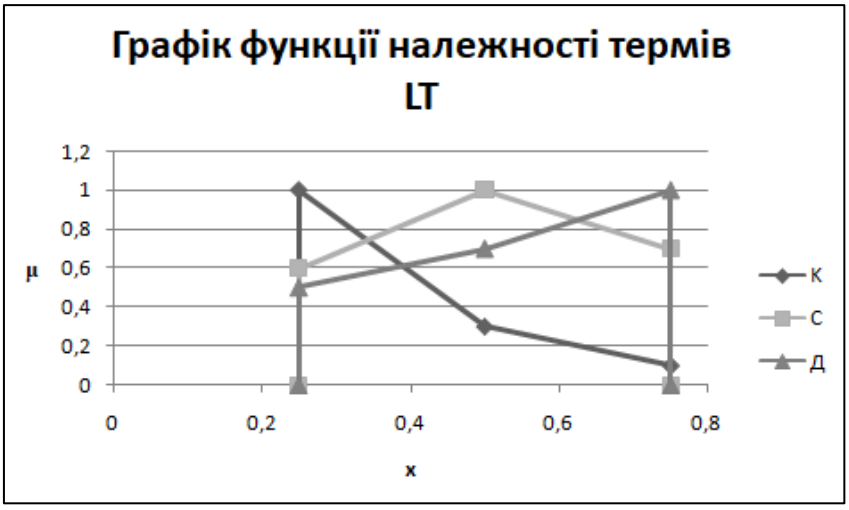


Рис. 2.2. Графік належності термів «Час проведення»

Для параметру EL характерні такі лінгвістичні оцінки: {маленькі (М), середні (С), високі (В)}. Інтервали для визначення еталонних значень = {[0-20], [21-50], [51-80]} протягом певного періоду часу. Сформуємо узагальнену таблицю оцінок і базову матрицю частот, що представлена у вигляді таблиці 2.2.

Таблиця 2.2

Узагальнена таблиця оцінок параметру EL

	0-20	21-50	51-80
М	16	8	1
С	7	12	3
В	1	5	8

$v = |24;25;12|$

$Max = 25$

Обрахуємо похідну матрицю частот:

$$\begin{vmatrix} 16,67;8;2,08 \\ 7,29;12;6,25 \\ 1,04;5;16,77 \end{vmatrix}$$

та вектор максимумів = ||16,67 12 16,67||

Обрахуємо матрицю належностей та супорти еталону для параметра:

$$\begin{vmatrix} 1;0,67;0,13 \\ 0,44;1;0,38 \\ 0,06;0,42;1 \end{vmatrix}$$

Супорти: $T_{log11}=T_{log21}=T_{log31}=20/80=0,25$, $T_{log12}=T_{log22}=T_{log32}=50/80=0,63$, $T_{log13}=T_{log23}=T_{log33}=80/80=1$. Здійснивши перетворення отримаємо набір еталонів параметра $EL=T_{log}$ = {мале (М), середнє (С), високе (В)} і терми лінгвістичних змінних для цього параметра:

$$M = \{0/0,25;\ 1/0,25;\ 0,67/0,63,\ 0,13/1,0/1\},$$

$$C = \{0/0,25;\ 0,44/0,25;\ 1/0,63;\ 0,38/1;\ 0/1\},$$

$$B = \{0/0,25;\ 0,06/0,25;\ 0,42/0,63;\ 0,1/1;\ 0/1\}.$$

Графік функції належності термів лінгвістичної змінної Зростання тенденційності показаний на рис. 2.3.

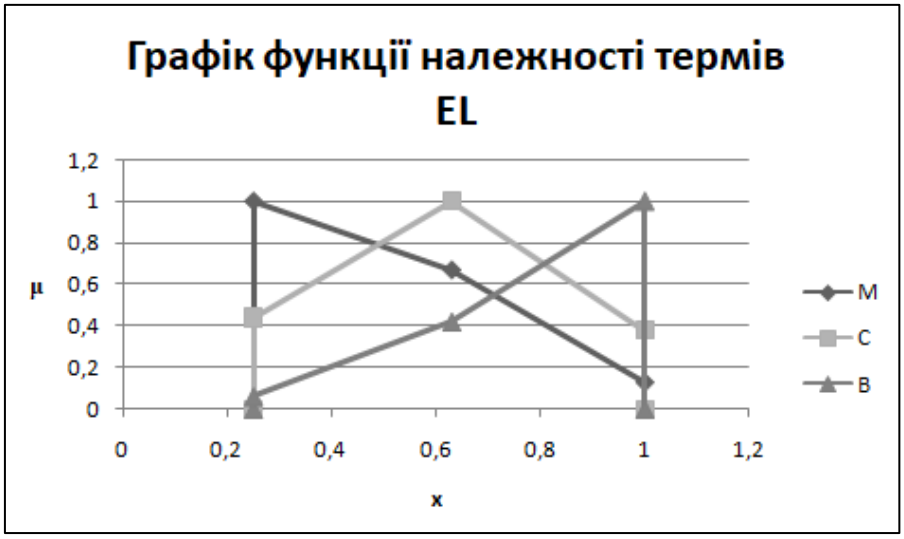


Рис. 2.3. Графік належності термів «Зростання тенденційності»

Для параметру РР характерні такі лінгвістичні оцінки: {маленька (М), середня (С), висока (В)}. Інтервали для визначення еталонних значень = {[0-33], [34-66], [67-100]} відсотків протягом місяця. Сформуємо узагальнену таблицю оцінок і базову матрицю частот, що представлена у вигляді таблиці 2.3.

Таблиця 2.3

Узагальнена таблиця оцінок параметру РР

	0-33	34-66	67-100
М	20	14	6
С	7	13	1
В	2	7	15

$v = |29;32;22|$

$Max = 32$

Обрахуємо похідну матрицю частот:

$$\begin{vmatrix} 24,83;16;9,82 \\ 8,69;13;1,64 \\ 2,48;7;24,55 \end{vmatrix}$$

та вектор максимумів = ||24,83 16 24,55 ||

Обрахуємо матрицю належностей та супорти еталону для параметра

$$\begin{vmatrix} 1;0,92;0,4 \\ 0,4;1;0,07 \\ 0,1;0,54;1 \end{vmatrix}$$

Супорти: $T_{log11}=T_{log21}=T_{log31}=33/100=0,33$, $T_{log12}=T_{log22}=T_{log32}=66/100=0,66$, $T_{log13}=T_{log23}=T_{log33}=100/100=1$. Здійснивши перетворення отримаємо набір еталонів параметра $PP=T_{log}$ = {маленьке (М), середнє (С), високе (В)} і терми лінгвістичних змінних для цього параметра:

М = {0/0,33; 1/0,33; 0,92/0,66; 0,4/1; 0/1},

С = {0/0,33; 0,4/0,33; 0,8/0,66; 0,07/1; 0/1},

B = {0/0,33; 0,1/0,33; 0,44/0,66; 1/1; 0/1}.

Графік функції належності термів лінгвістичної змінної Збільшення сенсаційності, що дивиться закордонне телебачення показаний на рис. 2.4:

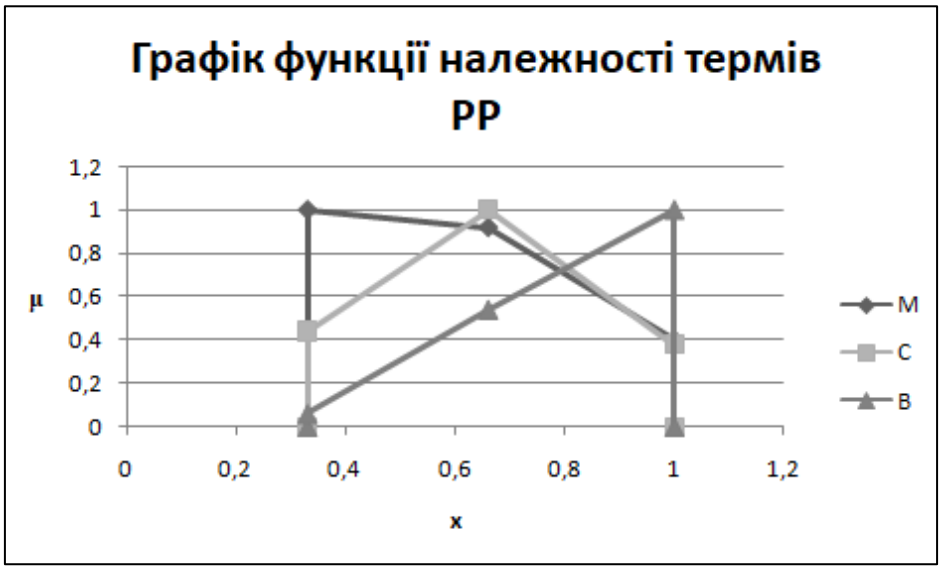


Рис. 2.4. Графік функції належності термів «Збільшення сенсаційності»

Для параметру PN характерні такі лінгвістичні оцінки: {мале (М), середнє (С), високе (В)}. Інтервали для визначення еталонних значень = {[0-33], [34-66], [67-100]}. Сформуємо узагальнену таблицю оцінок і базову матрицю частот, що представлена у вигляді таблиці 2.4.

Таблиця 2.4

Узагальнена таблиця оцінок параметру PN

	0-33	34-66	67-100
M	18	11	4
C	8	12	0
B	0	7	9

$v = |26;30;13|$

$Max = 30$

Обрахуємо похідну матрицю частот:

$$\begin{vmatrix} 22,85;14;10,15 \\ 10,15;12;0 \\ 0;7;22,85 \end{vmatrix}$$

та вектор максимумів = ||22,85 14 22,85 ||

Обрахуємо матрицю належностей та супорти еталону для параметра

$$\begin{vmatrix} 1;0,92;0,44 \\ 0,4;1;0 \\ 0;0,58;1 \end{vmatrix}$$

Супорти: $T_{log11}=T_{log21}=T_{log31}=33/100=0,33$, $T_{log12}=T_{log22}=T_{log32}=66/100=0,66$, $T_{log13}=T_{log23}=T_{log33}=100/100=1$. Здійснивши перетворення отримаємо набір еталонів параметра $PN=T_{log}$ = {позитивна (М), нейтральна (С), негативна (В)} і терми лінгвістичних змінних для цього параметра:

$$M = \{0/0,33;\ 1/0,33;\ 0,92/0,67;\ 0,44/1;\ 0/1\},$$

$$C = \{0/0,33;\ 0,4/0,33;\ 1/0,67;\ 0/1\},$$

$$B = \{0/0,33;\ 0,58/0,67;\ 1/1;\ 0/1\}.$$

Графік функції належності термів лінгвістичної змінної Тональності на рис. 2.5:

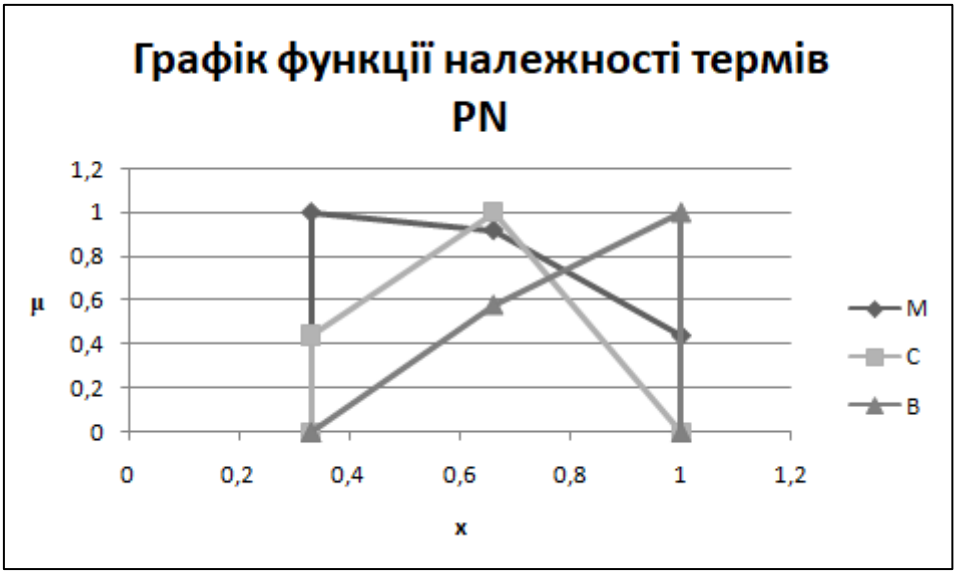


Рис. 2.5. Графік функції належності термів «Тональність»

Для параметру CG характерні такі лінгвістичні оцінки: {неузгоджені (Н), частково узгоджені (Ч), повноузгоджені (П)}. Інтервали для визначення еталонних значень = {[0-33], [34-66], [67-100]}. Сформуємо узагальнену таблицю оцінок і базову матрицю частот, що представлена у вигляді таблиці 2.5.

Таблиця 2.5.

Узагальнена таблиця оцінок параметру CG

	0-33	34-66	67-100
Н	29	15	6
Ч	20	25	18
П	0	5	22

$v = |49;45;46|$

$Max = 49$

Обрахуємо похідну матрицю частот:

$$\begin{vmatrix} 29;16,33;6,39 \\ 20;27,22;19,17 \\ 0;9;5,44;23,43 \end{vmatrix}$$

та вектор максимумів = ||29 27,22 23,43 ||

Обрахуємо матрицю належностей та супорти еталону для параметра

$$\begin{vmatrix} 1;0,6;0,27 \\ 0,69;1;0,82 \\ 0;0,2;1 \end{vmatrix}$$

Супорти: $T_{log11}=T_{log21}=T_{log31}=33/100=0,33$, $T_{log12}=T_{log22}=T_{log32}=66/100=0,66$, $T_{log13}=T_{log23}=T_{log33}=100/100=1$. Здійснивши перетворення отримаємо набір еталонів параметра $CG=T_{log}$ = {неузгоджені (Н), частково узгоджені (Ч), повноузгоджені (П)} і терми лінгвістичних змінних для цього параметра:

Н = {0/0,33; 1/0,33; 0,6/0,66; 0,27/1; 0/1},

Ч = {0/0,33; 0,69/0,33; 1/0,66; 0,82/1; 0/1},

П = {0/0,33; 0,2/0,66; 1/1, 0/1}.

Графік функції належності термів лінгвістичної змінної Взаємоузгодження дій суб'єктів здійснення показаний на рис. 2.6:

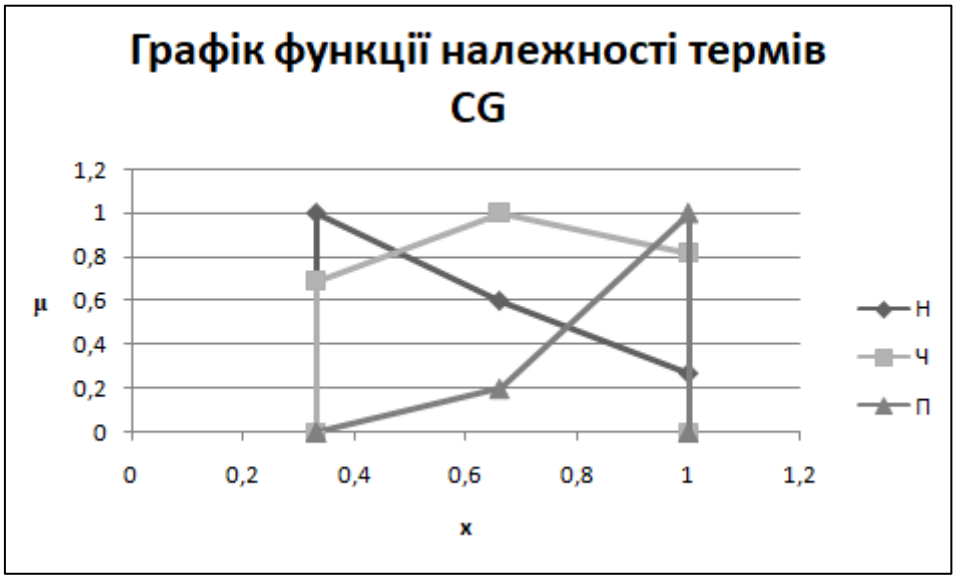


Рис.2.6. Графік функції належності термів «Взаємоузгодження дій суб'єктів здійснення»

Для параметру РМ характерні такі лінгвістичні оцінки: {низька (Н), середня (С), висока (В)}. Інтервали для визначення еталонних значень = {[0-33], [34-66], [67-100]} відсотків протягом певного періоду часу. Сформуємо узагальнену таблицю оцінок і базову матрицю частот, що представлена у вигляді таблиці 2.6.

Таблиця 2.6

Узагальнена таблиця оцінок параметру РМ

	0-33	34-66	67-100
Н	24	12	8
С	10	20	7
В	3	8	18

$v = |37;40;24|$

$Max = 40$

Обрахуємо похідну матрицю частот:

$$\begin{vmatrix} 25,95;12;9,14 \\ 10,81;20;8 \\ 3,24;8;22,86 \end{vmatrix}$$

та вектор максимумів = ||25,95 20 22,86 ||

Обрахуємо матрицю належностей та супорти еталону для параметра

$$\begin{vmatrix} 1;0,6;0,89 \\ 0,42;1;0,78 \\ 0,13;0,4;1 \end{vmatrix}$$

Супорти: $T_{log11}=T_{log21}=T_{log31}=33/100=0,33$, $T_{log12}=T_{log22}=T_{log32}=66/100=0,66$, $T_{log13}=T_{log23}=T_{log33}=100/100=1$ [32]. Здійснивши перетворення отримаємо набір еталонів параметра РМ=T_{log} = {низька (Н), середня (С), висока (В)} і терми лінгвістичних змінних для цього параметра:

$$H = \{0/0,33;\ 1/0,33,\ 0,95/0,66;\ \ 0,78/1;\ 0/1\},$$

$$C = \{0/0,33;\ 0,42/0,33;\ 1/0,66;\ 0,39/1;\ 0/1\},$$

$$B = \{0/0,33;\ 0,13/0,33;\ 0,4/0,66;\ 1/1,\ 0/1\}.$$

Графік функції належності термів лінгвістичної змінної Взаємоузгодження дій суб’єктів здійснення на рис. 2.7:

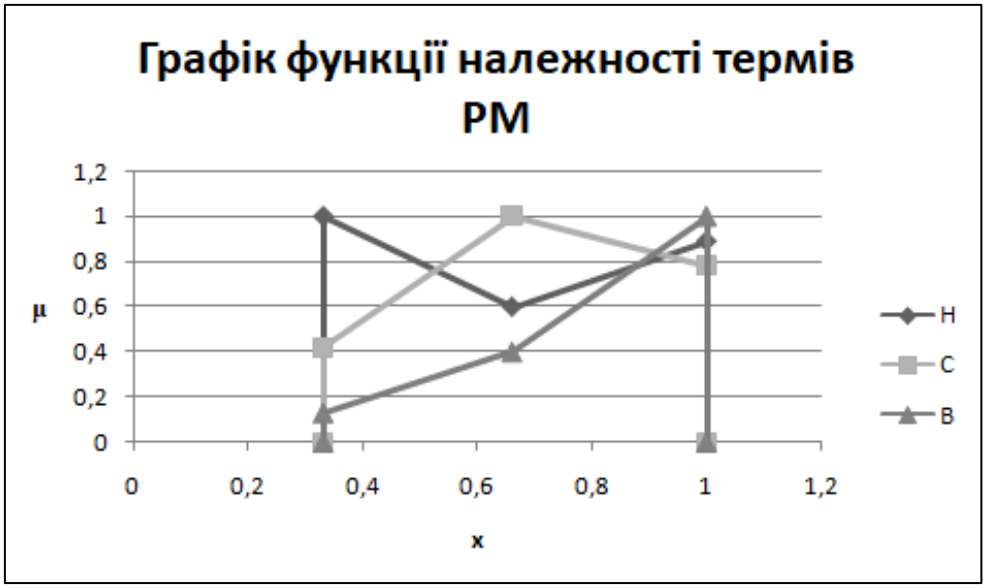


Рис. 2.7. Графік належності термів «Взаємоузгодження дій суб’єктів здійснення»

Для параметру IF характерні такі лінгвістичні оцінки: {низьке (Н), середнє (С), високе (В)}. Інтервали для визначення еталонних значень = {[0-33], [34-66], [67-100]} відсотків протягом певного періоду часу. Сформуємо узагальнену таблицю оцінок і базову матрицю частот, що представлена у вигляді таблиці 2.7.

Таблиця 2.7

Узагальнена таблиця оцінок параметру IF

	0-33	34-66	67-100
Н	28	15	10
С	19	32	12
В	9	12	20

$v = |56;59;42|$

$Max = 59$

Обрахуємо похідну матрицю частот:

$$\begin{vmatrix} 29,5;15;14,05 \\ 20,02;32;16,86 \\ 9,48;12;28,10 \end{vmatrix}$$

та вектор максимумів = ||29,5 32 28,10 ||

Обрахуємо матрицю належностей та супорти еталону для параметра

$$\begin{vmatrix} 1;0,47;0,5 \\ 0,68;1;0,6 \\ 0,32;0,38;1 \end{vmatrix}$$

Супорти: $T_{log11}=T_{log21}=T_{log31}=33/100=0,33$, $T_{log12}=T_{log22}=T_{log32}=66/100=0,66$, $T_{log13}=T_{log23}=T_{log33}=100/100=1$. Здійснивши перетворення отримаємо набір еталонів параметра $IF=T_{log}$ = {низьке (Н), середнє (С), високе (В)} і терми лінгвістичних змінних для цього параметра:

Н = {0/0,33; 1/0,33, 0,47/0,66; 0,5/1; 0/1},

С = {0/0,33; 0,68/0,33; 1/0,66; 0,6/1; 0/1},

B = {0/0,33; 0,32/0,33; 0,38/0,66; 1/1, 0/1}.

Графік функції належності термів лінгвістичної змінної Ступінь впливу зовнішніх чинників показаний на рис. 2.8:

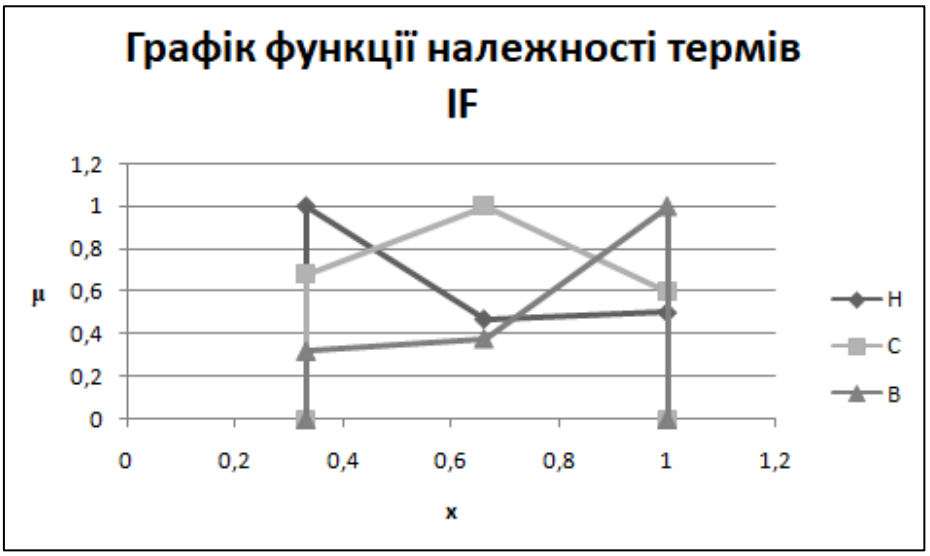


Рис. 2.8. Графік належності термів «Зростання емоційності»

Таким чином, щоб спрогнозувати можливість реалізації інформаційно-психологічного впливу або виявити його та ідентифікувати необхідно розробити систему, яка буде проводити моніторинг базових характеристик та на основі евристичних правил виявляти інформаційно-психологічний вплив.

2.3. Евристичні правила ідентифікації інформаційно-психологічного впливу

Наразі існує проблема ідентифікації методів інформаційно-психологічного впливу. Для її вирішення доцільно використати механізм евристичних правил, що допоможе провести ідентифікацію за базовими характеристиками методів.

Побудова правил зазвичай здійснюється на основі експертного підходу, особливо це важливо в тих випадках, коли необхідно дати перевагу одній з альтернатив. Для вибору одного рішення з множини альтернативних скористаємося методами визначення коефіцієнтів важливості [59].

Скористаємося методом рангових перетворень, оскільки він дозволяє залучити кількох експертів, в якості вхідних даних застосовуються табличні форми, вихідна функція лінійна, а трудомісткість низька [57].

Застосуємо апарат логіко-лінгвістичних зв'язок «метод-параметр» і взаємозалежність між показниками параметрів та можливістю реалізації інформаційної атаки, сформуємо евристичні правила для їх виявлення та ідентифікації за аналогією з [57]. Евристичні правила дають змогу оцінити можливість (степінь) реалізації тої чи іншої атаки в залежності від набору значень параметрів в певний момент часу.

В процесі дослідження були виділені наступні базові характеристики ІПВ: «лавиноподібність» - PM, «зростання емоційності» - IF, «зростання тенденційності» - EL; «збільшення сенсаційності» - PP; «збільшення кількості повідомлень негативного змісту» - PN; «взаємоузгодження дій суб'єктів здійснення» - CG; «час проведення» - LT, за якими здійснюється процес виявлення та ідентифікації. Характеристики можуть набувати значень, що визначаються лінгвістичними змінними – «Низький» (Н), «Середній» (С), «Високий» (В) для IF, PM, «Неузгоджені» (Н), «Частково узгоджені» (Ч), «Повноузгоджені» (П) для CG; «Маленька» (М), «Середня» (С), «Висока» (В) для PP та PN.

Метод «Переконання» може характеризуватися наступними оцінками: «Низька» (Н), «Підвищена» (П), «Висока» (В), «Критична» (К), що оцінюється на основі значення заданих для даного виду ІПВ характеристик (P_{LT}, P_{PN}, P_{PP}).

Сформуємо множину евристичних правил для виявлення та ідентифікації «Переконання» і представимо його в вигляді таблиці (табл. 2.8). Враховуючи всі можливі комбінації станів контрольованих параметрів можна сформувати 27 відповідних евристичних правила. Наведемо деякі з них.

Таблиця 2.8

Множина евристичних правил для виявлення «Переконання»

P	P_{LT}	P_{PN}	P_{PP}	Результат
1	К	М	М	Н
2	К	М	М	Н
3	К	М	М	Н
4	К	М	М	Н
5	К	М	М	Н
…	...	….	….	…
11	С	С	С	С
12	С	С	С	С
13	С	С	С	С
14	С	С	С	С
…	…	…	…	…
23	Д	В	В	К
24	Д	В	В	К
25	Д	В	В	К
26	Д	В	В	К
27	Д	В	В	К

Метод «Психологічна ізоляція» може характеризуватися: «Низька» (Н), «Середня» (С), «Висока» (В), що оцінюється на основі значення заданих для даного виду ІПВ характеристик (P_{LT}, P_{PP}, P_{IF}).

Сформуємо множину евристичних правил для виявлення та ідентифікації «Психологічна ізоляція» і представимо його в вигляді таблиці (табл. 2.9). Враховуючи всі можливі комбінації станів контрольованих параметрів можна сформувати 27 відповідних евристичних правила. Наведемо деякі з них.

Таблиця 2.9

Множина евристичних правил для виявлення «Психологічна ізоляція»

P	P_{LT}	P_{PP}	P_{IF}	Результат
1	К	М	М	Н
2	К	М	М	Н
3	К	М	М	Н
4	К	М	М	Н
5	К	М	М	Н
…	…	…	…	….
11	С	С	С	С
12	С	С	С	С
13	С	С	С	С
14	С	С	С	С
…	…	…	…	…
23	Д	В	В	В
24	Д	В	В	В
25	Д	В	В	В
26	Д	В	В	В
27	Д	В	В	В

Метод «Примус» може характеризуватися: «Низький» (Н), «Середній» (С), «Критичний» (К), що оцінюється на основі значення заданих для даного виду ІПВ характеристик (P_{DM}, P_{CG}, P_{PM}, P_{IF}).

Сформуємо множину евристичних правил для виявлення та ідентифікації «Примусу» і представимо його в вигляді таблиці (табл. 2.10). Враховуючи всі можливі комбінації станів контрольованих параметрів можна сформувати 27 відповідних евристичних правила. Наведемо деякі з них.

Таблиця 2.10

Множина евристичних правил для виявлення «Примусу»

P	P_{CG}	P_{PM}	P_{IF}	Результат
1	Н	Н	Н	Н
2	Н	Н	Н	Н
3	Н	Н	Н	Н
4	Н	Н	Н	Н
5	Н	Н	Н	Н
…	…	…	…	…
10	Ч	С	С	С
11	Ч	С	С	С
12	Ч	С	С	С
13	Ч	С	С	С
14	Ч	С	С	С
…	…	…	…	…
24	П	В	В	К
25	П	В	В	К
26	П	В	В	К
27	П	В	В	К

Метод «Дезінформація» може характеризуватися: «Низька» (Н), «Середня» (С), «Висока» (В), «Критична» (К), що оцінюється на основі значення заданих для даного виду ІПВ характеристик (P_{LT}, P_{PN}, P_{IF}).

Сформуємо множину евристичних правил для виявлення та ідентифікації «Дезінформації» і представимо його в вигляді таблиці (табл. 2.11). Враховуючи всі можливі комбінації станів контрольованих параметрів можна сформувати 27 відповідних евристичних правила. Наведемо деякі з них.

Таблиця 2.11

Множина евристичних правил для виявлення «Дезінформація»

P	P_{LT}	P_{PN}	P_{IF}	Результат
1	К	М	Н	Н
2	К	М	Н	Н
3	К	М	Н	Н
4	К	М	Н	Н
5	К	М	Н	Н
…	…	…	…	…
11	С	С	С	С
12	С	С	С	С
13	С	С	С	С
14	С	С	С	С
…	….	…	…	…
23	Д	В	В	К
24	Д	В	В	К
25	Д	В	В	К
26	Д	В	В	К
27	Д	В	В	К

Метод «Пропаганда» може характеризуватися: «Незначна» (Н), «Середня» (С), «Висока» (В), що оцінюється на основі значення заданих для даного виду ІПВ характеристик (P_{LT}, P_{PP}, P_{CG}).

Сформуємо множину евристичних правил для виявлення та ідентифікації «Пропаганда» і представимо його в вигляді таблиці (табл. 2.12). Враховуючи всі можливі комбінації станів контрольованих параметрів можна сформувати 27 відповідних евристичних правила. Наведемо деякі з них.

Таблиця 2.12

Множина евристичних правил для виявлення «Пропаганда»

P	P_{LT}	P_{PP}	P_{CG}	Результат
1	К	М	Н	Н
2	К	М	Н	Н
3	К	М	Н	Н
4	К	М	Н	Н
5	К	М	Н	Н
…	…	…	…	…
11	С	С	Ч	С
12	С	С	Ч	С
13	С	С	Ч	С
14	С	С	Ч	С
…	…	…	…	…
23	Д	В	П	В
24	Д	В	П	В
25	Д	В	П	В
26	Д	В	П	В
27	Д	В	П	В

Метод «Навіювання» може характеризуватися: «Низьке» (Н), «Середнє» (С), «Високе» (В), що оцінюється на основі значення заданих для даного виду ІПВ характеристик (P_{PP}, P_{CG}, P_{PN}).

Сформуємо множину евристичних правил для виявлення та ідентифікації «Навіювання» і представимо його в вигляді таблиці (табл. 2.13). Враховуючи всі можливі комбінації станів контрольованих параметрів можна сформувати 81 відповідних евристичних правила. Наведемо деякі з них.

Таблиця 2.13

Множина евристичних правил для виявлення «Навіювання»

P	P_{PP}	P_{CG}	P_{PN}	Результат
1	М	Н	М	Н
2	М	Н	М	Н
3	М	Н	М	С
4	М	Н	М	С
5	М	Н	М	С
…	…	…	…	…
11	С	Ч	С	С
12	С	Ч	С	С
13	С	Ч	С	С
14	С	Ч	С	С
…	…	…	…	…
23	В	П	В	В
24	В	П	В	В
25	В	П	В	В
26	В	П	В	В
27	В	П	В	В

Метод «Зараження» може характеризуватися: «Низьке» (Н), «Середнє» (С), «Високе» (В), що оцінюється на основі значення заданих для даного виду ІПВ характеристик (P_{PP}, P_{IF}, P_{PM}).

Сформуємо множину евристичних правил для виявлення та ідентифікації «Зараження» і представимо його в вигляді таблиці (табл. 2.14). Враховуючи всі можливі комбінації станів контрольованих параметрів можна сформувати 27 відповідних евристичних правила. Наведемо деякі з них.

Таблиця 2. 14

Множина евристичних правил для виявлення «Зараження»

P	P_{PM}	P_{PP}	P_{IF}	Результат
1	Н	М	Н	Н
2	Н	М	Н	Н
3	Н	М	Н	Н
4	Н	М	Н	Н
5	Н	М	Н	Н
…	…	…	…	…
11	С	С	С	С
12	С	С	С	С
13	С	С	С	С
14	С	С	С	С
…	…	…	…	…
23	В	В	В	В
24	В	В	В	В
25	В	В	В	В
26	В	В	В	В
27	В	В	В	В

Метод «Маніпулювання» може характеризуватися можливістю виникнення: «Низьке» (Н), «Підвищене» (П), «Високе» (В), що оцінюється на основі значення заданих для даного виду ІПВ характеристик (P_{PN}, P_{LT}, P_{CG},).

Сформуємо множину евристичних правил для виявлення та ідентифікації «Маніпулювання» і представимо його в вигляді таблиці (табл. 2.15). Враховуючи всі можливі комбінації станів контрольованих параметрів можна сформувати 27 відповідних евристичних правила. Наведемо деякі з них.

Таблиця 2.15

Множина евристичних правил для виявлення «Маніпулювання»

Р	P_{PN}	P_{LT}	P_{CG}	Результат
1	М	К	Н	Н
2	М	К	Н	Н
3	М	К	Н	Н
4	М	К	Н	Н
5	М	К	Н	Н
…	…	…	…	…
11	С	С	Ч	П
12	С	С	Ч	П
13	С	С	Ч	П
14	С	С	Ч	П
…	…	…	…	…
23	В	Д	П	В
24	В	Д	П	В
25	В	Д	П	В
26	В	Д	П	В
27	В	Д	П	В

Метод «Рефреймінг» може характеризуватися: «Некритичний» (Н), «Середній» (С), «Критичний» (К), що оцінюється на основі значення заданих для даного виду ІПВ характеристик (P_{PM}, P_{PN}, P_{CG}).

Сформуємо множину евристичних правил для виявлення та ідентифікації «Рефреймінг» і представимо його в вигляді таблиці (табл. 2.16). Враховуючи всі можливі комбінації станів контрольованих параметрів можна сформувати 27 відповідних евристичних правила. Наведемо деякі з них.

Таблиця 2.16

Множина евристичних правил для виявлення «Рефреймінг»

p	P_{PM}	P_{PN}	P_{CG}	Результат
1	Н	М	Н	Н
2	Н	М	Н	Н
3	Н	М	Н	С
4	Н	М	Н	С
5	Н	М	Н	С
…	…	…	…	…
11	С	С	Ч	П
12	С	С	Ч	В
13	С	С	Ч	П
14	С	С	Ч	П
…	…	…	…	…
23	В	В	П	В
24	В	В	П	В
25	В	В	П	В
26	В	В	П	К
27	В	В	П	К

Поширеними є випадки, коли одну ситуацію описують кілька евристичних правил, які належать до різних груп. Такий випадок називають колізією. Рішенням даної проблеми є система пріоритетів, у якій правило обирається відповідно до більшого рівня критичності, а у випадку однакового й даного показника – те, яке має більшу кількість параметрів [57].

На основі цієї моделі були розроблені приклади правил для виявлення і ідентифікації методів інформаційно-психологічного впливу.

Усі множини евристичних правил для ідентифікації інформаційно-психологічного впливу представлено у додатку А.

2.4. Метод виявлення та ідентифікації інформаційно-психологічного впливу

Виявлення та ідентифікація інформаційно-психологічного впливу допоможе більш ефективно обрати та впровадити засоби контрзаходів, що допоможе мінімізувати втрати від його негативної дії. Саме для цього було розроблено метод виявлення та ідентифікації інформаційно-психологічного впливу. Він дозволяє виявити та ідентифікувати впливи на населення чисельністю більше ніж 1000 осіб. В методі використовуються такі методи нечіткої логіки як метод лінгвістичних термів з використанням статистичних даних (МЛТС) – для побудови еталонних значень параметрів та оціночних еталонів, лінійної апроксимації по локальним максимумам (ЛАЛМ), узагальнена відстань Хемінга (ВХ) – для обробки нечітких даних та проведення операцій нечіткої логіки [55]. Крім того використовується також експертні методи оцінювання та ранжування: метод середніх рангів (СР). Метод складається з таких етапів:

Етап 1. Формування множин базових характеристик та методів інформаційно-психологічного впливу.

Аналіз понять і класифікацій щодо інформаційно-психологічного впливу показав, що на сьогодні відсутня єдина класифікація, що охоплювала б усі аспекти і характеристики його здійснення під час інформаційного протиборства [57].

В процесі дослідження були виділені наступні базові характеристики ІПВ: «лавиноподібність» - PM, «зростання емоційності» - IF, «зростання тенденційності» - EL; «збільшення сенсаційності» - PP; «тональність» - PN; «взаємоузгодження дій суб'єктів здійснення» - CG; «час проведення» - LT.

$$\mathbf{P}_{ig} = \{\bigcup_{j=1}^{m} P_j\} = \{P_1, ..., P_m\},$$

Узагальнивши роботи з даної тематики та проаналізувавши статистику інформаційних атак виділимо такі методи інформаційно-психологічного впливу як:

1) методи, що направлені на людей, які критично сприймають інформацію: зміна поглядів шляхом переконання; психологічна ізоляція об'єкту; примус.

2) методи, що направлені на людей, які некритично сприймають інформацію: дезінформація; пропаганда; зміна поглядів шляхом навіювання; зараження; маніпуляції; рефреймінг.

$$IPI = \{\bigcup_{i=1}^{n} IPI_{\mathbf{i}}\} = \{IPI_{\mathbf{1}}, \ldots, IPI_{\mathbf{n}}\}, (i = \overline{1,n})$$

Етап 2. Формування зв'язок базових характеристик з методами інформаційно-психологічного впливу.

$$IPI_{\mathbf{1}} \to P_{ig1}, ..., IPI_n \to P_{ign}$$

Формується набір зв'язок базових характеристик з методами інформаційно-психологічного впливу, на основі яких здійснюється ідентифікація конкретного виду ІПВ та побудова еталонних значень [83].

$$\{\bigcup_{i=1}^{n} P_{ig}\} = \{\bigcup_{i=1}^{n} \{\bigcup_{j=1}^{k_i} P_{igij}\}\} = \{\{P_{11}, ..., P_{1k_1}\}, ..., \{P_{n1}, ..., P_{nk_n}\}\}$$

Етап 3. Формування еталонів нечітких параметрів.

Цей етап направлений на отримання еталонних величин, з якими порівнюються поточні значення контрольованих параметрів [35].

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{T_i^e}\} = \{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \{\bigcup_{\mathbf{j=1}}^{\mathbf{k_i}} \mathbf{T_{ij}^e}\}\} = \{\bigcup_{i=1}^{n} \{\bigcup_{j=1}^{k_i} \{\bigcup_{s=1}^{r_{ij}} T_{ijs}^{e}\}\}\}$$

$$\underset{\sim}{T}_{ijs} = \{\bigcup_{q=1}^{r_{ij}} \mu_{ijsq} / x_{ijsq}\} = \{\mu_{ijs1} / x_{ijs1}, ..., \mu_{ijsr_{ij}} / x_{ijsr_{ij}}\}, (q = \overline{1, r_{ij}})$$

$$IPI_1 \to \mathbf{T}_1^{\mathbf{e}}, ..., IPI_n \to \mathbf{T}_n^{\mathbf{e}}$$

Етап 4. Формування множини евристичних правил.

$$\mathbf{ER} = \overset{n}{\underset{i=1}{U}}\{ \overset{R_i}{\underset{p=1}{U}} ER_{ip} = (LC_{ip} \to LI_{ip})\}$$

$$LC_i = \{\bigcup_{j=1}^{k_i} \wedge t_j\} = \bigcup_{j=1}^{k_i} \wedge (\bigcup_{s=1}^{r_{ij}} \vee (\underset{\sim}{P}_{ij} \cong T_{ijs}^e))$$

Створення наборів евристичних правил, що використовуються для виявлення інформаційно-психологічного впливу на основі зіставлення еталонних та поточних значень параметрів інформаційного простору за допомогою набору ідентифікаторів поточного стану, що є унікальним для кожного методу інформаційно-психологічного впливу [57].

$$\mathbf{LI} = \overset{D}{\underset{d=1}{U}} LI_d = \{LI_1, ..., LI_D\}$$

Етап 5. Фазифікація параметрів, що моніторяться з метою виявлення інформаційно-психологічного впливу.

На даному етапі відбувається перетворення множини поточних значень параметрів, що фіксуються кожні t проміжки часу протягом певного періоду часу T в одне нечітке число і таким чином отримаємо нечіткі числа, характеризуючі поточні значення ідентифікуючих параметрів [84].

$$\mathbf{P}_{\sim ig} = \{\bigcup_{j=1}^{k_i} \underset{\sim}{P}_{jg}\} = \{\underset{\sim}{P}_{1}, ..., \underset{\sim}{P}_{k_n}\}$$

Етап 6. Обробка поточних значень ідентифікуючих параметрів і формування результату.

Етап спрямований на прийняття рішення щодо наявності інформаційно-психологічного впливу. Сформовані на попередньому етапі нечіткі числа, які відображають поточні значення контрольованих параметрів, групуються відповідно до методу ІПВ, а функції належності їх елементів порівнюються з

еталонними значеннями. Задля ідентифікації ІПВ виконується зіставлення ідентифікатора поточної ситуації з евристичним правилом з заданого набору.

$$f(\underset{\sim}{P}_i, T_i^e, ER_i) = h(\underset{\sim}{P}_i, T_i^e)$$

$$IPI_1 : LI_1, ..., IPI_n : LI_n$$

Розробка методу відображає новий підхід до вирішення проблеми виявлення та ідентифікації інформаційно-психологічного впливу. Метод ґрунтується на основі нечіткої логіки. Під час його реалізації відбувається кілька етапів, які направлені на визначення еталонних та поточних значень певного інформаційного простору для виявлення ІПВ та побудові евристичних правил для ідентифікації його методів. Особливою рисою є забезпечення процесу ідентифікації ІПВ, що стане у нагоді при покращенні ефективності розробки та впровадження засобів протидії.

У додатку Б представлено схему відображення методу виявлення та ідентифікації ІПВ.

2.5 Висновки

1. Розроблено функціональну та цільову моделі інформаційно-психологічного впливу, які характеризують інформаційне протиборство в соціальних мережах. З даних моделей формуються множини ідентифікуючих та оціночних параметрів.

2. Розроблено еталони ідентифікуючих параметрів та евристичні правила ідентифікації інформаційно-психологічного впливу. Розроблено метод виявлення та ідентифікації інформаційно-психологічного впливу, який базується на теоретичних засадах нечіткої логіки та дозволяє виконувати свої дії у слабоформалізованому нечіткому середовищі й має можливість аналізувати контент соціальних мереж у режимі реального часу.

Розроблений метод дозволяє виявляти та ідентифіковувати конкретні види інформаційно-психологічного впливу, зважаючи на їх характеристики.

РОЗДІЛ 3. МЕТОД ОЦІНЮВАННЯ КРИТИЧНОСТІ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ВПЛИВУ

3.1 Формування оціночних параметрів

Опишемо можливу множину оціночних параметрів, що будуть найбільш універсальними у даному контексті. У цій роботі у якості оціночних параметрів було обрано 8 критеріїв, які, на основі аналізу було визначено максимально універсальними для більшості ІПВ, та такими, які мають найбільший вплив на успішність ІПВ. Такими критеріями є: CSA – «Повнота і сила аргументації», CGN – «Узгодженість з нормами загальносуспільної думки», PR – «Реакція громадськості», GAF – «Зростання фактора тривожності», VD – «Швидкість розповсюдження», NAT – «Кількість уражених цілей», DR – «Тривалість».

Параметр P_{o1} – повнота і сила аргументації, CSA. Даний параметр характеризує обґрунтованість приведених аргументів під час спеціальних інформаційних операцій та акцій інформаційного впливу, достовірність інформації, наявність прикладів. Також оцінюється сила логічних доводів під час аргументації інформаційно-психологічного впливу. Зв’язок між рівнем деструктивних впливів і даним параметром очевидний, оскільки сприйняття інформації пришвидшується, коли аргумент викликає стійкі образи у підсвідомості людини. Приведення конкретних прикладів посилює впевненість у можливому повторенні дії, а тому підвищує впевненість у інформації наданій джерелом.

Параметр P_{o2} – узгодженість з нормами загальносуспільної думки, CGA. Перед проведенням спеціальних інформаційних операцій зазвичай вивчаються характеристики інформаційного простору, оцінюються настрої та погляди населення. Дані параметри не можуть бути оцінені кількісно, однак залишається можливість лінгвістичного їх опису, що повинно враховуватись експертом. Якщо мета та кінцева ціль ІПВ більш схильні до тенденцій думки громадськості, то і рівень його успішності буде вищим.

Параметр P_{o3} – реакція громадськості, PR. Мова йде про появу пропагандистських чи екстремістських текстів, лозунгів, мітингів, акцій протестів, тобто як змінюються настрої громадськості і чи приведе ІПВ до запланованих результатів та наскільки цей фактор явно виражається.

Параметр P_{o4} – зростання фактора тривожності, GAF. Зростання фактора тривожності населення може мати різний вплив на перебіг ІПВ – сприяти йому, якщо тривожність проявляється у контексті антидержавних настроїв, що відповідають цілям ІПВ, або перешкоджати і ставати на заваді.

Параметр P_{o5} – швидкість розповсюдження, VD. Даний показник характеризує кількість цілей, що будуть уражені певним ІПВ за одиницю часу. Даний показник можна описати у контексті засобів масової інформації, наприклад телевізійного каналу, взявши кількість людей, що є його потенційною аудиторією та розділивши її на час, протягом якого триває ІПВ. Крім цього, необхідно враховувати постійне зростання потенційної аудиторії.

Параметр P_{o6} – кількість уражених цілей, NAT. Під кількістю уражених цілей будемо розуміти кількість осіб, що стають ціллю ІПВ, тобто кількість осіб, що сприйняли інформацію будь-якими способами поширення. Варто також враховувати той факт, що інформація, поширена масовими засобами, може збільшувати кількість цілей у ході проведення впливу, тому необхідно враховувати цей фактор при проведенні оцінки.

Параметр P_{o7} – тривалість, DR. Під тривалістю будемо розуміти час, який пройшов від початку дії ІПВ та чинників, що його спричинили, до завершення їх дії. Очевидно, що зі зростанням тривалості ІПВ, буде зростати і рівень критичності спричинений ним. Однак даний показник не можна оцінювати лише з одного боку, оскільки ІПВ можуть різнитися за ступенем інтенсивності, тому необхідно враховувати також і цей фактор.

Отже, було сформовано множину оціночних параметрів інформаційно-психологічного впливу, що буде використано під час розробки відповідного методу оцінювання.

3.2 Формування еталонних значень ідентифікуючих параметрів

В процесі дослідження були виділені наступні оціночні параметри ІПВ: CSA – «Повнота і сила аргументації», CGN – «Узгодженість з нормами загальносуспільної думки», PR – «Реакція громадськості», GAF – «Зростання фактору тривожності», VD – «Швидкість розповсюдження», NAT – «Кількість уражених цілей».

Еталонні значення було побудовано у відповідності [55, 86].

Для параметру CSA характерні такі лінгвістичні оцінки: {низька (Н), середня (С), висока (В)}. Інтервали для визначення еталонних значень = {[0-20], [21-40], [41-60]} проміжків часу. Сформуємо узагальнену таблицю оцінок і базову матрицю частот, що представлена у вигляді таблиці 3.1.

Таблиця 3.1

Узагальнена таблиця оцінок параметру CSA

	0-21	21-40	41-60
Н	9	5	3
С	2	8	4
В	3	6	7

ν= | 14; 19; 14 |

Max = 19

Обрахуємо похідну матрицю частот:

$$\begin{vmatrix} 12,21;5;4,07 \\ 2,71;8;5,43 \\ 4,07;6;9,50 \end{vmatrix}$$

та вектор максимумів = ||12,21 8 9,5||

Обрахуємо матрицю належностей та супорти еталону для параметра

$$\begin{vmatrix} 1;0,63;0,43 \\ 0,22;1;0,57 \\ 0,33;0,75;1 \end{vmatrix}$$

Супорти: $T_{log11} = T_{log21} = T_{log31} = 20 / 60 = 0,33$, $T_{log12} = T_{log22} = T_{log32} = 40 / 60 = 0,67$, $T_{log13} = T_{log23} = T_{log33} = 60 / 60 = 1$. Здійснивши перетворення отримаємо набір еталонів параметра CSA = T_{log} = {низька (Н), середня (С), висока (В)} і терми лінгвістичних змінних для цього параметра:

Н = {0/0,33; 1/0,33, 0,63/0,75; 0,43/1; 0/1},

С = {0/0,33; 0,22/0,33; 1/0,75; 0,57/1; 0/1},

В= {0/0,33; 0,33/0,33; 0,75/0,75; 1/1; 0/1}.

Графік функції належності термів лінгвістичної змінної Повнота і сила аргументації показаний на рис. 3.1:

Рис. 3.1. Графік належності термів «Повнота і сила аргументації»

Для параметру CGN характерні такі лінгвістичні оцінки: {неузгоджені (Н), середньоузгоджені (С), узгоджені (У)}. Інтервали для визначення еталонних значень = {[0-33], [34-66], [67-100]} відсотків. Сформуємо узагальнену таблицю оцінок і базову матрицю частот, що представлена у вигляді таблиці 3.2.

Таблиця 3.2

Узагальнена таблиця оцінок параметру CGN

	0-33	34-66	67-100
Н	20	14	6
С	7	13	1
У	2	7	15

ν= | 29; 32; 22 |

Max = 32

Обрахуємо похідну матрицю частот:

$$\begin{vmatrix} 24,83;16;9,82 \\ 8,69;13;1,64 \\ 2,48;7;24,55 \end{vmatrix}$$

та вектор максимумів = ||24,83 16 24,55 ||

Обрахуємо матрицю належностей та супорти еталону для параметра

$$\begin{vmatrix} 1;0,92;0,4 \\ 0,4;1;0,07 \\ 0,1;0,54;1 \end{vmatrix}$$

Супорти: $T_{log11}=T_{log21}=T_{log31}=33/100=0,33$, $T_{log12}=T_{log22}=T_{log32}=66/100=0,66$, $T_{log13}=T_{log23}=T_{log33}=100/100=1$. Здійснивши перетворення отримаємо набір еталонів параметра $CGN=T_{log}$ = {неузгоджені (Н), середньоузгоджені (С), узгоджені (У)} і терми лінгвістичних змінних для цього параметра:

Н = {0/0,33; 1/0,33; 0,92/0,66; 0,4/1; 0/1},

С = {0/0,33; 0,4/0,33; 0,8/0,66; 0,07/1; 0/1},

У = {0/0,33; 0,1/0,33; 0,44/0,66; 1/1; 0/1}.

Графік функції належності термів лінгвістичної змінної Узгодженість з нормами загальносуспільної думки показаний на рис. 3.2:

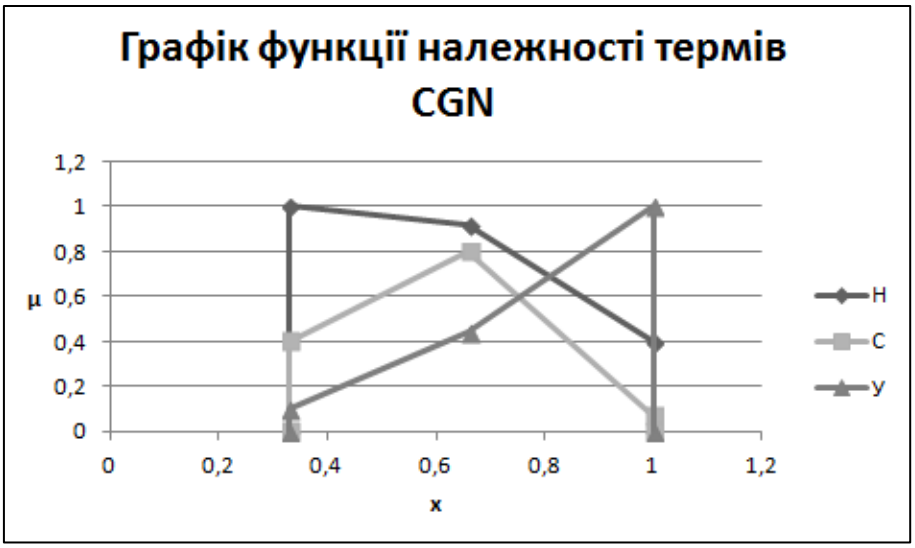


Рис. 3.2. Графік функції належності термів «Узгодженість з нормами загальносуспільної думки»

Для параметру PR характерні такі лінгвістичні оцінки: {мала (М), середня (С), висока (В)}. Інтервали для визначення еталонних значень = {[0-33], [34-66], [67-100]}. Сформуємо узагальнену таблицю оцінок і базову матрицю частот, що представлена у вигляді таблиці 3.3.

Таблиця 3.3.

Узагальнена таблиця оцінок параметру PR

	0-33	34-66	67-100
М	10	8	4
С	7	9	3
В	3	5	11

ν= | 20; 22; 18 |

Max = 22

Обрахуємо похідну матрицю частот:

$$\begin{vmatrix} 11;18;4,89 \\ 7,7;9;3,67 \\ 3,3;5;13,44 \end{vmatrix}$$

та вектор максимумів = ||11 9 13,44 ||

Обрахуємо матрицю належностей та супорти еталону для параметра

$$\begin{vmatrix} 1;0,89;0,36 \\ 0,7;1;0,27 \\ 0,3;0,56;1 \end{vmatrix}$$

Супорти: $T_{log11}=T_{log21}=T_{log31}=33/100=0,33$, $T_{log12}=T_{log22}=T_{log32}=66/100=0,66$, $T_{log13}=T_{log23}=T_{log33}=100/100=1$. Здійснивши перетворення отримаємо набір еталонів параметра $PR=T_{log}$ = {мала (М), середня (С), висока (В)} і терми лінгвістичних змінних для цього параметра:

М = {0/0,33; 1/0,33; 0,89/0,66; 0,36/1; 0/1},

С = {0/0,33; 0,7/0,33; 1/0,66; 0,27/1; 0/1},

В = {0/0,33; 0,3/0,33, 0,56/0,67; 1/1; 0/1}.

Графік функції належності термів лінгвістичної змінної Реакції громадськості повідомлень негативного змісту на рис. 3.3:

Рис. 3.3. Графік функції належності термів «Реакція громадськості»

Для параметру GAF характерні такі лінгвістичні оцінки: {повільне (П), середнє (С), високе (В)}. Інтервали для визначення еталонних значень = {[0-33], [34-66], [67-100]} відсотків. Сформуємо узагальнену таблицю оцінок і базову матрицю частот, що представлена у вигляді таблиці 3.4.

Таблиця 3.4

Узагальнена таблиця оцінок параметру GAF

	0-33	34-66	67-100
П	11	9	6
С	3	7	5
В	2	4	10

ν= | 16; 20; 21 |

Max = 21

Обрахуємо похідну матрицю частот:

$$\begin{vmatrix} 14,44;9,45;6 \\ 3,94;7,35;5 \\ 2,63;4,2;10 \end{vmatrix}$$

та вектор максимумів = ||14,44 9,45 10 ||

Обрахуємо матрицю належностей та супорти еталону для параметра

$$\begin{vmatrix} 1;0,78;0,6 \\ 0,27;1;0,5 \\ 0,18;0,44;1 \end{vmatrix}$$

Супорти: $T_{log11}=T_{log21}=T_{log31}=33/100=0,33$, $T_{log12}=T_{log22}=T_{log32}=66/100=0,66$, $T_{log13}=T_{log23}=T_{log33}=100/100=1$. Здійснивши перетворення отримаємо набір еталонів параметра GAF=T_{log} = {повільна (П), середня (С), висока (В)} і терми лінгвістичних змінних для цього параметра:

П = {0/0,33; 1/0,33, 0,78/0,66; 0,6/1; 0/1},

С = {0/0,33; 0,27/0,33; 1/0,66; 0,5/1; 0/1},

В = {0/0,33; 0,18/0,33; 0,44/0,66; 1/1, 0/1}.

Графік функції належності термів лінгвістичної змінної Зростання фактору тривожності на рис. 3.4:

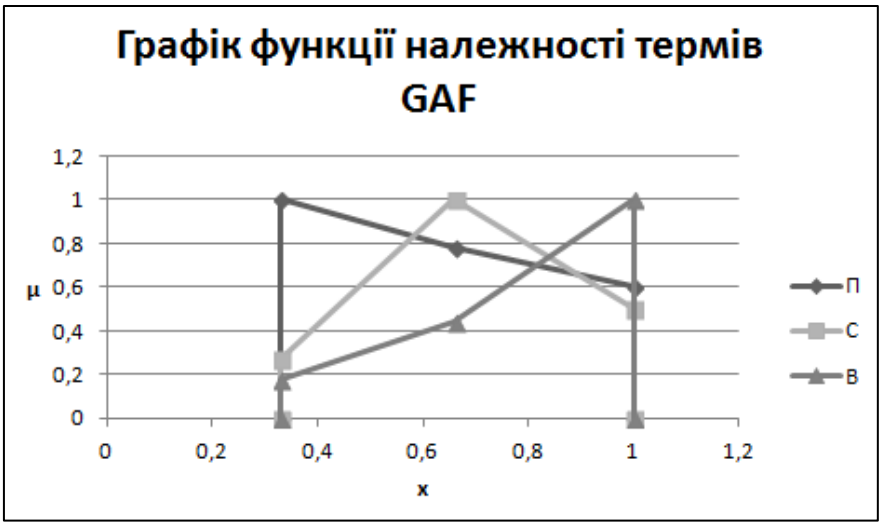


Рис. 3.4. Графік належності термів «Зростання фактору тривожності»

Для параметру VD характерні такі лінгвістичні оцінки: {повільно (П), середньо (С), високо (В)}. Інтервали для визначення еталонних значень = {[0-33], [34-66], [67-100]} відсотків. Сформуємо узагальнену таблицю оцінок і базову матрицю частот, що представлена у вигляді таблиці 3.5.

Таблиця 3.5

Узагальнена таблиця оцінок параметру VD

	0-33	34-66	67-100
П	13	11	9
С	7	10	4
В	3	8	12

ν= | 23; 29; 25 |

Max = 29

Обрахуємо похідну матрицю частот:

$$\begin{vmatrix} 16{,}39;11;10{,}44 \\ 8{,}83;10;4{,}64 \\ 3{,}78;8;13{,}92 \end{vmatrix}$$

та вектор максимумів = ||16,39 11 13,92 ||

Обрахуємо матрицю належностей та супорти еталону для параметра

$$\begin{vmatrix} 1;0,91;0,75 \\ 0,54;1;0,33 \\ 0,23;0,73;1 \end{vmatrix}$$

Супорти: $T_{log11}=T_{log21}=T_{log31}=33/100=0,33$, $T_{log12}=T_{log22}=T_{log32}=66/100=0,66$, $T_{log13}=T_{log23}=T_{log33}=100/100=1$. Здійснивши перетворення отримаємо набір еталонів параметра $VD=T_{log}$ = {повільно (П), середньо (С), високо (В)} і терми лінгвістичних змінних для цього параметра:

П = {0/0,33; 1/0,33, 0,91/0,66; 0,75/1; 0/1},

С = {0/0,33; 0,54/0,33; 1/0,66; 0,33/1; 0/1},

В = {0/0,33; 0,23/0,33; 0,73/0,67; 1/1, 0/1}.

Графік функції належності термів лінгвістичної змінної Взаємоузгодження дій суб'єктів здійснення на рис. 3.5:

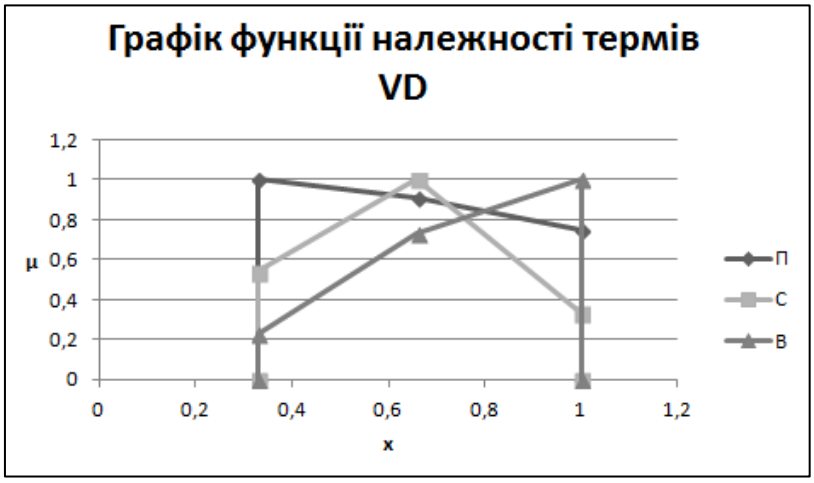


Рис. 3.5. Графік належності термів «Швидкість розповсюдження»

Для параметру NAT характерні такі лінгвістичні оцінки: {низька (Н), середня (С), висока (В)}. Інтервали для визначення еталонних значень = {[0-33], [34-66], [67-100]}. Сформуємо узагальнену таблицю оцінок і базову матрицю частот, що представлена у вигляді таблиці 3.6.

Таблиця 3.6

Узагальнена таблиця оцінок параметру NAT

	0-33	34-66	67-100
H	12	8	3
C	6	14	5
B	2	5	9

ν= | 20; 27; 17 |

Max = 27

Обрахуємо похідну матрицю частот:

$$\begin{vmatrix} 16,2;8;4,76 \\ 8,1;14;7,94 \\ 2,7;5;14,29 \end{vmatrix}$$

та вектор максимумів = ||16,2 14 14,29 ||

Обрахуємо матрицю належностей та супорти еталону для параметра

$$\begin{vmatrix} 1;0,57;0,33 \\ 0,5;1;0,56 \\ 0,17;0,36;1 \end{vmatrix}$$

Супорти: $T_{log11}=T_{log21}=T_{log31}=33/100=0,33$, $T_{log12}=T_{log22}=T_{log32}=66/100=0,66$, $T_{log13}=T_{log23}=T_{log33}=100/100=1$. Здійснивши перетворення отримаємо набір еталонів параметра $NAT=T_{log}$ = {низька (Н), середня (С), висока (В)} і терми лінгвістичних змінних для цього параметра:

H = {0/0,33; 1/0,33, 0,57/0,66; 0,33/1; 0/1},

C = {0/0,33; 0,5/0,33; 1/0,66; 0,56/1; 0/1},

B = {0/0,33; 0,17/0,33; 0,36/0,66; 1/1, 0/1}.

Графік функції належності термів лінгвістичної змінної Кількість уражених цілей на рис. 3.6:

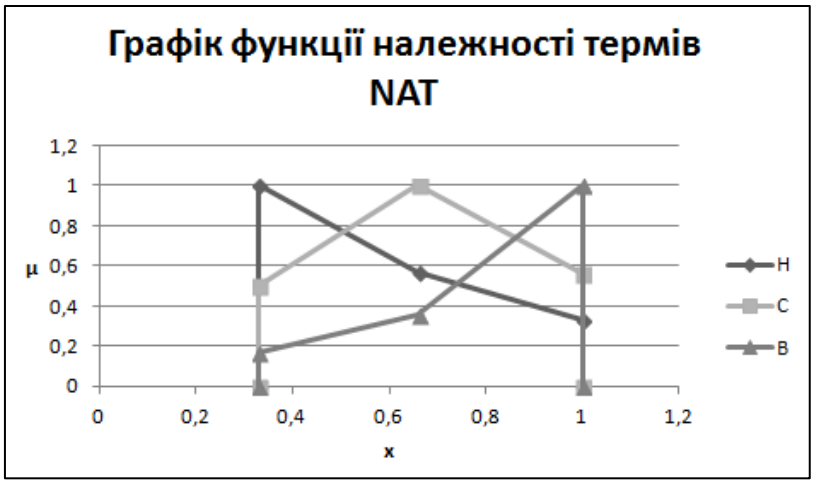


Рис. 3.6. Графік належності термів «Кількість уражених цілей»

Для параметру DR характерні такі лінгвістичні оцінки: {короткотривала (К), середньотривала (С), довготривала (Д)}. Інтервали для визначення еталонних значень = {[0-33], [34-66], [67-100]}. Сформуємо узагальнену таблицю оцінок і базову матрицю частот, що представлена у вигляді таблиці 3.7.

Таблиця 3.7

Узагальнена таблиця оцінок параметру DR

	0-33	34-66	67-100
К	24	12	8
С	10	20	7
Д	3	8	18

ν= | 37; 40; 24 |

Max = 40

Обрахуємо похідну матрицю частот:

$$\begin{vmatrix} 25,95;12;9,14 \\ 10,81;20;8 \\ 3,24;8;22,86 \end{vmatrix}$$

та вектор максимумів = ||25,95 20 22,86 ||

Обрахуємо матрицю належностей та супорти еталону для параметра

$$\begin{vmatrix} 1;0,6;0,89 \\ 0,42;1;0,78 \\ 0,13;0,4;1 \end{vmatrix}$$

Супорти: $T_{log11}=T_{log21}=T_{log31}=33/100=0,33$, $T_{log12}=T_{log22}=T_{log32}=66/100=0,66$, $T_{log13}=T_{log23}=T_{log33}=100/100=1$ [32]. Здійснивши перетворення отримаємо набір еталонів параметра $DR=T_{log}$ = {низька (Н), середня (С), висока (В)} і терми лінгвістичних змінних для цього параметра:

Н = {0/0,33; 1/0,33, 0,95/0,66; 0,78/1; 0/1},

С = {0/0,33; 0,42/0,33; 1/0,66; 0,39/1; 0/1},

В = {0/0,33; 0,13/0,33; 0,4/0,66; 1/1, 0/1}.

Графік функції належності термів лінгвістичної змінної Тривалість на рис. 3.7:

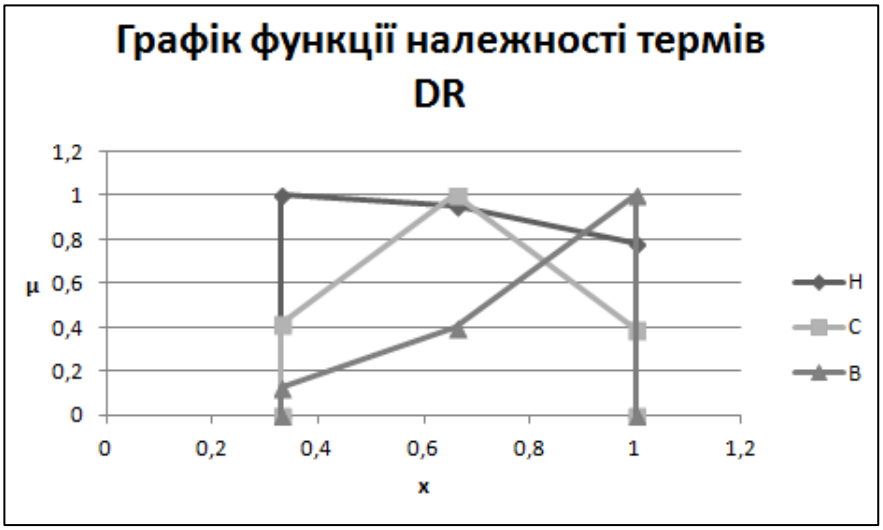


Рис. 3.7. Графік належності термів «Тривалість»

3.3 Метод оцінювання критичності інформаційно-психологічного впливу

Проблема оцінки рівня критичності інформаційно-психологічного впливу, як одного з процесів забезпечення інформаційно-психологічного впливу, визначається тим, що його виникнення та розвиток є важко прогнозованим (а часто і взагалі не прогнозованим), тобто маємо справу з подією в нечітко

формалізованому просторі. Також варто зазначити, що на сьогодні не існує єдиного підходу до оцінвання критичності дописів у соціальних мережах. Наявні методи та теорії мають різний математичний апарат та різні оціночні критерії. Тому формування параметрів та розробка методів для оцінки рівня критичності ІПВ та методів його визначення є актуальною задачею. В методі використовуються такі методи нечіткої логіки як метод лінгвістичних термів з використанням статистичних даних (МЛТС) – для побудови еталонних значень параметрів та оціночних еталонів, лінійної апроксимації по локальним максимумам (ЛАЛМ), узагальнена відстань Хемінга (ВХ) – для обробки нечітких даних та проведення операцій нечіткої логіки [58]. Крім того використовується також експертні методи оцінювання та ранжування: метод середніх рангів (СР).

В процесі реалізації методу оцінювання рівня критичності ІПВ застосуються процедури Експертного оцінювання (ЕО), що здійснюється відповідною експертною спільнотою, фахівці якої є незалежними. Під час процесу експертизи різні дописи, каскади повідомлень тощо оцінюються такими спільнотами відповідно до оціночних параметрів. Тому виникає потреба в інтепретації отриманих результатів для узагальнення та ініціалізації кінцевого результату. Під час процесу оцінювання виникає потреба у використанні як кількісних, так і якісних методів інтепретації отриманих результатів. Кількісні методи мають перевагу щодо свого застосування під час оцінювання критичності ІПВ. Задля агрегації результатів оцінювання та нівелювання похибки експертів використовують коефіцієнти важливості.

На даному етапі здійснюється оцінка критичності впливу кожного оціночного параметру і відповідного їх ранжування. Застосовуємо для цього метод кількісного парного порівняння із визначенням квадратного кореня, що є різновидом методу кількісного парного порівняння.

Парне порівняння – це матиматичний засіб визначення пріоритетнішого параметрну шляхом попарного порівнянні усіх можливих пара параметрів та

ранжування обєктів за результатами такого порівняння. Даний метод є одним із найбільш використовуваних серед експертних методів оцінювання для визначення важливості параметру.

В основі лежить порівняння кожного із параметрів таблиці та формування матриці парного порівняння $A = \left|\left|a_{ij}\right|\right|$, де a_{ij} вибирається відповідно до думки експерта за шкалою відносної важливості: 1 – альтернативні варіанти мають однакову важливість, 3 – помірна перевага одного параметру над іншим, 5 – суттєва перевага одного параметру над іншим, 7 – значна перевага (наявні переконливі свідчення), 9 – очевидна перевага одного з параметрів; 2, 4, 6, 8 – проміжні рішення.

Експерт заповнює клітини таблиці порівняння параметру самого з собою та записує в неї 1. У першій клітині першого рядка експерт повинен записати одиницю, в другій – результат порівняння першого фактора з другим, в третій – результат порівняння першого фактора з третім і т.д. Переходячи до другого рядка, експерт записує в першій клітині результат порівняння другого фактора з першим, в другій – одиницю, в третій – результат порівняння другого фактора з третім тощо [65].

Наступним кроком іде обчислення вагових коефіцієнтів згідно виразу $\omega_i = \sqrt[n]{\prod_{i`=1}^{I} a_{ij}}$, де $i` = \overline{1,I}$, I – кількість оціночних параметрів, у даному випадку 7. Після цього проводиться нормування отриманих коефіцієнтів за формулою: $\sigma_i = \omega_i/(\sum_{i=1}^{I} \omega_i)$, таким чином, що $\sum_{i=1}^{I} \sigma_i = 1$.

Слід відзначити також такі переваги методу парних порівнянь:

- метод парних порівнянь досить простий у реалізації. Він не вимагає складних обчислень або особливих навичок;
- метод може бути застосований до великої кількості задач і приймати рішення в різних областях, включаючи бізнес, менеджмент, наукові дослідження та інше;

- під час застосування методу парних порівнянь можна оцінити консистентність ваших виборів, що допомагає уникнути протиріччя в рішеннях;
- використання методу парних порівнянь сприяє обговоренню та врегулюванню поглядів різних учасників прийняття рішення;
- метод дозволяє аналізувати, наскільки важливі різні параметри для прийняття рішення;
- після визначення ваг параметрів можна відсортувати їх в порядку пріоритетності.

Розглянемо Метод оцінювання рівня критичності ІПВ, що складається з таких етапів:

Етап 1. Визначення параметрів оцінки рівня критичності.

Рівень критичності можна описати врахувавши функціональні залежності між P_o – параметрами оцінки рівня критичності. Параметри P_o можуть мати різну природу, характеризувати інформаційно-психологічний впливу з різних сторін, тому виникають проблеми в застосуванні їх відомими методами аналізу оцінювання критичності. Дані параметри можна представити в якісному (як лінгвістична зміна (ЛЗ) з певним числом термів) або кількісному вигляді. Провівши аналіз сучасних методик оцінки ризику, була сформована наступна множина: $P = \{\bigcup_{o=1}^{E} P_o\}$, за умови дослідження E=7 $P = \{\bigcup_{1}^{7} P_o\} = \{P_{o1} \dots P_{o7}\}$, де P_{o1} = CSA, P_{o2} = CGN, P_{o3} = PR, P_{o4} = GAF, P_{o5} = VD, P_{o6} = NAT, P_{o7} = DR ідентифікують такі параметри як «Повнота і сила аргументації», «Узгодженість з нормами загальносуспільної думки», «Реакція громадськості», «Зростання фактора тривожності», «Швидкість розповсюдження», «Кількість уражених цілей», «Тривалість» відповідно.

Етап 2. Формування зв'язок базових характеристик з методами інформаційно-психологічного впливу.

Формується набір зв’язок базових характеристик з методами інформаційно-психологічного впливу, на основі яких здійснюється ідентифікація конкретного виду ІПВ та побудова еталонних значень [36].

Етап 3. Формування оціночних еталонів.

Під час другого етапу формується оціночні еталони, що використовуватиметься для порівняння з нечіткими числами сформованим під час обчислення критичності усіх параметрів та загального рівня критичності. Для кожного параметру формується окремий еталон.

Етап 4. Обчислення коефіцієнтів важливості.

В основі лежить порівняння кожного із параметрів таблиці та формування матриці парного порівняння $A = \left|\left|a_{ij}\right|\right|$, де a_{ij} вибирається відповідно до думки експерта за шкалою відносної важливості: 1 – альтернативні варіанти мають однакову важливість, 3 – помірна перевага одного параметру над іншим, 5 – суттєва перевага одного параметру над іншим, 7 – значна перевага (наявні переконливі свідчення), 9 – очевидна перевага одного з параметрів; 2, 4, 6, 8 – проміжні рішення.

Експерт заповнює клітини таблиці порівняння параметру самого з собою дає одиницю. У першій клітині першого рядка експерт пише одиницю, в другій – результат порівняння першого фактора з другим, в третій – результат порівняння першого фактора з третім і т.д. Переходячи до другого рядка, експерт записує в першій клітині результат порівняння другого фактора з першим, в другій – одиницю, в третій – результат порівняння другого фактора з третім тощо [65].

Наступним кроком іде обчислення вагових коефіцієнтів згідно виразу $\omega_i = \sqrt[n]{\prod_{i`=1}^{I} a_{ij}}$, де $i` = \overline{1,I}$, I – кількість оціночних параметрів, у даному випадку 7. Після цього проводиться нормування отриманих коефіцієнтів за формулою: $\sigma_i = \omega_i/(\sum_{i=1}^{I} \omega_i)$, таким чином, що $\sum_{i=1}^{I} \sigma_i = 1$.

Етап 5. Вимірювання та фазифікація параметрів.

На даному етапі здійснюється обчислення нечітких чисел, що представляють поточні значення параметрів, виміряних системою та фазифікованих. Система оцінює параметри L_e відповідно до еталонних значень. На основі кількості T поточних вимірювань, що заміряються протягом певного певного встановленого періоду часу, формується нечітке число, яке символізує поточне значення параметру. Воно визначається як:

$$P_o = (\sum_{s=1}^{P} T_{Ets}^{E})/T = (T_{EP_{o1}}^{E} + T_{EP_{o2}}^{E} + T_{EP_{o3}}^{E} + \cdots T_{EPr}^{E})/T$$

де – T – загальна кількість вимірювань, T_{Ets}^{E}– поправочний еталон. T_{Ets}^{E} визначається за допомогою сенсорів і механізму лічильника. За своєю суттю процедура аналогічна з методом фазифікації параметрів, описаному в [83].

Етап 6. Обчислення рівня критичності.

На четвертому етапі здійснюються обчислення загальної оцінки рівня критичності ситуації. Спочатку з врахуванням визначених методів інформаційно-психологічного впливу формується НЧ:

$$LSC_i = \sum_{e=1}^{E} (\sigma_e * P_o)$$

Сформоване нечітке число порівнюється з оціночним еталоном за методом формування α- рівневої номіналізації нечітких чисел [89] і методом визначення ідентифікуючих термів [57]. Дана діє визначається в обчисленні нормалізованих еталонів та їх рівнів. У подольшому здійснюється калькуляція відстані Хемінга. Критерієм відповідності параметрів одному з термів оціночного еталону є найменша відстань Хемінга.

Етап 7. Візуалізація результатів.

Задля кращого відображення рівня критичності ІПВ пропонується відобразити параметри критичності за допомогою індикатора критичності. Для

цього відповідні параметри P_o слід попередньо дефазифікувати. Найбільш доцільним в даному випадку є застосування методу центру ваги [58], за яким нечітке число перетворюють в чітке за формулою:

$$L = 100 * (\sum_{i=1}^{q} X_{Lqi} * \mu(x_{Lqi}) / \sum_{i=1}^{q} \mu\left(x_{Lqi}\right))$$

де q – кількість супортів НЧ. Можливий випадок, коли значення окремих параметрів обчислюються напряму без використання експертних методів. В такому випадку вони на індикаторі відображаються гістограмою.

Для прикладу наведемо результати ранжування параметрів оцінювання критичності ІПВ, що здійснюється ЕГ.

Розглянемо приклад визначення коефіцієнтів важливості для заданих раніше оціночних параметрів (таблиця 3.8). Експерт оцінює важливість кожного із них у порівнянні з іншим та заносить інформацію у таблицю. Обраховуються коефіцієнти важливості та проводиться їх нормування.

Таблиця 3.8.

Результат попарного порівняння оціночних параметрів ІПВ P_i

i\i'	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	ω_i	Ω_i
P_1	1	5	2	1/5	1/7	3	4	6	1,459	0,155
P_2	1/5	1	¼	5	5	¼	1/3	½	0,690	0,073
P_3	5	1/5	7	1	1/5	4	5	2	1,654	0,176
P_4	7	1/5	5	5	1	5	6	3	2,737	0,292
P_5	1/3	4	¼	¼	1/5	1	¼	5	0,616	0,065
P_6	¼	3	2	1/5	1/6	4	1	7	1,043	0,110
P_7	1/6	2	3	½	1/3	1/5	1/7	1	0,508	0,054
									8,488	0,925

Наступним кроком є проведення ранжування оціночних параметрів по обчислених та нормованих коефіцієнтах важливості. В результаті проведення обчислень параметр «Зростання фактора тривожності» отримує найвищу

оцінку, а отже, на думку експерта, є найбільш пріоритетним серед решти параметрів.

Таблиця 3.9

Ранжування оціночних параметрів за коефіцієнтами важливості

Оціночний параметр, P_i	Коефіцієнт Важливості
Зростання фактора тривожності	0,292
Реакція громадськості	0,176
Повнота і сила аргументації	0,155
Кількість уражених цілей	0,110
Асоціації, які викликає джерело інформації	0,078
Швидкість розповсюдження	0,065
Тривалість	0,054

Розробка методу відображає новий підхід до вирішення проблеми оцінювання інформаційно-психологічного впливу. Метод ґрунтується на основі нечіткої логіки. Під час його реалізації відбувається кілька етапів, які направлені на визначення еталонних та поточних значень певного інформаційного простору для виявлення ІПВ. Особливою рисою є забезпечення процесу оцінювання ІПВ, що стане у нагоді при покращенні ефективності розробки та впровадження засобів протидії.

У додатку В представлено схему відображення методу оцінювання ІПВ.

3.4. Методика протидії інформаційно-психологічному впливу в соціальних мережах

Поширення інформаційних повідомлень у соціальних мережах зупинити надзвичайно важко. Наразі існують кілька методик обмеження контекту за ключовими словами.

Під час реєстрації в Facebook, Instagram та Twitter користувач повинен прийняти угоду, в якій зазначають правила використання особистого акаунту. За порушення такої угоди покаранням може стати видалення опублікованого контенту, або видалення акаунту користувача. У загальному опублікований контент не повинен стосуватися:

- зображення голого тіла;
- сексуального підтексту;
- дій сексуального характеру;
- зображення сцен насилля;
- жорстокого поводження з тваринами;
- закликів до самогубства;
- спаму;
- несанкціонованої торгівлі;
- розпалювання ворожнечі на грунті релігії, національності, статі, соціального стану, сексуальної орієнтації, інвалідності чи хвороби;
- тероризму.

У різних соціальних мережах межі дозволеного відрізняються. Наразі провідні інформаційні майданчики застосовують технології штучного інтелекту для виявлення потенційно неприйнятного контенту, який автоматично індексує усі повідомлення, які з’являються на сторінках і автоматично приймає рішення щодо подальших дій з контентом.

Окремим чинником стоїть поширення фейкових новин та дезінформації. Особливого резонансу боротьба з такими дописами набула після втручання росії у виборчу кампанію у США в 2016 році задля зменшення рейтингу кандидата від Демократичної партії Хіларі Клінтон та пісдя референдуму в Великобританії у 2017 році щодо виходу із Європейського союзу задля виходу країни із блоку, що викликало б кризу в інших країнах союзу.

У США втручання росії у хід голосування викликало широкий резонанс, що призвело до розслідування спецпрокурором Мюллером даного впливу. У своїй доповіді за підсумком розслідування Мюллер детально розписав усю структуру та механізми російського впливу [19]. Більша частина звіту відсутня у відкритому доступі, задля не розкриття методів дослідження. Проте, відповідно до доповіді, результат дослідження співпав із спільним звітом Центрального розвідувального управління (ЦРУ), Федерального бюро розслідування (ФБР), Агентства національної безпеки (АНБ) [19].

Відповідно до даного звіту, для виконання спеціальних інформаційних операцій керівництвом Російської Федерації було віддано накази для утворення Агентства Інтернет-досліджень (в Україні більш відомого під назвою «фабрика тролів»), яке офіційно було утворено Євгенієм Пригожином, який досить близькою особою до Володимира Путіна [19]. Працівники агентства розпочали дослідження аудиторії США ще з початку 2014 року [19]. Ними було визначено лідерів думок, групи, що мають найбільшу аудиторію. Також розпочалося дослідження важливих тем для населення країни, що потім будуть використані для таргетування аудиторій у соціальних мережах. У тому ж році розпочалося створення акантів та груп у найбільш популярних соціальних мережах – Facebook, Twitter, Instagram.

На початок 2016 року Агентство дослідило мільйони акаунтів американських громадян та володіло у власному розпоряджені тисячі акунтів та сотні груп [19]. З того ж часу розпочалася кампанія з дискредитації Хіларі Клінтон, що спочатку проявлялася із зневажливих постів. Через власні акаунти у соціальних мережах та форумах Агентство отримало можливість впливати на суспільну думку в США. З 2016 року розпочалося залучення до Агентства спеціалістів із просування контенту в Facebook, Twitter, Instagram та YouTub. Відбувалася постійна оцінка впливу контенту на аудиторію, що дозволяла постійно покращувати повідомлення та вибирати теми, що найбільше хвилюють громадян [19].

Окремо варто відзначити, що Агентство активно розвивало групи, що націлені на неформальну аудиторію – расистів, борців з емігрантами, ЛГБТ-меншин та релігійних фанатиків [19].

Відповідно до звіту, лише задля організації інформаційної кампанії у соціальній мережі Facebook (скупка акаунтів, розкручування груп та лідерів думок) Росією було витрачено щонайменше 100 000 доларів США [19].

Критичною точкою в інформаційній кампанії став інформаційний привід проти Хіларі Клінтон – пересилання таємних та конфіденційних документів звичайно електронною поштою та подальший її взлам [19]. Документи було викладено на кількох сайтах, серед який популярний у США - WikiLeaks. Дана інформація опосередковано свідчила про некомпетентність кандидата у президенти та була гостро сприйнята громадянами США [19]. Після даного інформаційного приводу увесь російський механізм інформаційного впливу розпочав його розкручувати та поширювати дану інформацію [19].

У підсумку, кандидат у президенти від Демократичної партії США Хіларі Клінтон програла вибори. Це свідчить про успішність механізму.

Можна зробити висновок, що росіянами було вироблено наступний алгоритм по впливу на процес голосування інших країн:

1. Створення групи спеціалістів.

2. Дослідження аудиторії щодо важливих тем для подальшого таргетування.

3. Дослідження соціальних мереж задля виявлення лідерів думок, груп із найбільшою аудиторією.

4. Створення розгалуженої мережі акаунтів та груп у соціальних мережах.

5. Включення традиційних ЗМІ.

6. Перевірка мережі акаунтів та груп, ЗМІ на можливість впливу на громадську думку аудиторії.

7. Інформаційний привід.

8. Розкручування інформаційного приводу.

9. Закріплення результату.

Після цих подій соціальні мережі розпочали відстежувати дописи на наявність у них дезінформації. У загальному використання штучного інтелекту для блокування неприйнятного контенту можна представити наступною схемою (рис. 3.8):

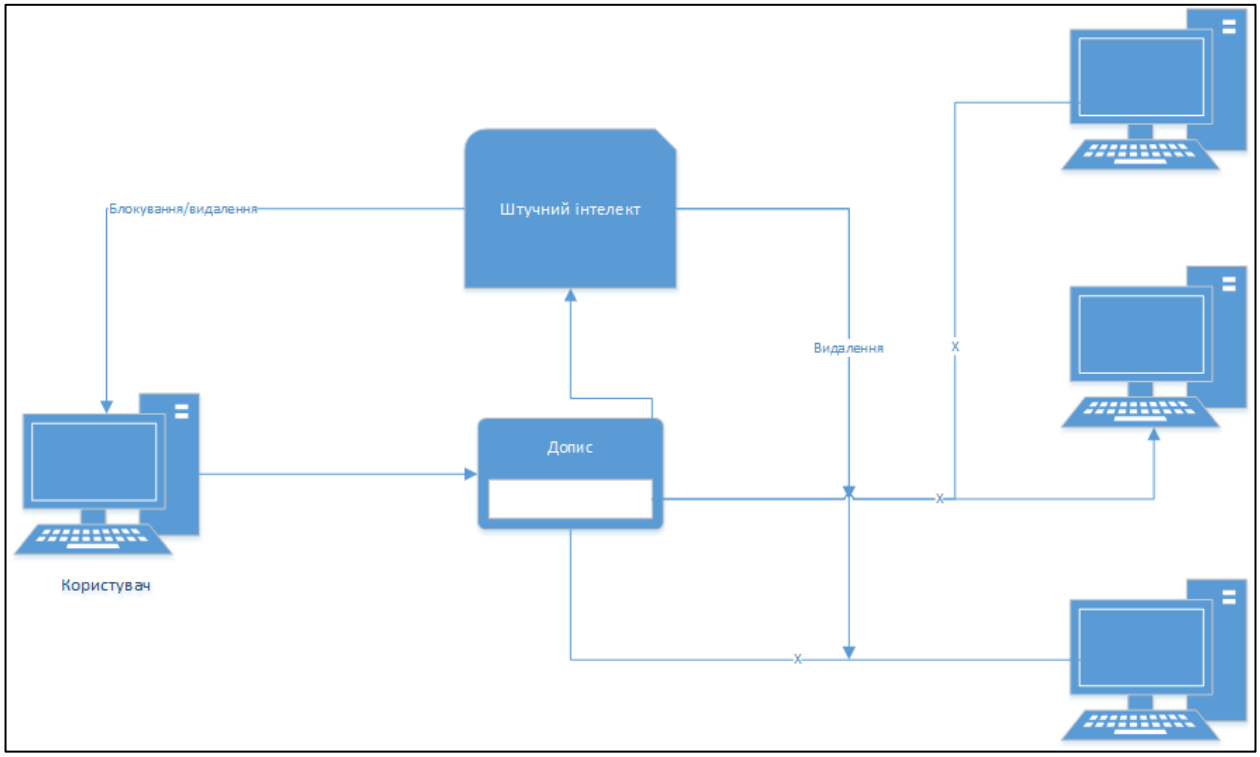


Рис. 3.8. Блокування неприйнятного контенту штучним інтелектом

Іншим важливим способом обмеження поширення неприйнятного контенту є тіньовий бан. Технологія тіньового бану побудована також на використанні штучного інтелекту та пошуку по ключовим словам. Основна ідея даної технології полягає у тому, щоб обмежити демонстрацію одного або усіх дописів користувача в соціальній мережі. Даний спосіб викликає найбільше критики, адже умови обмежень не зазначені в користувацькій угоді та

змінюються в залежності від рішень керівництва компаній, які здійснюють управління соціальною мережею. У загальному технологію використання тіньового бану можна продемонструвати наступною схемою (рис. 3.9):

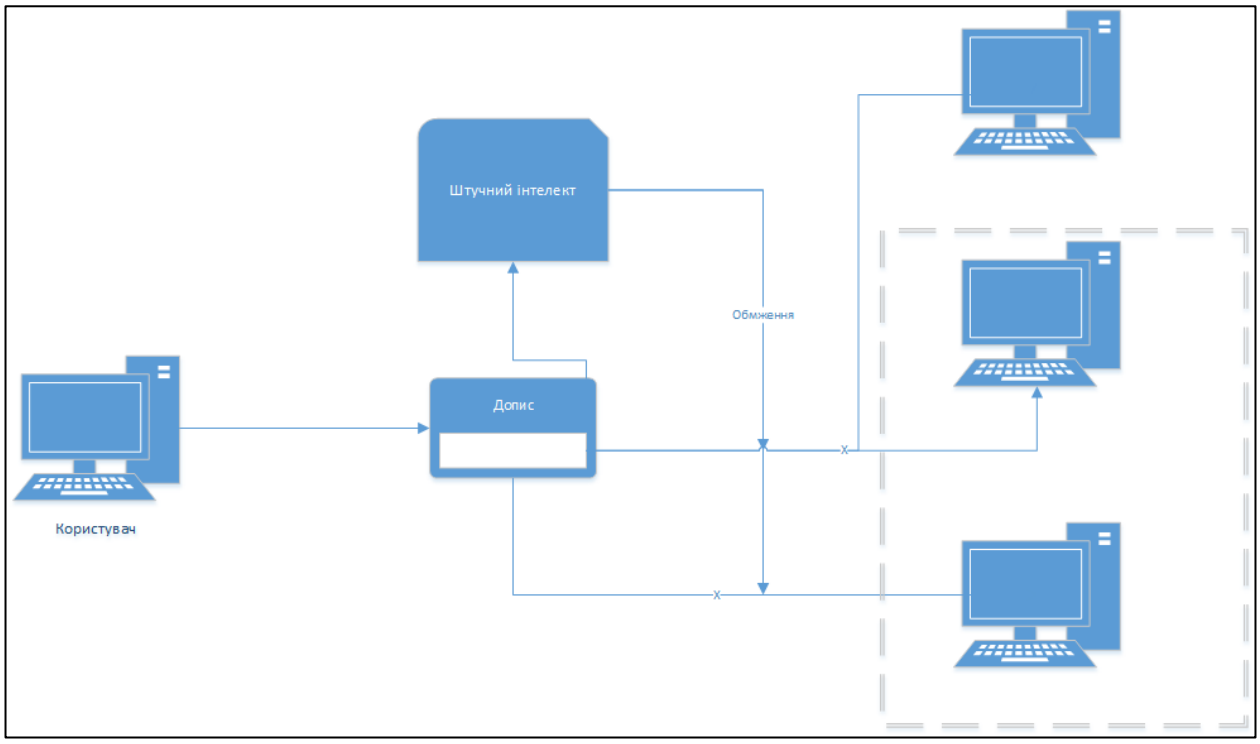


Рис. 3.9. Використання технології «тіньового бану»

Також соціальні мережі надають можливість користувачам самостійно скаржитися до адміністраторів інформаційного фонду щодо того чи іншого допису/користувача/спільноти. Варто зазначити, що Telegram практично немає жодних обмежень щодо поширення інформації, широко використовується злочинцями та пропагандистами для поширення власних товарів чи наративів.

В інформаційно-автоматизованих системах, які здійснюють управління інформаційним впливом у соціальних мережах ми пропонуємо додатково використовувати індекс джерела інформації та маркувати його відповідним чином.

Індекс джерела інформації ($Isrc$) ґрунтується на різниці тональності повідомлень джерела:

$$Isrc = Tp/Cm - Tn/Cm, \text{ де}$$

Tp - кількість дописів з позитивною тональністю;

Tn - кількість дописів з негативною тональністю;

Cm - кількість повідомлень.

Для ресурсів, де вдень публікується більше 10 повідомлень доцільно часовий проміжок для підрахунку кількості повідомлень доцільно брати за день, в інших випадках – за тиждень.

Підсумком підрахунку індексу джерела є позитивна, або негативна різниця тональностей. Якщо різниця негативна – ресурс є критично налаштованим та може використовуватися для здійснення спеціальних інформаційних операцій противником і необхідно вживати заходи протидії.

3.5. Висновки

У третьому розділі дисертаційного дослідження були отримані наступні вагомі результати:

1. Виділено та сформовано множину оціночних параметрів ІПВ, за якими у подальшому під час процесу оцінювання ІПВ він буде характеризуватися та оцінюватися.

2. Розроблено метод оцінювання критичності інформаційно-психологічного впливу в соціальних мережах, відповідно до оціночних параметрів.

Враховано усі виявлені в результаті аналізу недоліки існуючих систем оцінки. Визначено найбільш універсальні оціночні параметри. Даний метод ґрунтується на кількісних методах експертної оцінки, що дає переваги у відсутності необхідності збору великих кількостей статистичних даних та чіткої формалізації поточної ситуації та елементах нечіткої логіки. Розраховано еталони оціночних параметрів.

Розроблений метод надає можливість оцінювати критичність інформаційно-психологічного впливу щодо каскаду інформаційних повідомлень та конкретного допису. Таким чином він може допомогти в

точному встановленні загроз інформаційному простору, іміджу та вибору адекватних засобів реагування.

РОЗДІЛ 4. РОЗРОБКА АРХІТЕКТУРИ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИМ ВПЛИВОМ ТА ПРОГРАМНО-АПАРАТНОГО КОМПЛЕКСУ НА ЇЇ ОСНОВІ

4.1. Загальна архітектура системи управління інформаційно-психологічним впливом

Оскільки лише виявлення інформаційного впливу, враховуючи важливість захисту соціальних груп в поєднані з стрімким розвитком сучасних засобів та способів порушення інформаційної безпеки, на сьогодні є не достатнім. Виникає необхідність в його ідентифікації, так як вибір контрзаходів є більш ефективним для конкретного і заздалегідь відомого впливу. Тому основне призначення даної системи – прогнозування або виявлення та ідентифікація ІПВ. На сьогодні аналогічних систем практично немає. Подібні системи для управління інформаційно-психологічного впливу засновані на теорії ймовірності. Такий підхід не дозволяє виявляти невідомі методи впливу, контролювати слабоформалізований простір. Особливістю таких систем є те, що вони потребують великого масива статистичної вибірки, навчаня тощо. Тому під час розроблення нашої системи будемо використовувати методи нечіткої логіки та експертні, які непотребують великого масиву даних.

Призначенням СУІПВ є виявлення, ідентифікація та оцінювання ІПВ. Вхідними даними системи є ідентифікатори ІПВ, контрольовані параметри та їх значення. На виході системи – інформація щодо ІПВ, його ідентифікуючі дані та оцінка рівня критичності ІПВ.

СУІПВ складається з наступних підсистем: підсистема моніторингу, підсистема виявлення та ідентифікації ІПВ, підсистема оцінювання ІПВ.

4.1.1. Підсистема виявлення та ідентифікації інформаційно-психологічного впливу

Архітектура Підсистеми виявлення та ідентифікації ІПВ представлена у додатку Г. Вона включає наступні структурні елементи як: система датчиків (СД); модуль первинної обробки вхідних параметрів, що вміщує регістри ідентифікуючих параметрів (РІП), регістри ІПВ (РІПВ), блок формування зв'язки вплив-параметр (БФЗВП); модуль вторинної обробки ідентифікуючих параметрів, що складається з блоку фазифікації ідентифікуючих параметрів (БФІП) та блоку формування кортежів фазифікованих параметрів (БФКФП); модуль виконання нечітких арифметичних операцій, до якого відносяться блок формування ідентифікатора поточного стану і блок прийняття рішення; модуль формування еталонів та евристичних правил, до складу якого входять однойменні відповідні блоки; модуль представлення результату, що містить блок логічного висновку та блок візуалізації; а також модуль управління режимами (МУР), що переводить систему в режим корекції еталонів (РКЕ) або режим корекції евристичних правил (РКЕП).

СД розміщена в кібернетичному середовищі, що є нечітким та слабоформалізованим. Склад СД залежить від поставлених цілей. СД проводить моніторинг контексту в кібернетичному просторі.

В модулі первинної обробки вхідних параметрів задаються ІПВ, які система виявляє та ідентифікує, а також відповідні їм ідентифікуючі параметри. В РІПВ заносяться ідентифікатори основних методів інформаційно-психологічного впливу $IPI_i, i = \overline{1,n}$, а в РІП аналогічно заносяться з певною періодичністю поточні значення ідентифікуючих параметрів $P_{ij}, i=\overline{1,n}$, $j=\overline{1,m}$, що визначені і описані в попередніх підрозділах.

В БФЗВП формуються зв'язки $IPI_i \rightarrow P_i$ конкретного типу ІПВ з параметрами, що необхідні для його виявлення. Так для окремих методів ІПВ створюються підмножини P_i.

Основною задачею модуля вторинної обробки ідентифікуючих параметрів є їх фазифікаця та подальше групування відповідно до методів ІПВ, які вони визначають. У БФІП проводиться процедура фазифікації, у якій виміряні поточні значення параметрів за певний період перетворюються в нечіткі теми. У результаті цього формуються підмножини P_i. В БФКФП уже фазифіковані ідентифікуючі параметри групуються в підмножини у відповідністю з сформованими в БФЗІП групами. У модулі формування еталонів та евристичних правил обчислюються еталонні величини кожного ідентифікуючого параметру, які важливі під час вимірювання поточних значень Призначенням модуля БФНЕ є формування множини еталонів ідентифікуючих параметрів. Еталони описуються за допомогою термів як лінгвістичні змінні.

В БФЕП у процесі зіставлення ідентифікаторів поточного стану, що визначається комбінацією значень поточних параметрів, та лінгвістичних ідентифікаторів можливості реалізації ІПВ формується набір правил для всіх заданих методів впливу. Сформовані еталонні значення та евристичні правила є основними даними, що забезпечують роботу даної Підсистеми. Вони задаються перед початком роботи системи з виявлення ІПКВ. Існує можливість їх корекції. Призначенням модуля виконання нечітких арифметичних операцій є порівняння поточних значень параметрів з еталоними і визначення евристичного правала, що описує ситуацію.

В БФІПС виміряні і фазиковані ідентифікуючі параметри з використанням методу узагальненої відстані Хемінга порівнюються з еталонами, визначаючи відповідні (найбільш близькі) поточній ситуації терми, і на основі цього формується ідентифікатор поточного стану. В БПР ідентифікатор поточних станів порівнюється з наборами ЕП, в процесі чого шукається правило, що погоджує поточний ідентифікатор. Ймовірність появи ІПВ прирівнюється значенню лінгвістичного ідентифікатора можливості реалізації ІПВ правила, що спрацювало.

Призначення модуля представлення результату полягає в відображені отриманих результатів в зрозумілій для оператора системи вигляді. Отриманий результат може бути відображений в лінгвістичній формі.

4.1.2. Підсистема оцінювання інформаційно-психологічного впливу

До складу Підсистеми оцінювання інформаційно-психологічного впливу входять: модуль первинної обробки даних, що складається з регістри параметрів оцінки рівня критичності (РПО), блоку формування еталонів параметрів оцінки (БФЕПО) та блоку формування оціночних еталонів (БФОЕ); модуль обрахунку КВ, який містить у собі ругістри матриці попарного порівняння (РМПП), блок визначення КВ (БВКВ) і блок нормування КВ (БНКВ); модуль операцій нечіткої логіки, до якого входять блок лічильника сенсорів параметрів (БЛСП), блок фазифікації оціночних параметрів (БФОП), блок обрахунку рівня критичності (БОРК), блок обчислення відстані Хемінга (БОВХ); модуль формування і відображення результатів, до складу якого входять блок дефазифікації результатів (БДФР), блок логічного висновку (БЛВ), блок візуалізації результатів (БВР) модуль управління режимом роботи системи (МУР), що забезпечує функціонування режиму корекції еталонів (РКЕ) та інтерфейс користувача (експерта або оператора).

У модулі первинної обробки даних відбувається ініціалізація оціночних параметрів, а також формуються оціночні еталони. Значення параметрів оцінки рівня критичності та їх ідентифікатори з множини P_o заносяться до РПО. В БФЕПО за участю експерта параметричним методом формування НЧ будуються еталони, які відображаються відповідними термами. У БФОЕ будується оціночний еталон з аналогічними термами для визначення рівня критичності шляхом його порівняння з обрахованим значення рівня критичності ситуації.

Модуль обрахунку КВ функціонує з метою формування коефіцієнтів важливість, які є визначальними під час порівняння параметрів одним з одним. Оцінка важливості проводиться експертом з урахуванням умов функціонування

соціальної мережі, соціальної групи, публічної сторінки чи інших об’єктів, що впливають на ІПВ. В РМПП заносяться елементи матриці попарного порівняння $A = \left|\left|a_{ij}\right|\right|$, які відображають рішення експерта щодо пріоритетності того чи іншого параметра у конкректному дописі. В БОКВ розраховуються КВ для кожного параметра за формулою $\omega_i = \sqrt[n]{\prod_{i`=1}^{I} a_{ij}},\ i` = \overline{1,I},$ а в БНКВ проходить процедура їх нормування.

Модуль операцій нечіткої арифметики призначений для обробки значень параметрів оцінки рівня критичності та визначення рівня критичності з застосуванням методів нечіткої логіки та експертних підходів. У БЛСП реалізований механізм сенсорів, що покладений в основу процедури фазифікації. Показники значень оціночних параметрів демонструють покази їх сенсорів у відповідності з вказаними інтервалами термів їх еталонів. Вихідними даними БЛСП є поправочні еталони. В БФОП у подальшому на їх основі обраховується фазифікація показників оціночних параметрів, результатом якої є нечітке число, яке демонструє поточний рівень оціночних параметрів за період, отриманої шляхом виконання Т вимірювань. У БОВХ з використанням методу, описаного в [57], обчислюється узагальнена ВХ між отриманим значенням рівня критичності ситуації та термами оціночного еталону.

Модуль формування і відображення результатів реалізує формування кінцевого результату системи і відображення його в формі зрозумілій оператору. У БЛВ за отриманим рівнем критичності система приймає демонструє рівнь впливу виду ІПВ на аудиторію. Для цього обраховані УВХ порівнюються між собою і знаходиться мінімальна, а отриманий в результаті терм і буде відповідати рівню критичності. БВР відображає результати користувачу. Так, тут формується індикатор рівня критичності, в якому відображаються значенні параметрів та рівня критичності, а також ідентифікатор методу інформаційно-психологічного впливу, що спричинив його. Інтерфейс реалізує процеси вводу/виводу інформації експертом чи оператором системи.

Архітектура Підсистеми оцінювання ІПВ представлена у додатку Д.

4.2. Програмна реалізація системи виявлення та ідентифікації інформаційно-психологічного впливу

У якості середовища розробки програмних засобів обрано технологічну платформу Microfocus IDOL. Micro Focus IDOL (Intelligent Data Operating Layer) – це програмний продукт, який призначений для аналізу та обробки надмірної кількості даних різних типів, включаючи текст, зображення, аудіо та відео. IDOL володіє розширеними функціональними можливостями, які дозволяють витягувати інформацію з навіть найскладніших та неструктурованих даних. Основні характеристики та функції IDOL включають наступне:

- автоматично індексує дані, що дозволяє швидко та ефективно здійснювати пошук та доступ до них. Індексування охоплює різні мови та типи контенту;
- використовує семантичний аналіз для розуміння значень слів та контексту в текстових документах. Це дозволяє виявляти схожість документів, здійснювати класифікацію та розпізнавати ключові слова;
- може визначати тон або настрій тексту, що допомагає в аналізі суспільних думок та реакцій;
- підтримує аналіз зображень та відео для виявлення об'єктів, тексту, обличчя, руху та іншої інформації у мультимедійних контентах;
- може використовувати методи машинного навчання для надання рекомендацій та прогнозування;
- підтримує багато мов і може виконувати аналіз тексту у багатьох мовах, включаючи морфологію, синтаксис і семантику;
- має API, який дозволяє легко інтегрувати його з іншими програмами та системами;
- надає можливості захисту та контролю доступу до даних, що важливі для дотримання стандартів безпеки та конфіденційності.

IDOL використовується в різних галузях, включаючи аналітику соціальних мереж, пошук та видобуток інформації, обробку медіа-змісту, бізнес-аналітику та багато інших сфер. Він може бути використаний для створення різних застосунків, включаючи експертні системи, які ви плануєте розробити для аналізу інформаційних повідомлень у соціальних мережах.

Програмне забезпечення «СУІПВ v.1.0»

Для проведення експерименту, на основі методу виявлення ІПВ, було розроблено програмне забезпечення «СВІПВ v.1.0». Дане програмне забезпечення реалізує виявлення ІПВ різного характеру в умовах слабоформалізованого нечіткого середовища. В ньому реалізовані процеси побудови еталонів ідентифікуючих параметрів, наборів ЕП, фазифікації значень поточних параметрів та їх порівняння з еталонними за рахунок розрахунку УВХ; визначення коефіцієнтів важливості і ранжування параметрів, фазифікації значень поточних параметрів, обрахунку показника рівня критичності, що представлений в формі НЧ, та їх дефазифікація для відображення в вигляді індикатора рівня критичності. В регістри системи заносяться ідентифікуючі параметри та ідентифікатори ІПВ, склад і кількість яких може коригуватися. Інтерфейс програми представлено на рис. 4.1.

На початку реалізації необхідно підключити Microfocus IDOL через API до соціальних мереж. Будемо підключатися до Facebook, Twitter, Instagram та Телеграм. Для підключення до Facebook необхідно використовувати Facebook Graph API. Наведемо програмний код на мові Python підключення до даної соціальної мережі:

```
import requests
from bs4 import BeautifulSoup
content_Facebook={
access_token = {
        "event_name": "Purchase",
        "event_time": 1636712168,
        "user_data": {
          "em": [
            "309a0a5c3e211326ae75ca18196d301a9bdbd1a882a4d2569511033da23f0abd"
          ],
          "ph": [
            "254aa248acb47dd654ca3ea53f48c2c26d641d23d7e2e93a1ec56258df7674c4",
            "6f4fcb9deaeadc8f9746ae76d97ce1239e98b404efe5da3ee0b7149740f89ad6"
          ],
          "client_ip_address": "123.123.123.123",
          "client_user_agent": "$CLIENT_USER_AGENT",
          "fbc": "fb.1.1554763741205.AbCdEfGhIjKlMnOpQrStUvWxYz1234567890"}

# Отримання даних з Facebook Graph API для публікацій на сторінці
def get_facebook_posts(page_id):
    url = f'https://graph.facebook.com/v12.0/{page_id}/posts'
    params = {
        'access_token': access_token,
        'limit': 10,  # Кількість публікацій для отримання
    }
    response = requests.get(url, params=params)
    data = response.json()}
    return data['data']
```

Далі необхідно задати в програмний комплекс еталонні значення. Основна обробка інформації здійснюється у модулі Niagara Files, а програмування його роботи здійснюється шляхом побудови процесів у модулі та задання виконуючих файлів на мові Lua. Представимо задання еталонних значень для виду ІПВ «Повнота і сила аргументації»:

```
local gnuplot = require("gnuplot")
-- Задання точок на графіку
local x1 = {0, 1, 0.63, 0,43, 0}
local x2 = {0, 0,22, 1, 0,57, 0}
local x3 = {0, 0,33, 0,75, 1, 0}

local y1 = {0,33, 0,33, 0,75, 1, 1}
local y2 = {0,33, 0,33, 0,75, 1, 1}
local y2 = {0,33, 0,33, 0,75, 1, 1}

-- Створення графіку
gnuplot.plot(
    {'H', x1, y1, '-'}
    {'C', x2, y2, '-'}
…{'B', x3, y3, '-'}
)
```

У подальшому необхідно ввести еврестичні правила, це можна зробити підтягнувши відомості з файлу у відповідний модуль системи:

```
local file = io.open(‘Рефреймінг.txt', 'r')
if file then
   -- Зчитування вмісту файлу
local content = file:read('*all')
   -- Закриття файлу
   file:close()
```

У подальшому необхідно створити нейронну мережу, яка буде аналізувати контент соціальних мереж та виставляти оцінки повідомленням за ідентифікуючими параметрами від 1 до 5. Мережа повинна виставити оцінки кожному такому параметру:

```
import numpy as np
import tensorflow as tf
from tensorflow import keras
from tensorflow.keras import layers
# Підготовка даних навчання
data = np.array([[0.8, 0.7, 0.6, 0.9, 0.2, 0.5, 0.8],
                 [0.6, 0.5, 0.4, 0.7, 0.3, 0.6, 0.7],
……..[0.2, 0.3, 0.2, 0.1, 0.3, 0.7, 0.5],
                ])
# Відповідні оцінки
labels = np.array([1, 3, 4, 2, 5])  # Оцінки від 1 до 5
# Створення моделі нейронної мережі
model = keras.Sequential([
    layers.Input(shape=(7,)),  # Вхідний шар з 7 нейронами
    layers.Dense(64, activation='relu'),  # Прихований шар з 64 нейронами і активацією ReLU
    layers.Dense(32, activation='relu'),  # Додатковий прихований шар з 32 нейронами і активацією ReLU
    layers.Dense(5, activation='softmax')  # Вихідний шар з 5 нейронами і активацією softmax
])
# Компіляція моделі
model.compile(optimizer='adam',  # Вибір оптимізатора
              loss='sparse_categorical_crossentropy',  # Функція втрат для задачі класифікації
              metrics=['accuracy'])  # Метрика для оцінки точності
# Тренування моделі
model.fit(data, labels, epochs=50, batch_size=1)
```

```
# Тренування моделі
model.fit(data, labels, epochs=50, batch_size=1)
# Отримання оцінки
predicted_rating = np.argmax(predictions) + 1  # +1
```

У подальшому необхідно здійснити фазифікацію отриманої оцінки та обчислити відстань Хемінга для кожного параметра.

```
import numpy as np

def fuzzify_number(x, low, medium, high):
    low_membership = max(0, min((x - low) / (medium - low), 1))
    medium_membership = max(0, min((high - x) / (high - medium), 1))
    high_membership = max(0, min((x - medium) / (high - medium), 1))
    return low_membership, medium_membership, high_membership
# Функція для фазифікації числа
def fuzzify_number(x, low, medium, high):
    low_membership = max(0, min((x - low) / (medium - low), 1))
    medium_membership = max(0, min((high - x) / (high - medium), 1))
    high_membership = max(0, min((x - medium) / (high - medium), 1))
    return low_membership, medium_membership, high_membership

# Функція для фазифікації оцінок
def fuzzify_ratings(ratings):
    fuzzified_ratings = []
    for rating in ratings:
        fuzzified_rating = fuzzify_number(rating, low_criteria, medium_criteria, high_criteria)

        # Додавання фазифікованих оцінок до списку
        fuzzified_ratings.append(fuzzified_rating)
```

```
# Функція для обчислення відстані Хемінга між двома послідовностями

def calculate_hamming_distance(seq1, seq2):
    return sum(el1 != el2 for el1, el2 in zip(seq1, seq2))

# Оцінки, які надає попередня нейронна мережа
neural_network_ratings = predicted_rating

# Еталонні значення
etalon_ratings = etalon

# Фазифікація оцінок
fuzzified_neural_ratings = fuzzify_ratings(neural_network_ratings)
fuzzified_etalon_ratings = fuzzify_ratings(etalon_ratings)

hamming_distances_array = []

# Додавання результату обчислення відстані Хемінга до масиву
hamming_distances_array.append(hamming_dist)
```

У подальшому необхідно порівняти результати вимірювання відстані Хемінга з повідомлень з евристичними правилами та промаркувати відповідним чином повідомлення:

```
# Порівняння відстаней Хемінга з відомостями та маркування
for i, distance in enumerate(hamming_distances_array):
    if distance == 0:
        # Якщо відстань Хемінга дорівнює 0, оновіть значення за замовченням на "ІПВ"
        Euristic_rules[i]["Value"] = "ІПВ"

# Маркування повідомлення символом "ІПВ"
for i, rule in enumerate(Euristic_rules):
    if rule["Value"] == "ІПВ":
        print(f"Content_Facebook {i + 1} ‘ІПВ'.")
```

Варто зазначити, що даний метод працює для серії повідомлень, тому під час маркування використаємо стандартні механізми Microfocus IDOL для визначення подібності повідомлень, їх трендовості та спільної тематичності. Під час навчання нейронної мережі для виставлення оцінювання ідентифікуючим параметрам також використовуються стандартні механізми Microfocus IDOL.

Для оцінювання інформаційних повідомлень створюються відповідні модулі в Niagara Files, а процес їх наповнення та запуску аналогічних процесу виявлення інформаційно-психологічному впливу та створено відповідно до методу зазначеному в п. 3.3. У підсумку повідомлення маркується також і числовим значенням.

У програмно-апаратному комплекс наступним чином виглядає перегляд дописів з соціальних мереж:

Рис. 4.1. Перегляд дописів в програмно-апаратному комплексі

Структура модуля Niagara Files представлено на рис. 4.2.

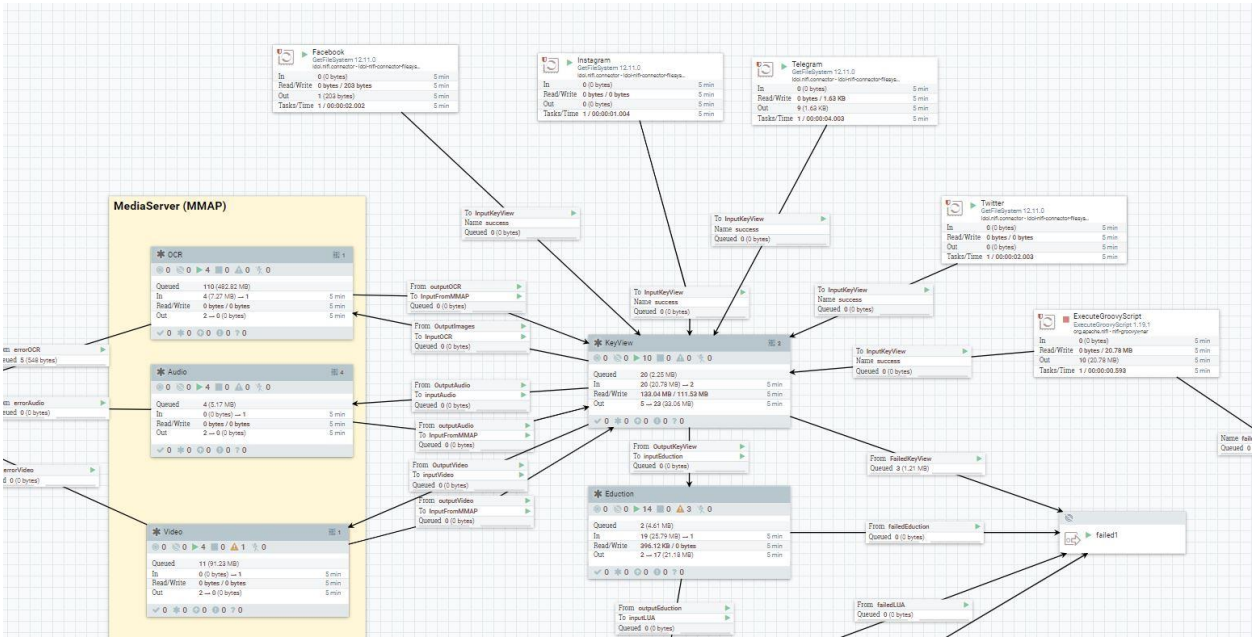


Рис. 4.2. Модуль Niagara Files

4.3. Експериментальне дослідження Системи управління інформаційно-психологічним впливом

Відповідно до розробленої методики було проведено експериментальні дослідження СУІПВ. Далі опишемо хід проведення експериментів, а також обробку та аналіз їх результатів.

Метою будь-якого експериментального дослідження є встановлення характеристиких об’єктів, які досліджуються; перевірка достовірності сформульованих гіпотез, а також вивчення досліджуваної наукової галузі. У науковій літературі описано велику кількість різних класифікацій експериментальних досліджень, які залежать від галузі знань, мети, структури, підготовчих заходів тощо. Важливим елементом експерименту є чітке формулюванн методики – визначеної послідовност подій, яка дозволяє досягти мету дослідження.

Гіпотеза

Експеримент базується на припущені, що запропонована СУІПВ адекватно реагує на зміну ідентифікуючих та оціночних параметрів за різними вхідними даними.

Мета та задачі експерименту

Метою експерименту є перевірка адекватності запропонованих моделей (пп. 2.1), методів (п 2.4, 3.3) і структурних рішень (пп. 4.3.1, 4.3.2) за допомогою розробленого програмного забезпечення управління ІПВ, а саме:

– дослідження запропонованої СУІПВ на основі експертних методів та нечіткої логіки стосовно ефективності її роботи, а саме коректності виявлення різних видів ІПВ у соціальних мережах;

– дослідження запропонованої СУІПВ на основі експертних методів та нечіткої логіки стосовно ефективності її роботи, а саме коректності оцінювання критичності впливу каскаду дописів, інформаційних сторінок чи окремо взятого допису на аудиторію.

Для досягнення поставленої мети необхідно вирішити наступні **задачі:**

– дослідження розробленого програмно-апаратного комплексу;

– обробка і верифікація отриманих результатів;

– проведення виявлення ІПВ та оцінювання критичності видів ІПВ в середовищі соціальних мереж під час зміни ідентифікуючих та оціночних параметрів.

Вибір вхідних та вихідних параметрів

Для Підсистеми виявлення та ідентифікації ІПВ СУІПВ вхідні параметри – нечіткі PM; IF; EL; PP; PN; CG; LT; вихідні параметри – степінь впевненості експерта (нейронної мережі) в рішенні щодо виявлення факту реалізації ІПВ та його виду. Для Підсистеми оцінювання ІПВ вхідні параметри – нечіткі CSA, CGN, PR, GAF, VD, NAT, DR, а також порівняльні судження експертів щодо важливості оціночних параметрів між собою відповідно до методу кількісного парного порівняння з визначенням квадратного кореня; вихідні параметри – показник рівня критичності ситуації, спричиненої впливом ІПВ, відображений індикатором критичності.

Послідовність дій в експериментальному досліджені

Для дослідження СУІПВ виконуються в повній відповідності до етапів методу виявлення та ідентифікації ІПВ, методу оцінювання ІПВ та режиму

роботи системи (див. п.4.3.1 і 4.3.2) – задається множина ідентифікуючих та оціночних параметрів; вимірюються і фазифікуються їх поточні значення, які підлягають порівнянню з раніше побудованими еталонами; перевіряються ідентифікатори поточної ситуації на відповідність заданим правилам з набору сформованих евристичних правил, формується результат), визначаються коефіцієнти важливості кожного оціночного параметру, обчислюється показник рівня критичності каскаду дописів, джерела інформації, одного допису; отриманий показник порівнюється з оціночним еталоном, на основі чого приймається рішення щодо його критичності впливу на аудиторію; проводиться дефазифікації значень оціночних параметрів та рівня критичності і на основі отриманих даних створюється індикатор критичності.

Засоби проведення експерименту

Для дослідження, створення необхідного програмного забезпечення, імітаційного модулювання, обробки результатів та представлення їх в табличному та графічному вигляді використовувалося програмно-апаратний комплекс на основі Microfocus IDOL. Для відображення індикатора рівня критичності поточної ситуації Microsoft Excel 2013.

Аналіз результатів

Аналіз результатів імітаційного моделювання буде представлено у підрозділах 4.3.1, 4.3.2, 4.3.3 даної роботи. Результати представлені в табличній формі та у вигляді графіків і діаграм.

4.3.1. Дослідження здійснення білоруськими опозиційними телеграм-каналами інформаційного протиборства

Експеримент проводився з 1 вересня по 1 грудня 2021 року. За цей час аналізу підлягали усі повідомлення телеграм-каналів «Nexta TV», «Nexta Live», «Беларусь головного мозга», «Мая Краіна Беларусь», «Хартия’97%».

Опозиційні інформаційні ресурси, за відсутності великого фінансування, основним чином представлені Інтернет-ресурсами – передусім Telegram-

каналами, що дозволяють забезпечити авторам дописів анонімність, а значить і безпеку, та YouTube на якому виходять розслідування про злочини режиму самопроголошеного президента Білорусі.

На основі даних «Telegram Analytics» та СУІПВ, спираючись на структурно-функціональний аналіз та мережевий підхід було розглянуто найбільш популярні білоруські опозиційні телеграм-канали.

Канал «Nexta» був створений 19 квітня 2018 р. у Польщі білоруським блогером Степаном Путіло. На ресурсі публікують фото, відео і тексти протестів, а також методичні рекомендації щодо організації обструкції і ненасильницьких акцій в Білорусі. Станом на 28 жовтня 2021 р. канал «Nexta» налічує 437 493 підписників. Охоплення 1 публікації – 175 тис. чол. Денне охоплення – 3,8 млн. чол. Статистика переглядів каналу по місяцях за 2021 р. представлено на рис. 4.3.

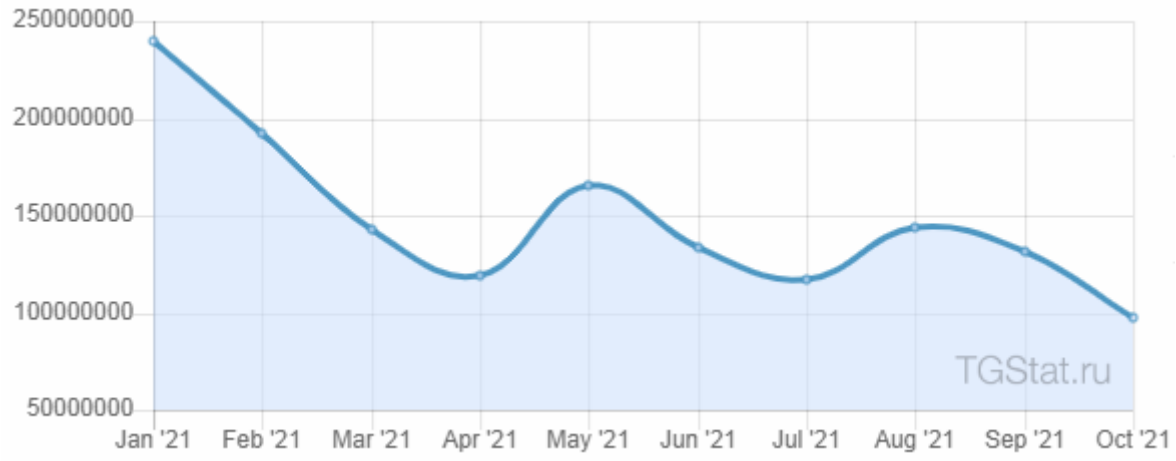


Рис.4.3. Статистика переглядів каналу «Nexta»

«Nexta Live» створено 14 лютого 2019 р. Степаном Путіло. До 27 вересня 2020 р. редактором каналу був Роман Протасевич, журналістом – Катерина Єрусалимська. У період максимальної активності протестів у серпні 2020 р. – це був найбільш популярний медіаресурс опозиції, де публікували новини, заклики до повалення влади, злочини правоохоронців, програми дій на короткострокову і довгострокову перспективи. Станом на 28 жовтня 2021 р. канал «Nexta Live» налічує 928 356 тис. підписників. Охоплення 1 публікації –

313 тис. чол. Денне охоплення – 2,1 млн. чол. Статистика переглядів каналу по місяцях за 2021 р. представлено на рис. 4.4.

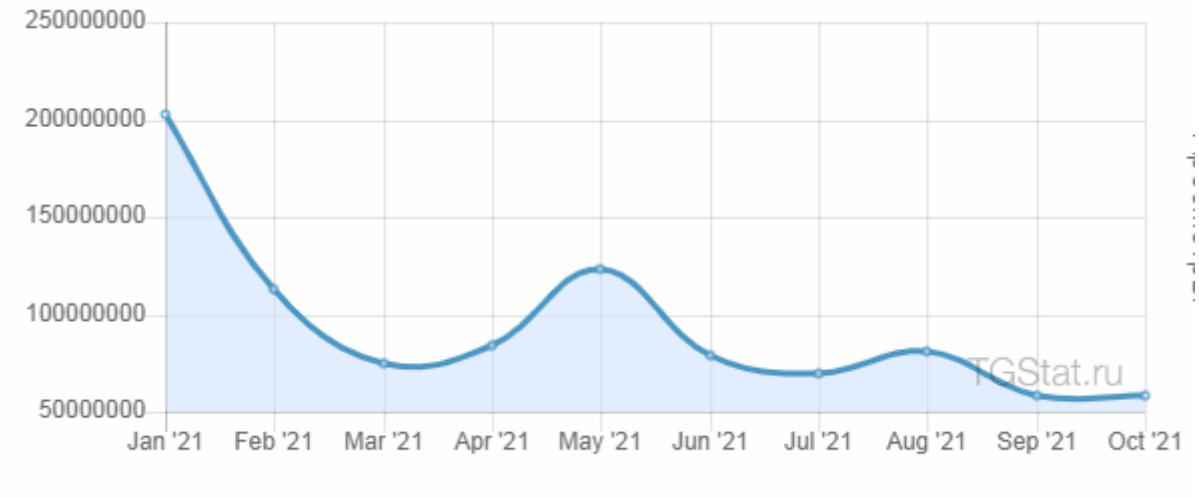


Рис. 4.4. Статистика переглядів каналу «Nexta Live»

«Білорусь головного мозку» – опозиційний Telegram-канал новинного характеру, створений 15 травня 2016 р. Станом на 28 жовтня 2021 р. канал нараховує 92 тис. підписників. Охоплення 1 публікації – 71 тис. чол. Денне охоплення – 1,1 млн. чол. Статистика переглядів каналу по місяцях за 2021 р. представлено на рис. 4.5.

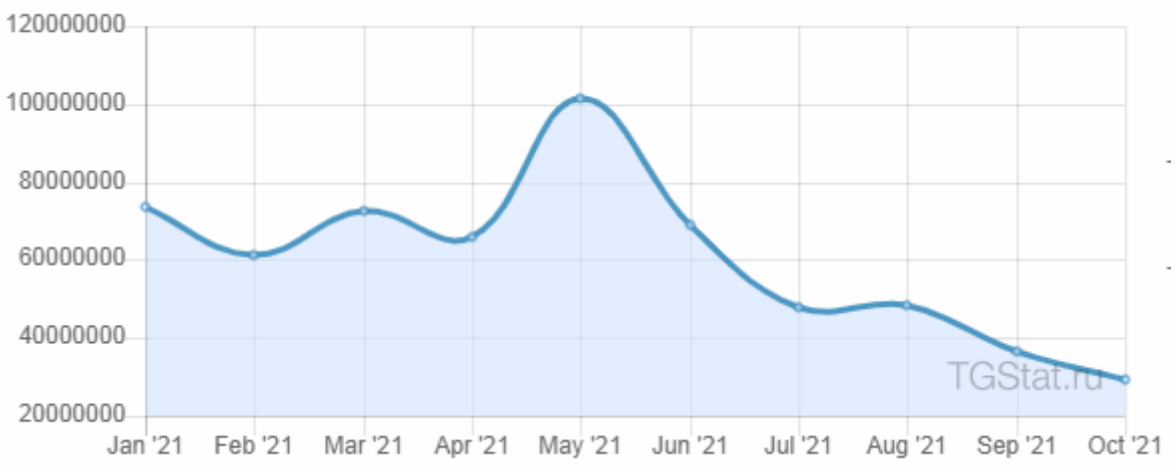


Рис. 4.5. Статистика переглядів каналу «Білорусь головного мозку»

«Мая Краіна Беларусь», – канал створений 20 листопада 2017 р. опозиційним журналістом «Радіо Свобода» Сергієм Беспаловим. На ресурсі висвітлюються новини про протести, злочини правоохоронців. Охоплення 1

публікації – 28 тис. чол. Денне охоплення - 436 тис. чол. Статистика переглядів каналу по місяцях за 2021 р. представлено на рис. 4.6.

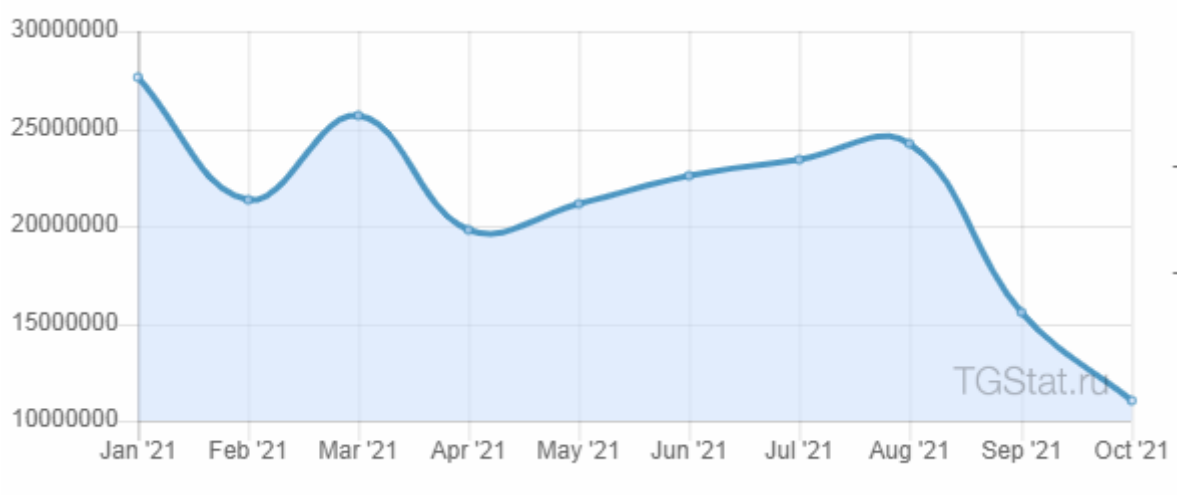


Рис. 4.6. Статистика переглядів каналу «Мая Краіна Беларусь»

«Хартия’97%» - канал найбільшого опозиційного новинного порталу Білорусі, націоналістичного характеру. Публічна сторінка в Telegram створена 31 січня 2018 р. після блокування в Білорусії 24 січня 2018 р. новинного порталу Sharter97.org. На ресурсі публікують новини опозиції та протестів. Охоплення 1 публікації – 26 тис. чол. Денне охоплення – 1,7 млн. чол. Статистика переглядів каналу по місяцях за 2021 р. представлено на рис. 4.7

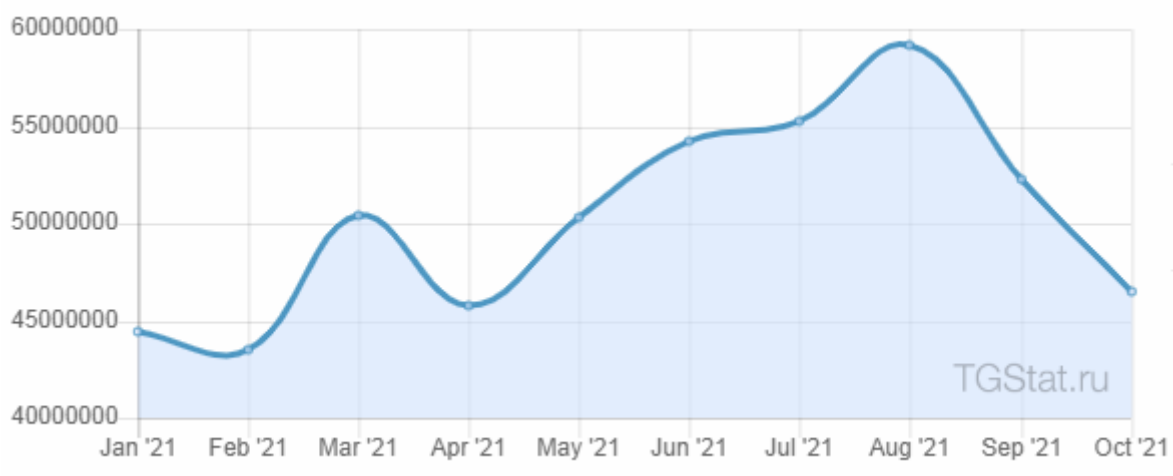


Рис. 4.7. Статистика переглядів каналу «Хартия’97%»

Завдяки месенджеру Telegram організатори протестів у Білорусі зуміли об'єднати розрізнену країною активність у єдиний інформаційний потік. Розсіяні в просторі та часі акції формувалися у ведучу безперервну стрічку,

створюючи для читача ефект масовості. Образи протесту формувалися на принципах, які дослідники Є.В. Бродовська та А.Ю. Домбровська позначили як композиційно-мобілізаційну модель інформування. Тобто існує прямий зв'язок між активністю протестуючих і обсягом публікованого матеріалу в комунікаційному середовищі.

Завдяки використанню СУІПВ в телеграм-каналі «Nexta» протягом вищевказаного періоду часу було виявлено наступну кількість видів інформаційно-психологічного впливу:

Табл. 3.1.

Результати виявлення та ідентифікації інформаційно-психологічного впливу в телеграм-каналі «Nexta»

Вид інформаційно-психологічного впливу	Кількість
Маніпулювання	19
Навіювання	22
Переконання	39
Дезінформація	11
Пропаганда	21
Рефреймінг	6
Зараження	6
Психологічна ізоляція	3
Примус	2

Найбільш популярними дописами на каналі стала тематика незаконної міграції з Білорусі до країни Європейського союзу. Варто зазначити, що під час публікації новин даної тематики були використані усі виявлені методи ІПВ, а пости часто перегукувалися з іншими телеграм-каналами. Індикація рівнів критичності за оціночними параметрами каналу взагальному представлена на рис. 4.8.

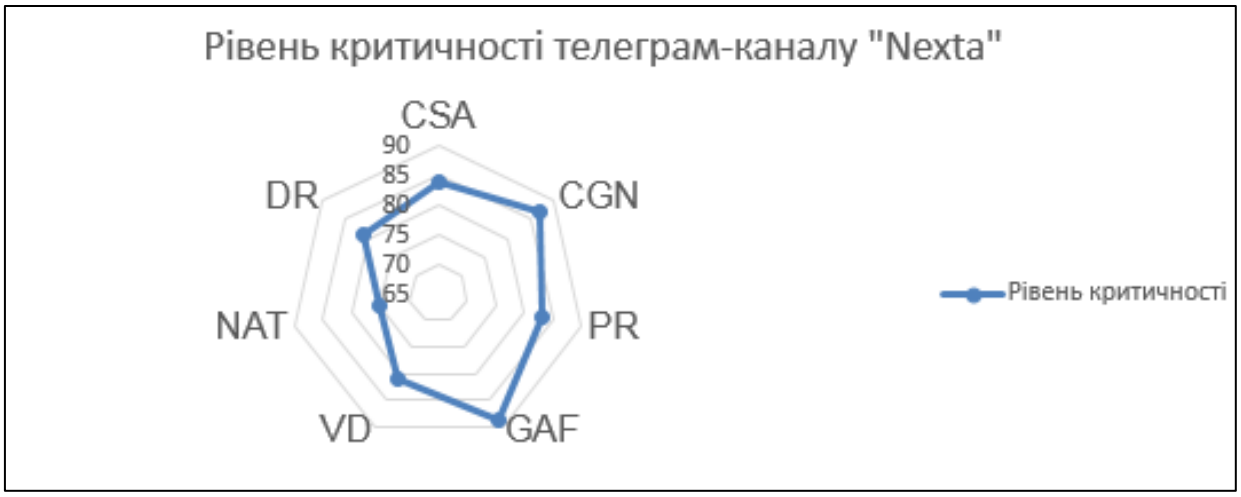


Рис. 4.8. Рівень критичності телеграм-каналу «Nexta»

У телеграм-каналі «Nexta Live» протягом вищевказаного періоду часу було виявлено наступну кількість видів інформаційно-психологічного впливу:

Табл. 4.2.

Результати виявлення та ідентифікації інформаційно-психологічного впливу в телеграм-каналі «Nexta Live»

Вид інформаційно-психологічного впливу	Кількість
Маніпулювання	32
Навіювання	33
Переконання	84
Дезінформація	15
Пропаганда	29
Рефреймінг	10
Зараження	12
Психологічна ізоляція	4
Примус	2

Найбільш популярними дописами на каналі також стала тематика незаконної міграції з Білорусі до країни Європейського союзу.. Індикація рівнів критичності за оціночними параметрами каналу взагальному представлена на рис. 4.9.

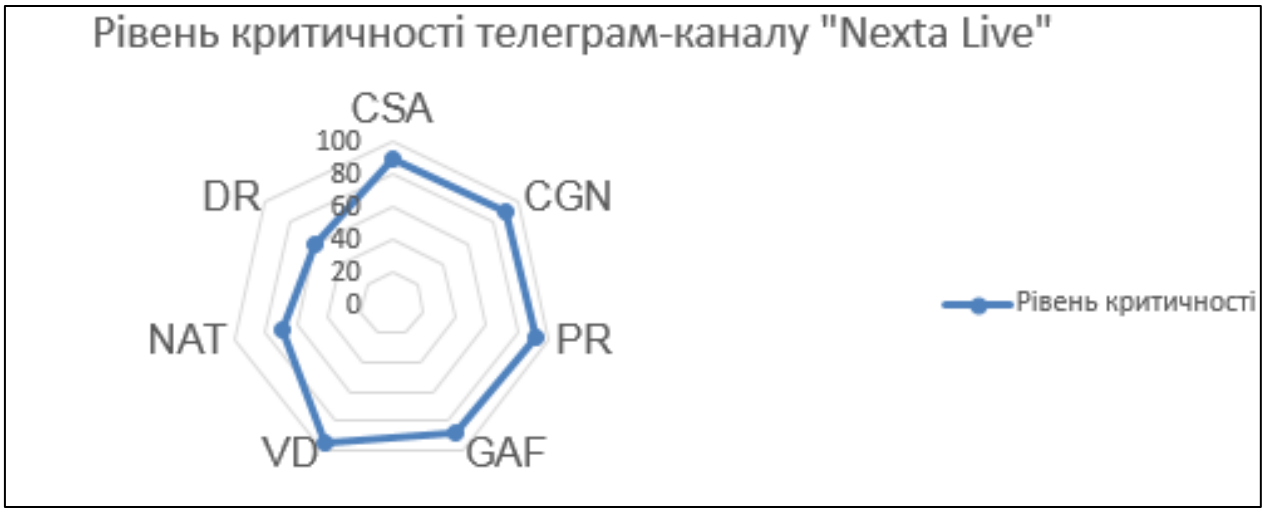


Рис. 4.9. Рівень критичності телеграму-каналу «Nexta Live»

У телеграм-каналі «Білорусь головного мозку» протягом вищевказаного періоду часу було виявлено наступну кількість видів інформаційно-психологічного впливу:

Табл. 4.3.

Результати виявлення та ідентифікації інформаційно-психологічного впливу в телеграм-каналі «Білорусь головного мозку»

Вид інформаційно-психологічного впливу	Кількість
Маніпулювання	15
Навіювання	19
Переконання	26
Дезінформація	3
Пропаганда	10
Рефреймінг	2
Зараження	3
Психологічна ізоляція	1
Примус	1

Найбільш популярними дописами на каналі також стала тематика незаконної міграції з Білорусі до країни Європейського союзу. Індикація рівнів критичності за оціночними параметрами каналу взагальному представлена на рис. 4.10.

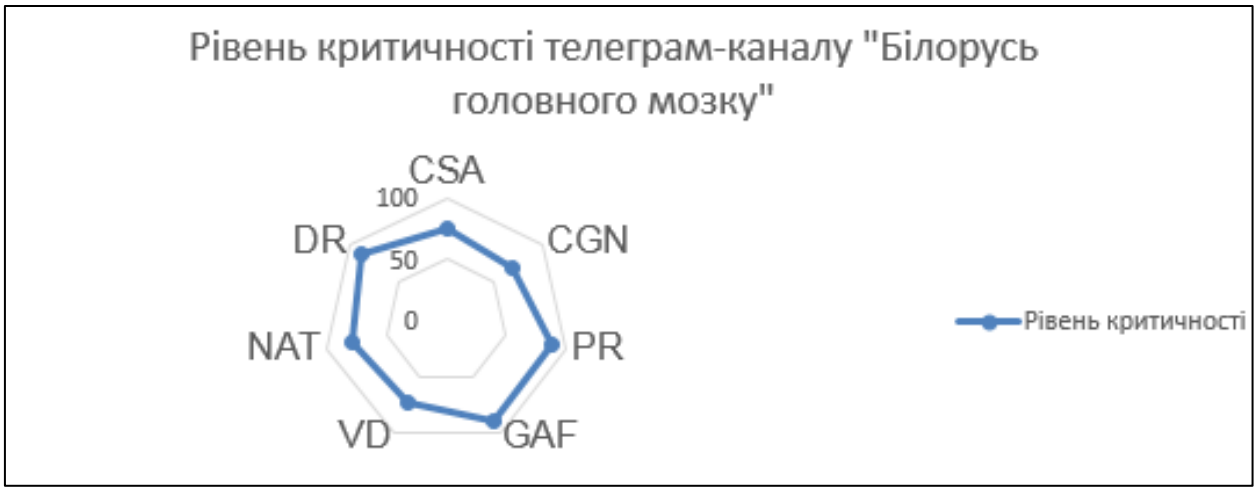


Рис. 4.10. Рівень критичності телеграму-каналу «Білорусь головного мозку»

У телеграм-каналі «Мая Краіна Беларусь» протягом вищевказаного періоду часу було виявлено наступну кількість видів інформаційно-психологічного впливу:

Табл. 4.4

Результати виявлення та ідентифікації інформаційно-психологічного впливу в телеграм-каналі «Мая Краіна Беларусь»

Вид інформаційно-психологічного впливу	Кількість
Маніпулювання	7
Навіювання	12
Переконання	18
Дезінформація	1
Пропаганда	11
Рефреймінг	2
Зараження	2
Психологічна ізоляція	0
Примус	2

Найбільш популярними дописами на каналі стала тематика підпільних антиурядових рухів. Індикація рівнів критичності за оціночними параметрами каналу взагальному представлена на рис. 4.11.

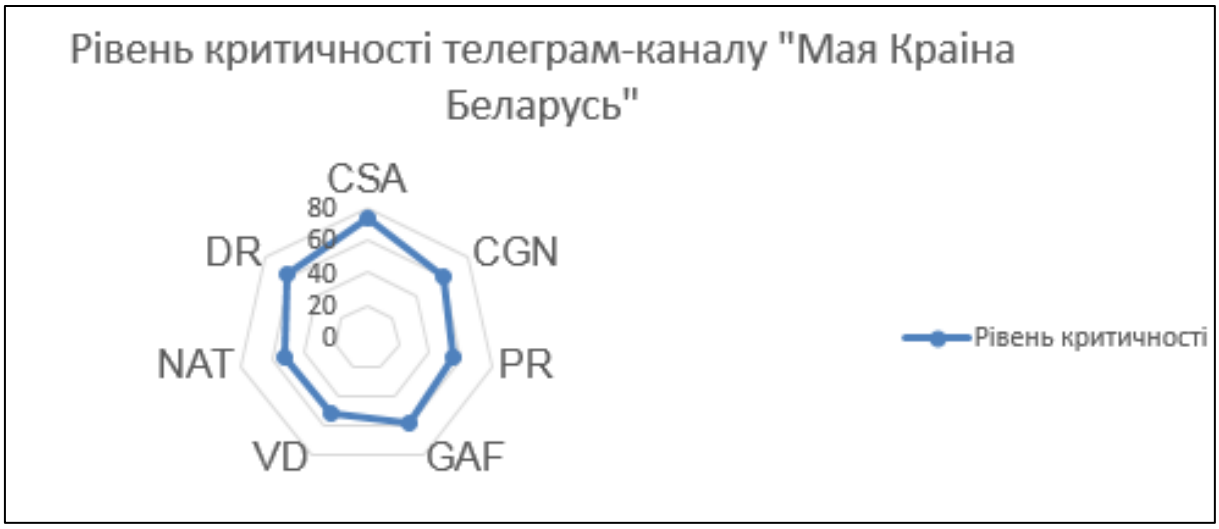


Рис. 4.11. Рівень критичності телеграму-каналу «Білорусь головного мозку»

У телеграм-каналі «Хартия’97%»» протягом вищевказаного періоду часу було виявлено наступну кількість видів інформаційно-психологічного впливу:

Табл. 4.5.

Результати виявлення та ідентифікації інформаційно-психологічного впливу в телеграм-каналі «Хартия’97%»»

Вид інформаційно-психологічного впливу	Кількість
Маніпулювання	5
Навіювання	10
Переконання	11
Дезінформація	1
Пропаганда	4
Рефреймінг	2
Зараження	5
Психологічна ізоляція	0
Примус	0

Найбільш популярними дописами на каналі стала тематика порушення прав людини в Білорусі. Індикація рівнів критичності за оціночними параметрами каналу взагальному представлена на рис. 4.12.

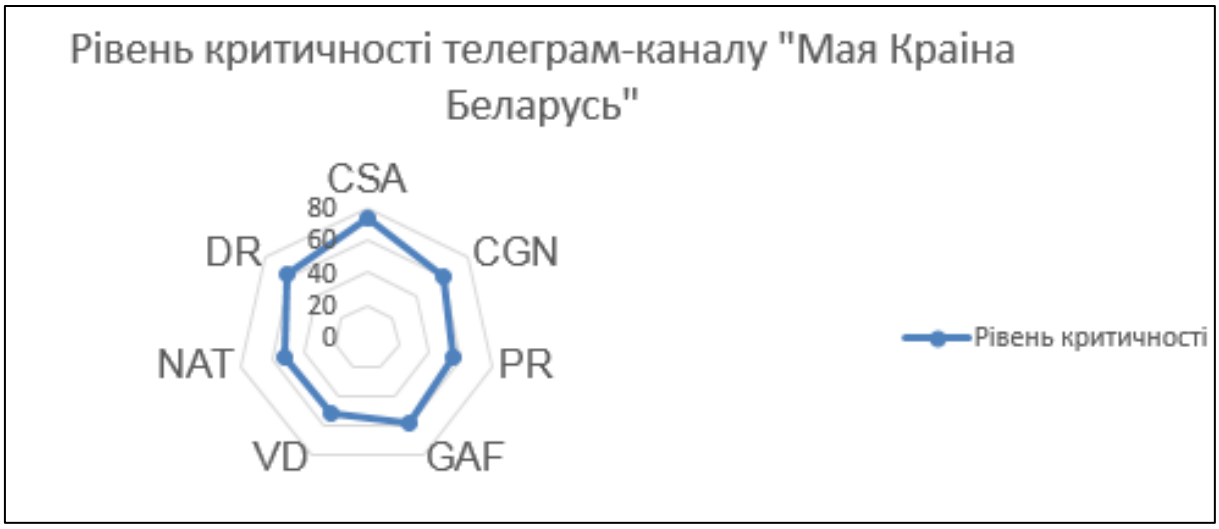


Рис. 4.12. Рівень критичності телеграму-каналу «Хартия'97%»

З вищенаведеного аналізу можна зробити висновок, що СУІПВ дала можливість користувачу проаналізувати та оцінити телеграм-канали на використання методів інформаційно-психологічного впливу, а також надала розуміння основних особливостей каналів, зважаючи на показники рівня критичності.

4.3.2. Дослідження спеціальних інформаційних операцій у пулі проросійських телеграм-каналів в українському інформаційному полі

Телеграм-канали в Україні стали незамінним джерелом новин, особливої популярності вони набули під час повномасштабного вторгнення росії до України 24 лютого 2022 року, як джерело альтернативної інформації та новин, про які ніколи не скажуть офіційні представники влади. Враховуючи особливості Telegram, а також майже повну відсутність модерації контенту, новинні канали заполонили собою український інформаційних простір. Цим намагалася скористатися рф створивши на початку вторгнення десятки псевдоофіційних регіональних каналів, де поширювала власні наративи. Як приклад можна назвати сітку каналів з назвами міст та приставкою «ru», а також канали угрупувань військ «Южный плацдарм» тощо. Але у зв'язку з численними поразками вони стали не актуальними і були або видалені, або їхня підтримка значно скоротилася. Інше місце займають новинні канали, які були створено задовго до дати вторгнення. Вони набирали популярність на тлі

політичних скандалів як джерела альтернативної точки зору та т.з. «інсайдів» з кабінетів влади. До цього пулу можна віднести наступні канали: «Легитимный», «Женщина с косой», «Резидент», «Разведчик», «Белый рыцарь», «Джокер», «Крокодил», «Соросята», «Картель», «Сплетница», «Чорний квартал» тощо. Їх перелік постійно оновлюється. Вони часто передруковують один одного, залучають ботів задля збільшення аудиторії, у деякій мірі можна зробити висновок про те, що вони керуються одним підрозділом, який має спільні задачі.

Експеримент з дослідження контенту пулу даних каналів тривав протягом грудня 2022 року – лютого 2023 року. Ціллю дослідження було виявлення трендів поширення інформації, ідентифікація видів ІПВ у них, а також оцінювання критичності публікацій.

Під час дослідження стандартними засобами Microfocus IDOL було виявлено 3 найбільш популярні тематики їхніх дописів: «розгром ЗСУ в Бахмуті», «енергетична криза», «західні партнери не надають належної підтримки Україні».

Продемонструємо результат експерименту з першої тематики – «розгром ЗСУ в Бахмуті». За досліджувальний час було зафіксовано 4 993 повідомлень у вищевказаному пулі каналів на дану тематику. Було визначено, що дані канали використовували наступні види ІПВ:

Табл. 4.6.

Результати виявлення та ідентифікації інформаційно-психологічного впливу в проросійсьму пулі телеграм-каналів на тематику «розгром ЗСУ в Бахмуті»

Вид інформаційно-психологічного впливу	Кількість
Маніпулювання	4 529
Навіювання	4 223
Переконання	3 597
Дезінформація	4 554
Пропаганда	1 891
Рефреймінг	1 421

Зараження	4 673
Психологічна ізоляція	3 268
Примус	2 001

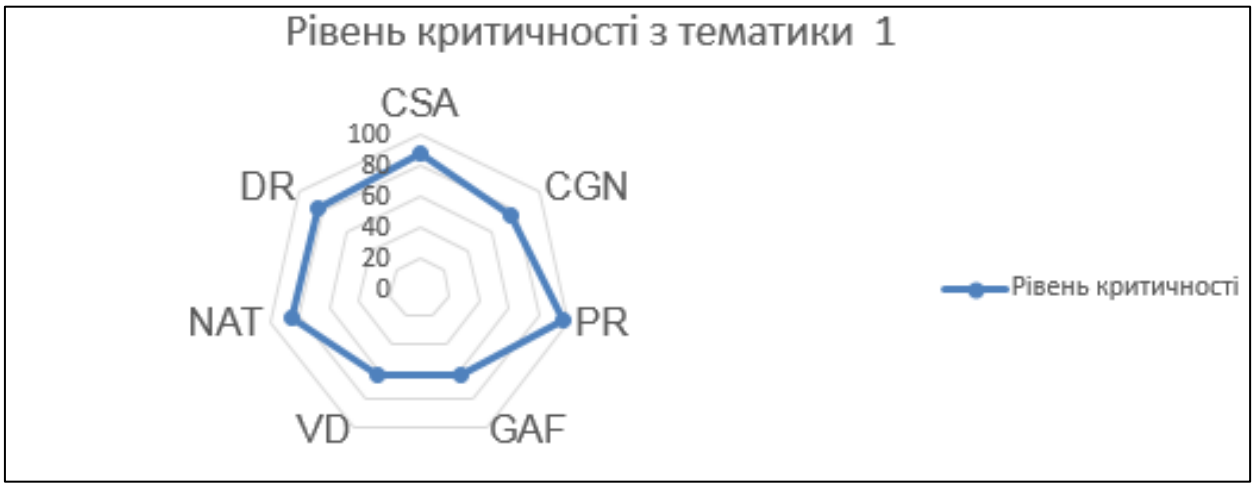


Рис. 4.13. Рівень критичності з тематики «розгром ЗСУ в Бахмуті»

Отже, як видно з рис. 4.13 пул каналів продемонстрував надзвичайно високий рівень критичності інформаційних матеріалів з тематики, отримавши менші оцінки лише за показниками «Зростання фактора тривожності» та «Швидкість розповсюдження». Перший показник можна пояснити тим, що вони постійно тримали у напрузі користувачів, не змінюючи тональності дописів, а другий тим, що вони перепощують дописи один одного, тим самим не значно збільшуючи свою аудиторію. Ці два показники імовірно постійно будуть триматися на одному й тому ж рівні.

4.3.3. Дослідження рівня критичності інформаційних повідомлень про Національний авіаційний університет

Під час цього дослідження перевірялася можливість СУІПВ оцінювати окремі дописи задля визначення їх впливу на аудиторію для управління іміджем в соціальних мережах. Предметом дослідження було обрано згадування про Національний авіаційний університет в провідних освітніх спільнотах. Дослідження проводилося з 1 по 30 квітня 2023 року. Об’єктом дослідження є групи в Facebook «Новини вищої освіти», «Вища освіта – портал», «Міністерство освіти і науки України» та окремі дописи, де згадується НАУ.

28 квітня 2023 року на інформаційній сторінці «Українська правда» було опубліковано наступний допис:

«Ректор Національного авіаційного університету Максим Луцький під час фестивалю «Студвесна» погрожував студентам через жарти про ексміністра освіти Сергія Шкарлета»

Рис. 4.14. Допис на сторінці «Українська правда» в мережі Facebook

Програмний засіб встановив наступі оціночні параметри для даного допису: CSA «Повнота та сила аргументації», CGN «Узгодженість з нормами загальносуспільної думки», GAF «Зростання фактора тривожності».

Нейронна мережа розробила наступні коефіцієнти важливості нечітких оціночних параметрів: $\Omega_1 = 0{,}115$; $\Omega_2 = 0{,}333$; $\Omega_3 = 0{,}552$.

Виміряні та аналітичні дані заносяться до таблиці і після процесу фазифікації визначається значення оціночних параметрів та обраховується показник рівня критичності в нечіткій формі, що далі після дефазифікації

переводиться в чітку форму, а результати відображаються на індикаторі критичності ситуації. В табл.. 4.7. наведені результати оцінки критичності обраного допису

Табл.4.7.

Результати оцінювання допису

Параметр	Коефіцієнт важливості	Нечітке число, що характеризує значення параметра	Дефазифіковане значення
CSA	0,115	{0/0,33; 0,75/0,75; 1/1}	80
CGN	0,333	{0/0,33; 0,92/0,66; 0,4/1}	57
GAF	0,552	{0/0,33; 0,44/0,66; 1/1}	83

Для відображення показника рівня критичності ситуації в лінгвістичній формі здійснюється процедура визначення відстань Хемінга між термами оціночного еталону та рівнем LCS. Провівши необхідні обчислення відстані Хемінга, за допомогою СОКС отримали, шо поточний рівень критичності ситуація «Високий». На рисунку 4.14 наведений індикатор критичності ситуації в процесі розвитку ІПВ для допису.

Рис. 4.15. Індикатор критичності ситуації

4.4. Висновки

1. Було розроблено систему управління інформаційно-психологічним впливом, яка включає в себе підсистеми моніторингу соціальних мереж, виявлення, ідентифікацію, оцінювання та маркування джерела дописів. Система побудована на основі методів виявлення та ідентифікації інформаційно-психологічного впливу, методу оцінювання критичності інформаційно-

психологічного впливу, а також методи протидії інформаційно-психологічному впливу в соціальних мережах.

У якості середовища розробки програмних засобів на основі системи обрано технологічну платформу Microfocus IDOL. MicroFocus IDOL (Intelligent Data Operating Layer) – це програмний продукт, який призначений для аналізу та обробки надмірної кількості даних різних типів, включаючи текст, зображення, аудіо та відео. IDOL володіє розширеними функціональними можливостями, які дозволяють витягувати інформацію з навіть найскладніших та неструктурованих даних. Завдяки використанню модуля NiagaraFiles платформа дозволяє налаштовувати свою роботу, а завдяки використанню в ньому штучного інтелекту вдалося автоматизувати та замінити роботу експертів з управління інформаційно-психологічним впливом.

2. Програмний комплекс перевірявся шляхом проведення 3 видів експериментів, які полягали в аналізі дописів конкретних публічних сторінок у соціальних мережах, аналізі пулу інформаційних повідомлень та оцінюванні конкретного допису за ключовими словами. Під час експериментів комплекс виконав усі поставлені до нього вимоги.

Програмно-апаратний комплекс «СУІПВ v.1.0» було впроваджено в роботу Центру психологічного, фізичного та мовленнєвого розвитку дитини «Динаміка» та почав використовуватися з 01.06.2023 року. За час роботи збільшися кількість відвідувань сторінок у соціальних мережах Центру, реакція на дописи, а також покращилося ставлення до бренду вцілому, про що опосередковано свідчить збільшення кількості відвідувачів.

Табл. 4.8.

Порівняння відвідування та реакції на дописи сторінок у соціальних мережах Центру психологічного, фізичного та мовленнєвого розвитку дитини «Динаміка»

Характеристика/проміжок часу	**01.03.2023-31.05.2023**	**01.06.2023-31.08.2023**	**Відсоткове відношення**
Відвідування сторінок у соціальних мережах	2253	3897	+73%

Кількість реакцій на дописи у соціальних мережах	411	624	+51,8%
Кількість відвідувачів	183	269	+47%

Як бачимо із табл. 4.8 використання «СУІПВ v.1.0» допомогло Центру психологічного, фізичного та мовленнєвого розвитку дитини «Динаміка» змінити свою стратегію в соціальних мережах, тим самим збільшивши кількість відвідувачів власних інформаційних сторінок та їх реакцію на дописи.

ВИСНОВКИ

У дисертаційній роботі, на основі запропонованих методів та проведених експериментальних досліджень розроблено систему управління інформаційно-психологічним впливом. В ході даної роботи було виконано ряд науково-технічних задач. А саме:

1. Проведено аналіз сучасних теоретичних підходів та засад, виявлення, ідентифікації та оцінювання інформаційно-психологічного впливу. Встановлено, що розроблені наразі методи мають як свої переваги, так і недоліки.

Проведено дослідження сучасних систем аналізу ефективності публічних сторінок у соціальних мережах. Встановлено, що вони не можуть ідентифікувати та оцінити інформаційні кампанії, які здійснюються щодо певних об’єктів.

Також проведено аналіз сучасних методів дослідження соціальних мереж, що дало можливість встановити характеристики поширення ІПВ в них, а також визначити ідентифікуючі параметри..

2. Розроблено функціональну та цільову моделі інформаційно-психологічного впливу, які характеризують інформаційне протиборство в соціальних мережах. З даних моделей формується множини ідентифікуючих і оціночних параметрів, евртситичних правил встановлення відповідності типу ІПВ до його харектристик.

Розроблено еталони ідентифікуючих та оціночних параметрів, набори евристичних правил ідентифікації інформаційно-психологічного впливу, що дозволяють використовувати методи нечіткої логіки в задачах ідентифікації та оцінювання критичності ІПВ.

3. Вперше розроблено метод виявлення та ідентифікації інформаційно-психологічного впливу, який базується на теоретичних засадах нечіткої логіки та дозволяє виконувати свої дії у слабоформалізованому нечіткому середовищі

й має можливість аналізувати контент соціальних мереж у режимі реального часу.

Розроблений метод дозволяє виявляти та ідентифіковувати конкретні види інформаційно-психологічного впливу, ефктивність якого буде максимальною під час аналізу каскаду інформаційних повідомлень у різних соціальних мережах, зважаючи на їх характеристики.

4. Розроблено метод оцінювання критичності інформаційно-психологічного впливу в соціальних мережах, відповідно до оціночних параметрів. Даний метод ґрунтується на кількісних методах експертної оцінки, що дає переваги у відсутності необхідності збору великих кількостей статистичних даних та чіткої формалізації поточної ситуації та елементах нечіткої логіки.

Розроблений метод надає можливість оцінювати критичність інформаційно-психологічного впливу щодо каскаду інформаційних повідомлень та конкретного допису. Таким чином він може допомогти в точному встановленні загроз інформаційному простору, іміджу та вибору адекватних засобів реагування.

5. Розроблено систему управління інформаційно-психологічним впливом. Дана система ґрунтується на раніше розроблених методах виявлення, ідентифікації та оцінювання інформаційно-психологічних впливів.

Розроблена система включає в себе підсистеми моніторингу, виявлення, ідентифікації та оцінювання критичності інформаційно-психологічних впливів та забезпечує процеси управління ІПВ від їх виявлення до формування рекомендацій щодо заходів протидії деструктивному інформаційно-психологічному впливу в соціальних мережах.

6. Розроблено програмно-апаратний комплекс на основі системи управління інформаційно-психологічного впливу, який дає змогу виявляти, однозначно ідентифікувати ІПВ, оцінювати його критичність в аспекті впливу на інформаційний простір та автоматизувати підбір відповідних типові ІПВ контрзаходів.

Роботу програмно-апаратного комплексу досліджено шляхом проведення експериментів. Експериментальні дослідження полягали в аналізі дописів конкретних публічних сторінок у соціальних мережах, аналізі пулу інформаційних повідомлень та оцінюванні конкретного допису за ключовими словами. Під час експериментів комплекс виконав усі поставлені до нього вимоги.

Крім того, використання «СУІПВ v.1.0» допомогло Центру психологічного, фізичного та мовленнєвого розвитку дитини «Динаміка» змінити свою стратегію в соціальних мережах, тим самим збільшивши кількість відвідувачів власних інформаційних сторінок на 73% та їх реакцію на дописи на 51,8%.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. A. Peleschyshyn, T. Klynina, & S. Gnatyuk (2019). Legal Mechanism of Counteracting Information Aggression in Social Networks: from Theory to Practice. *CEUR Workshop Proceedings*, Vol. 2392, pp. 111-121.

2. Al-Yazidi, S., Berri, J., Al-Qurishi, M., & Al-Alrubaian, M. (2020). Measuring reputation and influence in online social networks: a systematic literature review. *IEEE Access*, *8*, pp. 105824-105851.

3. Ananthaswamy, V., & Seethalakshmi, B. (2015). Mathematical analysis of information dissemination model for social networking services. *American Journal of Modeling and Optimization*, 3(1), pp. 26-34.

4. Banerjee, S., Jenamani, M., & Pratihar, D. K. (2020). A survey on influence maximization in a social network. *Knowledge and Information Systems*, *62*, pp. 3417-3455.

5. Cui, P., Yin, B., & Xu, B. (2023). The application of social recommendation algorithm integrating attention model in movie recommendation. *Scientific Reports*, *13*(1), pp. 169-188.

6. Dash, P., Dara, S., & Mishra, J. (2023). A fuzzy inference supportive social media market analysis for predicting crowd influence in national elections. *Multimedia Tools and Applications*, pp. 1-17.

7. Di Pietro, R., Raponi, S., Caprolu, M., Cresci, S., Di Pietro, R., Raponi, S., & Cresci, S. (2021). *New dimensions of information warfare*, pp. 1-4.

8. Dong, J., Chen, B., Liu, L., Ai, C., & Zhang, F. (2018). The analysis of influencing factors of information dissemination on cascade size distribution in social networks. *IEEE Access*, 6, 54185-54194.

9. Fedushko S, Davidekova M (2019) Analytical service for processing behavioral, psychological and communicative features in the online communication. Procedia Comput Sci 160:509–514.

10. Fraccastoro S, Gabrielsson M, Chetty S (2021) Social media firm specific advantages as enablers of network embeddedness of international entrepreneurial ventures. *J World Bus*, 56(3), pp. 101-164.

11. Gizun, A., Avkurova, Z., Hriha, V., Monashnenko, A., Akatayev, N., & Aleksander, M. (2021). Method for the Criticality Level Assessment for Crisis Situations with Parameters Fuzzification. *In Advances in Computer Science for Engineering and Education IV,* pp. 147-161.

12. Gizun, A., Hriha, V., Roshchuk, M., Yevchenko, Y., & Hu, Z. (2019). Method of informational and psychological influence evaluation in social networks based on fuzzy logic Control. *Optimisation and Analytical Processing of Social Networks: Proceedings of the 1st International Workshop (Lviv, May 16–17, 2019),* pp. 10–11.

13. Gizun, A., Pisarchuk, A., Hriha, V., Buriachok, V., & Berdibayev, R. (2019). Incidents Correlation Mechanism for Assessing Average and Total Criticality Level of Situation in the Infosphere. *In Proceedings of the International Workshop on Cyber Hygiene (CybHyg-2019)*. Vol. 2654, pp. 654-664.

14. Gnatyuk, S., Akhmetova, J., Sydorenko, V., Polishchuk, Yu., & Petryk, V. (2019). Quantitative Evaluation Method for Mass Media Manipulative Influence on Public Opinion. *CEUR Workshop Proceedings*, Vol. 2362, pp. 71-83.

15. Gnatyuk, S., Yudin, O., Sydorenko, V., Smirnova, T., & Polozhentsev, A. (2022) The model for calculating the quantitative criteria for assessing the security level of information and telecommunication systems. *CEUR Workshop Proceedings* 3156, 390–399.

16. Gong, Q., Chen, Y., He, X., Xiao, Y., Hui, P., Wang, X., & Fu, X. (2021). Cross-site prediction on social influence for cold-start users in online social networks. *ACM Transactions on the Web (TWEB)*, *15*(2), pp. 1-23.

17. Griga, V., Gizun, A., & Lanovyi, I. (2017). Formation of identifying parameters reference values of information and psychological impact. *VII Міжнародний Молодіжний Науковий Форум "Litteris Et Artibus",* С. 404-408.

18. Hriha, V. (2018). Information psychological impact detection and identification as a basis for counteracting information aggression. *Aviation in the XXI-st century. Safety in Aviation and Space Technologies: proceedings of the VIII world congress*, Рз. 3.1.16-3.1.18.

19. Hriha, V., Blidar, A., & Zakharchuk, O. (2019). Information interference of Russia in the election process in Ukraine in 2019. *9th International Youth Science Forum "Litteris et Artibus" & 14th International Conference «Young Scientists Towards The Challenges Of Modern Technology»*, pp. 65-74.

20. Hriha, V., Blidar, A., Roshchuk, M., & Derkach, S. (2019). Insider attacks system identification. *Project interdyscyplinarny projektem XXI wieku, Tom 2*, pp. 155-166.

21. Hriha, V., Gizun, A., & Shchudlyck, I. (2017) Information psychological impact detection and identification system. *Project interdyscyplinarny projektem XXI wieku. Tom 2,* pp. 131-149.

22. Hriha, V., Gizun, A., & Shchudlyck, I., (2017) Information psychological impact detection and identification system, *Project interdyscyplinarny projektem XXI wieku, Tom 2*, pp. 131-149.

23. Hryshchuk, R., & Molodetska, K. (2017). Synergetic control of social networking services actors' interactions. In Recent Advances in Systems. *Control and Information Technology: Proceedings of the International Conference SCIT 2016, May 20-21, 2016, Warsaw, Poland*, pp. 34-42.

24. Hryshchuk, R., & Molodetska-Hrynhchuk, K. (2018). Methodological foundation of state's information security in social networking services in conditions of hybrid war. *Information & Security*, 41.

25. Hryshchuk, R., Molodetska, K., & Syerov, Y. (2019). Method of improving the information security of virtual communities in social networking services.

26. Hryshchuk, R., Zhovnovatiuk, R., & Nosova, H. (2019). Гібридні загрози у кіберпросторі: фактори впливу на природу виникнення. *Сучасні інформаційні технології у сфері безпеки та оборони*, *36*(3), С. 53-58.

27. Hryshchuk, R.; Molodetska, K.; & Syerov, Y (2020) Method of Improving the Information Security of Virtual Communities in Social Networking Services. *Proceedings of the CEUR Workshop*, pp. 1754-1764.

28. Hryshchuk, R.; Molodetska, K.; & Syerov, Y (2020) Method of Improving the Information Security of Virtual Communities in Social Networking Services. Proceedings of the CEUR Workshop.

29. Khoroshko, V., Hryshchuk, R., Brailovskyi, N., & Shcherbak, T. (2020). The use of Game Theory to Study Processes in the Informational Confrontation. *Scientific and practical cyber security journal*.

30. Korobiichuk, I, Snitsarenko, P, Katsalap, V, Hryshchuk, R (2019) Determination and Evaluation of Negative Informational and Psychological Influence on the Military Personnel Based on the Quantitative Measure. *International Workshop On Control, Optimisation And Analytical Processing Of Social Networks*, 2392, pp. 66–78.

31. Lakhno, V.A., Kasatkin, D.Y., Blozva, A.I., Kozlovskyi, V., Balanyuk, Y., & Boiko, Y. (2020) The Development of a Model of the Formation of Cybersecurity Outlines Based on Multi Criteria Optimization and Game Theory *Advances in Intelligent Systems and Computing*, 1295, pp. 10-22.

32. Lande, D., & Feher, A. (2023). OSINT Time Series Forecasting Methods Analysis. *Theoretical and Applied Cybersecurity*, *5*(1).

33. Promoting Psychological Resilience in the U.S. Military. (2011). *Published Santa Monica. RAND Corporation*. 186 p.

34. Pysarchuk, O., Gizun, A., Dudnik, A., Griga, V., Domkiv, T., & Gnatyuk, S. (2019). Bifurcation Prediction Method for the Emergence and Development Dynamics of Information Conflicts in Cybernetic Space. *In Proceedings of the International Workshop on Cyber Hygiene (CybHyg-2019)*. Vol. 2654, pp. 692-709.

35. R. Hryshchuk, K. Molodetska, & Y. Tymonin, (2019) Modelling of conflict interaction of virtual communities in social networking services on an example of anti-vaccination movement, *Proc. of the Int. Workshop on Conflict Management in Global Information Networks*, vol. 2588, pp. 250-264.

36. R. Hryshchuk, K. Molodetska, & Y. Tymonin, (2019). Modelling of conflict interaction of virtual communities in social networking services on an example of anti-vaccination movement. *Proc. International Workshop on Conflict Management in Global Information Networks*, pp. 250-264.

37. Ryabyy M., Hatyan O., & Bagatskyy S. (2015) The model of PR-impact detection by means of Internet mass-media. *Ukrainian Scientific Journal of Information Security*, vol. 21, issue 2, p. 131-139.

38. Tolubko, V., Kozelkov, S., Zybin, S., Kozlovskyi, V., & Boiko, Y. (2019). Criteria for evaluating the effectiveness of the decision support system. *Advances in Intelligent Systems and Computing*, 754, pp. 320–330.

39. Yevseiev, S., Katsalap, V., Mikhieiev, Y., Savchuk, V., Pribyliev, Y., Milov, O., & Korol, I. (2022). Development of a method for determining the indicators of manipulation based on morphological synthesis. *Eastern-European Journal of Enterprise Technologies*, 117(9).

40. Yevseiev, S., Ryabukha, Y. ., Milov, O., Milevskyi, S., Pohasii, S., Melenti, Y., Ivanchenko, Y., Ivanchenko, I., Opirskyy, I., & Pasko, I. (2021). Development of a method for assessing forecast of social impact in regional communities. *Eastern-European Journal of Enterprise Technologies*, 6(114), pp. 30–43.

41. Zahran, B., Al-Azzeh, J., Gizun, A., Griga, V., & Bystrova B. (2019). Developing an expert system for assessment of information-psychological influence. *Indonesian Journal of Electrical Engineering and Computer Science*, 15(3), pp. 1571-1577.

42. Zgurovsky, M., Lande, D., Dmytrenko, O., Yefremov, K., Boldak, A., & Soboliev, A. (2023). Technological Principles of Using Media Content for Evaluating Social Opinion. In *System Analysis and Artificial Intelligence*, pp. 379-396.

43. Zgurovsky, M., Lande, D., Yefremov, K., Dmytrenko, O., Boldak, A., & Soboliev, A. (2022, October). Extracting and Identifying Relationships of Key Phrases in Information Flows. In *2022 IEEE 3rd International Conference on System Analysis & Intelligent Computing (SAIC)*, pp. 1-5.

44. Zhang, M., Zhao, Y., Ivanovych, S. Y., Lande, D., Zhu, S., Yu, J., ... & Li, S. (2022, December). Evaluation and Analysis of Shandong Digital Economy Construction. In *2022 International Conference on Computer Science, Information Engineering and Digital Economy (CSIEDE 2022)*, pp. 628-638.

45. Zhuravskaya, E., Petrova, M., & Enikolopov, R. (2020). Political effects of the internet and social media. *Annual review of economics*, *12*, pp. 415-438.

46. А., Гізун, & В., Гріга (2020). Модель інформаційного впливу Російської Федерації на виборчий процес в Україні в 2019 році. *Матеріали Шостої всеукраїнської науково-практичної конференції «Перспективні напрями захисту інформації»*, С. 60-64.

47. А., Гізун, & В., Гріга (2023). Визначення базових параметрів для оцінювання інформаційно-психологічного впливу. *Захист інформації і безпека інформаційних систем: матеріали IX Міжнар. наук.-техн. конф. Львів: Видавництво Львівської політехніки,* С. 23-24.

48. Бєльська, Т. В. (2014) Інформаційно-психологічна війна як спосіб впливу на громадянське суспільство та державну політику держави.*Технології та механізми державного управління*, 3, С. 49-56.

49. Богданович, В.Ю., & Висідалко, А.Л. (2014). Концептуальна модель інформаційно-моніторингової системи національної безпеки. *Захист інформації,* 16, С. 81-89.

50. Бойко, Ю. В. (2021). Соціальні мережі як зброя та інструмент впливу в умовах інформаційної війни. *Вісник студентського наукового товариства ДонНУ імені Василя Стуса*, *1*(13), С. 235-239.

51. Бочаров, М. М., & Приймак, М. В. (2016) Досвід використання методик оцінювання негативного інформаційно-психологічного впливу в прогнозуванні морально-психологічного стану військ у бойових умовах. *Сучасні інформаційні технології у сфері безпеки та оборони*, 1, С. 15-19.

52. Бочаров, М.М. (2015). Завдання захисту загальновійськових підрозділів від негативного інформаційно-психологічного впливу в ході антитерористичної операції. *Сучасні інформаційні технології у сфері безпеки та оборони*, 1. С. 139-143.

53. Браіловський, М. М., Іванченко, І. С., Опірський, І. Р., & Хорошко, В. О. (2019). Інформаційно-психологічне протиборство в Україні. *Безпека інформації*, 25(3), С. 144-149.

54. В., Гріга, & А. ,Гізун (2019). Експериментальне дослідження методу виявлення та ідентифікації інформаційно-психологічного впливу. *ITSec: Безпека інформаційних технологій: IX міжнародна науково-технічна конференція, 22-27 березня 2019 р.*, С. 30-31.

55. Волянська, В. В., Гізун, А. І., & Гнатюк, В. О. (2013) Моделі еталонів лінгвістичних змінних для систем виявлення та ідентифікації порушника інформаційної безпеки. *Безпека інформації*. 19 (1). С. 13-21.

56. Гізун, А., & Гріга, В. (2016). Аналіз сучасних теорій інформаційно-психологічних впливів в аспекті інформаційного протиборства. *Безпека інформації*, 22(3), С. 272-282.

57. Гізун, А.І. (2013). Евристичні правила на основі логіко–лінвистичних зв'язок для виявлення та ідентифікації порушника інформаційної безпеки. *Захист інформації*, 3(60), С.251-257.

58. Гізун, А.І. (2013). Основні параметри для ідентифікації порушника інформаційної безпеки. *Захист інформації,* 1(58), С.66-75.

59. Гізун, А.І. (2015) Формалізована модель побудови евристичних правил для виявлення інцидентів. *Вісник Інженерної академії України*, №1, С. 110-115.

60. Гнатієнко, Г.М., & Снитюк, В.Є. (2012). Експертні технології прийняття рішень. *Системи підтримки прийняття рішень. Теорія і практика,* 3, С. 24-29.

61. Говоруха В.В., Даник Ю.Г, & Кливець В.М. (2008). Сучасні форми інформаційно-психологічного протиборства в міждержавних стосунках, *Теорія та практика державного управління*, 3, С. 3-10.

62. Горбань, Ю. О. (2015). Інформаційна війна проти України та засоби її ведення. *Вісник Національної академії державного управління при Президентові України*, 1, С. 136-141.

63. Горбулін, В. П. (2014). Гібридна війна як ключовий інструмент російської геостратегії реваншу. *Стратегічні пріоритети*, 4, С. 5.

64. Горбулін, В. П. (2014). Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія. Інтертехнологія. 164 с.

65. Горніцька, Д. А., Волянська, В. В., & Корченко, А. О. (2012). Визначення коефіцієнтів важливості для експертного оцінювання у галузі інформаційної безпеки. *Захист інформації,* 14(1), с. 54-62.

66. Гоцур, О. (2021). Соціальні мережі та блоги як інструменти реалізації PR-кампанії. *Вісник Львівського університету. Серія Журналістика.. Випуск 50. С. 3–12.*

67. Грабовецький, Б.Є. (2010). Методи експертних оцінок: теорія, методологія, напрямки використання. ВНТУ. 171 с.

68. Грига, В. С., & Кобильнык, Б. Ю. (2018). Функциональная и целевая модели информационнопсихологического воздействия . *Современные средства связи: тезисы доклада XXIII междунар. науч.-тех. конф.(г. Минск, 18-19 октября 2018 г.)*, С. 32 -36.

69. Грига, В., Гнатюк, С., & Гизун, А. (2015). Информационно-психологическая безопасность общества, как средство сохранения народа. *Безпека інформації*, 21(2), С. 179-190.

70. Грищук, Р. В. (2013). Методика оцінювання рівня небезпеки кібернетичних загроз. *Сучасний захист інформації*, Спецвипуск, С. 23-28.

71. Грищук, Р., Даник, Ю., (2010) Основи кібернетичної безпеки, ЖНАЕУ, 636 с.

72. Гріга, В. (2017). Цільова та функціональна моделі інформаційно-психологічного впливу. *Збірник тез X Всеукраїнської студентської науково-технічної конференції „Природничі та гуманітарні науки. Актуальні питання*“, С. 49-50.

73. Гріга, В. С., & Гізун, А. І. (2023). Інформаційно-психологічний вплив як чинник військового протиборства. *Інтегровані інтелектуальні робототехнічні комплекси (ІІРТК-2023). Шістнадцята міжнародна науково-практична конференція 23-24 травня 2023 р., Київ, Україна,* С. 316-317.

74. Гріга, В. С., Гізун А. І., & Іванченко І. С., (2016). Характеристика базових складових інформаційного протиборства. *Матеріали Другої всеукраїнської науково-практичної конференції «Перспективні напрями захисту інформації»*, С. 22-25.

75. Гріга, В. С., Каданова, В. О., & Гізун, А. І. (2017). Архітектура системи виявлення та ідентифікації інформаційно-психологічного впливу. *Матеріали Третьої всеукраїнської науково-практичної конференції «Перспективні напрями захисту інформації»*, 26-28.

76. Гріга, В.С., Щудлик, І.А. (2018) Формування множини параметрів оцінки інформауійнопсихологічного впливу. *Стан та удосконалення безпеки*

інформаційнотелекомунікаційних систем (SITS'2018): тези доп. X Всеукр. наук.практ. конф. (Миколаїв-Коблево, 21-23 червня 2018 р.), С. 21-23.

77. Дудатьев, А. В. (2016). Метод оценки информационной устойчивости социотехнических систем в условиях информационной войны. *Восточно-Европейский журнал передовых технологий*, 1, С.4-11.

78. Дудатьєв, А. В., & Войтович, О. П. (2017). Інформаційна безпека соціотехнічних систем: Модель інформаційного впливу. *Інформаційні технології та комп'ютерна інженерія*, 1(38), С. 16-21.

79. Жаровська, І., & Ортинська, Н. (2020). Інформаційна війна як сучасне глобалізаційне явище. *Вісник Національного університету «Львівська політехніка». Серія: Юридичні науки*, 2(26), С. 56-61.

80. Інформаційна безпека держави у контексті протидії інформаційним війнам.Навчальний посібник (2008), НАОУ. 177с.

81. Інформаційна безпека: Підручник (2010). КНТ, 776 с.

82. Історія інформаційно-психологічного протиборства: підруч. (2012), Наук.-вид. відділ НА СБ України, 212 с.

83. Карпінський ,М.П. (2015). Метод виявлення інцидентів/потенційних кризових ситуацій. *Захист інформації*, 17(2), С. 124-130.

84. Карпінський, М.П. (2015). Інтегрована модель представлення кризових ситуацій та формалізована процедура побудови еталонів ідентифікуючих параметрів. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. 1(29), С. 76 - 85.

85. Кондратюк, М. О. (2013). Інформаційна війна та роль мас-медіа в міжнародних конфліктах. *Вісник Харківської державної академії культури*, 41, С. 108-113.

86. Корченко, А. (2014). Метод формирования лингвистических эталонов для систем выявления вторжений. *Захист інформації*, 16(1), С. 5-12.

87. Корченко, А.А. (2014). Метод фаззификации параметров на лингвистических эталонах для систем выявления кибератак. *Безпека інформації*, 1(20), С. 21-28.

88. Корченко, А.Г. (2006). Построение систем защиты информации на нечетких множествах : Теория и практические решения. МКПресс, 320 с.

89. Корченко, А.О. (2014). Метод α–рівневої номіналізації нечітких чисел для систем виявлення вторгнень. *Захист інформації*, 16(4), С. 304-311.

90. Ланде, Д. В., & Дмитренко, О. О. (2022). Побудова семантичних мереж та визначення ступеня розбіжності текстів. *Інформація і право*, 2(41), С. 44-51.

91. Ландэ, Д.В., Снарский, А.А., & Безсуднов, И.В. (2009). Интернетика. Навигация в сложных сетях: модели и алгоритмы. Книжный дом «ЛИБРОКОМ», 264 с.

92. М.Г., Луцкий, А.А., Корченко, А.В., Гавриленко, А.А., Охрименко (2012). Модели эталонов лингвистических переменных для систем выявления атак. *Захист інформації*, 2(55), С. 71- 78.

93. Магда, Є. В. (2014). Виклики гібридної війни: інформаційний вимір. *Scientific Papers of the Legislation Institute of the Verkhovna Rada of Ukraine*, 5, С. 138-142.

94. Мак-Квейл, Д. (2010). Теорія масової комунікації. Літопис. 537 с.

95. Молодецька-Гринчук, К. В. (2017). Метод виявлення ознак інформаційних впливів у соціальних інтернет-сервісах за змістовними ознаками. *Радіоелектроніка, інформатика, управління,* 2, С. 117-126.

96. Нікіфорова, Л.О. (2014). Моделювання вибору оптимального методу протидії загрозам інформаційній безпеці. *Реєстрація, зберігання і обробка даних*, 16(4), С.28-33.

97. Нікіфорова. Л.О. (2014). Модель та методи управління інформаційною безпекою соціальних груп під час впровадження другого рівня пенсійної реформи в Україні. *Безпека інформації,* 20(3), С. 300-305.

98. Пелещишин, А.М. (2014). Модель інформаційного середовища віртуальної спільноти. *Східно-Європейський журнал передових технологій*, 2/2 (68), С. 10-16.

99. Почепцов, Г. (2015). Сучасні інформаційні війни. Вид. дім «Києво-Могилянська академія», 497 с.

100. Редчук, Р. О. (2022). Особливості використання соціальних мереж у публічному управлінні як сучасного каналу комунікації. *Вчені записки ТНУ імені ВІ Вернадського. Серія: Публічне управління та адміністрування*, *33*(72), С. 72-76.

101. Синчак, Б. (2022). Прямоефірна інформаційна війна та російсько-українська війна 2022-го на медійному плацдармі. *Український інформаційний простір*, 2(10), С. 85–97.

102. Теорія інформації і кодування : навч. посіб. (2008). Вінниц. нац. техн. ун-т. Вінниця, 145 с.

103. Фролов, П.Д. (2008). Види інформаційно-психологічних впливів та проблема прогнозування їхніх наслідків. *Людина у світі інформації: Матеріали наукового семінару "Соціально-психологічні проблеми медіа освіти: від медіа безпорадності до медіа залежності"*, С. 5- 8.

104. Хатян, О.А. (2011). Інформаційно-комунікативна модель суспільної комунікації як основа дослідження соціально-економічних явищ. *Сучасні інформаційні технології у сфері безпеки та оборони*, 3(12), С. 66–71.

105. Шиян, А.А. (2014). Метод захисту людини від негативного інформаційно-психологічного впливу на основі типології діяльності. *Інформаційна безпека*, 3(15), С.92-99.

106. Шиян, А.А. (2014). Модель та методи захисту структурованої соціальної групи від негативного інформаційно-психологічного впливу. *Захист інформації*, 16(4), С. 311-317.

107. Шиян, А.А. (2015). Модель процесу просторового розповсюдження суспільної думки в задачах управління інформаційною безпекою. *Сучасний захист інформації*, 2, С. 34-39.

108. Шиян, А.А., & Яремчук, Ю.Є. (2014). Модель та методи захисту структурованої соціальної групи від негативного інформаційно-психологічного впливу. *Захист інформації*, 16(4), С.311-317.

109. Штефанюк, Є.Ф., Опірський, І.Р., & Гарасимчук, О.І. (2020). Аналіз застосування існуючих технік розпізнавання фейкових новин для протидії інформаційній пропаганді. *Безпека інформації*, 26(3), С. 139-144.

110. Яремчук, Ю. Є. (2015). Моделювання взаємодії державних структур і ЗМІ під час надзвичайних ситуацій. *Реєстрація, зберігання і обробка даних,* 17(1), С. 121-128.

ДОДАТОК А

Множина евристичних правил для виявлення «Переконання»

P	P_{LT}	P_{PN}	P_{PP}	Результат
1	К	М	М	Н
2	К	М	М	Н
3	К	М	М	Н
4	К	М	М	Н
5	К	М	М	Н
6	К	М	М	Н
7	К	М	М	Н
8	К	М	М	С
9	К	М	М	С
10	С	С	С	С
11	С	С	С	С
12	С	С	С	С
13	С	С	С	С
14	К	М	М	С
15	С	С	С	В
16	С	С	С	В
17	С	С	С	В
18	С	С	С	В
19	Д	В	В	В
20	Д	В	В	В
21	Д	В	В	В
22	Д	В	В	К
23	Д	В	В	К
24	Д	В	В	К
25	Д	В	В	К
26	Д	В	В	К
27	Д	В	В	К

Множина евристичних правил для виявлення «Психологічна ізоляція»

P	P_{LT}	P_{PP}	P_{IF}	Результат
1	К	М	Н	Н
2	К	М	Н	Н
3	К	М	Н	Н
4	К	М	Н	Н
5	К	М	Н	Н
6	К	М	Н	Н
7	К	М	Н	Н
8	К	М	Н	Н
9	К	М	Н	Н
10	С	С	С	С
11	С	С	С	С
12	С	С	С	С
13	С	С	С	С
14	С	С	С	С
15	С	С	С	С
16	С	С	С	С
17	С	С	С	С
18	С	С	С	С
19	Д	В	В	В
20	Д	В	В	В
21	Д	В	В	В
22	Д	В	В	В
23	Д	В	В	В
24	Д	В	В	В
25	Д	В	В	В
26	Д	В	В	В
27	Д	В	В	В
P	P_{LT}	P_{PP}	P_{IF}	Результат

Продовження додатку А

Множина евристичних правил для виявлення «Дезінформації»

p	P_{LT}	P_{PN}	P_{IF}	Результат
1	К	М	Н	Н
2	К	М	Н	Н
3	К	М	Н	Н
4	К	М	Н	Н
5	К	М	Н	Н
6	К	М	Н	Н
7	К	М	Н	Н
8	К	М	Н	Н
9	К	С	Н	Н
10	С	С	С	С
11	С	С	С	С
12	С	С	С	С
13	С	С	С	С
14	С	С	С	С
15	С	С	С	С
16	С	С	С	С
17	С	С	С	С
18	С	С	С	С
19	Д	В	В	В
20	Д	В	В	В
21	Д	В	В	В
22	Д	В	В	В
23	Д	В	В	В
24	Д	В	В	В
25	Д	В	В	В
26	Д	В	В	В
27	Д	В	В	В

Множина евристичних правил для виявлення «Пропаганди»

P	P_{LT}	P_{PP}	P_{CG}	Результат
1	К	М	Н	Н
2	К	М	Н	Н
3	К	М	Н	Н
4	К	М	Н	Н
5	К	М	Н	Н
6	К	М	Н	Н
7	К	М	Н	Н
8	К	М	Н	Н
9	К	М	Н	Н
10	С	С	Ч	С
11	С	С	Ч	С
12	С	С	Ч	С
13	С	С	Ч	С
14	С	С	Ч	С
15	С	С	Ч	С
16	С	С	Ч	С
17	С	С	Ч	С
18	С	С	Ч	С
19	Д	В	П	В
20	Д	В	П	В
21	Д	В	П	В
22	Д	В	П	В
23	Д	В	П	В
24	Д	В	П	В
25	Д	В	П	В
26	Д	В	П	В
27	Д	В	П	В

Продовження додатку А

Множина евристичних правил для виявлення «Зараження»

P	P_{PM}	P_{PP}	P_{IF}	result
1	Н	М	Н	Н
2	Н	М	Н	Н
3	Н	М	Н	Н
4	Н	М	Н	Н
5	Н	М	Н	Н
6	Н	М	Н	Н
7	Н	М	Н	Н
8	Н	М	Н	Н
9	Н	М	Н	Н
10	С	С	С	С
11	С	С	С	С
12	С	С	С	С
13	С	С	С	С
14	С	С	С	С
15	С	С	С	С
16	С	С	С	С
17	С	С	С	С
18	С	С	С	С
19	В	В	В	В
20	В	В	В	В
21	В	В	В	В
22	В	В	В	В
23	В	В	В	В
24	В	В	В	В
25	В	В	В	В
26	В	В	В	В
27	В	В	В	В

Множина евристичних правил для виявлення «Маніпулювання»

p	P_{PN}	P_{LT}	P_{CG}	Результат
1	М	К	Н	Н
2	М	К	Н	Н
3	М	К	Н	Н
4	М	К	Н	Н
5	М	К	Н	Н
6	М	К	Н	Н
7	М	К	Н	Н
8	М	К	Н	Н
9	М	К	Н	С
10	С	С	Ч	С
11	С	С	Ч	С
12	С	С	Ч	С
13	С	С	Ч	С
14	С	С	Ч	С
15	С	С	Ч	С
16	С	С	Ч	С
17	С	С	Ч	С
18	С	С	Ч	С
19	В	Д	П	В
20	В	Д	П	В
21	В	Д	П	В
22	В	Д	П	В
23	В	Д	П	В
24	В	Д	П	В
25	В	Д	П	В
26	В	Д	П	В
27	В	Д	П	В

Продовження додатку А

Множина евристичних правил для виявлення «Рефреймінгу»

P	P_{PM}	P_{PN}	P_{CG}	Результат
1	Н	М	Н	Н
2	Н	М	Н	Н
3	Н	М	Н	Н
4	Н	М	Н	Н
5	Н	М	Н	Н
6	Н	М	Н	Н
7	Н	М	Н	Н
8	Н	М	Н	Н
9	Н	С	Н	Н
10	С	С	Ч	С
11	С	С	Ч	С
12	С	С	Ч	С
13	С	С	Ч	С
14	С	С	Ч	С
15	С	С	Ч	С
16	С	С	Ч	С
17	С	С	Ч	С
18	С	С	Ч	С
19	В	В	П	В
20	В	В	П	В
21	В	В	П	В
22	В	В	П	В
23	В	В	П	В
24	В	В	П	В
25	В	В	П	В
26	В	В	П	В
27	В	В	П	В

Множина евристичних правил для виявлення «Навіювання»

P	P_{PN}	P_{PP}	P_{CG}	result
1	М	М	Н	Н
2	М	М	Н	Н
3	М	М	Н	Н
4	М	М	Н	Н
5	М	М	Н	Н
6	М	М	Н	Н
7	М	М	Н	Н
8	М	М	Н	Н
9	М	М	Н	Н
10	С	С	Ч	С
11	С	С	Ч	С
12	С	С	Ч	С
13	С	С	Ч	С
14	С	С	Ч	С
15	С	С	Ч	С
16	С	С	Ч	С
17	С	С	Ч	С
18	С	С	Ч	С
19	В	В	П	В
20	В	В	П	В
21	В	В	П	В
22	В	В	П	В
23	В	В	П	В
24	В	В	П	В
25	В	В	П	В
26	В	В	П	В
27	В	В	П	В

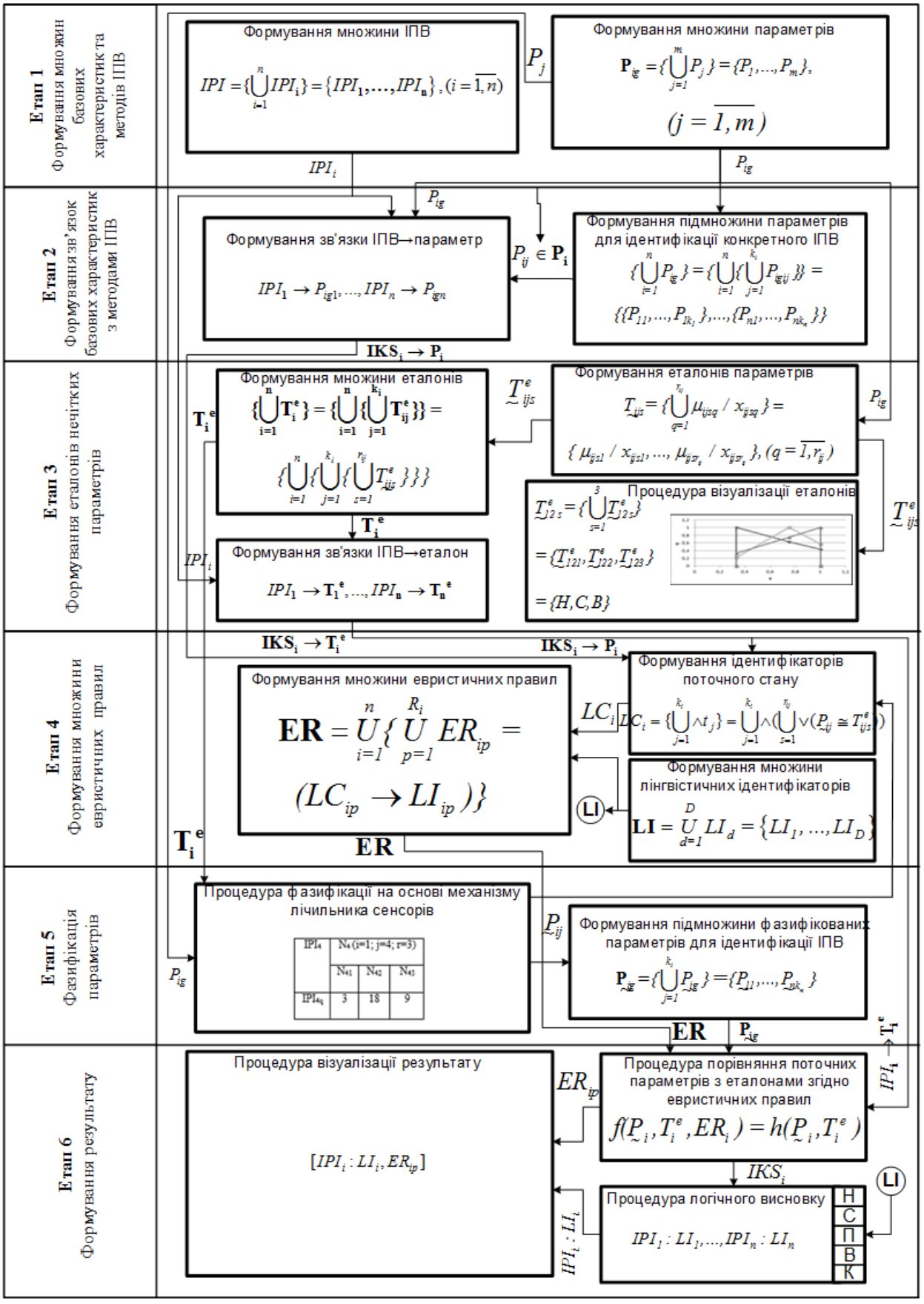
Продовження додатку А

Множина евристичних правил для виявлення «Примус»

p	P_{CG}	P_{PM}	P_{IF}	Результат
1	Н	Н	Н	Н
2	Н	Н	Н	Н
3	Н	Н	Н	Н
4	Н	Н	Н	Н
5	Н	Н	Н	Н
6	Н	Н	Н	Н
7	Н	Н	Н	Н
8	Н	Н	Н	Н
9	Н	Н	Н	Н
10	Ч	С	С	С
11	Ч	С	С	С
12	Ч	С	С	С
13	Ч	С	С	С
14	Ч	С	С	С
15	Ч	С	С	С
16	Ч	С	С	С
17	Ч	С	С	С
18	Ч	С	С	С
19	П	В	В	Д
20	П	В	В	Д
21	П	В	В	Д
22	П	В	В	Д
23	П	В	В	Д
24	П	В	В	Д
25	П	В	В	Д
26	П	В	В	Д
27	П	В	В	Д

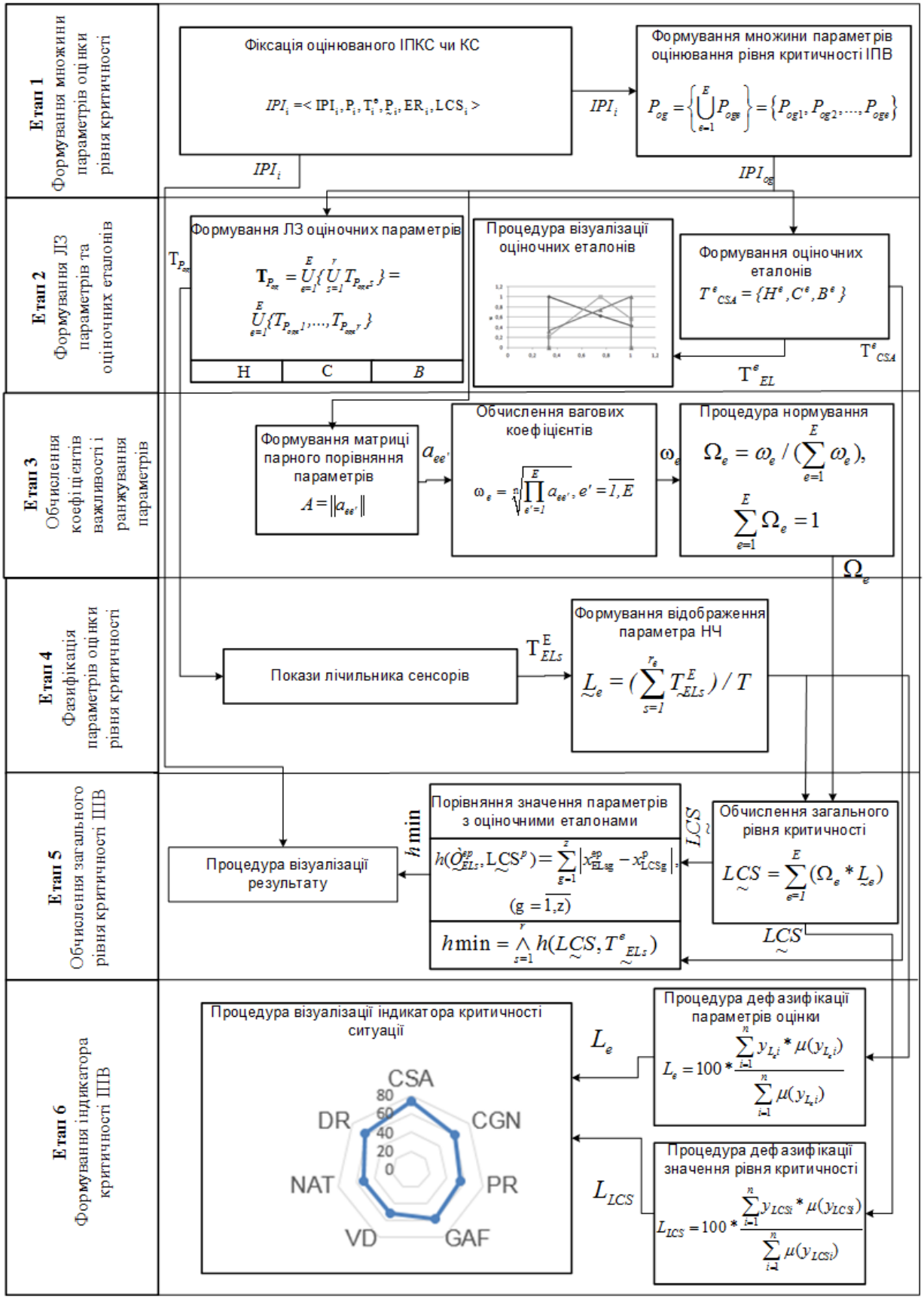
ДОДАТОК Б

Метод виявлення та ідентифікації ІПВ



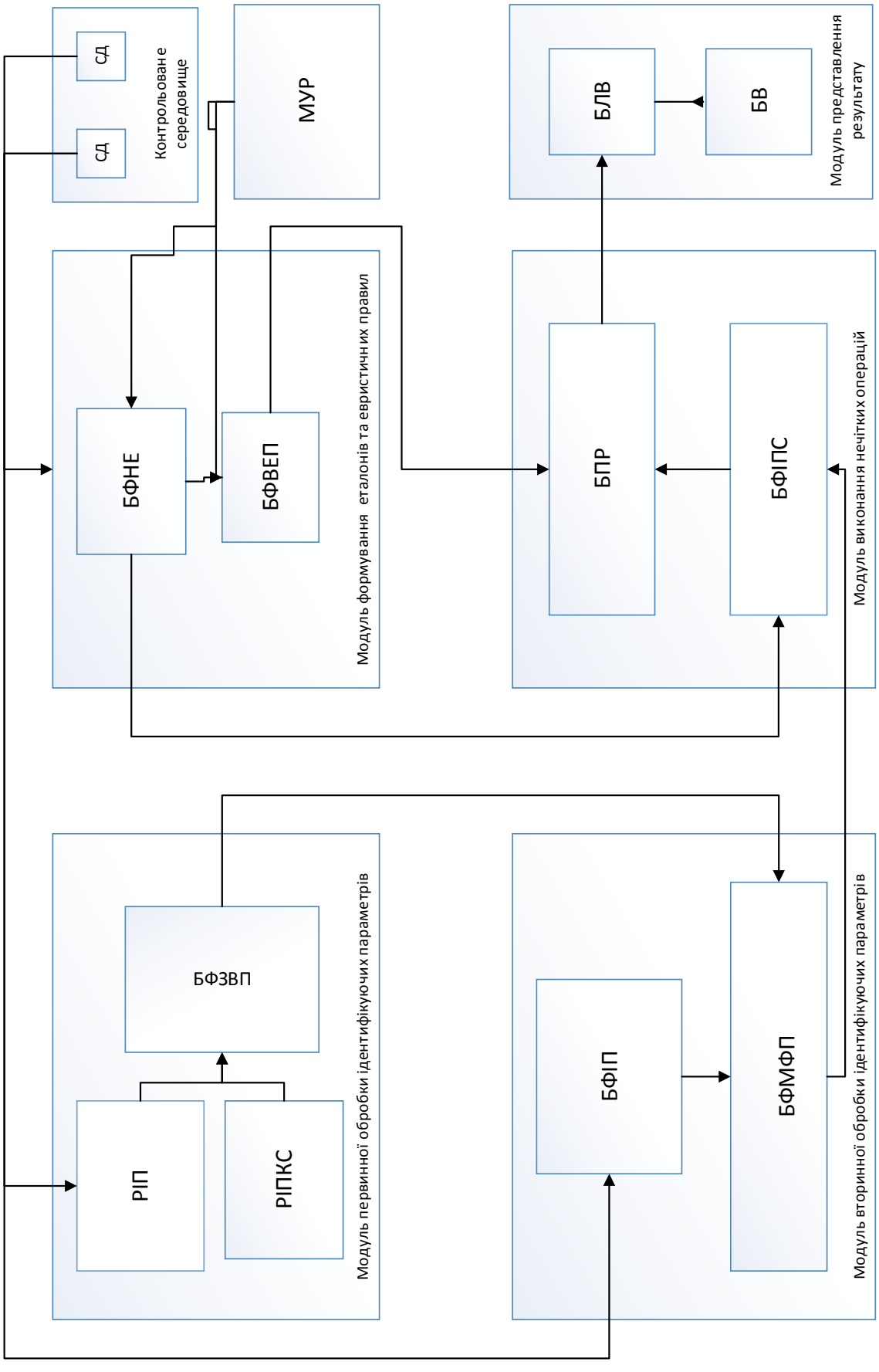
ДОДАТОК В

Метод оцінювання ІПВ



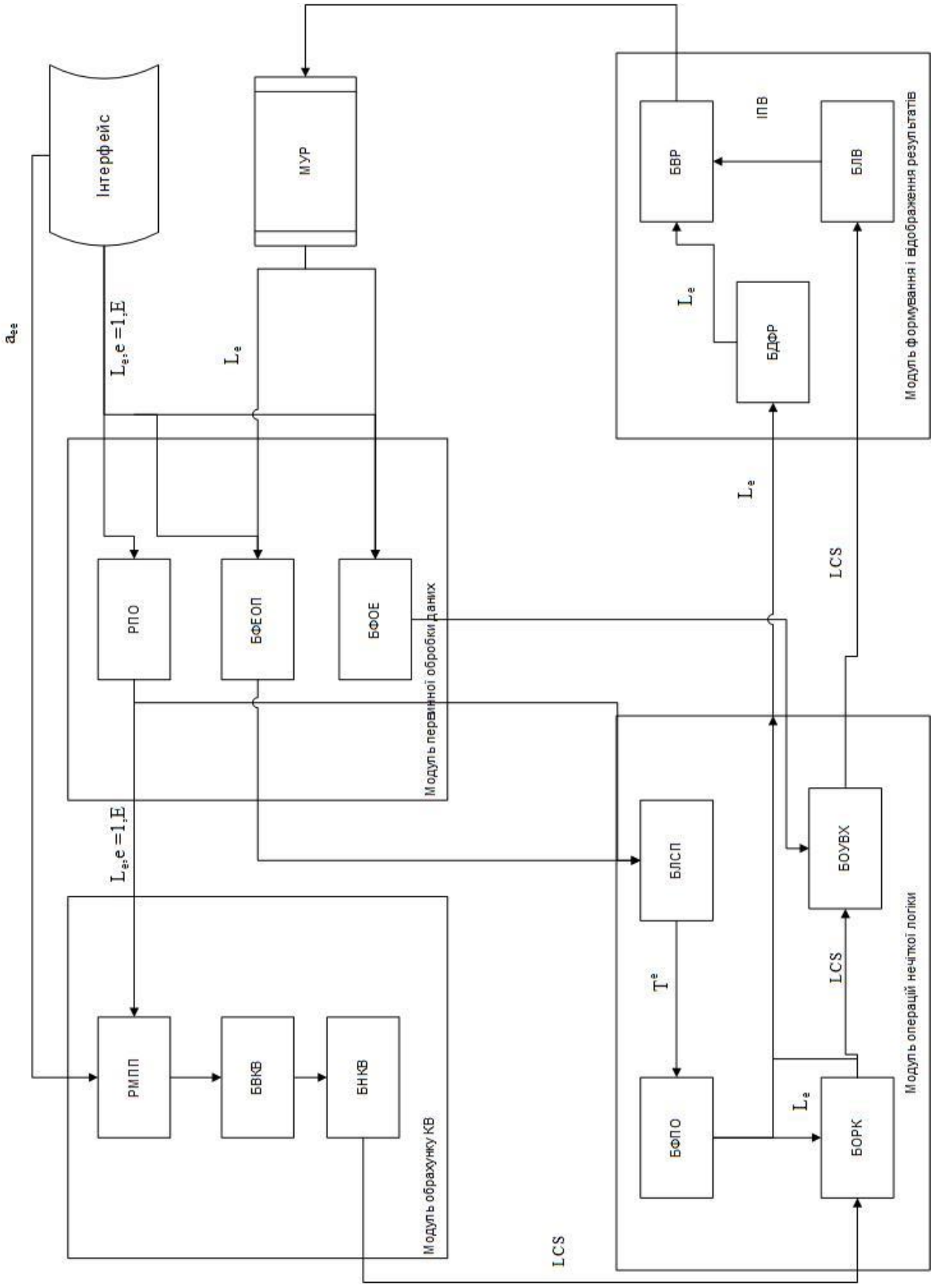
ДОДАТОК Г

Підсистема виявлення та ідентифікації ІПВ



ДОДАТОК Д

Підсистема оцінювання ІПВ



ДОДАТОК Е

Акт впровадження 1

Динаміка
dynamika-center.com

Україна,01135, Київ
вул.Андрющенка, 4д
+380667742320

Вих. 03/0923 від 04.09.23

АКТ

впровадження результатів дисертаційної роботи
Гріги Владислава Сергійовича «Методи та моделі управління інформаційно-психологічним впливом у соціальних мережах» на здобуття наукового ступеню доктора філософії зі спеціальності 122-комп'ютерні науки у діяльності Центру психологічного, фізичного та мовленнєвого розвитку дитини «Динаміка» (ФОП *Маркова О.В.*)

Комісія, у складі директора Маркової О.В., адміністраторів Дзюбан Д.Д., Янковенко М.С., склали цей акт про те, що під час реалізації SMM-стратегії використовуються результати дисертаційного дослідження Гріги Владислава Сергійовича «Методи та моделі управління інформаційно-психологічним впливом у соціальних мережах», а саме програмно-апаратний комплекс «СУІПВ v.1.0».

Програмно-апаратний комплекс «СУІПВ v.1.0» було впроваджено в роботу Центру психологічного, фізичного та мовленнєвого розвитку дитини «Динаміка» та почав використовуватися з 01.06.2023 року. Згаданий комплекс використовується для виявлення та оцінювання дописів та згадок про Центр, а також щодо оцінювання ефективності власних дописів у соціальних мережах. За час роботи збільшилася кількість відвідувань сторінок у соціальних мережах Центру, реакція на дописи, а також покращилося ставлення до бренду вцілому, про що опосередковано свідчить збільшення кількості відвідувачів.

Порівняння відвідування та реакції на дописи сторінок у соціальних мережах Центру психологічного, фізичного та мовленнєвого розвитку дитини «Динаміка»

Характеристика/проміжок часу	**01.03.2023-31.05.2023**	**01.06.2023-31.08.2023**	**Відсоткове відношення**
Відвідування сторінок у соціальних мережах	2253	3897	+73%
Кількість реакцій на дописи у соціальних мережах	411	624	+51,8%
Кількість відвідувачів	183	269	+47%

Отже, результати, отримані Грігою В.С. під час написання дисертаційної роботи дозволили підвищити ефективність SMM-стратегії Центру психологічного, фізичного та мовленнєвого розвитку дитини «Динаміка».

Директор
Центру Олександра МАРКОВА

Маркова Олександра Валеріївна

ДОДАТОК Є

Акт впровадження 2

"ПОГОДЖЕНО"
Проректор з навчальної роботи
Анатолій ПОЛУХІН
«21» вересня 2023 р.

"ЗАТВЕРДЖУЮ"
Проректор з наукової роботи
та інноваційного розвитку
Олексій ШКУРАТОВ
М.П. «27» вересня 2023 р.

АКТ
про впровадження результатів дисертаційної роботи Гріги Владислава Сергійовича «Методи та моделі управління інформаційно-психологічним впливом у соціальних мережах»
в навчальний процес
Національного авіаційного університету

Комісія у складі:

Голова комісії	Нестеренко К.С.	д.т.н., проф., в.о. декана ФКПІ
Члени:	Горський О.М.	к.т.н., доц., завідувач кафедри інженерії програмного забезпечення
	Талалаєв В.О.	к.т.н., доц., доцент кафедри інженерії програмного забезпечення
	Волкогон В.О.	к.т.н., доцент кафедри інженерії програмного забезпечення

встановила, що результати дисертаційної роботи ***Гріги Владислава Сергійовича*** за темою «Методи та моделі управління інформаційно-психологічним впливом у соціальних мережах» впроваджені в 2022-2023 та 2023-24 н.рр. у навчальний процес кафедри інженерії програмного забезпечення:

- шляхом використання у курсах лекцій з дисциплін «Групова динаміка і комунікації» та «Основи технологій R&D»;
- впроваджено методику проведення експерименту та лабораторні роботи з дисципліни «Основи технологій R&D».

Голова комісії — підпис — Катерина НЕСТЕРЕНКО

Члени комісії:
підпис — Олексій ГОРСЬКИЙ
підпис — Володимир ТАЛАЛАЄВ
підпис — Вікторія ВОЛКОГОН