Міністерство освіти і науки України
Національний університет “Львівська політехніка”

Кваліфікаційна наукова
праця на правах рукопису

ВУС ВОЛОДИМИР АНТОНОВИЧ

УДК 004.652.4004.738.5:001.102-049.5:351.862.4(043)

ДИСЕРТАЦІЯ

МАТЕМАТИЧНЕ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ ІНФОРМАЦІЙНІЙ ПРОПАГАНДІ В СОЦІАЛЬНИХ СЕРЕДОВИЩАХ ІНТЕРНЕТУ

Спеціальність 01.05.03 – Математичне та програмне забезпечення обчислювальних машин і систем

05 «Технічні науки»
(галузь знань)

Подається на здобуття наукового ступеня кандидата технічних наук

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело _____/Вус В.А./

Науковий керівник:
Пелещишин Андрій Миколайович,
доктор технічних наук, професор

Ідентичність усіх примірників дисертації
ЗАСВІДЧУЮ:
Вчений секретар спеціалізованої
вченої ради Д 35.052.05 **/Р. А. Бунь/**

Львів - 2019

АНОТАЦІЯ

Вус В.А. Математичне та програмне забезпечення протидії інформаційній пропаганді в соціальних середовищах Інтернету. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 01.05.03 «Математичне та програмне забезпечення обчислювальних машин та систем». – Національний університет «Львівська політехніка», МОН України, Львів, 2019.

Дисертаційну роботу присвячено розв’язанню завдань захисту інформаційного простору держави від агресивних та шкідливих форм пропаганди у соціальних середовищах Інтернету, таких як соціальні мережі та Веб-форуми. Це відображається у зростанні кількості та якості інформаційного наповнення національного сегменту соціальних середовищ Інтернету, відповідному збільшенні аудиторії соціальних середовищ та її резистентності до шкідливих, деструктивних впливів. Першочерговим завданням досліджень є методологічні, методичні та технічні питання організації комплексної інформаційної активності у соціальних середовищах Інтернету на регіональному та загальнодержавному рівнях з метою протистояння цілеспрямованій ворожій пропагандистській діяльності.

Через недостатність розвитку апарату досліджень процесів інформаційного протистояння у соціальних середовищах Інтернету, структурну та змістовну складність об'єкта досліджень й істотність впливу результатів на практичну реалізацію спеціалізованих інформаційних систем, комплекс досліджень має проблемний характер і значне прикладне значення, особливо відчутне при плануванні, формуванні і подальшому захисті інформаційного простору держави, а також при формуванні стратегій розвитку систем цифрових соціальних комунікацій на глобальному та національному рівнях.

Розроблення методів та засобів захисту держави від шкідливих та агресивних впливів у соціальних середовищах Інтернету та вироблення науково обгрунтованих практичних підходів до його ефективної організації повинні базуватися на аналізі проблемної області. Важливим є визначення наявних підходів до вирішення як вказаної задачі, так і суміжних з нею завдань з інших предметних областей.

Зокрема, для формалізації інформаційного поля, у якому здіснюється протиборство, є аналіз соцільних середовищ Інтернету у сучасних умовах, практичні підходи до їхнього використання в інформаційній та рекламно-маркетинговій діяльності. Враховуючи наявність значних професійних результатів та досвіду в цих областях, доцільно проаналізувати поняття та види активної інформаційної діяльності в соціальних середовищах Інтернету, їхнє наукове підгрунтя та перспективи.

Іншим важливим напрямком аналізу є визначення шляхів і методів розвитку віртуальних спільнот на інфраструктурі Інтернету, мотивацій їхніх учасників, шляхів самореалізації особистості в інформаційному просторі. Важливим також є аналіз принципів та завдань інформаційної взаємодії між державою, окремими організаціями та суспільством.

Ключовим аспектом аналізу є формалізація основних видів агресії проти держави в соціальних середовищах, методики та інструментарію їхнього провадження.

У першому розділі дисертації досліджено соціальні середовища Інтернету як джерело позитивних та негативних впливів у системі національної безпеки.

У розділі здійснено системний аналіз основних класів соціальних середовищ: Веб-форумів та standalone-блогів; електронних ЗМІ та колективних блогів; самомодерованих енциклопедій; сервісів соціальних мереж. Проаналізовано особливості кожної з платформ та правила організації контенту.

Проведено аналіз форм публічної інформаційної діяльності в описаних вище класах соціальних середовищ, здійснено класифікацію за ознаками «колективність» та «контрольованість» результатів діяльності.

Технології інформаційної та маркетингової діяльності в ССІ, які за змістом та характером є суміжними із завданнями захисту інформаційного простору, є важливими орієнтирами для наукових досліджень у даній сфері, - тому, на завершення розділу досліджено окремі тенденції онлайн-маркетингу, а саме: використання лідерів думок при формуванні громадської думки; використання віртуальних спільнот як інструменту для PR, окремі питання взаємодії з користувачами соціальних середовищ.

У другому розділі дисертації запропоновано ряд формальних моделей суб'єктів інформаційної діяльності.

У розділі здійснено формалізацію користувачів соціальних середовищ Інтернету, у якій враховано особливості завдань захисту інформаційного простору, зокрема введено у розгляд спеціальні характеристики, які дозволяють виділити спеціальні ролі користувача: лідер думок, опонент, транслятор, троль. Детально формалізовано поняття фізичної та мережевої ідентифікації користувачів.

Окрім моделі користувачів, у розділі запропоновано спеціальну модель віртуальних спільнот як середовища протиборства у інформаційному просторі. Визначено ряд характеристик, які згруповано у такі групи: технічна, аудиторна, суспільної значимості, змісту та комунікації, державної безпеки.

У третьому розділі дисертаційної роботи розроблено ряд спеціальних методів та алгоритмів, покликаних підвищити якість та ефективність діяльності з захисту інформаційного простору держави.

Розроблено методи визначення ряду зведених показників віртуальних спільнот, зокрема показники комунікативного комфорту та

близькості завданням державної безпеки. Показано їхнє застування для пріоритезації спільнот у відповідних завданнях.

Далі у розділі наведено методи планування заходів із захисту інформаційного простору, а саме: загальний алгоритм організації заходів у спільнотах; алгоритм персоналізації суб'єктів інформаційної діяльності, методи виявлення впливових лідерів думок; методи продидії шкідливим лідерам думок та модераторам; виявлення тролів та опонентів, що провадять наперед плановану діяльність.

На завершення розділу запроновано підхід до організації ефективної ресурсної підтримки корисних заходів, що базуються на понятті дисбалансу у співвідношеннях між окремими показниками.

У четвертому розділі дисертаційної роботи наведено практичні результати, втілені в комплексній системі захисту інформаційного простору держави.

Описано багаторівневу архітектуру програмного комплексу, в розробленні якої використано результати теоретичних розділів роботи та загальні підходи до розробки систем аналогічних класів. Визначено категорії користувачів системи: командна ланка, оперативна ланка, базова ланка, контрольна ланка. З програмно-технічної точки зору система реалізується на комплексі технологій, орієнтованих на системи з відкритим кодом та засобами, орієнтованими на опрацювання великих масивів даних. Далі у розділі наведено орієнтовну структуру бази даних комплексу в ERD нотації, яка базується на формальних моделях, розроблених у попередніх розділах.

У розділі також описано функції компонент системи за її рівнями. Відзначено методи та алгоритми, розроблені у роботі, на яких базуються відповідні компоненти, визначено основні вимоги до користувальницького інтефейсу системи.

На завершення розділу подано окремі результати практичної апробації дисертаційних досліджень у інформаційному просторі України.

У дисертаційній роботі вирішено важливе наукове завдання - підвищення рівня захисту інформаційного простору держави шляхом розроблення математичного та програмного забезпечення протидії інформаційній пропаганді в соціальних середовищах Інтернету та їхнього практичного втілення, зокрема отримано такі результати:

- проведений системний аналіз розвитку та функціонування соціальних середовищ Інтернету показав актуальність наукової задачі як розробки методів та засобів протидії інформаційній пропаганді;
- розроблено формальну модель користувача соціальних середовищ Інтернету шляхом уведення спеціальних характеристик мережевого, інформаційного, соціокомунікаційного змісту, орієнтованих на завдання захисту інформаційного простору, що дало змогу формалізувати та вирішити важливі завдання організації ефективної взаємодії з користувачами соціальних середовищ Інтернету;
- розроблено формальну модель віртуальних спільнот шляхом опису їх як середовища інформаційного протиборства з характеристиками аудиторії, суспільної значимості, змісту, комунікації, державної безпеки, що стало основою для побудови інформаційної моделі системи управління заходами з захисту інформаційного простору;
- побудовано систему зведених показників віртуальних спільнот, орієнтованих на завдання захисту інформаційного простору держави на основі базових характеристик формальної моделі, яка стала основою для розроблення ряду прикладних методів протидії інформаційній пропаганді;
- побудовано методи планування заходів із протидії інформаційній пропаганді у соціальних середовищах Інтернету, що базуються на запропонованих формальних моделях та зведених показниках і

забезпечують можливість організації неперервним системної протидії компексним загрозам безпеці національного інформаційного простору;

- побудовано методи та алгоритми виявлення та протидії окремим групам користувачів, які здійснюють деструктивну діяльність у інформаційному просторі держави, а також грунтуються на уведених у роботі спеціальних ролях користувачів, що забезпечує можливість ефективного виконання оперативних завдань з інформаційного протиборства;
- побудовано методи ресурсної підтримки заходів із протидії інформаційній пропаганді з використанням апарату дисбалансів у показниках користувачів та віртуальних спільнот соціальних середовищ Інтернету;
- розроблено комплексну систему управління заходами з протидії пропаганді, яка базується на запропонованих у роботі формальних моделях, методах та алгоритмах, забезпечує автоматизацію та ефективне виконання основних завдань організації і координації дій відповідальних осіб та волонтерів щодо захисту інформаційного простору держави;
- проведено апробацію запропонованих методів і засобів протидії інформаційній пропаганді у соціальних середовищах Інтернету шляхом використання їх у окремих, критичних для національної безпеки, спільнотах.

Ключові слова: соціальне середовище Інтернету, захист інформації, безпекова модель користувача, соціальний портрет користувача, мережева активність, характеристики державної безпеки.

Список опублікованих праць за темою дисертації

1. Добровольська В. В., Пелещишин А. М., Вус В. А. Фактор соціальних мереж у завданнях захисту суспільного інформаційного образу закладів культури. Вісник Національної академії керівних кадрів культури і мистецтв. 2018. № 4. С. 132–137. (Особистий внесок здобувача: запропоновано концепцію переходу до суспільноактивної діяльності в соціальних мережах)

2. Vus V., Albota S., Dobrovolska V. The analysis of online communities as platforms for informational influences. Journal of Scientific and Engineering Research. 2019. Vol. 6, is. 2. P. 72–78. (Особистий внесок здобувача: описано види спілкування в онлайн-спільнотах та їхні характеристики)

3. Пелещишин А. М., Вус В. А., Тимовчак-Максимець О. Ю. Спеціальна безпекова модель користувача соціальних середовищ Інтернету. Безпека інформації. Ukrainian Scientific Journal of Information Security. 2018. 24 (1). С. 62–68. (Особистий внесок здобувача: опис формальної моделі користувача соціальних середовищ Інтернету)

4. Пелещишин А. М., Вус В. А., Марковець О. В. Побудова формальної моделі віртуальних спільнот як середовища соціокомунікативного протиборства. Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Технічні науки. 2018. Т. 29 (68), № 4, ч. 1. С. 201–207. (Особистий внесок здобувача: визначення правил формування контенту у соціальних середовищ Інтернету, визначення характеристик віртуальних спільнот)

5. Пелещишин А. М., Вус В. А. Фактори соціальних середовищ інтернету в системі національної безпеки. Вісник інженерної академії України. 2018. № 2. С. 78–82. (Особистий внесок здобувача: визначено фактори соціальних середовищ Інтернету як середовища, у яких здійснюється як корисна так і шкідлива інформаційна діяльність та типи соціальних середовищ з точки зору системної організації процесу

комунікації.)

6. Трач О. Р., Вус В. А. Визначення параметрів показників організації життєвого циклу віртуальних спільнот. Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Технічні науки. 2019. Т. 30 (69), № 1, ч. 1. С. 143–148. (Особистий внесок здобувача: розподіл ролей користувачів соціальних середовищ Інтернету)

7. Вус В. А., Пелещишин А. М. Зведені показники віртуальних спільнот та пріоритезація спільнот з точки зору державної безпеки. Стандартизація, сертифікація, якість. 2019. № 2 (114). С. 73–80. (Особистий внесок здобувача: визначення зведених показників віртуальних спільнот, орієнтованих на завдання захисту інформаційного простору держави)

8. Вус В. Соціальні мережі як інструмент інформаційного протиборства // Інформація, комунікація, суспільство (ICS-2015) : матеріали 4 Міжнар. наук. конф., 20–23 трав. 2015 р. Львів : Вид-во Львів. політехніки, 2015. С. 28–29.

9. Вус В. А., Пелещишин А. М. Аналіз проблеми створення спеціального програмного забезпечення для протидії пропаганді в соціальних мережах // Інформація, , суспільство (ICS-2016) : матеріали 5 Міжнар. наук. конф., 19–21 трав. 2016 р. Львів : Вид-во Львів. політехніки, 2016. С. 38–39. (Особистий внесок здобувача: визначено основні завдання для програмного забезпечення протидії пропаганді в соціальних мережах)

10. Trach O., Vus V., Tymovchak-Maksymets O. Typical algorithm of stage completion when creating a virtual community of a HEI // Сучасні проблеми радіоелектроніки, телекомунікацій, комп’ютерної інженерії (TCSET’2016) : матеріали XIII Міжнар. конф., 23–26 лют. 2016 р. Львів : Вид-во Львів. політехніки, 2016. С. 849–851. (Особистий внесок здобувача: визначено етапи створення віртуальної спільноти).

11. Пелещишин А. М., Вус В. А. Показники віртуальної спільноти,

що впливають на безпеку національного інформаційного простору // Стан та перспективи реформування сектору безпеки і оборони України : матеріали Міжнар. наук.-практ. конф., 24 листоп. 2017 р. Київ, 2017. Т. 1. С. 320–322. (Особистий внесок здобувача: характеристики показників віртуальної спільноти).

12. Пелещишин А., Тимовчак-Максимець О., Вус В. Характеристики формальної моделі віртуальних спільнот як середовища поширення інформаційної агресії // Безпекові виклики у геополітиці XXI століття : матеріали Міжнар. наук.-практ. конф., 23–24 листоп. 2017 р. Львів, 2017. С. 149. (Особистий внесок здобувача: описано показники рівня державного впливу у формальної моделі віртуальних спільнот).

13. Пелещишин А. М., Вус В. А. Особливі категорії користувачів соціальних середовищ Інтернету, що впливають на безпеку інформаційного простору держави // Освіта і наука у сфері національної безпеки: проблеми та пріоритети розвитку : зб. наук. пр. за матеріалами Міжнар. наук.-практ. конф., Острог, 1 груд. 2017 р. Острог : Вид-во Нац. ун-ту «Остроз. акад.», 2017. С. 27–29. (Особистий внесок здобувача: визначення категорій користувчів у соціальних середовищах Інтернету).

14. Вус В. Аналіз основних класів соціальних середовищ // Інформація, комунікація, суспільство (ICS-2018) : матеріали 7 Міжнар. наук. конф., 17–19 трав. 2018 р., Чинадієво. Львів : Вид-во Львів. політехніки, 2018. С. 39–40.

15. Peleshchyshyn A., Markovets O., Vus V., Albota S. Identifying specific roles of users of social networks and their influence methods // Комп'ютерні науки та інформаційні технології (CSIT-2018) : матеріали XIII Міжнар. наук.-техн. конф., Львів, 11–14 верес. 2018 р. Львів, 2018. С. 39–42. (Особистий внесок здобувача: формальний опис активності користувача соціальних середовищах Інтернету).

16. Peleshchyshyn A., Vus V., Albota S., Markovets O. A formal

approach to modeling the characteristics of users of social networks regarding information security issues // Advances in Intelligent Systems and Computing. 2019. Vol. 902 : Advances in Artificial Systems for Medicine and Education II. The Second International Conference of Artificial Intelligence, Medical Engineering, Education (AIMEE2018), 6–8 Oct. 2018. Springer, 2019. P. 485–494. (Особистий внесок здобувача: описано структуру бази даних користувачів соціальних середовищах Інтернету).

17. Вус В. Аналіз форм публічної інформаційної діяльності в соціальних середовищах Інтернету // Інформація, комунікація, суспільство (ICS-2019) : матеріали 8 Міжнар. наук. конф., 16–18 травня 2019 р., Чинадієво. Львів : Вид-во Львів. політехніки, 2019. С. 41–43.

ABSTRACT

Vus V.A. Mathematical and software counter to informational propaganda in social Internet environments. – Qualification scientific work on the rights of manuscript.

Thesis for a Ph.D. degree in specialty 01.05.03 «Mathematical and software of computing machines and systems». – Lviv Polytechnic National University Ministry of Education and Science of Ukraine, L'viv, 2019.

In the thesis, the important scientific task of the protection of the state's information space from aggressive and harmful forms of propaganda in Internet social environments, such as social networks and Web-forums, is solved. This is reflected in the increase in the number and quality of the information content of the national segment of the Internet social environment, corresponding to an increase in the audience of social environments and its resistance to harmful, destructive influences. Methodological, methodical and technical issues of organizing a comprehensive information activity in the social Internet environments at the regional and national levels with the aim of counteracting purposeful hostile propaganda activities is a priority task of research.

The complex of researches has a problematic character and considerable applied value, especially noticeable in planning, formation and further protection of the information space of the state, as well as in the formation of strategies for the development of digital social communication systems at the global and national levels. This is due to the inadequate development of the apparatus of investigation of the processes of information confrontation in the social Internet environments, the structural and content complexity of the object of research and the significance of the impact of the results on the practical implementation of specialized information systems.

The development of methods and means of protecting the state from harmful and aggressive influences in the Internet social media and the development of scientifically grounded practical approaches to its effective

organization should be based on the analysis of the problem area. Identifying existing approaches to solving both the specified task and related tasks from other subject areas is an important task.

In particular, for the formalization of the information field in which the confrontation is carried out, is an analysis of the social Internet environments in modern conditions, practical approaches to their use in information and advertising and marketing activities. Taking into account the presence of significant professional results and experience in these areas, it is advisable to analyze the concepts and types of active information activities in the social Internet environments, their scientific background and perspectives.

Identifying ways and means of developing virtual communities on the Internet infrastructure, motivating their participants, ways of self-realization of the individual in the information space is another important area of analysis. An analysis of the principles and objectives of information interaction between the state, individual organizations and society is also important.

The key aspect of the analysis is the formalization of the main types of aggression against the state in social environments, the methods and tools for their conduct.

The first chapter the social Internet environments as a source of positive and negative influences in the system of national security is researched.

The chapter provides a systematic analysis of the main classes of social environments: Web forums and standalone blogs; electronic media and collective blogging; self-maintained encyclopedias; social networking services. The peculiarities of each platform and content organization rule are analyzed. The chapter analyzes forms of public information activities in the above-described classes of social environments, carried out the classification on the basis of "collective" and "controllability" of the results of activities. Technologies of informational and marketing activities in the SNE, which by their content and character are adjacent to the tasks of protecting the information

space, are important benchmarks for scientific research in this field. Therefore, at the end of the chapter, some trends in online marketing are explored, in particular: use of opinion leaders in forming public opinion; the use of virtual communities as a tool for PR, individual issues of interaction with users of social environments.

In the second chapter of the thesis, a number of formal models of subjects of informational activity are proposed. In this section, the formalization of users of social Internet environments that takes into account the specifics of the tasks of protecting the informational space has been made, including the introduction of special features that allow you to highlight the user's special roles: the opinion leader, opponent, translator, troll. The concept of physical and network identification of users is formalized.

In addition to the user model, the section proposes a special model of virtual communities as an environment of confrontation in the information space. Number of characteristics are identified, which are grouped into such groups: technical, auditorium, social significance, content and communication, state security.

In the third chapter of the thesis, a number of special methods and algorithms designed to improve the quality and effectiveness of activities in protecting the state of the information space have been built.

Methods of determination of a number of consolidated indicators of virtual communities, in particular indicators of communicative comfort and proximity to the tasks of state security, were constructed. Their arrangement is shown to prioritize communities in their respective tasks.

The following parts of chapter describes the methods of planning measures for the protection of the information space, in particular: a general algorithm for organizing activities in communities; algorithm of personalization of subjects of information activity, methods of revealing influential opinion

leaders; methods of counteracting harmful opinion leaders and moderators; detection of trolls and opponents, who carry out planned activities in advance.

At the end of the chapter, an approach is proposed to organize effective resource support for useful activities based on the concept of imbalance in the relationships between individual indicators.

The fourth chspter presents the practical results of the thesis, which are implemented in the complex system of protection of the state information space.

A multilevel architecture of the software complex is described, the development of which is used as a result of theoretical chapters of work and general approaches to the development of systems of similar classes. Categories of system users are defined: the command line, the operational link, the basic link, the control link. From the software and engineering point of view, the system is implemented in a set of technologies focused on open source systems and tools focused on processing large amounts of data. The approximate structure of the complex database in the ERD of the notation, which is based on the formal models developed in the previous chapters are next in the chapter.

In the chapter also describes the features of the system component at its levels. The methods and algorithms developed in the work on which the corresponding components are based are defined, the basic requirements to the user interface of the system are determined. At the end of the chapter, individual results of practical testing of dissertation research in the information space of Ukraine are presented.

In the thesis, it is solved an important scientific task of raising the level of protection of the state information space by the development of mathematical and software counteraction to informational propaganda in social Internet environments and their practical implementation is solved. In particular, the following results were obtained:

- a systematic analysis of the development and functioning of the social Internet environments has shown the relevance of the scientific problem as

the development of methods and means of counteracting information propaganda;

- the formal model of the social Internet environments' user has been developed by introducing special characteristics of network, informational, social and communication content focused on the task of protecting the informational space, which allowed to formalize and solve important tasks of organizing effective interaction with users of social Internet environments;
- the formal model of virtual communities was developed by describing them as a medium of information confrontation with audience characteristics, social significance, content, communication, state security, which became the basis for building an information model of a management system for measures to protect the information space;
- a system of aggregated indicators of virtual communities focused on the task of protecting the information space of the state based on the basic characteristics of the formal model, which became the basis for the development of a number of applied methods of counteracting information propaganda built;
- methods of planning measures to counter informational propaganda in the social media on the Internet, based on the proposed formal models and consolidated indicators and provide the possibility of organizing a continuous system response to the compact threats to the security of the national information space built$
- methods and algorithms for detecting and responding to individual users' groups, that carry out destructive activity in the state information space and based on special user roles are constructed. This provides the opportunity to effectively perform operational tasks in the information confrontation;
- methods of resource support for measures to counter informational propaganda using the apparatus of imbalances in indicators of users and virtual communities of social Internet environments;

- developed a comprehensive system for managing anti-propaganda measures, based on the formal models, methods and algorithms proposed in the work, and provides for the automation and effective implementation of the main tasks of the organization and coordination of actions of responsible persons and volunteers on the protection of the state's information space;
- approbation of the proposed methods and means of counteracting information propaganda in the social Internet environments through their use in separate, critical for national security communities.

Keywords: social Internet environment, information protection, security user's model, social user's portrait, network activity, state security characteristic.

List of publications by the subject of dissertation

1. Dobrovolska V.V., Peleschyshyn A.M., Vus V.A. The factor of social networks in the tasks of protecting the public information image of cultural institutions // Bulletin of the National Academy of Leaders of Culture and Arts. 2018. No. 4. P. 132-137.

2. Vus V., Albota S., Dobrovolska V. The analysis of online communities as platforms for informational influences. Journal of Scientific and Engineering Research. 2019. Vol. 6, iss. 2. P. 72–78.

3. Peleschyshyn A.M., Vus V.A., Tymovchak-Maksymets O. Yu. Special security model of social Internet environments' user // Information Security. Ukrainian Scientific Journal of Information Security. 2018. Vol. 24, No. 1. P. 62-68.

4. Peleschyshyn A.M., Vus V.A., Markovets O. V. Construction of the virtual communities formal model as a medium of socio-communicative confrontation // Scientific notes of the Taurida National University named after VI Vernadsky. Series: Technical Sciences. 2018. Vol. 29 (68), No. 4, part 1. P. 201-207.

5. Peleschyshyn A.M., Vus V.A. Factors of the social Internet environments in the system of national security // Bulletin of the Engineering Academy of Ukraine. 2018. No 2. P. 78-82.

6. Trach O.R., Vus V.A. Definition of parameter parameters of organization of virtual communities life cycle // Scientific notes of the Taurida National University named after VI Vernadsky. Series: Technical Sciences. 2019. Vol. 30 (69), No. 1, part 1. P. 143-148.

7. Vus V.A., Peleschyshyn A.M. Summary of virtual communities and prioritization of communities in terms of state security // Standardization, certification, quality. 2019 No. 2 (114). P. 73-80.

8. Vus V.A. Social networks as an instrument of information confrontation // Information, communication, society (ICS-2015): materials of

the 4th International sciences conference, May 20-23. 2015, Lviv, Slavske. 2015. P. 28-29.

9. Vus V.A., Peleschyshyn A.M. Analysis of the special software creation problem for counteraction to propaganda in social networks // Information, society (ICS-2016): Materials of the 5th International sciences Conference, 19-21 May. 2016, Lviv, Slavske. 2016. C. 38-39.

10. Trach O., Vus V., Tymovchak-Maksymets O. Typical algorithm of stage completion when creating a virtual community of a HEI // Modern problems of radio electronics, telecommunications, computer engineering (TCSET'2016): Materials XIII International Conference. Lviv, Slavske, February 23-26. 2016. P. 849-851.

11. Peleschyshyn A.M., Vus V.A. Indicators of virtual community influencing the security of the national information space // Status and prospects of the reform of the security and defense sector of Ukraine: materials of the international. scientafic conference. Kyiv, November 24. 2017. Vol. 1. P. 320-322.

12. Peleschyshyn A., Tymovchak-Maksymets O., Vus V. Characteristics of the virtual communitie’s formal model as a medium of dissemination of information aggression // Security challenges in the geopolitics of the XXI century: materials of the international scientific and practical conference, Lviv, November 23-24. 2017 Lviv, 2017. P. 149.

13. Peleschyshyn A.M., Vus V.A. Special categories of social Internet environments’ users that affect the security of the state's information space // Education and science in the field of national security: problems and priorities of development. December. 2017. Ostrog. P. 27-29.

14. Vus V. Analysis of the main classes of social media // Information, communication, society (ICS-2018): materials of the 7th International. sciences conference, 17-19 May. 2018, Chinadievo. Lviv. 2018. P. 39-40.

15. Peleshchyshyn A., Markovets O., Vus V., Albota S. Identifying

specific roles of users of social networks and their influence methods // Computer Science and Information Technology (CSIT-2018). Lviv, 2018. P. 39-42.

16. Peleshchyshyn A., Vus V., Albota S., Markovets O. A formal approach to modeling the characteristics of users of social networks regarding information security issues // Advances in Intelligent Systems and Computing. 2019. Vol. 902 : Advances in artificial systems for medicine and education II. The second international conference of artificial intelligence, medical engineering, education (AIMEE2018), 6–8 Oct. 2018, Moscow, Russia. P. 485–494.

17. Vus V. Analysis of forms of public information activity in the social Internet environments // Information, communication, society (ICS-2019): materials of the 8th International. sciences Conference, May 16-18, 2019, Chinadievo. Lviv. 2019. P. 41-43.

Зміст

Список рисунків

Список таблиць

Вступ

Дисертаційну роботу присвячено розв’язанню завдань захисту інформаційного простору держави від агресивних та шкідливих форм пропаганди у соціальних середовищах Інтернету, таких як соціальні мережі та Веб-форуми. Це відображається у зростанні кількості та якості інформаційного наповнення національного сегменту соціальних середовищ Інтернету, відповідному збільшенні аудиторії соціальних середовищ та її резистентності до шкідливих, деструктивних впливів. Першочерговим завданням досліджень є методологічні, методичні та технічні питання організації комплексної інформаційної активності у соціальних середовищах Інтернету на регіональному та загальнодержавному рівнях з метою протистояння цілеспрямованій ворожій пропагандистській діяльності.

Через недостатність розвитку апарату досліджень процесів інформаційного протистояння у соціальних середовищах Інтернету, структурну та змістовну складність об'єкта досліджень й істотність впливу результатів на практичну реалізацію спеціалізованих інформаційних систем, комплекс досліджень має проблемний характер і значне прикладне значення, особливо відчутне при плануванні, формуванні і подальшому захисті інформаційного простору держави, а також при формуванні стратегій розвитку систем цифрових соціальних комунікацій на глобальному та національному рівнях.

Актуальність теми. Різні форми інформаційного протистояння у глобальному та національному вимірах є доволі чітко сформованим напрямом як наукових, так і прикладних досліджень. Можна стверджувати, що історичний контекст таких досліджень широкий, проте стрімкий розвиток технологій соціальних комунікацій у глобальній мережі Інтернет та чітка тенденція до зростання значення та популярності

соціально-орієнтованих сервісів та вебсайтів зумовили появу принципово нових підходів до ведення інформаційно-прогандистської діяльності (аж до нових форм інформаційних війн), а також до захисту держави та громадян від таких шкідливих впливів. Водночас, можна стверджувати, що значний спектр традиційного інструментарію та методик інформаційного протистояння відійшов у минуле.

З очевидних причин значна частина досліджень у даній сфері носить закритий характер, особливо в частині агресивних, «атакуючих» дій. Проте як показує практика, методики захисту в різних формах інформаційних протистоянь є достатньо ефективними саме за умови певної їхньої відкритості, зрозумілості суспільством та обгрунтованістю на науковому рівні.

Наукові дослідження останніх років зорієнтовані на підвищення рівня безпеки в глобальному інформаційному просторі, зберігають ще певний традиційний поділ на дві основні категорії: «технічні», що охоплюють питання мережевої, апаратної та програмної безпеки, та «соціально-гуманітарні», які зосереджені на гуманітарних проблемах надання інформації споживачеві та різних форм суспільної взаємодії.

З певних причин основна увага науковців та висококваліфікованих фахівців технічної сфери привернута до першої категорії досліджень, за якою закріпився узагальнений термін «кібербезпека». Серед інших у цьому напрямі виділимо: дослідження із захисту програмних систем та комплексів різних класів, під’єднаних до глобальних мереж; захист інформації та криптографічні засоби; дослідження із надійності функціонування глобальних мереж та їх регіональних сегментів, стійкості в надзвичайних ситуаціях. Такі дослідження сформували певний необхідний базис для подальших робіт із захисту інтересів держави і громадян від загроз іншого рівня – соціально-комунікаційного.

Указана сфера досліджень, як було зазначено вище, переважно реалізується на сьогодні шляхом адаптації створених впродовж попередніх історичних періодів підходів, що носять типогуманітарний характер. Традиційно, це дослідження політологічного, психологічного, юридичного характеру з використанням спеціальних методик пропаганди, риторики, психологічних маніпулятивних технік та технологій піару та маркетингу. Такий підхід забезпечив певний прогнозований рівень наукових та практичних результатів на ранніх етапах розвитку глобальних мереж. Проте з настанням системних змін у характері використання Інтернету, а саме з початком домінування в ньому соціальних середовищ (соціальних мереж, форумів, блогів, колаборативних баз знань) з'ясувалося, що без необхідних системних та технологічних досліджень указані підходи уже не працюють [46, 49, 55, 56, 57, 77, 114].

Фактично, на сьогодні існує значна прогалина між указаними технічним та гуманітарним інструментарієм захисту інформаційного простору, що призвело до появи ряду негативних явищ глобального та регіонального масштабу, які стали результатом цілеспрямованих агресивних дій окремих держав та угрупувань, і носили синтетичний характер, у якому успішно поєднали технічні можливості глобальних соціальних середовищ та наявний гуманітарний соціально-комунікаційний інструментарій інформаційних війн та пропаганди [25, 37, 47, 92]. Результати таких дій набули великого резонансу і в значній мірі вплинули на зниження стабільності в глобальному вимірі. Для України такі дії стали фактично інструментом гібридної війни з тяжкими наслідками для держави [67, 68].

Отже, стає очевидним існування *актуального наукового завдання:* розроблення нового математичного та програмного забезпечення для ефективної протидії ворожим впливам та пропаганді в умовах інформаційної війни у соціальних середовищах Інтернету, що є

актуальним напрямком наукових досліджень у галузі комп’ютерних наук та інформаційних технологій. Першочерговим завданням досліджень є методологічні, методичні та технічні питання організації комплексної взаємодії громадських організацій та силових структур з глобальним середовищем, з метою підвищення стійкості до ворожих впливів. Внаслідок структурної та змістовної складності об'єкта досліджень і істотності впливу результатів на практичну реалізацію, комплекс досліджень має проблемний характер і значне прикладне значення, особливо відчутне в умовах поглиблення інформаційного протистояння в глобальному вимірі, здійснення актів інформаційної війни проти України та її союзників. Таким чином, результати дослідження також можуть бути використаними при формуванні стратегій розвитку національних сегментів Інтернету, зокрема українського мережного сегмента.

Слід зазначити, що заповнення указаної науково-прикладної прогалини повинно базуватися на достатньо розвинутому на сьогодні комплексі наукових досліджень у сфері моделювання та забезпечення соціально-інформаційних процесів у Інтернеті. Даний напрям досліджень формально сформувався лише в останні десять-двадцять років, проте на сьогодні вже є добре розвинутим і знайшов широкий спектр практичних впроваджень. Серед таких досліджень особливо близькі завданням захисту інформаційного простору такі:

- моделювання соціальних мереж та спільнот, розроблення методів проектування та управління [7, 60, 91, 93, 116];
- моделювання процесів накопичення даних та знань у глобальних мережах [82, 83, 84];
- інформаційний пошук у соціальних середовищах [21, 80, 87];
- виявлення та опрацювання суб’єктивно створеної інформації (opinion mining, sentiment analysis) [6, 10, 29, 30,110, 123];

- ідентифікація та класифікація користувачів соціальних мереж та спільнот, визначення окремих ролей та класів [41, 42, 43, 59, 99, 112, 127];
- комерціалізація соціальних мереж та спільнот, піар та реклама в них [130, 131];
- інтеграція суспільних та державних інституцій, соціальних середовищ Інтернету (електронне урядування, електронна демократія, електронна освіта) [1, 48, 73, 74, 87, 112];
- ідентифікація спаму, оцінювання значимості інформації [80, 128].

Окрім того, важливими базовими напрямами досліджень є побудова інформаційних технологій та засобів:

- накопичення, опрацювання та інтелектуальний аналіз великих масивів даних;
- опрацювання гіпертексту та слабоструктурованих даних;
- штучний інтелект та інтелектуалізація програмних засобів;
- управління складними системами.

Дослідження у наведених вище напрямах є безпосередньою теоретичною основою для подальших робіт зі створення загальнонаціональних систем захисту інформаційного простору, управління державою у сфері інформаційної безпеки, а також наукових досліджень з гармонізації інтересів держави, соціуму та громадян у соціальних середовищах Інтернету (ССІ), математичного моделювання процесів соціальних комунікацій у глобальному вимірі.

Зв'язок роботи з науковими програмами, планами, темами. Тема дисертації відповідає науковому напряму кафедри соціальних комунікацій та інформаційної діяльності Національного університету «Львівська політехніка» «Соціальні комунікації в глобальному інформаційному просторі» (номер державної реєстрації 0115U000460). У межах цієї теми розроблено модель веб-спільнот як середовища соціокомунікативного протиборства та загальний розподілений алгоритм типового процесу організації заходів у веб-спільнотах.

Мета і завдання дослідження. Метою дисертаційної роботи є підвищення рівня захисту інформаційного простору держави за допомогою розроблення математичного та програмного забезпечення протидії інформаційній пропаганді в ССІ. Мета дисертаційної роботи передбачає виконання таких завдань:

- виконання аналізу розвитку та функціонування ССІ як майданчик інформаційного протиборства та пропаганди;
- побудова формальних моделей користувачів ССІ та віртуальних спільнот, які орієнтовані на опис та вирішення завдань захисту інформаційного простору й охоплюють загальну формалізацію характеристик мережевого, інформаційного, соціокомунікаційного змісту;
- створення формальної моделі віртуальних спільнот, яка охоплює комплекс базових та зведених показників і передбачає опис суспільної значущості та характеристик державної безпеки;
- побудова методів загального планування заходів із захисту інформаційного простору держави та виконання окремих оперативних заходів із протидії інформаційній пропаганді у соціальних середовищах Інтернету;
- розроблення методів та алгоритмів виявлення та протидії окремим групам користувачів, які провадять деструктивну діяльність в інформаційному просторі держави;
- створення методів ресурсної підтримки заходів із протидії інформаційній пропаганді з використанням апарату дисбалансів у показниках користувачів та віртуальних спільнот соціальних середовищ Інтернету;
- розроблення комплексної системи управління заходами із протидії пропаганді, що забезпечує автоматизацію та ефективне виконання

основних завдань організації та координації дій відповідальних осіб та волонтерів щодо захисту інформаційного простору держави;

- здійснення апробації запропонованих методів і засобів протидії інформаційній пропаганді у соціальних середовищах Інтернету з використанням їх у окремих, критичних для національної безпеки, спільнотах.

Об'єктом дослідження є процеси інформаційного впливу у соціальних середовищах Інтернету.

Предметом дослідження є розроблення математичного та програмного забезпечення протидії інформаційній пропаганді в соціальних середовищах Інтернету.

Методи дослідження. Під час вирішення завдань моделювання користувачів соціальних середовищ Інтернету та віртуальних спільнот використано теоретико-множинні підходи, загальну теорію систем, апарат теорії реляційних баз даних, нечітких множин та теорії відношень. Для формування зведених показників користувачів та віртуальних спільнот застосовано сучасні підходи до формального оцінювання соціальних процесів, а для опису процесів та методів протидії інформаційній пропаганді – алгоритмічний підхід та відповідний інструментарій. Способи організації ресурсної підтримки заходів із протидії інформаційній пропаганді розроблено за допомогою інструментарію для аналізу дисбалансів у соціальних системах. Під час проєктування комплексної системи управління заходами із протидії інформаційній пропаганді використано підходи до побудови розподілених інформаційних систем класу "клієнт-сервер" та веб-сервісів, моделювання бази даних комплексу виконано за допомогою діаграмних засобів «сутність-співвідношення».

Наукова новизна отриманих результатів. Наукова новизна результатів роботи полягає у науковому обґрунтуванні та вирішенні наукового завдання розроблення нових методів та засобів протидії

інформаційній пропаганді в соціальних середовищах Інтернету. Отримано такі наукові результати:

- набули подальшого розвитку формальні моделі користувачів соціальних середовищ Інтернету з уведенням спеціальних характеристик мережевого, інформаційного, соціокомунікаційного змісту, орієнтованих на завдання захисту інформаційного простору, що дало змогу формалізувати та вирішити важливі завдання організації ефективної взаємодії з користувачами соціальних середовищ Інтернету;
- удосконалено формальні моделі віртуальних спільнот за допомогою опису їх як середовища інформаційного протиборства з характеристиками аудиторії, суспільної значущості, змісту, комунікації, державної безпеки, що стало основою для побудови інформаційної моделі системи управління заходами із захисту віртуального інформаційного простору;
- уперше побудовано метод оцінювання віртуальних спільнот за допомогою зведених показників, орієнтованих на завдання захисту інформаційного простору держави на підставі базових характеристик формальної моделі цих спільнот, яка стала основою для розроблення низки прикладних методів протидії інформаційній пропаганді;
- уперше розроблено методи планування заходів із протидії інформаційній пропаганді у соціальних середовищах Інтернету, що ґрунтуються на запропонованих формальних моделях користувачів і спільнот та їхніх зведених показниках, і забезпечують можливість організації неперервної системної протидії комплексним загрозам для безпеки національного віртуального інформаційного простору.

Практичне значення отриманих результатів. Практичне значення отриманих результатів дисертаційної роботи полягає у підвищенні ефективності процесу захисту інформаційного простору держави. Зокрема, практично цінні є такі результати:

- побудовано алгоритми виявлення окремих груп користувачів (та протидії їм), які ведуть деструктивну діяльність в інформаційному просторі держави, що ґрунтуються на уведених у роботі спеціальних ролях користувачів, а це уможливлює ефективне виконання оперативних завдань з інформаційного протиборства;
- розроблено підхід до організації ресурсної підтримки заходів із протидії інформаційній пропаганді з використанням апарату дисбалансів у показниках користувачів та віртуальних спільнот соціальних середовищ Інтернету;
- розроблено комплексну систему управління заходами з протидії пропаганді, яка основана на запропонованих у роботі формальних моделях, методах та алгоритмах і забезпечує автоматизацію й ефективне виконання основних завдань організації та координації дій відповідальних осіб і волонтерів щодо захисту інформаційного простору держави.

Результати дисертаційного дослідження упроваджено в таких організаціях: онлайн-спільноті «Варта 1», Управлінні Служби Безпеки України у Львівській області, а також використано у навчальному процесі Національного університету «Львівська політехніка» для проведення лабораторних робіт з курсу «Соціальні комунікації в мережі Інтернет», що підтверджено відповідними актами.

Особистий внесок здобувача. Усі наукові результати дисертаційної роботи отримано автором самостійно. У друкованих працях, опублікованих у співавторстві, внесок автора такий: [69] – запропоновано концепцію переходу до суспільноактивної діяльності в соціальних мережах, [32] – описано види спілкування в онлайн-спільнотах та їхні характеристики; [109] – опис формальної моделі користувача соціальних середовищ Інтернету, [108] – визначення правил формування контенту у соціальних середовищах Інтернету, визначення характеристик віртуальних

спільнот, [107] – визначено фактори соціальних середовищ Інтернету як середовища, у яких здійснюється як корисна, так і шкідлива інформаційна діяльність та типи соціальних середовищ з точки зору системної організації процесу комунікації, [126] – розподіл ролей користувачів соціальних середовищ Інтернету, [53] – визначення зведених показників віртуальних спільнот, орієнтованих на завдання захисту інформаційного простору держави, [52] – визначено основні завдання для програмного забезпечення протидії пропаганді в соціальних мережах, [27] – визначено етапи створення віртуальної спільноти, [106] – особистий внесок здобувача: характеристики показників віртуальної спільноти, [109] – описано показники рівня державного впливу у формальній моделі віртуальних спільнот, [105] – визначення категорій користувачів у соціальних середовищах Інтернету, [18] – формальний опис активності користувача соціальних середовищ інтернету, [19] – описано структуру бази даних користувачів соціальних середовищ Інтернету.

Апробація результатів дисертації. Основні результати дисертаційного дослідження неодноразово висвітлювалися на міжнародних та всеукраїнських наукових конференціях, зокрема: на XIII Міжнародній конференції «Сучасні проблеми радіоелектроніки, телекомунікацій, комп'ютерної інженерії» (TCSET'2016) (Львів, Славське, 2016); XIII Міжнародній науково-технічній конференції «Комп'ютерні науки та інформаційні технології» CSIT'2018 (Львів, 2018); 4, 5, 7, 8 Міжнародних наукових конференціях «Інформація, комунікація, суспільство» (Львів, 2015, 2016, 2018, 2019); Міжнародній науково-практичній конференції «Стан та перспективи реформування сектору безпеки і оборони України», (Київ, 2017); Міжнародній науково-практичній конференції «Безпекові виклики у геополітиці XXI століття» (Львів, 2017); Міжнародній науково-практичній конференції «Освіта і наука у сфері національної безпеки: проблеми та пріоритети розвитку»

(Острог, 2017). Про результати дисертаційних досліджень автор регулярно доповідав на наукових семінарах кафедри соціальних комунікацій та інформаційної діяльності Національного університету «Львівська політехніка» (2015, 2017-2019).

Публікації. За результатами виконаних досліджень опубліковано 17 наукових праць, з них: 1 – у виданні, що включене до наукометричної бази Web of Science; 1 – опублікована у періодичному виданні іншої держави; 5 – у фахових виданнях України; 10 тез міжнародних конференцій.

Розділ 1. Аналіз сучасних підходів до інформаційного протиборства та протидії пропаганді

Розроблення методів та засобів захисту держави від шкідливих та агресивних впливів у соціальних середовищах Інтернету та вироблення науково обгрунтованих практичних підходів до його ефективної організації повинні базуватися на аналізі проблемної області. Важливим є визначення наявних підходів до вирішення як вказаної задачі, так і суміжних з нею завдань з інших предметних областей.

Зокрема, для формалізації інформаційного поля, у якому здіснюється протиборство, – є аналіз соцільних середовищ Інтернету у сучасних умовах, практичні підходи до їхнього використання в інформаційній та рекламно-маркетинговій діяльності. Враховуючи наявність значних професійних результатів та досвіду в цих областях, доцільно проаналізувати поняття та види активної інформаційної діяльності в соцільних середовищах Інтернету, їхнє наукове підгрунтя та перспективи.

Іншим важливим напрямком аналізу є визначення шляхів і методів розвитку віртуальних спільнот на інфраструктурі Інтернету, мотивацій їхніх учасників, шляхів самореалізації особистості в інформаційному просторі. Важливим також є аналіз принципів та завдань інформаційної взаємодії між державою, окремими організаціями та суспільством.

Ключовим аспектом аналізу є формалізація основних видів агресії проти держави в соціальних середовищах, методики та інструментарію їхнього провадження.

Основні результати розділу опубліковані в працях [51, 54, 69, 106, 107].

1.1. Фактор соціальних середовищ Інтернету в системі національної безпеки

Захист від різних видів інформаційних впливів небажаного характеру був одним із головних факторів безпеки впродовж всієї сучасної історії людства. Пропаганда, дезінформація, поширення внутрішньої напруги та панічних настроїв серед населення були одним із інструментів отримання переваги в конфліктах, одним з елементів навіть прямого військового протистояння [45, 46, 49, 57, 79].

Особливого значення цей фактор набув у XX столітті, ставши одним із ключових елементів поширення глобальних впливів великих держав через ідеологічні та культурні впливи. В кінці XX сторіччя з'явився спеціальний термін «м'яка сила» щодо впливів даного класу, проте з появою Інтернету та його трансформацією в соціоінформаційну систему глобального масштабу характер та можливості таких інформаційних впливів драматично змінилися. Відкрилися нові напрямки для таких впливів та інструменти їх реалізації, а саме соціальні середовища Інтернету [2, 45, 76, 85, 102].

Серед факторів, що визначають їхнє критично важливе значення, є такі [70, 76, 85]:

- охоплення більшої частки населення;
- висока швидкість поширення інформації;
- високий рівень соціальних зв'язків (до кількох тисяч на акаунт);
- відчуття певної психологічної близькості;
- значні можливості по фальшивій персоніфікації.

Дані фактори визначають ССІ як середовища, у яких здійснюється як корисна, так і шкідлива інформаційна діяльність. Корисне значення таких середовищ є безсумнівним, важливим для всіх сфер політичного, економічного, культурного життя держави, проте їхній аналіз виходить за

межі роботи. Шкідлива інформаційна діяльність серед іншого може проявлятися у [75, 114]:

- **знищенні позитивних ефектів від ССІ** - руйнування спільнот, дискредитація корисних проектів тощо;
- **поширенні дезінформації** – наклепів, панічних настроїв тощо;
- **розпалюванні ворожнечі** – стимулювання громадянських конфліктів, ворожнечі за конфесійними, національними, расовими ознаками тощо;
- **шахрайство** – організація фінансових афер та пірамід, обман тощо.

Наведені (та інші неперераховані) загрози та фактори визначають актуальність завдань із захисту та безпеки інформаційного простору держави. Слід відзначити, що, за своєю суттю, вони значно відрізняються від суміжніх до них завданнями кібербезпеки. Значна частина завдань кібербезпеки також стосується ССІ та інших динамічних сервісів Інтернету, притому частка таких завдань усе зростає, проте характер таких завдань лежить у вдосконаленні мережевого та програмного забезпечення, виявленні та усуненні вразливостей тощо. Відповідно, відрізняються інструментарій та кваліфікація виконавців. Часто завдання кібербезпеки є допоміжними, утилітарними, в загальній системі безпеки інформаційного простору.

В умовах глобальних інформаційних протистоянь, у рамках яких задіюються сучасні інструменти деструктивних комунікативних впливів, гостро постає питання захисту національного інформаційного простору України на законодавчому рівні.

На сьогоднішній день в нашій державі створено значну нормативно-правову базу щодо забезпечення інформаційної безпеки країни, основою якої є Конституція України, яка визначає її захист як одну з найважливіших функцій держави. Відносини у цій сфері також регулюються низкою законів та підзаконних нормативно-правових актів, до яких, зокрема, належать закони України: «Про національну безпеку

України», «Про інформацію», «Про доступ до публічної інформації», «Про державну таємницю»; затверджені указами Президента України рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України», «Про нову редакцію Воєнної доктрини України», «Про Стратегію національної безпеки України», «Про Доктрину інформаційної безпеки України»; інші нормативно-правові акти, в тому числі міжнародні договори, згода на обов'язковість яких надана Верховною Радою України.

В той же час, одним із найбільш вагомих концептуальних документів щодо протидії російській пропаганді та зовнішнім інформаційним загрозам стала уведена в дію рішенням Ради національної безпеки і оборони України від 29 грудня 2016 року Доктрина інформаційної безпеки України, покликана закласти основи системного реагування на новітні виклики національній безпеці в інформаційній сфері. В документі вказано, що збереження інформаційного суверенітету та формування ефективної системи безпеки в інформаційній сфері є основними пріоритетами державної політики в такій сфері, в рамках якої передбачається створення та розвиток структур, що відповідають за інформаційно-психологічну безпеку держави та забезпечують, насамперед, більш суворий контроль за інформацією, яка циркулює в українському сегменті мережі Інтернет.

З огляду на викладене, набуває актуальності питання формування та врегулювання механізму виявлення, належної фіксації, блокування і видалення з інформаційного простору держави матеріалів, які можуть використовуватися як інструмент маніпулятивних пропагандистських технологій для руйнівного інформаційного вторгнення. В той же час, в Україні відсутній реально працюючий механізм координації діяльності силових структур, експертних, волонтерських та урядових організацій у сфері забезпечення інформаційної безпеки. Тому, зважаючи на реальні й потенційні загрози та деструктивні пропагандистсько-маніпулятивні

впливи Росії, консолідація зусиль усіх структур, які задіяні в інформаційному протиборстві з РФ, є гарантією інформаційної безпеки України та захисту національного інформаційного простору.

Одночасно, 22 лютого 2017 р. Міноборони Російської Федерації оголосило про створення військ інформаційних операцій, тим самим здійснивши легалізацію вже існуючих підрозділів, до складу яких також входять так звані "Ольгінські тролі", що задіяні в проведенні інформаційних атак з використанням бот-мереж в ССІ на території України. Метою діяльності вказаної організації є знищення інформаційного суверенітету противника з використанням маніпулятивних пропагандистських технологій та деструктивного інформаційного вторгнення з витісненням вже існуючих каналів поширення контенту. В свою чергу, можна виокремити такі основні методи роботи "Ольгінських тролів", як дезінформування, поширення чуток та залякування населення, пропаганда, маніпулювання та диверсифікація громадської думки, психологічний тиск, тощо.

В той же час, протягом останніх років фіксувалися випадки автоматичного видалення українських користувачів російських соціально-орієнтованих мереж з патріотичних онлайн-груп без згоди їх учасників та адміністраторів. Так, частина IP адрес, які належать українським Інтернет-провайдерам (ПАТ “Київстар” та ПАТ “Укртелеком”) відображалися в базі даних соцмереж «Вконтакті» та «Одноклассники» як російські. Під час проходження авторизації, у разі надання користувачам зазначених IP, їх автоматично видаляли зі спільнот заборонених Роскомнаглядом РФ. Крім того, в зазначений період відбувалося блокування проукраїнських спільнот із боку адміністрацій «Вконтакті» та «Одноклассники» під приводом використання так званого забороненого (автоматизованого ПЗ копіювання контенту) програмного забезпечення для їх наповнення. В той же час Інтернет-спільноти розважального типу, які використовувалися для

поширення російської пропаганди, адміністрація мережі не блокувала, не зважаючи на наявність фактів використання аналогічного програмного забезпечення для автоматичного наповнення груп контентом.

Зазначені дії адміністраторів російських соціальних мереж значно зменшили активність українських патріотичних груп та негативно вплинули на національний інформаційний простір. Користувачів обмежили у виборі джерел отримання інформації та нав'язливо пропонували підписатися на антиукраїнські Інтернет-спільноти, що активно поширювали викривлені або недостовірні дані, які спрямовані на дестабілізацію ситуації в Україні, дискредитацію керівництва держави та недовіри до правоохоронних органів.

1.2. Аналіз основних класів соціальних середовищ

Для подальшого дослідження з протидії шкідливим впливам через ССІ необхідно в цілому проаналізувати сучасні соціальні середовища в Інтернеті, виділити їхні основні класи та спільні ознаки.

Зазначимо, що, з технічної точки зору, на сьогодні існує широкий спектр програмно-технічних рішень, які зводяться до двох основних технологічних класів:

- тиражовані програмні системи;
- пропієтарні програмно-технічні комплекси.

Тиражовані програмні системи є основою для більшості автономних соціальних середовищ, часто реалізуються у формі вільно вживаного ПЗ, мають ряд усталених базових взаємоінтегрованих технологій у своїй основі (таких як LAMP – Linux, Apache, Mysql, PHP).

Пропієтарні охоплюють соціальні середовища глобального масштабу, технологічні рішення є закритими та унікальними. Формально число таких систем є невелике, хоча успішні системи цього класу забезпечують більшу частку публічних соціальних комунікацій.

Обидва технологічні класи рішень породжують велику кількість варіацій ССІ з окремими особливостями. Попри те, переважно усі ССІ мають ряд спільних для усіх соціальних середовищ характеристик, які лягають далі в основу спеціальної формальної моделі (див. Розділ 2. «Побудова формальних моделей ССІ з врахуванням безпекового фактору»).

Визначимо такі характеристики далі. Основою визначення є усталені на практиці схеми рішень та окремі наукові дослідження [110, 112, 116, 117, 118].

Організація за схемою «стаття + обговорення». Практично для всіх ССІ характерною є наступна структура контенту (див. рис. 1.1):

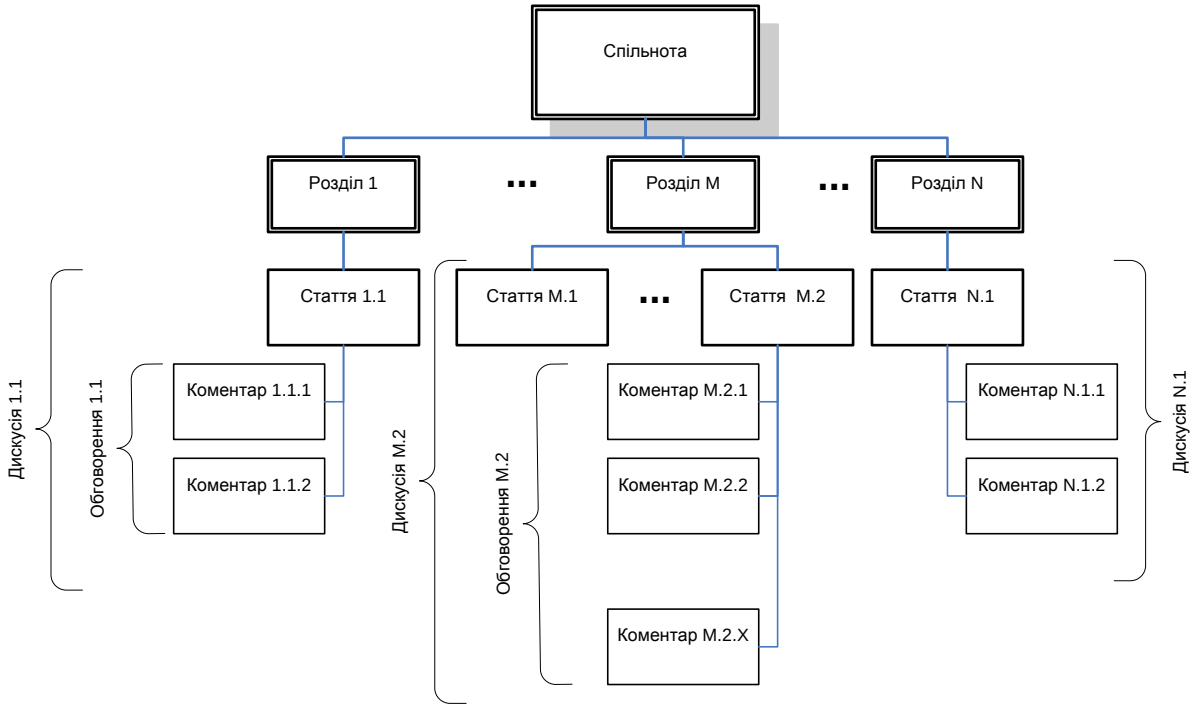

Рис. 1.1. Структура контенту ССІ

Весь контент складається з певних структурних одиниць («дискусій»), які можуть бути погрупованими певним чином. У самій дискусії визначено два основних структурних елементи: *початкова стаття* (варіанти: перше повідомлення, актуальна версія) та її *обговорення* у формі дописів користувачів (коментарі, повідомлення у

дискусії, правки). Порядок сортування і форма подачі усієї дискусії та коментарів залежать від конкретного класу ССІ.

Реактивність середовища. Здійснення дій із створення нового контенту породжує зворотну реакцію середовища у різних формах, у тому числі найважливіших: зміна множини учасників ССІ (наприклад, поява нових користувачів, які зацікавилися темою; вихід користувачів через обурення) та *зміна контенту* (наприклад, поява нових коментарів у відповідь).

Наявність типових ролей користувачів. У кожному соціальному середовищі у процесі комунікації неминуче визначаються окремі типові ролі для користувачів. Ряд ролей визначається наперед (наприклад модератори). Перелік і характеристики ролей не є фіксованим і залежить як від ССІ, так і від завдань, для вирішення яких необхідна формалізація ролей. Так, ряд спеціальних ролей, актуальних для завдань безпеки інформаційного простору запропоновано далі в роботі (див. розділ 2.1.7 «Спеціальні ролі користувачів у процесах соціокомунікативного протиборства в інформаційному просторі»).

Наявність системи правил для управління. Кожне ССІ у першу чергу є соціальною системою, яка утворюється внаслідок взаємодії людей між собою. Стабільність системи, динаміка та перспективи її розвитку визначаються регулятивними механізмами, які найчастіше подаються у формі певних правил. Навіть якщо вони чітко не прописані, вони всеодно наявні в тій чи іншій формі і за необхідності можуть бути чітко формалізованими. Регулюванню переважно підпадають характер та зміст контенту, способи та стилістика комунікації учасників, система рангування та ієрархізації користувачів, система мотивацій користувачів.

Спільні ознаки можуть по-різному проявлятися в різних типах ССІ. У загальному випадку повноцінна типізація ССІ є неможливою, так як існує значне число змішаних середовищ, крім того, постійно з’являються

нові спільноти з новими рисами, проте з точки зору системної організації процесу комунікації можливим і доцільним є виділення наступних типів соціальних середовищ, які розглянуті у наступних підрозділах та є основою для елементів формальної моделі спільнот (див. розд. 2.2.2 «Технічні характеристики віртуальних спільнот»).

1.2.1. Веб-форуми та standalone-блоги

Веб-форуми та класичні персональні автономні (standalone) блоги історично є першими формами соціальних середовищ Інтернету, Веб-форуми фактично є прямим продовженням популярних до появи WWW інших форм спільнот, відповідно вони довгий час домінували в інформаційному просторі.

З середини 2000х інші форми ССІ почали створювати відчутну конкуренцію форумам та блогам, проте вони на сьогодні не втратили актуальності як суттєва складова інформаційного простору. Особливо велике значення вони мають як певні регіональні площадки та як площадки для інформаційної діяльності відомих персоналій.

На сьогодні практично всі значущі форуми та блоги реалізуються на ряді типових програмних платформ (часто вільновживаних) у вигляді автономних веб-сайтів. Даний підхід забезпечує використання глобальних пошукових систем у окремих завданнях державної безпеки (глибокий пошук важливого контенту, виявлення важливих спільнот). Використання даного інструментарію описано в наукових працях вітчизняних вчених [66, 68, 110].

Водночас, автономність сайтів форумів та блогів суттєво ускладнює систему ідентифікації користувачів [39, 41, 42, 43]. На кожному сайті існують окремі логіни, як правило, поширена можливість анонімної (під псевдонімом) активної діяльності. Це і є одним із факторів, які на сьогодні визначають популярність даного типу ССІ. Водночас, беручи до уваги

завдання інформаційної безпеки, анонімність користувачів є відчутним викликом.

З огляду на організацію контенту у випадку форумів діють наступні правила:

- коментарі об'єднано з статтею в єдину дискусію;
- дискусії згруповано за розділами;
- Впорядкування дискусій в розділах – хронологічне, свіжо коментовані зверху;
- впорядкування коментарів у дискусіях – хронологічне, нові знизу.

Для блогів мають місце наступні правила:

- коментарі об'єднано з статтею у єдину дискусію;
- дискусії згруповано за ключовими словами;
- впорядкування дискусій – хронологічне, свіжо створені зверху;
- впорядкування коментарів в дискусіях – хронологічне, нові знизу.

Дані правила важливі з огляду на тактику інформаційної протидії в ССІ і визначають доцільність і форму реакції на ті чи інші дописи.

1.2.2. Електронні ЗМІ та колективні блоги

Дані ССІ є певним гібридом класичних блогів та новинних видань. Вони є зручними майданчиками для авторів-волонтерів, знімаючи з них ряд складних завдань з технічної організації площадки. Часто існує система комерційних мотивацій авторів. Окремі площадки даного типу мають глобальний масштаб та значення (Reddit, Livejournal тощо). Попри відносно невелику частку трафіку та контенту в загальному обсязі вони часто відіграють роль стартової площадки значних інформаційних кампаній, що характеризує їх, як критично важливі для національної безпеки.

Організація інформації аналогічна блогам, з додатковою рубрикацією за авторами. Часто коментарі відділені від основних статтей,

що зменшує їхню важливість. Окремою характерною рисою є наявність порталів, де відображаються найважливіші (з точки зору редакцій) матеріали, що також нерідко стає об’єктом інформаційно-психологічних маніпуляцій.

Система логінів дозволяє зв’язати автора матеріалів з його коментарями до інших авторів, що значно спрощує завдання пошуку.

1.2.3. Електронні самомодеровані енциклопедії

Даний клас ССІ на сьогодні має чітко вираженого лідера – проєкт «Вікіпедія» та ще кілька авторитних аналогічних проблемно-орієнтованих сайтів. Їхня роль та значення в сучасному інформаційному протиборстві є винятково важливі, адже вони в очах звичайних користувачів сприймаються як головне джерело об’єктивної довідкової інформації. Саме статті Вікіпедії по кожному об’єкту формують перше початкове враження про об’єкт, стають ключовими аргументами в дискусіях тощо.

З технічної точки зору дані проекти реалізуються на схожому програмному забезпеченні, з певними типовими рішеннями (оформлення, мова розмітки тощо). Вікі-проєкти мають доволі своєрідне структурування інформації, відмінне від усіх інших ССІ:

- стаття існує автономно від дискусії, зміни в статті відображають певний консенсус в межах дискусії;
- дискусія розміщена окремо, впорядкування коментарів деревовидне, хронологічне;
- ведеться версійний облік статті, доступні і актуальна і архівні версії.

Системи даного класу мають розвинуті внутрішні інструменти пошуку та адаптовані до глобального пошуку за допомогою ГПС.

Наявна можливість (в омежених масштабах) анонімного редагування, проте інформація про IP-адреси є загальнодоступною, що спрощує вирішенння завдань ідентифікації авторів при необхідності.

1.2.4. Сервіси соціальних мереж

Сервіси соціальних мереж, хоча є найновішим видом ССІ і захопили більшу частку приватних та публічних соціальних комунікацій в Інтернеті, проте їх номенклатура є вкрай обмежена, фактично можна стверджувати, що весь світовий ринок даних послуг розділено менше, ніж між десятьма учасниками, серед яких домінують Facebook, Vkontakte та RenRen.

За структурою організації інформації та системи коментування дані сервіси майже аналогічні колективним блогам (у випадку персональної подачі інформації) та форумам (у випадку розгортання спільноти), характер подання коментарів завжди ієрархічно-хронологічний.

Особливістю є явно організована система соціальних зв'язків між користувачами, що в поєданні з наскрізною для всього сервісу ідентифікацією користувача відкриває додаткові можливості з соціального моніторингу. Водночас суттєво обмежені можливості застосування ГПС для глибинного пошуку в цих ССІ.

Критичність даного виду ССІ визначається їхнім домінуванням в інформаційному просторі та охопленням більшості користувачів Інтернету. Проте, водночас, більшість інформації в ССІ носить вторинний характер, запозичається з інших джерел (особливо з колективних блогів). Відчутним є брак якісного контенту з високими споживчими якостями, що робить соціальні мережі вразливими для певних видів повідомлень вірусного характеру.

1.2.5. Проблемно-орієнтовані сервіси та соціальні мережі з обмеженим функціоналом

Даний вид ССІ є відгалуженням від попереднього виду ССІ, часто є певним чином інтегрованим з головним соціальним сервісом (Instagram та Facebook, Youtube та GooglePlus тощо). Зазвичай дані сервіси мають обмежений функціонал в частині організації спільнот і соціальних зв'язків

та роблять акценти на одному типі контенту (короткі повідомлення, відео, фото).

Особливістю даних сервісів є висока зручність користування, оперативність поширення інформації, інтегрованість в мобільні платформи (окремі сервіси, такі як Viber та Telegram розглядають мобільні платформи як первинні).

Організація інформації зазвичай або відповідає блоговому типу або носить примітивний потоковий характер. Пошук інформації часто ускладнений. У силу певних психологічних механізмів дані середовища часто використовуються як первинні лідерами думок регіонального та глобального масштабу (прикладом є Twitter-акаунт Президента США Д.Трампа).

Важливість для національної безпеки визначається певними традиціями використання даних сервісів у випадку ескалації напруженості в суспільстві. Крім того, ряд сервісів активно використовуються для секретної комунікації в межах певних спільнот.

1.3. Аналіз форм публічної інформаційної діяльності в ССІ

Дослідимо питання щодо наявних на сьогодні форм публічної інформаційної діяльності у соціальних середовищах Інтернету. Дане питання перегукується з аналізом ССІ, проведеним вище, проте важливо відзначити, що форми публічної діяльності не обов’язково є фіксованими певними класами ССІ, можуть здійснюватися в межах різних ССІ наявними у них засобами.

Основними ознаками для типізації наявних форм виберемо наступні:

- колективність створення – персонально чи колективно формується контент;
- контроль над контентом – наявність контролю над контентом, що формується, чи делегування його.

Колективна робота над контентом передбачає технічне забезпечення багатокористувацького опрацювання контенту та наявність правил та процедур його формування, вирішення колізій.

Контроль над контентом передбачає забезпечення певних технічних інструментів для накопичення, опрацювання, публікації контенту.

З урахуванням наведених вище ознак отримуємо наступні форми інформаційної діяльності:

- ведення персонального інформаційного каналу;
- організація та ведення власної спільноти;
- участь у існуючих чужих спільнотах;
- інформаційний паразитизм.

Розподіл між ознаками наведено далі у табл. 1.1.

Таблиця 1.1. Форми інформаційної діяльності

Контроль\Колективність	**Ідивідуально**	**Колективно**
Контрольовано	Персональний канал	Власна спільнота
Безконтрольно	Паразитизм	Чужа спільнота

Розглянемо їх детальніше.

Ведення персонального інформаційного каналу полягає в організації системи публікації контенту автором у межах певного автономного персонального простору. Найбільш значимою ця форма є для осіб з високими творчими характеристиками та вмінням створювати контент, часто такі особистості характеризуються термінами «лідер думок», «блогер», «незалежний журналіст», «колумнист» тощо. Як правило, ця форма реалізується наступними засобами (для різних середовищ):

- standalone-блог – для блогів та форумів;
- авторська колонка – для ЗМІ та колективних блогів;
- власна сторінка – для соціальних мереж та інших сервісів;

- канал новин – для сервісів електронних повідомлень типу Viber або Telegram.

Організація та ведення власної спільноти полягає в організації системи публікації контенту автором у межах колективного простору з певними правилами. Найбільш значимою ця форма є для осіб з високими організаційними характеристиками та вмінням організувати комунікацію, часто такі особистості характеризуються термінами «модератор», «адміністратор», «редактор» тощо. Як правило, ця форма реалізується наступними засобами:

- Веб-форум – для блогів та форумів;
- Група – для соціальних мереж та сервісів електронних повідомлень;
- Власна автономна енциклопедія – для енциклопедій.

Участь у чужій спільноті полягає у використанні системи публікації контенту автором у межах існуючого колективного простору, створеного незалежно від автора. Найбільш значимою ця форма є для осіб з високими потребами у комунікації, часто такі особистості характеризуються термінами «мережевий активіст», «експерт», «активний учасник», «авторитетний учасник» тощо. Як правило, ця форма реалізується наступними засобами:

- веб-форум – для блогів та форумів;
- групи – для соціальних мереж та сервісів електронних повідомлень;
- глобальні енциклопедії – для енциклопедій;
- система хеш-тегів – для обмежених соціальних мереж.

Інформаційний паразитизм полягає у використанні ресурсу популярності автора у межах його персонального простору, створеного незалежно від автора. Найбільш значимою ця форма є для осіб з психологічними проблемами у комунікації, часто такі особистості характеризуються термінами «троль» або «мережевий фан» (залежно від характеру комунікації). Найчастіше ця форма реалізується як:

- коментування колумністів - у ЗМІ та колективних блогах з обмеженими правами модерування авторів;
- позначки відомих людей у малозначимих авторських дописах – у соціальних мережах;
- надокучливе гіперактивне коментування – в обмежених соціальних мережах типу Instagram.

Проведена вище класифікація форм публічної інформаційної діяльності та класів соціальних середовищ лягають в основу окремих елементів формальної моделі, що побудована у наступному розділі дисертації («Побудова формальних моделей ССІ з врахуванням безпекового фактору»).

1.4. Аналіз окремих тенденцій у інформаційній та маркетинговій діяльності в ССІ

Більшість практичних результатів з інформаційного протиборства та захисту національного інформаційного простору лежать, опираючись на практичні та теоретичні напрацювання у певних суміжних областях людських знань. Серед них, у першу чергу, слід зазначити такі галузі, як маркетинг у соціальних середовищах Інтернету (Social Media Marketing, SMM) та окремі види онлайн-бізнесу з надання рекламних послуг, які зводяться до надання різних площадок (різних типів: спільноти, персональні блоги, сайти тощо) для реклами з відповідною подальшою монетизацією. Окрім того, близькими за контекстом є дослідження з розвитку електронної демократії на інфраструктурі Інтернету.

З наукової точки зору дані напрямки на сьогодні є дослідженими рядом вітчизняних [71, 72, 81] і закордонних учених [16, 24, 86, 88], водночас існує широкий спектр практичних напрацювань, методологічна основа яких є закритою для наукового загалу і носить характер «ноу-хау». Слід відзначити, що такий підхід не дозволяє отримати повторювальні

результати, хоча би з певним рівнем задовільної імовірності, та породжує системні ризики для суб'єктів, що ними користуються.

Далі проаналізуємо окремі тенденції, що спостерігаються в сучасних практичних напрямках інформаційної діяльності та їхнє науково-методологічне підгрунтя.

Слід відзначити, що домінуючим трендом у маркетинговій і рекламній діяльності в соціальних мережах стали форми непрямого прихованого впливу на користувачів. Формально активність і форми використання непрямого впливу стали певною межею між «білим» та «чорним» маркетингом. До першого виду можна віднести більше класичні рекламні моделі та традиційні моделі інформування населення. Відповідно, для таких форм застосовується термін «інформаційна діяльність» установи чи іншого суб'єкта. Другий вид впливу носить більше маніпулятивний характер, спрямований не на свідоме прийняття рішення користувачами, а на інші форми несвідомого впливу (з різного виду маніпуляціями). Основою даного напрямку є створення інформаційного тиску на користувачів ССІ з боку інших, формально незаангажованих користувачів, використання їх як носіїв відповідних впливів (як свідомо так і несвідомо). У принципі, і в «білій» рекламно-маркетинговій діяльності також використовується даний підхід, проте він носить неприхований характер (відомий навіть термін «партизанський маркетинг»), а є певним чином наперед задекларованим [78, 113]. Відповідно, навколо даного тренду виділилося декілька основних напрямків, проаналізованих далі.

1.4.1. Використання лідерів думок у процесах маркетингу та пропаганди

Одним із головних напрямків практичної інноваційної активності в сфері маркетингу останньої декади є активне залучення (як правило,

частково або повністю приховане) конкретних осіб, які мають високий вплив на суспільство в певній тематичній ніші. Їхні впливи проявляються, як правило, в формі високої популярності особи або, створених нею, матеріалів у певних суспільних колах. Для таких осіб з'явилася усталена назва «лідери думок» [6, 30]. Існує чітка тенденція до вирішення маркетингових та пропагандиських завдань через пошук, ідентифікацію та подальші домовленості з лідерами думок щодо поширення необхідної тенденційної інформації [29]. Її подання також відбувається у певному персоналізованому форматі, як особисті судження автора та його переконання, або факти, достовірність яких він підтверджує особисто.

Основними завданнями у роботі з лідерами думок є:

- виявлення лідерів думок, визначення рівня їхньої суспільної значимості в певних вимірювальних одиницях та їхньої аудиторії;
- знаходження системи впливів на лідера думок, як правило – домовленості, найчастіше фінансового характеру;
- підготовка матеріалів, які потім поширюватимуться від імені лідера думок;
- моніторинг ефективності співпраці з лідером думок.

Реалізація указаних завдань на практиці може здійснюватися вкрай ефективно, особливо враховуючи той факт, що можливість монетизації свого неформального статусу підштовхує лідерів думок до завищення показників своєї популярності та суспільної значимості. Це актуалізує ряд завдань з формалізації показників лідерів думок та обліку їхньої активності, які вирішені далі у даній роботі.

1.4.2. Віртуальні спільноти як інструмент інформаційних впливів

Іншим практичним напрямком, який активно використовується останніми роками, є здійснення впливів через спільноти. Певною мірою він схожий до попереднього, проте відрізняється ширшим інструментарієм

та завданнями впливу. Окрім поширення думок від імені особи, можливим є організація більш системного тиску на громадську думку шляхом появи відчуття певної солідарності між учасниками. Такий вплив характеризується певним рівнем самопідтримки, у силу механізмів зворотнього зв'язку в спільнотах маркетолог може розраховувати на залучення додаткових учасників без необхідності забезпечувати їм винагороду. Особливо цей фактор важливим є у політичній пропаганді, так як дозволяє задіювати ресурси небайдужих громадян у власних цілях [8, 11, 13, 34, 36, 38, 96].

Реалізація впливу на саму спільноту здійснюється кількома шляхами, хоча зазвичай освновним є отримання підтримки від адміністрації спільноти та кількох активних учасників. Для співпраці зі спільнотами використовуються аналогічні підходи як для лідерів думок, окрім того, активно розвиваються додаткові напрямки в роботі зі спільнотами:

- формування власних, повністю підкотрольних спільнот;
- руйнування спільнот, які здійснюють невигідну діяльність.

Перший напрям характерний та активно використовується в маркетингу великих корпорацій, особливо таких, що орієнтовані на масового користувача. Завдяки таким спільнотам корпорації вдається об'єднати прихильних до себе споживачів продукції, отримуючи потужний додатковий ресурс для подальшого її просування. Окрім суто виконання рекламних завдань, такі спільноти відіграють вкрай важливу роль зворотнього зв'язку «споживач-виробник». Завдяки їм виробнику вдається сформувати великі бази знань щодо ефективної експлуатації продукції (наприклад Microsoft TechNet) та отримання інформації щодо необхідних вдосконалень та доопрацювань. У даному напрямку існує значне число публічно доступних досліджень, зокрема роботи [62, 115, 129] та іноземні [1, 28, 33].

Окрім корпорацій, формування власних спільнот є важливим інструментом діяльності політичних сил, які використовують їх водночас і як інструмент пропаганди, і як інформаційну технологію обліку прихильників та координації їхніх дій. Відзначимо, що в сучасних умовах даний підхід усе частіше дозволяє політичним рухам «віртуалізуватися», повністю здійснюючи внутрішньопартійну діяльність через Інтернет.

Враховуючи дану тенденцію, проявляється також і протилежний напрямок діяльності – цілеспрямоване руйнування корисних опоненту спільнот. У сферах бізнесу даний феномен практично не прослідковується, проте він є поширений у політичному протиборстві як інструмент послаблення противника. Серед досліджень у даному напрямку слід виділити роботи Р.Гумінського [64, 65, 66, 67, 68], який побудував математичні моделі агресивних дій щодо спільнот.

1.4.3. Завдання з ідентифікації користувачів та їхніх прихованих характеристик

Одним із найбільш динамічних напрямків досліджень останніх років є дослідження з виявлення прихованих характеристик користувачів ССІ на основі їхньої активності в мережі, розміщеного ними текстового та мультимедійного контенту та їхніх соціальних зв’язків. Комплексний огляд таких досліджень та актуального стану технологій подано у роботі [21]. У цьому напрямку активно використовуються технології опрацювання великих даних, інтелектуального аналізу даних різних типів, автоматизованого збору інформації з гетерогенних джерел тощо. В основі цих методів лежать статистичні моделі, структурні лінвістичні моделі та нейронні мережі. Результати таких досліджень мають величезне прикладне значення в маркетингу (для роботи з цільовою аудиторію, персоналізацією споживачів, пошуку нових споживачів тощо), в управлінні інформаційною діяльністю (для визначення прихованих мотивів і характеристик

користувачів) та в національній безпеці (для ідентифікації окремих користувачів, виявлення прихованих зв’язків та груп тощо).

Можливість проведення такого типу досліджень є сильно регульована наявністю безпосереднього доступу до первинних даних, а саме до БД ССІ. Враховуючи сучасну тенденцію певного «перекосу» в бік кількох глобальних соціальних мереж, можна стверджувати, що в більшості випадків такий доступ є відсутній (окрім власників таких мереж та, можливо, спеціальних служб держав, яким формально належать ці мережі, у першу чергу США, Китай та РФ). Як результат, методи аналізу користувачів ССІ змушені використовувати лише неповні, слабо структурувані дані, що ставить нові вимоги до них. У даному напрямку цікавими є дослідження з автоматизованого виявлення окремих соціально-демографічних ознак користувачів на основі автоматизованого структурного та статистично-лінгвістичного аналізу, створеного ними текстового контенту [3].

1.4.4. Форми ресурсної підтримки у процесах інформаційних впливів у ССІ

Допоміжним, але вкрай важливим, напрямком досліджень з використання ССІ у прикладних задачах є визначення ефективних форм ресурсної підтримки процесів, що відбуваються в ССІ.

Очевидно, що з точки зору маркетолога, підтримці підлягають лише ті процеси, результат яких є корисним для корпорації. Це обумовлює необхідність визначення підходів до точкової ресурсної підтримки. Традиційно, ресурсна підтримка носить фінансовий характер або певний його еквівалент, проте на сьогодні, існують і інші форми підтримки. Визначимо наступні форми підтримки:

- **фінансова** – пряма фінансова підтримка суб’єктів процесу;

- **інформаційна** – забезпечення суб’єкту необхідною інформацією, що спрощує його діяльність, робить її ефективнішою та менш затратною (якщо суб’єкт витрачає кошти на створення контенту);
- **популяризаційна** – забезпечення суб’єкта суспільною увагою (читачами, цитуваннями тощо), що робить його діяльність більше значущою та, можливо, більш вигідною з фінансової точки зору (якщо суб’єкт монетизує трафік);
- **акційна** – забезпечення суб’єкта допоміжними ресурсами та можливостями (мережеві ресурси, консультації), у тому числі і правового характеру (юридична консультація, фізичний захист тощо), що забезпечує суб’єкту можливість надійного довготривалого виконання завдань.

Конкретні форми та методи надання ресурсів різняться як для кожного ССІ, так і для кожної предметної області. Окрім маркетингу, аналогічні ресурси задіюються і в процесах інформаційного протиборства та пропаганди, причому стимулюванню підлягають не лише конструктивні, але й необхідні, з точки зору замовника, деструктивні дії.

Дана типізація ресурсного забезпечення використовується далі у формальній моделі користувача ССІ, визначенні спеціальних ролей (див. розд. 2.1.7 «Спеціальні ролі користувачів у процесах соціокомунікативного протиборства в інформаційному просторі») та в алгоритмах захисту інформаційного простору держави (див. розд. 3.2 «Планування заходів із захисту інформаційного простору держави»).

1.4.5. Сучасний інструментарій для реалізації окремих завдань інформаційної діяльності в ССІ

Значна частина завдань, що виконуються в ССІ, є достатньо рутинними і трудомісткими. У той же час, ССІ, зазвичай, не дають змоги працювати з сильно структурованими базами даних та інтерфейсами

обміну даними, що ускладнює обробку масивів даних традиційними програмними засобами. Це актуалізувало широкий спектр досліджень з використання цілого спектру інтелектуальних технологій в роботі з соціальними середовищами. Далі коротко їх проаналізуємо. Важливо зазначити, що адміністрація ССІ категорично не зацікавлена в будь-яких формах автоматизованого впливу внутрішніми суб'єктами з ряду причин, у тому числі системного і економічного характеру, і, відповідно, організовує певні захисні механізми. Натомість пропонуються фінансово витратні і функціонально обмежені схеми купівлі послуг в ССІ та взаємодії з ССІ певних типів (в першу чергу, розроблення онлайн-ігор для ССІ).

Інтелектуальні засоби збору, парсингу даних застосовуються для ССІ, у яких, зазвичай, є обмежені можливості роботи традиційних роботів пошукових систем та відсутні можливості безпосереднього доступу до даних (на сьогодні такі обмеження характерні практично для всіх систем за винятком wiki-середовищ та окремих колективних блогів). Засоби даної групи у різні способи маскуються або використовують класичні Веб-браузери (автоматизуючи їх), і збирають первинну інформацію у формі HTML-сторінок, маскуючи при цьому свою поведінку (інтенсивність, шлях навігації тощо) під звичайного користувача. Далі зібрана слабоструктурована інформація проходить трансформацію в структуровані дані, на цьому етапі застосовуються інтелектуальні засоби виявлення регулярних структур в гіпертексті [44, 90, 95]. Задача суттєво ускладнюється наявністю динамічних елементів сторінок, частою зміною їхньої структури та певними захисними механізмами різної складності (CAPCHA тощо).

Програмні засоби автоматизації рутинних технічних дій є одним з найпоширеніших і, водночас, найменш контраверсійним видом спеціалізованого ПЗ. У першу чергу, вони охоплюють завдання підвищення зручності та ефективності верстання тексту та підготовки

фото, відео матеріалів. Інші варіанти засобів можуть охоплювати завдання автоматизованого моніторингу новин, автоматизоване оцінювання та ретрансляцію матеріалів. Окремим видом є засоби автоматизованої реєстрації акаунтів та формування мережі друзів для них, які потім активно використовуються в «чорних» методах маркетингу та пропаганди, таких як спам.

Інтелектуальні засоби автогенерації тексту все ширше використовуються в цілому спектрі завдань, причому як в завданнях «білого» класу, так і «чорного». Набули велику популярність в маркетингу та системах класу CRM так звані «**чат-боти**», які здатні надавати прості інформаційні послуги від імені працівників корпорацій, підвищуючи оперативність та зменшуючи затратність підтримки. Крім того, автогенерація усе частіше використовується для побудови текстів новин за певними «реперними» даними. Так, за деякими прогнозами, більшість новин навіть провідних світових видань уже за 10-15 років будуть автогенеруватися такими засобами, проте вони можуть активно використовуються і в деструктивних цілях. Зокрема, такі засоби усе частіше використовуються для написання текстів руйнівного характеру (тролінгу, флейму тощо), створення масового інформаційного тиску, генерації фейкових новин. Особливо серйозний вплив на інформаційний простір такі засоби здатні здійснити за умови поєднання в один комплекс з засобами автореєстрації акаунтів. Наукові дослідження з автогенерації текстів мають значну історію, і є продовженням досліджень з організації природномовних інтерфейсів . Дотичними до них є також дослідження з детектування автогенерованих текстів, зокрема спаму в електронній кореспонденції [26].

1.5. Висновки до розділу

У першому розділі дисертації досліджено соціальні середовища Інтернету як джерело позитивних та негативних впливів у системі національної безпеки.

У розділі здійснено системний аналіз основних класів соціальних середовищ: Веб-форумів та standalone-блогів; електронних ЗМІ та колективних блогів; самомодерованих енциклопедій; сервісів соціальних мереж. Проаналізовано особливості кожної з платформ та правила організації контенту.

Далі проведено аналіз форм публічної інформаційної діяльності в описаних вище класах соціальних середовищ, здійснено класифікацію за ознаками «колективність» та «контрольованість» результатів діяльності.

Технології інформаційної та маркетингової діяльності в ССІ, які за змістом та характером є суміжними з завданнями захисту інформаційного простору, є важливими орієнтирами для наукових досліджень у даній сфері, тому на завершення розділу досліджено окремі тенденції онлайн-маркетингу, зокрема: використання лідерів думок при формуванні громадської думки, використання віртуальних спільнот як інструменту для PR, окремі питання взаємодії з користувачами соціальних середовищ.

Розділ 2. Побудова формальних моделей ССІ з врахуванням безпекового фактору

Як було показано вище, соціальні dсередовища Інтернету на сьогодні є ключовим елементом інформаційного простору держави, і, водночас, найбільш вразливим до ряду загроз соціокомунікативного характеру.

Підвищення рівня захисту соціальних середовищ Інтернету вимагає широкого комплексу заходів, у тому числі інформаційно-технологічних: комп'ютерних програм, інформаційних систем та сервісів, високотехнологічних людино-машинних систем з елементами штучного інтелекту.

Реалізація таких систем є неможливою без формалізації предметної області, як основи для алгоритмів їхнього функціонування та відповідних моделей даних. Далі в розділі пропонується формалізація соціальних середовищ Інтернету, як двохкомпонентної стуктури.

Перша компонента – користувачі Інтернету, які використовують соціально орієнтовані сервіси, тобто є користувачами соціальних середовищ.

Друга компонента – об'єдання людей (спільноти), які власне і є інструментом для широкого обміну інформацією, і відповідно – соціокомунікативного протиборства.

Далі у розділі пропонуються формальні моделі обох компонент, які орієнтовані на застосування в задачах підвищення безпеки та захисту інформаційного простору держави.

Основні результати розділу автором опубліковано в роботах [105, 108, 109, 111].

2.1. Формалізація користувачів соціальних середовищ Інтернету з точки зору безпеки інформаційного простору держави

На сьогодні існує ряд підходів до класифікації користувачів соціальних середовищ Інтернету, зокрема в роботах, проте переважно пропоновані класифікації зосереджені на проблематиці організації ефективного функціонування віртуальних спільнот. У роботі [118] виділено ряд спеціальних категорій учасників спільнот з огляду на їхні поведінкові характеристики. У роботі [15] виділено методи оцінки користувачів соціальних середовищ Інтернету, що базуються на характері їхньої взаємодії з органами державної влади. Ці підходи є доволі близькими до проблематики захисту національного інформаційного простору, враховуючи загальні принципи цих класифікацій – поведінка в межах віртуального соціуму, характер впливу на державні інституції. Попри це, згадані дослідження не охоплюють окремі, важливі саме з точки зору соціоінформаційної безпеки, аспекти: оцінку рівня впливу окремих користувачів на соціум чи віртуальну спільноту, змістовну характеристку діяльності, готовність до взаємодії в завданнях захисту, керованість ворожими структурами.

Окрім того, поза рамками досліджень залишаються такі маргінальні, але поширені в сфері інформаційного протиборства, категорії користувачів як «алгоритмізовані оператори соцільних комунікацій» різного рівня інтелектуальності. У цю категорію потрапляють як люди – виконавці простих алгоритмізованих завдань (імовірно за засадах відрядної оплати праці) з мінімальними елементами творчості, так і програмні агенти (комп'ютерно-лінгвістичні роботи, «боти») з елементами штучного інтелекту. Врахування, формалізація та алгоритмізація їхнього виявлення є важливою складовою наукових досліджень у сфері соціоінформаційної безпеки.

2.1.1. Спеціальна безпекова модель користувача соціальних середовищ Інтернету

На сьогодні створено ряд спеціальних моделей користувачів соціальних середовищ Інтернету, орієнтованих на вирішення окремих завдань інформаційної діяльності, придатних для формалізації структур прикладних баз даних. Такі моделі наведено зокрема в роботах [4, 40, 89], проте спеціалізація моделей не дозволяє безпосередньо їх використати в завданнях безпеки. Окрім того, окремі, важливі з точки зору безпеки, аспекти в згаданих моделях не враховані (зокрема соціальні зв'язки користувачів Інтернету), так як вони більше орієнтовані не на соцільні мережі, а традиційні Веб-форуми. Водночас, наявні на сьогодні спеціальні безпекові моделі користувачів соціальних сервісів [59, 94, 99], попри свою безсумнівну цінність, не містять достатньої деталізації з точки зору прямого застосування у завданнях проектувань спеціальних проблемно-орієнтованих баз даних, орієнтованих, зокрема, на глибоке архівування та документування даних.

Складові моделі користувача об'єднані в окремі групи за змістовою ознакою. Виділимо такі групи:

- ідентифікатор та персональні дані;
- характеристики державної безпеки;
- активність;
- читачі контенту;
- постачальники контенту;
- спільноти користувача.

Таким чином користувач описується кортежем:

$$User_i = \langle UI_i, US_i, UA_i, UF_i, UH_i, UC_i \rangle, \qquad (2.1)$$

де елементами кортежа є відповідні складові моделі.

Розглянемо далі ці складові детальніше.

2.1.2. Ідентифікатор та персональні дані користувача

Ідентифікація користувача Інтернету в значній мірі може бути зведена до ідентифікації фізичної особи, яку представляє користувач, проте на сьогодні поширеною є ситуація, коли одна фізична особа має багато втілень в мережі, часто – формально незалежних між собою. Окрім того, все більшу частку користувачів-учасників соціальних середовищ інтернету складають віртуальні особистості різних способів реалізації. Детально проблема формалізації користувача ССІ є досліджена в роботах [39, 41, 42, 43]. У цій роботі далі виділяються спеціальні групи користувачів із розбіжністю між фізичною та віртуальною особистістю (див. табл. 2.1).

Таблиця 2.1. Показники ідентифікації користувача (група UI)

Показник	**Позначення**	**Тип даних**	**Коментар**
Унікальний ідентифікатор	UIId	Рядок символів	Ідентифікатор для внутрішньої БД користувачів ССІ
Показники мережевої ідентифікації *UIS* (багаторазово)			
Сфера зацікавлень	UITh	Ключові слова	Тематика, в якій проявляється активність
Адреса ССІ, де розміщено профіль	UISN	URI	Мережева адреса сайту ССІ, головний URI площадки
Ідентифікатор профілю користувача	UISNId	Рядок символів	Ідентифікатор у межах ССІ
Адреса профілю користувача	UISNA	URI	Адреса профілю користувача
Мережеве ім’я	UISName	Рядок символів	Ім’я, закріплене за користувачем (нікнейм)
Показники фізичної ідентифікації *UIR*			
Ім’я особи	UIRName	Повне ім’я та прізвище	
Засоби зв’язку	UIRTele	Група характеристик	Мобільний, пошта, месенджери тощо
Мережеві та технічні дані	UIRNet	Група характеристик	IP-адреси тощо
Демографічні дані	UIRDem	Група характеристик	Вік, стать, освіта, мова тощо
Юридичні дані	UIRJur	Група характеристик	Адреса, документи, ІПН тощо
Показники віртуальної ідентифікації *UIV*			
Рівень віртуалізації	UIVirt	[0,1]	Можливість прив’язки та впливу на користувача через фізичну особу
Рівень інтелектуалізації	UIVIntel	[0,1]	Інтелектуальність ПЗ, що реалізує бота
Типові завдання	UIVBT	Перелік типів	Коментування, трасляція, реагування тощо

Ряд очевидних характеристик даної групи не розкрито, вони є типовими та традиційними для систем моніторингу Інтернет-активності. Показники фізичної ідентифікації мають сенс для користувачів – фізичних осіб, показники віртуальної індентифікації – для ботів (див. далі).

Окремі показники відображають певну нечіткість у формалізації характеристик користувача. Такий підхід відповідає запропонованих у роботах [112, 119] методам моделювання аудиторії сайтів та спільнот.

Важливо, що набір показників мережевої ідентифікації для кожного користувача не є єдиним. Даний розділ характеристик є множиною кортежів з елементами указаного типу. Тобто для однієї особи може бути визначено декілька записів з адресою профіля, ідентифікатором, нікнеймом тощо. Таким чином:

$$UI_i = \langle UIID_i, UIS_i, UIR_i, UIV_i \rangle, \tag{2.2}$$

де $UIS_i = \left\{ \langle UISN_{ij}, UISNId_{ij}, UISA_{ij}, UISName_{ij} \rangle \right\}_{j=1}^{N_i^{(UIS)}}$, $N_i^{(UIS)}$ – кількість мережевих ідентифікацій *i*-ї особи.

Враховуючи, що у багатьох задачах аналізу соціальної структури Інтернету первинною є інформація щодо власне мережевої, а не фізичної ідентифікації, важливою є наступна множина.

$$UIS = \bigcup_{i=1}^{N^{(UI)}} \left\{ \langle UISN_{ij}, UISNId_{ij}, UISA_{ij}, UISName_{ij} \rangle \right\}_{j=1}^{N_i^{(UIS)}}, \tag{2.3}$$

де $N^{(UI)}$ – число фізичних користувачів.

Множина *UIS* являє собою множину усіх мережевих ідентифікацій (умовно – множину віртуальних особистостей в ССІ).

2.1.3. Характеристики державної безпеки

При формуванні бази даних користувачів у задачах захисту інформаційного простору вкрай важливим є облік його окремих

спеціальних характеристик, пов'язаних з державною безпекою. Слід зазначити, що для формалізації даних показників використано апарат нечітних змінних, який успішно зарекомендував себе при описі даної предметної області, зокрема в роботах [59, 94, 98, 100]

Характеристики цієї групи наведено далі у табл. 2.2.

Таблиця 2.2. Показники державної безпеки для користувача (група US)

Показник	**Позначення**	**Тип даних**	**Коментар**
Ставлення до держави	USG	[-1,1]	[антидержавне…патріотичне]
Незалежність суджень	USIn	[0,1]	[повністю керований..самостійний]
Стабільність позиції	USSt	[0,1]	[позиція постійно змінюється..змін немає]
Готовність до діалогу	USDl	[0,1]	[неготовий…відкритий]

Показники даної групи є складними у визначенні, з розвитком технологій штучного інтелекту в сфері опрацювання природномовних текстів на предмет оцінки суджень та виявлення почуттів вони зможуть опрацьовуватися автоматизовано. У принципі, наявний на сьогодні технологічний потенціал і наукові напрацювання [21, 121, 122, 123, 124] дозволяють автоматизувати окремі трудомісткі ділянки (відбір значущих повідомлень, реферування), особливо для англійської та російської мов (враховуючи наявні електронні словники та антології).

Для зменшення трудозатрат ручного опрацювання показники даної групи пропонується визначати лише для користувачів певного рівня значущості або наявності ролей (див. далі).

Попри певну семантичну близькість ознак, на базовому рівні вони розділені саме з міркувань простішого автоматизованого визначення. Так *USSt* «*Стабільність позиції*» відстежується шляхом аналізу зміни лексики протягом тривалого часу, *USIn* «*Незалежність суджень*» ідентифікується як відсутність кореляції між тональністю співрозмовників та тональністю автора в близькі моменти часу. Ознака *USDl* «*Готовність до діалогу*» в автоматизованому режимі ідентифікується найпростіше, шляхом аналізу

лексики на предмет відсутності та наявності відповідних лінгівістичних маркерів (зокрема, лайки, увічливих звертань тощо).

На основі показників табл. 2.2 ми можемо визначити інтегрований показник **гнучкості позиції користувача:**

$$UserFlex(User_i) = USIn_i * USSt_i * USDl_i . \quad (2.4)$$

Цей показник відображає здатність користувача сприймати думку опонентів у дискусіях, змінювати свої погляди у процесі аргументованої дискусії. Далі у роботі показник пропонується використати для визначення методів взаємодії з лідерами думок різних спрямувань.

2.1.4. Формальний опис активності користувача

На сьогодні конкретні форми активності користувача соціальних середовищ Інтернету може проявлятися в різних формах. Узагальнюючи їх на основі типових функцій соціальних мереж, визначимо такі форми активності з формування контенту (див. табл. 2.3):

- **публікація нового контенту** – як допису на сторінці соцмережі, створення нової дискусії на Веб-форумі, запису в блозі;
- **публікація коментаря** – змістовний коментар до дискусії чи запису;
- **ретрансляція контенту** – у формі поширення в соціальній мережі або цитування (на інших платформах);
- **оцінка контенту** – у формі висловлення емоцій в соціальній мережі, виставлення оцінок або написання короткого оцінкового коментаря на інших платформах;
- **акція впливу –** спеціальний вид дії, що спрямований не на контент безпосередньо, а на регулювання дій інших користувачів; наприклад, модерація контенту та користувачів, запрошення нових користувачів, ресурне забезпечення; не всі акції впливу залишають документований інформаційний слід у сучасних ССІ.

Таблиця 2.3. Показники активності користувача (група UA)

Показник	**Позначення**	**Тип даних**	**Коментар**
Розміщений авторський контент	UAUC	Множина записів	Унікальний авторський контент
Суспільно значимий авторський контент	UAIC	Множина записів	Якісний контент для масового споживача
Коментарі	UACom	Множина записів	
Ретрансльований контент	UART	Множина записів	Посилання або репости
Оцінки контенту	UAOM	Множина записів	Лайки, короткі повідомлення, що обмежені оцінкою
Акція впливу	UAIA	Множина записів	
Середня частота розміщення контенту	UACF	Натуральне число	Кількість повідомлень за контольний період (тиждень або місяць).

Формалізуємо авторський контент як:

$$UA_i = \langle UAUC_i, UAIC_i, UACom_i, UART_i, UART_i, UAOM_i, UAIA_i \rangle, \qquad (2.5)$$

де складові кортежа є відношеннями, які описані далі.

Контент, що створено користувачем і розміщено в ССІ:

$$UAUC_i = \left\{ \left\langle ID_{ij}^{(UAUC)}, URI_{ij}^{(UAUC)}, Home_{ij}^{(UAUC)}, Content_{ij}^{(UAUC)}, Date_{ij}^{(UAUC)} \right\rangle \right\}_{i=1}^{N_i^{(UAUC)}}, \quad (2.6)$$

де $ID_{ij}^{(UAUC)}$ - унікальний ідентифікатор контенту; $URI_{ij}^{(UAUC)}$ – мережевий адрес контенту; $Home_{ij}^{(UAUC)}$ – базовий (головний) адрес ресурсу, на якому розміщено ресурс; $Content_{ij}^{(UAUC)}$ – інформаційне наповнення (текст, зображення); $Date_{ij}^{(UAUC)}$ – дата публікації; $N_i^{(UAUC)}$ – кількість записів авторського контенту *i*-го користувача.

Показник $UAIC_i$ відображає контент, що був створений користувачем свідомо для масового ознайомлення. Більша частина традиційного контенту користувачів є цікавою для певного кола друзів (наприклад, побутові фотографії користувача). Деякі записи навпаки, носять характер повідомлення для суспільства (статті, твори тощо). Для певних типів

користувачів частка таких повідомлень може бути значною і навіть переважною.

З точки зору формалізації **суспільно значимий контент** має аналогічну структуру елементів контенту і є підмножиною усього авторського контенту:

$$UAIC_i \subseteq UAUC_i . \tag{2.7}$$

Коментарі включають у себе результати реактивних дій користувача у текстовій формі на появу нового контенту користувачів, яких він відстежує. Відповідно, опишемо їх наступним відношенням:

$$UACom_i = \left\langle ID_{ij}^{(UACom)}, URI_{ij}^{(UACom)}, MainID_{ij}^{(UACom)}, TargetID_{ij}^{(UACom)}, \right. \\ \left. , Content_{ij}^{(UACom)}, Date_{ij}^{(UACom)} \right\rangle_{i=1}^{N_i^{(UACom)}}, \tag{2.8}$$

де $ID_{ij}^{(UAUC)}$ – унікальний ідентифікатор контенту; $URI_{ij}^{(UACom)}$ – мережевий адрес коментаря (якщо його можливо визначити); $MainUri_{ij}^{(UACom)}$ – ідентифікатор головного допису, до якого написано коментар; $TargetID_{ij}^{(UACom)}$ – ідентифікатор цільового контенту, до якого написано коментар; $Content_{ij}^{(UACom)}$ – інформаційне наповнення (текст, зображення); $Date_{ij}^{(UACom)}$ – дата публікації; $N_i^{(UACom)}$ – кількість записів авторського контенту *i*-го користувача.

Ретрансльований контент за структурою своїх елементів відповідає коментарям. Відмінності лежать у технічному аспекті реалізації – ретрансльований контент для читачів подається автономно і може сприйматися як авторський. Описується наступним відношенням:

$$UART_i = \left\langle ID_{ij}^{(UART)}, URI_{ij}^{(UART)}, MainID_{ij}^{(UART)}, TargetID_{ij}^{(UART)}, \right. \\ \left. Content_{ij}^{(UART)}, Date_{ij}^{(UART)} \right\rangle_{i=1}^{N_i^{(UART)}}, \tag{2.9}$$

де опис складових кортежа аналогічний до складових коментаря.

Оцінки контенту описують реакції користувача на контент, які не містять змістовної складової, лише емоційну. На практиці, в соціальних мережах та багатьох інших технічно розвинутих платформах для цього використовується механізм «лайків» (маркерів емоцій) та оцінок, проте на простіших платформах масово використовуються короткі текстові повідомлення з традиційними позначками «+», «*+1*» або короткими текстами на кшалт «*згоден*», «*підтримую*». Описується наступним відношенням:

$$UAOM_i = \left\{ \left\langle ID_{ij}^{(UAOM)}, MainID_{ij}^{(UAOM)}, TargetID_{ij}^{(UAOM)}, Opinion_{ij}^{(UAOM)}, Date_{ij}^{(UAOM)} \right\rangle \right\}_{i=1}^{N_i^{(UAOM)}}, \quad (2.10)$$

де опис складових кортежа аналогічний до складових коментаря, окрім елемента $Opinion_{ij}^{(UAOM)} \in [-1,1]$, який є формалізованим описом реакції користувача на контент. Значення «-1» відповідає повністю негативній, а «1» повністю позитивній оцінці. Уведення такого показника обумовлене відсутністю єдиного механізму передачі емоцій.

Акції впливу описують адміністративні реакції користувачів з додатковими правами на контент користувачів, що розміщено в ССІ. Джерелом акцій впливу є або власники контенту або користувачі з спеціальними правами (адміністратори та модератори спільнот). Описується наступним відношенням:

$$UAIA_i = \left\{ \left\langle ID_{ij}^{(UAIA)}, MainID_{ij}^{(UAIA)}, TargetID_{ij}^{(UAIA)}, Action_{ij}^{(UAIA)}, Date_{ij}^{(UAIA)} \right\rangle \right\}_{i=1}^{N_i^{(UAIA)}}, \quad (2.11)$$

де опис складових кортежа аналогічний до складових коментаря, окрім елемента $Action_{ij}^{(UAIA)} \in [0,1]$, який описує зміну видимості контенту в результаті дій модератора. Значення «0» відповідає повному усуненню видимості контенту, а «1» - максимальному збільшенню видимості контенту до 100% усієї аудиторії, що споживає інформацію з головної сторінки $Home_{ij}^{(UAUC)}$, для якого $MainID_{ij}^{(UAIA)} = ID^{(UAUC)}$. Уведений показник не відображає усього спектру можливих дій з підтримки через їхню

різноманітність і відсутність інформаційного сліду, проте більшість модеративних дій може бути зведена до даної схеми.

У наведених вище виразах, окрім ідентифікатора допису *MainID*, до якого формується додатковий контент, наявний елемент *TargetID*, який покликаний відображати можливість реагування не на початковий допис, а вже на сформовану реакцію (у формах коментарів, трансляцій тощо). Таким чином, множина ідентифікаторів цільового контенту є об'єднанням множин наявних ідентифікаторів кожного типу контенту:

$$TargetID = ID^{(UAUC)} \cup ID^{(UACom)} \cup ID^{(UART)} \cup ID^{(UACom)} \cup ID^{(UAOM)} \cup ID^{(UAIA)}. \quad (2.12)$$

У такому разі, для кожного, з вище наведених виразів, має місце обмеження:

$$TargetID_{ij} \in TargetID. \quad (2.13)$$

Фактично *TargetID* – множина, яка описує єдине адресне поле для всіх типів контенту, що є в соціальних середовищах Інтернету.

2.1.5. Формальний опис соціального портрету користувача

Як було сказано вище, кожен користувач соціальних середовищ Інтернету характеризується не лише контентом, що він генерує, але і системою соціальних зв'язків з іншими користувачами. Формалізуємо їх наступним чином, об'єднавши в **соціальний потрет користувача ССІ**.

Розглянемо його складові.

Читачі (споживачі) контенту – користувачі ССІ, які мають оформлену підписку на автоматизоване отримання нового контенту, що створюється користувачем. Домінуючою на сьогодні є технологія підписки через системи відстеження та друзів у соціальних мережах. Крім того, для середовищ Веб-форумів та блогів активно використовуються традиційні підписки засобами електронної пошти або електронними месенджерами. У зв'язку з цим не можна не відзначити стрімко зростаючу популярність

месенджера Telegram для реалізації підписок на контент. Окрім того, використовуються можливості RSS каналів та оповіщень Веб-браузерів.

На сьогодні, у силу технологічних особливостей, ефективному моніторингу зі сторони третіх осіб підлягають лише підписки через соціальні мережі. Для власників платформи доступна також інформація щодо користувачів email та месенджерів. Користувачі, що оформляють автоматизований доступ через RSS та оповіщення браузера, в загальному випадку обліку не підлягають.

Споживачів контенту формально опишемо як підмножину усіх множин віртуальних особистостей в ССІ:

$$UF_i \subset UIS. \qquad (2.14)$$

Аналогічно, постачальники контенту теж є підмножиною тієї є множини

$$US_i \subset UIS. \qquad (2.15)$$

Постачальниками контенту вважатимемо тих користувачів, від яких, за технологіями описаними вище, здійснюється доставка контенту *i*-му користувачу.

Окремим гібридним видом соціальних зв'язків є участь у спільнотах. Спільноти забезпечують зв'язок між користувачами за іншою схемою, з проміжними центрами дистрибуції інформації. Кожен користувач спільноти використовує її для постачання контенту і для споживання контенту. Усі учасники спільноти є споживачами створеного ними контенту в межах спільноти.

Визначимо для кожного користувача такі підмножини множини усіх його спільнот UC_i:

Спільноти з правом перегляду – множина мережевих ідентифікаторів спільнот $UComR_i = \{CIN_j, \text{де i - й користувач читачем}\}_{j=1}^{N^{(Com)}}$, $N^{(Com)}$ – число спільнот.

Спільноти з правом публікації – множина мережевих ідентифікаторів спільнот $UComP_i = \{CIN_j, \text{де i - й користувач є дописувачем}\}_{j=1}^{N^{(Com)}}$, $N^{(Com)}$ – число спільнот.

Контрольовані ресурси – множина мережевих ідентифікаторів спільнот $UComC_i = \{CIN_j, \text{де i - й користувач модерує контент}\}_{j=1}^{N^{(Com)}}$, $N^{(Com)}$ – число спільнот.

2.1.6. Тематична проекція активності користувача

В описі показників мережевої ідентифікації користувача (див. вище) наявний показник *UITh* для кожного мережевого втілення. Таким чином, для певної фізичної особи наявна множина зацікавлень

$$UITh_i = \{UITh_{ij}\}_{j=1}^{N_i^{(UIN)}}, \qquad (2.16)$$

де $N_i^{(UIN)}$ – число мережевих ідентифікацій *i*-го користувача.

Далі в роботі у різного роду алгоритмах та формулах використовуватимемо **тематичну проєкцію** користувача, яка полягає у врахуванні за замовчуванні в моделі того факту, що цікавим, з точки зору завдань безпеки, є лише певна група тематик. Тобто, у конкретній прикладній задачі формується певний базовий набір тематичних маркерів (ключових слів) *BaseTh*, за якими формуються масиви даних. Відповідно до моделі враховується не вся множина зацікавлень користувача, а лише релативна до базової тематики. Мережеві ідентифікації, що не відповідають базовій тематиці (тобто $\{UITh_{ij}\} \notin BaseTh$) не розглядаються.

Відповідно, далі у роботі, при розгляді певних алгоритмів та методів обмеження на відповідність базовій тематиці, з метою спрощення виразів не наводяться, якщо в цьому немає додаткової необхідності. З точки зору моделі даних та архітектури інформаційних систем, що базуються на розробленій формальній моделі, врахування лише певних тематик не має суттєвого значення і відображається на наповненню.

Сам вибір важливих для безпеки держави тематик не є фіксованим і змінюється залежно від стратегічних і оперативних завдань та в зв’язку з появою нових чи декактуалізацією старих загроз.

2.1.7. Спеціальні ролі користувачів у процесах соціокомунікативного протиборства в інформаційному просторі

Як зазначалося вище, дослідження з безпеки соціальних середовищ Інтернету не можуть обходити стороною наявність окремих класів користувачів, що визначені за їхніми соціокомунікаційними ролями. З точки зору сучасних прикладних методик впливу, які використовуються в онлайн-маркетингу та в пропаганді, доцільно виділити такі користувацькі ролі:

- **лідери думок** – особистості з високим рівнем суспільного впливу та числом послідовників;
- **модератори** – особистості з високим рівнем мережевого авторитету та організаційними здібностями;
- **транслятори** – особистості з обмеженими комунікативними функціями поширення інформації;
- **опоненти** – особистості з високим рівнем критичного мислення та мережевим авторитетом;
- **тролі** – особистості з спеціальними руйнівними комунікативними функціями;
- **боти** – віртуальні особистості з обмеженими комунікативними функціями допоміжного характеру.

Далі уведені ролі користувачів розглянемо детальніше.

Для усіх ролей уведено ознаку мінімальної активності з власним для кожної ролі пороговим значенням. Визначення цих констант здійснюється в межах формування комплексного завдання із захисту інформаційного

простору в певному тематичному напрямку з врахуванням актуальних на цей момент характеристик середовищ.

Лідери думок – особистості, які характеризуються високим рівнем креативності, компетентності у предметній області та великою кількістю читачів та цитувань матеріалу. Лідери думок, як правило, не генерують інтенсивного інформаційного потоку, проте всі їхні матеріали є авторськими не лише за формою, але й за змістом, мають певне суспільне значення. Досконало володіють вмінням створювати доступні, легкі для розуміння тексти, іншими літературними прийомами.

В окремих випадках дописи лідерів думок можуть базуватися на попередньо опублікованих матеріалах інших авторів (зокрема новин), проте в будь-якому разі носять авторський характер (аналітичний огляд, критичне судження тощо).

Основна функція лідерів думок – формування нового процесу з поширення певної суспільнозначимої інформації, зокрема такої, як нові трактування фактів, аналітичні огляди та проголошення нових ідей.

На основі уведеної вище моделі сформуємо наступні ознаки для визначення лідера думки:

$$\frac{Count(UAIC_i)}{Count(Content_i)} \geq C_C^{(OL)} \text{ – сильна ознака,} \qquad (2.17)$$

$$\frac{Count(UAUC_i)}{Count(Content_i)} \geq C_C^{(OL)} \text{ – слабка ознака,} \qquad (2.18)$$

де $Content_i = UAUC_i \cup UACom_i \cup UART \cup UAIA_i$ – весь змістовний контент користувача (без оцінок контенту), $C_C^{(OL)} \in [0;1]$ – константа, що визначає необхідну для лідера думок частку авторських матеріалів. Включення до даного числа оцінок є неможливим у силу того, що сьогодні будь-які користувачі ССІ (особливо соціальних мереж) беруть до уваги оцінки контенту безсистемно, часто бездумно та переважно під емоційним

впливом. Число оцінок суттєво (на порядки) перевищує кількість дій інших типів, що може деформувати загальну картину при внесенні його як доданка.

Окрім того, для лідера думки повинна виконуватися ознака достатньої активності:

$$UACF_i \geq C_F^{(OL)}. \quad (2.19)$$

Як правило, доцільно застосовувати сильну ознаку лідера думок. Слабка ознака застосовується у випадках, коли в певній тематиці відсутні лідери думок за сильною ознакою.

Модератори – авторитетні мережеві особистості, які, в силу наявних ресурсів чи персональних характеристик, здатні формувати віртуальні спільноти із залученням лідерів думок та звичайних користувачів. Володіють високими комунікативними та психологічними навичками, креативністю. Знання у предметній області можуть бути поверхневими.

Основна функція модераторів – координація дій користувачів (як звичайних, так і рольових) та їхнє ресурсне забезпечення.

На основі уведеної вище моделі сформуємо наступні ознаки для визначення модератора:

$$\frac{Count(UAIA_i)}{Count(Content_i)} \geq C^{(MC)} \text{ – змістовна ознака,} \quad (2.20)$$

де $C^{(MOC)} \in [0;1]$ – константа, що визначає необхідну для модератора частку дій з існуючим контентом.

$Count(UComC_i) \geq 1$ – адміністративна ознака.

Як правило, для модератора повинні виконуватися обидві ознаки, окрім того, повинна виконуватися ознака активності:

$$UACF_i \geq C_F^{(MC)}. \quad (2.21)$$

Транслятори – особистості, які характеризуються великою мережевою активністю, часто наявністю значного числа читачів та низькою креативністю. Поширюють обсяги схожого тексту з іншого джерела, власних текстів практично не мають. Можуть використовувати спеціальне програмне забезпечення та діяти в режимі флешмобу у спілці з аналогічними користувачами. В окремих випадках транлятори можуть змінювати форму контенту (в тому числі і модифікувати текст), залишаючи зміст незмінним. Слід відзначити, що в окремих дослідженнях роль транлятора змішують з роллю лідера думок, акцентуючи увагу не на інформативних функціях, а на здатності поширювати інформацію серед значної кількості споживачів [10], проте такий підхід обмежує можливість вибору ефективного соціокомунікативного інструментарію для підтримки або протидії у процесах інформаційного протиборства.

Основна функція трансляторів – підтримка та підсилення впливу лідерів думок та підтримка актуальності спільнот шляхом наповнення контентом.

Для визначення транслятора пропонується ознака:

$$\frac{Count(UART_i)}{Count(Content_i)} \geq C^{(TR)}, \qquad (2.22)$$

де $C^{(TR)} \in [0;1]$ – константа, що визначає необхідну для транслятора частку дій з трансляції контенту.

Та ознака активності:

$$UACF_i \geq C_F^{(TR)}. \qquad (2.23)$$

Характерно, що для трансляторів межа активності $C_F^{(TR)}$ повинна бути визначеною доволі високо, значно вище (щонайменше у 10 разів), ніж для лідерів думок, що пов’язано з простішим характером створення контенту.

Опоненти – особистості, які характеризуються специфічним набором характеристик: високою компетентністю у предметній області,

комунікативними навичками з ведення онлайн-дискусій та низьким рівнем креативності. Опоненти можуть продукувати власні матеріали, але тематично матеріали є прив'язаними до тих, що були створені лідерами думок, заперечуючи ідеї та факти, наведені у них. Досконало володіють і активно використовують такі риторичні прийоми як іронія та сарказм, часто володіють значним мережевим авторитетом.

Основна функція опонентів – опонування лідерам думок, нівелювання їхніх впливів та матеріалів.

Ознака опонента формується на основі врахування того, кого саме і в якій тональності коментує коруристувач. У якості такої ознаки пропонується одночасна відповідність наступним двом умовам:

$$\frac{Count(UACom_i)}{Count(Content_i)} \geq C^{(OPC)}, \qquad (2.24)$$

де $C^{(OPC)} \in [0;1]$ – константа, що визначає необхідну для опонента частку дій з коментування;

$$\frac{Count(UACom_i(OpinionLeaders, Negative))}{Count(UACom_i)} \geq C^{(OP)}, \qquad (2.25)$$

де $UACom_i(OpinionLeaders, Negative)$ – число негативних коментарів до контенту створеного лідерами думок;

$Count(UACom_i(OpinionLeaders, Negative)) >> UACom_i((OpinionLeaders, Positive))$, тобто – число негативних коментарів до лідера думок значно переважає число позитивних. Тональність коментарів можна оцінювати експертним шляхом або за допомогою програмних засобів Sentiment Analisys.

Ознака активності для опонента

$$UACF_i \geq C_F^{(OP)}. \qquad (2.26)$$

Межа мінімальної активності для опонента очевидним чином є прив’язана до межі активності лідера думок, співпадає або перевищує її у 2-3 рази.

Тролі – спеціальний тип мережевоактивих особистостей, що характеризується високими комунікативними навичками та психологічною стійкістю, які використовуються в руйнівних цілях щодо спільноти та контенту, що створюється. Головними інструментами є розпалювання ворожнечі в межах спільноти (комунікативне явище «флейму»), зміна акцентів діяльності зі змістовних на порожні балачки (комунікативне явище «флуду»), та перевантаження модераторів спільноти організаційними запитами та скаргами. і активно використовують такі риторичні прийоми як сарказм та перехід на особистості.Діють індивідуально або в межах невеликих кампаній.

Основна функція тролів – руйнування впливу модераторів, пониження впливу лідерів думок та трансляторів.

Ознака опонента формується на основі врахування того, кого саме і в якій тональності коментує користувач. У якості такої ознаки пропонується одночасна відповідність наступним трьом умовам:

$$\frac{Count\left(UACom_i\right)}{Count\left(Content_i\right)} \geq C^{(TrollC)}, \qquad (2.27)$$

де $C^{(TRC)} \in [0;1]$ – константа, що визначає необхідну для троля частку дій з коментування;

$$\frac{Count\left(UACom_i\left(Moderators \cup OpinionLraders \cup Trans, Negative\right)\right)}{Count\left(UACom_i\right)} \geq C^{(TrollC)}, \qquad (2.28)$$

де $UACom_i\left(OpinionLeaders, Negative\right)$ – число негативних коментарів до контенту створеного модераторами, лідерами думок та трансляторами;

$$Count\left(UACom_i\left(Moderators \cup OpinionLraders \cup Trans, Negative\right)\right) >> \\ >> Count\left(UACom_i\left(Moderators \cup OpinionLraders \cup Trans, Positive\right)\right), \qquad (2.29)$$

тобто – число негативних коментарів до модераторів, лідерів думок та трансляторів значно переважає число позитивних.

У випадках, коли важливою є не безпосередня інформаційна протидія, а лише захист спільноти від руйнування (наприклад, науково-просвітницька спільнота, яка є безумовно корисною державі), у виразах, наведених вище, можна усунути складові коментарів до лідерів думок та трансляторів, обмеживши ідентифікацію тролів їхньою поведінкою щодо модераторів спільнот. Таке звуження принципово зменшує об'єми завдання з оцінювання тролів.

В ознаці активності для тролів

$$UACF_i \geq C_F^{(Troll)}. \qquad (2.30)$$

Межа активності є найвищою серед усіх ролей, адже для виконання своїх завдань тролі повинні створювати велику кількість дрібного контенту.

Боти – віртуальні особистості, які виконують у великих обсягах прості рутинні процедури у соціальних мережах. Прикладами таких процедур є: проставлення уподобань під дописами, написання коротких або малозмістовних коментарів. Боти на практиці реалізуються або як екземпляри активності спеціальних інтелектуальних програмних засобів або як екземпляри активності низькокваліфікованих виконавців (для однієї анонімної фізичної особи багато окремих екземплярів), які виконують одні й ті ж мережеві процедури згідно чітко визначених алгоритмів (часто з використанням спеціального ПЗ). Сучасні технології штучного інтелекту усе більше змінюють акценти в сторону інтелектуальних програм (зокрема сучасний стан створення ботів на основі технологій штучного інтелекту подано у роботі [31]), проте з точки зору системної організації протистояння в інформаційній війні особливої різниці між двома способами організації ботів немає.

Основне призначення ботів – підсилення ефекту дії користувачів наведених вище ролей.

Для формального визначення ботів одного математичного виразу недостатньо через широкий спектр завдань і форм їхньої активності. Проте в більшості випадків боти відрізняються значною перевагою дій з оцінки контенту над його публікацією:

$$\frac{Count(UAOM_i)}{Count(Content_i)} \geq C^{(Bot)}, \qquad (2.31)$$

де $C^{(Bot)}$ - константа, велике число, не менше 1000, проте дана ознака не дає змоги відділити ботів від звичайних користувачів з високою активністю, але низькою креативністю (інтенсивністю створення контенту).

2.2. Побудова формальної моделі віртуальних спільнот як середовища соціокомунікативного протиборства

У широкому спектрі завдань захисту національного інформаційного простору, адміністративної діяльності у сфері інформаційної політики, а також у завданнях інформаційно-аналітичної діяльності та моніторингу громадської думки виникає задача обліку та каталогізації різних форм соціальних груп, що проводять свою діяльність у соціальних середовищах Інтернету. З точки зору національної інформаційної безпеки значення та вплив суспільних групи у формі віртуальних спільнот постійно зростає, вони стають одним з головних засобів як індикації, так і формування суспільної думки на національному та регіональному рівнях.

Повноцінна каталогізація віртуальних спільнот вимагає опису значного числа параметрів спільнот. Спільноти є складним об’єктом з точки зору інформаційного опрацювання, їхні характеристики потребують формалізації, категоризації та певної уніфікації в рамках єдиної спеціальної моделі.

Формальна модель віртуальної спільноти частково наявна в окремих існуючих дослідженнях з каталогізації сайтів, проте на сьогодні даний

напрямок досліджень (формування загальних каталогів сайтів переживає певну кризу). Імовірно, технічні параметри спільнот детально пропрацьовані в системах автоматизованого поширення рекламних повідомлень та пошукового спаму, проте з очевидних причин такі прикладні розробки не мають наукового підґрунтя та опрацювання.

Навіть в указаних напрямках прикладних розробок, як показує аналіз результатів їхнього використання, відсутні ряд принципово важливих груп характеристик, необхідних для повноцінного використання спільнот як середовища інформаційної взаємодії.

Дослідимо додаткові показники, які мали би бути частиною формальної моделі предметної області – віртуальних спільнот як фактору національної безпеки. Аналіз будемо проводити у таких напрямках:

- характеристики віртуальних спільнот як середовища колаборативного обміну інформацією;
- додаткові характеристики спільнот, як середовища інформаційної агресії.

Формалізація характеристик буде використана далі в спеціальних алгоритмах захисту від інформаційної агресії та як основа для проектування структури програмного комплексу (див. розділ 3.2 «Планування заходів із захисту інформаційного простору держави»).

2.2.1. Групи характеристик віртуальних спільнот

Завдання із захисту інформаційного простору від агресії у віртуальних спільнотах вимагають наявність різнотипних інструментів як програмно-технічного класу, так соціокомунікативного класу. Для забезпечення формальної основи таких інструментів у моделі віртуальних спільнот пропонується включити такі групи характеристик:

- технічні характеристики;
- показники аудиторії;

- показники суспільної значимості;
- характеристики змісту та комунікації;
- характеристики державної безпеки.

Окремо виділятимемо базові та інтегровані показники. Базові показники отримуються безпосередньо з соціальних середовищ інтернету або шляхом аналізу і моніторингу, або шляхом безпосереднього (за можливості – автоматизованого) зйому даних з публічно або широко доступних джерел. Інтегровані показники обчислюватимуться на основі базових, певним чином їх узагальнюючи.

Формально, віртуальна спільнота Cm_i у такому разі описується кортежем наступного виду:

$$Cm_i = \langle CT_i, CA_i, CI_i, CC_i, CS_i \rangle, \qquad (2.32)$$

де елементами кортежа є наведені вище групи характеристик.

2.2.2. Технічні характеристики віртуальних спільнот

Технічні показники характеристики віртуальних спільнот описують способи забезпечення її функціонування в мережевому середовищі: засоби хостингу, програмні засоби, мови розмітки, оформлення розміщених матеріалів, їхня доступність зовні спільноти та для автоматизованих сервісів збору даних (таких як глобальні пошукові системи).

Зазначимо, що на сьогодні існує два головні класи технічної організації спільнот:

- на базі автономних програмно-технічних платформ;
- на базі глобальних соціальних сервісів, зокрема соціальних мереж та спеціалізованих мультимедійних хостингів.

З точки зору комунікативних процесів та впливу на інформаційний простір держави обидва підходи до організації спільнот є важливими і в значній мірі схожими. На практиці основні відмінності між використанням обох типів середовищ в інформаційній діяльності і в процесах

інформаційного протистояння лежать саме в програмно-технічній сфері. Пропонований далі перелік формальних показників є узагальненим для обох підходів, відмінності є лише між алгоритмами, що їх використовують, та ступенем програмної реалізації таких алгоритмів (див. табл. 2.4).

Таблиця 2.4. Технічні показники віртуальної спільноти (група CT)

Показник	**Позначення**	**Тип даних**	**Коментар**
Тип платформи	CPT	Список типів	(форум, мультимед. хостинг, соцмережа…)
Мережевий ідентифікатор платформи	CPIN	Universal resource identificator	Мережева адреса сайту платформи, головний URI платформи
Вербальний ідентифікатор платформи	CPIV	Рядок символів	Гасло або назва сайту платформи, за яким він знаходиться у випадку зміни адреси
Мережева адреса спільноти	CIN	Universal resource identificator	Адреса головної сторінки спільноти
Вербальна адреса спільноти	CIV	Рядок символів	Гасло або назва спільноти, за яким він знаходиться у випадку зміни адреси
Макрокод внутрішнього пошуку	CISE	Код на мові програмування високого рівня	Спосіб пошуку в межах спільноти
Макрокод зовнішнього пошуку	CESE	Код на мові програмування високого рівня	Спосіб пошуку в межах спільноти

Характеристика *CIN* подається у форматі URI, враховуючи той факт, що всі реально функціонуючі на сьогодні мережеві платформи дозволяють виділити певний унікальний URI для чільної сторінки спільноти. Теоретично можливе існування платформ, які такого виділення не дають. У такому разі воно повинне бути замінене парою «*CIV* + *CESE*».

Характеристики *CESE* та *CISE* (макрокоди пошуку) описують процедури пошуку в межах інформаційного наповнення спільноти в термінах, придатних для безпосередньої програмної реалізації. Одним з таких варіантів є шаблон фрагменту коду, який може бути викликаний з автоматизованих програмних засобів із заміною параметрів шаблону на

конкретні пошукові терміни та переданий далі на виконання. Сам код може передбачати декілька етапів як підготовчого (логін у пошукову систему, розпізнавання CAPTCHA тощо), так і пошукового характеру (попередній та уточнюючий пошук, пошук різними мовами та алфавітами тощо).

В окремих випадках показники *CESE* та *CISE* принципово відрізняються. Завданням показника *CISE* є документування способу пошуку, який здійснюється (зокрема в частково автоматизованому режимі), засобами технічної реалізації спільноти, тобто процедуру пошуку забезпечують власники платформи, на якій розгорнута спільнота. Це породжує ряд суттєвих аспектів пошуку, зокрема адміністратори платформи можуть здійснювати:

- обмеження пошуку;
- детальне документування факту пошуку;
- поглиблений аналіз суб'єкта пошуку;
- дезінформацію та приховування інформації.

Показник «Макрокод зовнішнього пошуку» призначений для документування способу пошуку, слабозалежного від адміністрації платформи спільноти за допомогою зовнішніх щодо платформи сервісів, таких як пошукові системи.

У випадку реалізації спільноти в формі традиційного Веб-форуму чи схожих (wiki-середовища, колективні блоги тощо) у якості CESE достатньо подати шаблони стрічки розширеного пошуку з відповідними директивами локалізації пошуку (такими *як site:* чи *inurl:* для Google*)*. Детально питання використання глобальних пошукових систем для пошуку на форумах пропрацьовано в наукових працях [12, 104].

У випадку, коли в якості платформи використовується сервіс глобальної соціальної мережі, засоби зовнішнього та внутрішнього пошуку є однаковими або близькими, і зводяться до використання стандартних

пошукових засобів соціальної мережі. На практиці для окремих соціальних мереж (зокрема Фейсбук) існує і доцільність можливості використання класичних ГПС. У такому разі в макрокод для *CESE* краще включати два пошуки: через СМ та через ГПС.

Усі значення технічних характеристик визначаються експертами при аналізі спільноти. Такі показники як *CISE* та *CESE* є схожими для більшості спільнот, що функціонують на одній платформі.

2.2.3. Показники аудиторії віртуальних спільнот

Показники аудиторії віртуальних спільнот описують популярність спільноти серед користувачів Інтернету та її обсяги в різних аспектах. Ці показники є важливим фактором для оцінки важливості спільноти як середовища інформаційної взаємодії і протистояння агресії (див. табл. 2.5).

Таблиця 2.5. Показники аудиторії віртуальної спільноти (група CA)

Показник	**Позначення**	**Тип даних**	**Коментар**
Кількісні характеристики аудиторії			
Кількість учасників	CAM	Натуральне число	
Кількість спостерігачів	CAAF	Натуральне число	
Кількість читачів	CAAR	Натуральне число	
Кількість активних учасників	CAAM	Натуральне число	
Кількість лідерів думки	CAOL	Натуральне число	З високим особистим авторитетом та впливом
Таргетингові характеристики			
Мова спільноти	CCLang	Перелік мов	На основі правил спільноти або реально існуючого контенту
Регіон	CCReg	Перелік регіонів або країн	
Вік	CCAge	Домінуюча вікова група	
Вид діяльності	CCAct	Перелік видів	Фах, галузь активності
Реальність інформаційної потреби	CCInt	[0,1]	[беззмістовний флейм.. ділова комунікація]
Тематика спільноти	CCTh	Ключові слова	

Учасниками спільноти вважатимемо осіб із зареєстрованими в спільноті обліковими записами. Спостерігачами – зареєстрованих учасників без активності, проте на деяких платформах є можливість окремої реєстрації як спостеріча (follower), а не учасника спільноти або підключення до читання спільноти через ті чи інші формати (типу стрічки новин у RSS-форматі). У такому випадку для спільнот зі строгим регламентом активної участі та наявністю авторитетних осіб, число спостерігачів може суттєво (на порядки) перевищувати число учасників.

У моделі пропонується розділяти поняття «*спостерігач*» та «*читач*». До спостерігачів відносяться ті користувачі Інтернету, які у якись зі способів використовують примусове доставлення нового контенту або його анонсів (push-технології). Реалізація такої доставки залежить від типу платформи (підписка на RSS-канал, отримання сповіщень у браузері, підписка у стрічці новин акаунта соціальної мережі, email-підписка, оповіщення робочого столу тощо), проте в будь-якому разі вона вимагає цілеспрямованих активних дій користувача з автоматизованого доступу до контенту.

Читачами вважатимемо користувачів Інтернету, які долучаються до контенту спільноти епізодично, без підписки, виходячи з наявності миттєвого зацікавлення, але не рідше ніж раз на місяць. Можна стверджувати, що спостерігачі складають ту частину аудиторії, яку можна назвати «ядром» або ж «довіреною частиною».

Визначення показника *CAAR* (читачів) для деяких типів платформ є тривіальним (Веб-форуми і інші автономні платформи), для деяких – інколи можлива лише груба оцінка на основі показника *CAAF* (деякі соціальні мережі з обмеженим доступом до статистики, зокрема Фейсбук).

Для різних платформ методи і складність визначення показників аудиторії значно відрізняється. Фактично, лише показник *CAM* («кількість учасників») як правило є легко доступним. Решту показників є

складнішими і можуть бути визначені лише приблизно. Зазначимо, що інформативність показника *CAM* також залежить від типу платформи – для спільнот на платформі соціальних мереж він є важливішим, ніж для форумів внаслідок активного донесення інформації до користувача соціальної мережі (на відміну від форумів, у яких власники акаунтів за замовчуванням не отримують додаткових сповіщень).

Окремим питанням є визначення поняття «активний учасник». Воно також залежить від типу платформи, на якій функціонує спільнота. У будь-якому разі активним вважатимемо учасника, який здійснює певну документовану дію щодо контенту спільноти в межах її платформи. Так, у випадку побудови спільноти на інфраструктурі соціальної мережі необхідно враховувати активні дії у формі «лайків», у той час як на традиційних форумах вони відсутні. У кожному разі активними діями вважатимемо розміщення текстового коментаря до існуючого контенту та початок нової дискусії.

Лідерами думки (opinion leaders) вважатимемо окремих учасників з високим рівнем суспільного пріоритету та персоналізацією, яка проявляється в таких формах:

- наявності окремого мас-медійного статусу особи;
- високого політичного, державного, ділового чи іншого суспільного статусу особи;
- наявності високого мережевого статусу, що проявляється у великій кількості друзів чи читачів в соціальних мережах, наявності популярного блогу тощо.

Виявлення лідерів думки в спільноті в загальному випадку є доволі складним завданням, проте в більшості випадків воно спрощується інформаційною політикою спільноти. Адміністрація спільнот зазвичай анонсує або рекламує наявність таких персон серед учасників.

У випадку, коли такі суспільно значимі особи діють на форумі анонімно, в величині *CAOL* вони не враховуються, адже на спільноту їхній вплив не поширюється.

Окремою підгрупою показників аудиторії спільноти є показники, які дозволяють здійснити таргетинг, виділити потенційно зацікавлених у спільності з множини усіх користувачів Інтернету.

Набір показників є доволі традиційним, відповідає класичним способам таргетингу, що використовується в системах контекстної та цільової Інтернет-реклами. Аналогічно, набір можливих значень показників відповідає усталеним у галузі.

Показник «Реальність інформаційної потреби» відображає практичну цінність контенту, який створюється в спільноті на основі потреб користувачів. Низькі значення відповідають спільнотам, де переважають беззмістовні дискусії (флейм), високі – спільнотам, де задовольняються реальні інформаційні потреби (практичні поради, розміщення документальної інформації тощо).

2.2.4. Показники суспільної значимості

Якщо показники аудиторії вказують на маштаби впливу інформаційної діяльності спільноти всередині неї, на учасників спільноти, то показники суспільної значимості показують її вплив на зовнішнє середовище.

Виділимо наступні показники, які наведено далі у табл. 2.6.

Таблиця 2.6. Показники суспільної значимості (група CI)

Показник	Позначення	Тип даних	Коментар
Кількість посилань на контент спільноти	CILC	Натуральне число	У формі гіперпосилання
Кількість цитувань	CICC	Натуральне число	У формі цитати або запозичення тексту
Конкурентний рейтинг	CICR	Натуральне число	Місце у списку однотипних спільнот
Конкурентна частка аудиторії	CICP	[0;1]	

Цитування спільноти та посилання на спільноту є основними індикаторами, які вказують на авторитетність матеріалів спільноти серед усіх користувачів Інтернету. У випадку цитування доступ до матерілу здійснюється напряму, що підвищує його важливість. Цитування, як правило, супроводжуватися посиланням.

Спосіб цитування визначається технічними особливостями типу платформи. Найбільш розширені засоби цитувань на сьогодні є наявними в популярних соціальних мережах типу Фейсбук, і, фактично, в автоматичному режимі заміняють посилання на цитування.

Показник *CICP* «*Конкурентна частка аудиторії»* описує, яку відносну частину цільової аудиторії має спільнота серед конкурентів. Можливим трактуванням цього показника є імовірність використання спільноти для здійснення необхідних дій користувачем Інтернету при виникненні у нього потреб соціокомунікаційного характеру. Даний показник може бути визначений експертним шляхом або за допомогою опитування представників цільової аудиторії. Ще одним варіантом грубого визначення даного показника є використання суміжного з ним *CICR.*

Показник *CICR* «*Конкурентний рейтинг»,* на відміну від частки аудиторії, описує лише умовну позицію серед конкурентів («головний», «другий» і так далі). Показник доволі легко встановлюється експертом. *Головна цінність даного показника – можливість оцінити частку цільової*

аудиторії, яку охоплює спільнота та її кількісні характеристики, якщо відсутні інші способи або вони є надто трудомісткими. Для цього використаємо гіпотезу про те, що аудиторія розподіляться між рейтингованими спільнотами згідно закону Зіпфа. У такому разі приблизна оцінка кількості читачів:

$$CAAR_i = \frac{CAAR\left(\overline{Cm}\right)}{CICR_i}, \qquad (2.33)$$

де $CAAR\left(\overline{Cm}\right)$ – показник кількості читачів найпопулярнішої з існуючих спільнот у межах даної цільової аудиторії.

В аналогічний спосіб можна визначити й інші подібні показники груп *CA* та *CI* .

Таким чином, показники спільноти-лідера стають певним еталоном, за яким можна здійснювати оцінку інших спільнот.

Очевидно, отримані одним з указаних способів (експерти, опитування, рейтингова оцінка) показники є неточними, однак і в такому стані вони можуть використовуватися для широкого спектру задач планування та організації захисту інформаційного простору держави, зокрема при визначенні трудомісткості, пріоритетності та резервування ресурсів.

2.2.5. Характеристики змісту та комунікації

Даний блок характеристик спільнот описує характер спільноти, її спрямування та призначення і, таким чином, визначає вибір щодо неї завдань із захисту інформаційного простору держави.

Пропоновані показники цієї групи наведено у табл. 2.7.

Таблиця 2.7. Характеристики змісту та комунікації (група CC)

Показник	Позначення	Тип даних	Коментар
Правила реєстрації та ідентифікації			
Рівень персоніфікації	CCPL	[0..1]	[анонімний…достовірний]
Акаунт соціальної мережі	CCSN	перелік соціальних мереж	
Комунікативні характеристики			
Рівень агресії	CCAgr	[0,1]	[неагресивний..агресивний]
Наявність порушень закону	CClaw	[0,1]	[відсутній..очевидно наявні]
Наявність ненормативної лексики та матеріалів порнографічного характеру	CCAdult	[0,1]	[відсутній..очевидно наявні]
Нестрогість модерації	CCMod	[0,1]	[премодерований .. немодерований]
Некерованість спільноти	CCCtrl	[0,1]	[повністю контрольована.. неконтрольована]

Головними завданнями прикладного значення, яким служить формалізація та подальший облік показників змісту та комунікації, є:

- можливість побудови програмно-алгоритмічних засобів з елементами штучного інтелекту для виконання рутинних комунікативних процедур;
- розроблення та чітка формалізація процедур юридичного та адміністративного характеру щодо протистояння антизаконним діям;
- вибір комунікативних стратегій та вербальних технік для підвищення ефективності діяльності в спільноті.

Показник *CCPL* «*Рівень персоніфікації*» вказує на вимоги спільноти до визначення правдивості і повноти даних, що були подані учасником. У випадку Веб-форумів даний показник визначається вимогами до назви акаунту та повноти заповнення реєстраційної анкети (в окремих випадках також і спеціального вітального повідомлення). У випадку спільнот на платформі соціальних мереж ідентифікація учасника здійснюється за єдиним обліковим записом користувача, що не виключає технічну можливість використання фейкового акаунта. Фактично, даний показник

відображає ступінь готовності та бажання адміністрації спільноти верифікувати персональні дані учасників.

Показник *CCSN «Акаунт соціальної мережі»* відображає технічну можливість використання для реєстрації в спільноті зовнішний обліковий запис із основних соціальних сервісів.

Показники комунікативного блоку встановлюються експертним шляхом, хоча частково дана процедура може бути автоматизована за допомогою інструментарію автоматизованого опрацювання природномовних текстів, зокрема інструментів Sentiment та Opinion Mining.

Адміністрація спільнот не завжди контролює інформаційну діяльність спільноти, часто процеси і тематика формування контенту регулюються слабо. Показники *CCMod «Строгість модерації»* та *CCCtrl «Керованість спільноти»* відображають рівень прямої відповідальності та зацікавленості адміністрації у розміщенні матеріалів певної тематики, зокрема таких, що несуть загрозу державній безпеці і, відповідно, дозволяють приймати рішення з вибору інструментарію захисту.

Відмінність між *CCMod* та *CCCtrl* полягає в оцінці способів досягнення керованості спільноти – через прямий вплив модераторів чи через інші комунікативні інструменти (лідерів думок, психологічні маніпуляції тощо). Значні відмінності між цими показниками для одної спільноти є індикатором нетипової поведінки, яка вимагає детальнішого аналізу (як варіанти – агресивні «тролі» руйнують політику модерації, адміністрація штучно створює ілюзію неконтрольованості спільноти з метою зменшення персональної відповідальності тощо).

Облік показників *Cclaw* та *CCAdult* дозволяє за необхідності швидше приймати рішення щодо задіяння правових та адміністративних інструментів для регулювання дії спільноти.

Рівень агресії *CCAgr* описує загальну тенденцію щодо тональності та змісту висловлювань щодо опонентів, що наявна в спільноті. Даний показник також використовується у процесі прийняття рішень щодо стратегії і комунікативних технологій у роботі зі спільнотою.

2.2.6. Характеристики державної безпеки

Для вирішення науково-практичних завдань в такій специфічній галузі, як захист інформаційного простору держави, необхідним є включення в модель окремих вузькоспеціалізованих показників. Такими є показники групи «Характеристики державної безпеки». Якщо наведені вище характеристики можуть використовуватися в ширшому спектрі завдань, пов’язаних із віртуальними спільнотами (інтернет-маркетинг, позиціювання в WWW, інформаційна аналітика бізнесу), то дана група характеристик спільнот є вужче спеціалізованою, орієнтованою власне на завдання зі сфери соціокомунікаційної безпеки і включає в себе дві підгрупи:

- показники рівня державного впливу;
- показники напрямку інформаційної діяльності в сфері безпеки.

Далі наведено ряд спеціальних показників віртуальних спільнот (див. табл. 2.8).

Запропоновані показники в комплексі з рештою показників дозволяють ідентифікувати спільноти, які бути опрацьовані в процесах захисту інформаційного простору держави, причому як в напрямку протистояння та нейтралізації, так і в напрямку захисту та підтримки. Окремі наведені характеристики мають «політичний» характер, проте вони є необхідними для ідентифікації спільнот, і повинні базуватися на методах політологічної безпекової експертизи. Доцільний також і формальний комп’ютерно-лінгвістичний аналіз контенту, зокрема на наявність очевидних ознак антидержавної та шовіністичної активності (наприклад,

заклики до кровопролиття та масове використання принизливих назв громадян держави), а також на наявність консесусу думок у спільноті.

Таблиця 2.8. Спеціальні показники спільноти з державної безпеки (група CS)

Показник	Позначення	Тип даних	Коментар
Показники рівня державного впливу			
Розміщення фізичних серверів	CSGP	[-1,1]	[під юрисдикцією агресора.. під повною юрисдикцією держави]
Розміщення юр.особи, що адмініструє спільноту	CSGJ	[0,1]	[під юрисдикцією агресора..... під повною юрисдикцією]
Наявність сталих зв'язків з сайтами та спільнотами держ.органів, авторитетних організацій, ЗМІ	CSGR	[0,1]	[жодних..повна інтегрованість]
Наявність сталих зв'язків з сайтами та спільнотами країн, що здійснюють агресію	CSFR	[0,1]	[жодних..повна інтегрованість]
Показники напрямку інформаційної діяльності в сфері безпеки			
Наявність завдання учасників зі інформбезпеки	CSTD	[0,1]	[не простежуються.. очевидні]
Ставлення до держави загалом	CSSR	[-1,1]	[«ворожа».. «дружня»]
Ставлення до державних інститутів	CSGR	[-1,1]	[«ворожа».. «дружня»]
Рівень консолідації думки учасників щодо держави	CSCV	[0,1]	[відсутні.. переважна більшість]

Показники «рівня державного впливу» *CSGP, CSGJ, CSGR, CSFR* описують можливість прямого втручання правоохоронних структур держави (зокрема і за силовими сценаріями) в діяльність спільноти. Відповідно, вони враховуються в алгоритмах визначення доцільних заходів щодо спільноти.

2.3. Висновки до розділу

У другому розділі дисертації запропоновано ряд формальних моделей суб’єктів інформаційної діяльності.

Здійснено формалізацію користувачів соціальних середовищ Інтернету, у якій враховано особливості задач захисту інформаційного простору, зокрема введено у розгляд спеціальні характеристики, які дозволяють виділити спеціальні ролі користувача: лідер думок, опонент, транслятор, троль. Детально формалізовано поняття фізичної та мережевої ідентифікації користувачів.

Окрім моделі користувачів, у розділі запропоновано спеціальну модель віртуальних спільнот як середовища протиборства у інформаційному просторі. Визначено ряд характеристик, які згруповано у такі групи: технічна, аудиторна, суспільної значимості, змісту та комунікації, державної безпеки.

Розділ 3. Методи та алгоритми ефективної протидії інформаційній пропаганді

У попередніх розділах було обгрунтовано необхідність проведення системних досліджень із захисту інформаційного простору держави в соціальних середовищах Інтернету та побудовано формальну модель предметної області, яка охоплює користувачів Інтернету та спільноти, в які вони об’єднуються.

Така модель забезпечує теоретичну основу для побудови методів та алгоритмів захисту інформаційного простору від ворожих впливів з рівнем формалізації, який дозволяє автоматизувати ряд процесів (у формі програмного забезпечення) або спростити окремі дії, доручивши їх виконання операторам (людино-машинні алгоритми).

Далі у розділі пропонується ряд відповідних методів та алгоритмів, які, зокрема:

- забезпечують формування зведеної системи показників для аналізу та пріоретизації спільнот з точки зору державної безпеки;
- допомагають планувати та організовувати заходи з захисту інформаційного простору держави;
- забезпечують ефективне виконання окремих оперативних завдань із захисту інформаційного простору держави.

Основні результати розділу автором опубліковано в роботах [18, 19, 32, 53].

3.1. Зведені показники віртуальних спільнот та пріоритезація спільнот з точки зору державної безпеки

Формалізація показників віртуальних спільнот (див. розд. 2.2 «Побудова формальної моделі віртуальних спільнот як середовища соціокомунікативного протиборства») дає можливість побудови

інтегрованих показників – основи для процедур прийняття рішень у окремих завданнях інформаційного захисту. Уведемо ряд інтегрованих показників, актуальних для завдань соціокомунікаційної безпеки. Враховуючи значне число показників та складність взаємозв'язків між ними, систематизуємо їх наступним чином.

Показники впливовості носять доволі універсальний характер і можуть застосовуватися в широкому спектрі завдань з інформування населення, рекламно-маркетингової діяльності тощо. З точки зору державної безпеки дані показники є засобом вимірювання масштабу впиву спільноти на суспільство. До даної групи показників віднесемо:

- популярність віртуальної спільноти;
- показник авторитетності віртуальної спільноти;
- абсолютна важливість віртуальної спільноти;
- відносна важливість віртуальної спільноти.

Показники комфортності спілкування також універсальні і описують трудомісткість і складність процесу спілкування, визначаючи, зокрема, можливість широкого залучення користувачів до виконання комунікативних завдань. До даної групи показників віднесемо:

- комунікативний комфорт віртуальної спільноти;
- комунікативне сприйняття віртуальною спільнотою.

Показники **близькості завданням державної безпеки** носять спеціальний проблемний характер і визначають політику щодо даної спільноти. До даної групи показників відносяться:

- лояльність віртуальної спільноти;
- релевантність віртуальної спільноти.

3.1.1. Показники впливовості віртуальних спільнот

Одним із ключових завдань, що постають у процесі захисту інформаційного простору держави в ССІ, – є інформаційно-комунікаційне

протиборство в спільнотах. Спільноти є основним механізмом поширення різних видів інформації, у тому числі пропагадистського та деструктивного характеру.

На сьогодні існують ряд методів протидії ворожим впливам через спільноти, які відносяться до різних класів: силові, юридичні, інформаційні тощо, проте в кожному випадку для таких заходів необхідна ресурсна підтримка зі сторони державних або громадських організацій. Можливості підтримки за сучасних умов є доволі обмеженими, що актуалізує *задачу пріоретизації спільнот з точки зору доцільності впливів*.

Таку пріоретизацію доцільно грунтувати на формальних характеристиках спільнот, уведених вище, що дає змогу визначати її об’єктивно, в автоматизованому режимі.

Уведемо до розгляду **показник популярності** спільноти, як узагальнення базових показників групи «Популярність» (див. розділ 2.2.3 «Показники аудиторії віртуальних спільнот») шляхом лінійної згортки

$$Popular(CM_i) = CAM_i * VC_{(CAM)}^{(P)} + CAAF_i * VC_{(CAAF)}^{(P)} + CAAR_i * VC_{(CAAR)}^{(P)}, \qquad (3.1)$$

де $VC_{(CAM)}^{(P)}, VC_{(CAAF)}^{(P)}, VC_{(CAAR)}^{(P)}$ – вагові коефіцієнти при відповідних базових показниках.

Популярність спільноти є важливим показником, який характеризує обсяги аудиторії, що споживає інформацію. Такий показник має зміст у широкому спектрі завдань, що пов’язані з інформуванням населення, включно з маркетинговими, промоційними завданнями і завданнями інформаційного протиборства, проте у сучасних умовах інформація, що має суспільне значення, проходить певне дискусійне осмислення в споживачів і, як правило, не має гарантованого впливу.

Рівень впливу інформації на споживача визначається авторитетністю джерела, що її поширює, тому доцільно ввести до розгляду **показник авторитетності** спільноти. Слід відзначити, що питання довіри та авторитетності на сьогодні певною мірою є дослідженими в суміжних областях – довіри користувачів до онлайн-медіа та поширенню фейкових новин [5, 8, 14, 17, 20, 34, 36], що дає змогу опиратися в дослідженні на вже наявні результати з моделювання та обчислення таких показників.

Базовою авторитетністю вважатимемо рівень впливу спільноти на думку наявної аудиторії спільноти. Показник формується шляхом лінійної згортки ряду показників спільнот, уведених у розділі 2.2 «Побудова формальної моделі віртуальних спільнот як середовища соціокомунікативного протиборства».

$$AuthBase(CM_i) = CCInt_i * \left(\frac{CAAM_i}{CAM_i} * VC_{(CAAM)}^{(AB)} + \frac{CAOL_i}{CAM_i} * VC_{(CAOL)}^{(AB)} + CICP_i * VC_{(CICP)}^{(AB)} \right), \quad (3.2)$$

де $VC_{(CAAM)}^{(AB)}, VC_{(CAOL)}^{(AB)}, VC_{(CICP)}^{(AB)}$ – вагові коефіцієнти лінійної згортки, підібрані таким чином, щоби $0 \le AuthBase(CM_i) \le 1$.

Показник інформаційної потреби $CCInt_i$ використаний як множник результату згортання для масштабування авторитетності, відповідно до характеру спілкування. Необхідність його введення в дану формулу пов’язана з тим, що в окремих випадках можуть існувати спільноти з користувачами високого суспільного значення, які проте носять доволі «легкий» характер (наприклад, для неформального спілкування, хобі, відпочинку) і думка одних користувачів ніяк не впливає на інших.

Значення базової авторитетності лежить в діапазоні [0;1]. Крайні значення відповідають: «0» - інформація не має впливу на споживача, відсутня довіра та увага до неї, «1» - інформація має повний вплив і не ставиться споживачем під сумнів.

Значення базової авторитетності в указаному діапазоні дозволяє використати її в якості коректуючого множника для популярності, отримуючи вираз для загальної авторитетності:

Показник абсолютної важливості віртуальної спільноти вказує в певних абсолютних одиницях важливість спільноти з точки зору безпеки держави. Це дає змогу рангувати спільноти однієї категорії (зі схожими тематикою, спобом організації тощо) за пріоритетом, з метою оптимізації використання наявних в органах безпеки ресурсів при виконанні завдань у межах однієї цільової аудиторії. За розмірністю цей показник відповідає показнику аудиторії сайту і формується з обчисленого показника популярності та базових показників суспільної значимості.

Показник важливості обчислюватимемо за наступною формулою:

$$CmAI_i = \frac{1}{3} AuthBase(CM_i) * \left(Popular(CM_i) * VC_{(Pop)}^{(CAI)} + CILC_i * VC_{(CILC)}^{(CAI)} + CICC_i * VC_{(CICC)}^{(CAI)} \right), \quad (3.3)$$

де $VC_{(Pop)}^{(CAI)}, VC_{(CILC)}^{(CAI)}, VC_{(CICC)}^{(CAI)}$) – відповідні вагові коефіцієнти. На відміну від попереднього виразу на них не накладається додаткових умов, окрім значення більше 0.

Розміри коефіцієнтів можуть різнитися дуже сильно, це обумовлено необхідністю приведення до однієї шкали показників з різними розмірностями. Так, наприклад, число лідерів думки у спільноті може не перевищувати кількох одиниць, а обсяги аудиторії сягати сотень тисяч. У такому разі вагові коефіцієнти повинні сумістити дані показники в одному масштабі. Це саме стосується розмірностей показників цитування та посилань у порівнянні з аудиторією, проте у визначенні конкретних значень коефіцієнтів важливим є зміст завдання, для якого обчислюються величини. Фактично, вони є керівними впливами вищих рівнів управління, визначаючи у формалізованому вигляді важливість окремих аспектів функціонування спільнот.

У якості множника у виразі (3.3) використано авторитетність спільноти $AuthBase(CM_i)$, адже незалежно від обсягів спільноти та зовнішньої репутації, важливим є реальний рівень впливу на аудиторію. Відсутність такого інформаційного впливу повністю нівелює її значення у питаннях інформаційного протистояння.

Показник відносної важливості віртуальної спільноти забезпечує порівняння між собою спільнот різних типів та тематик, дозволяючи сумістити їх при виборі та пріоритизації для виконання різного роду комплексних завдань, які охоплюють різні цільові аудиторії. Обчислюватимемо її наступним чином:

$$CmRI_i = \frac{CmAI_i}{CmAI(\overline{Cm})}, \qquad (3.4)$$

де $\overline{Cm}$ – спільнота з найбільшою абсолютною важливістю та з даною цільовою аудиторією.

3.1.2. Показники комунікативного комфорту віртуальної спільноти

Показники даної групи характеризують спільноту, як середовище зручного поширення інформації. Наведені показники не є «симетричними», вони торкаються різних аспектів комунікації.

Показник комунікативного комфорту віртуальної спільноти вказує на якість спільноти з точки зору стилю її спілкування, що проявляється в якості контенту, який вона формує. Спільноти з високою комфортністю спілкування мають потенційно вищий вплив на суспільну думку, а також володіють значним потенціалом росту, за необхідності вони можуть бути збільшені без надмірних зусиль і залучення спеціальних фахівців.

Вплив спільнот з низькою комфортністю навіть за умови великих обсягів аудиторії не може бути стабільно високим і може бути

нівельований без затрат значних ресурсів. Сам показник обчислюватимемо наступним чином:

$$CmComf_i = \frac{1}{4}\left(CCAggr_i * VC_{(CCAggr)}^{(Comf)} + CCMod_i * VC_{(CCMod)}^{(Comf)} + CCPL_i * VC_{(CCPL)}^{(Comf)} + CCAdult_i * VC_{(CCAdult)}^{(Comf)}\right), (3.5)$$

де $VC_{(CCAggr)}^{(CV)}, VC_{(CCMod)}^{(CV)}, VC_{(CCPL)}^{(CV)}, VC_{(CCAdult)}^{(CV)}$ – вагові коефіцієнти при відповідних показниках в діапазоні [0;1], причому $VC_{(CCAggr)}^{(Comf)} + VC_{(CCMod)}^{(Comf)} + VC_{(CCPL)}^{(Comf)} + VC_{(CCAdult)}^{(Comf)} = 1$.

Відповідно, значення показника комунікативної цінності лежать також в діапазоні [0;1].

Показник комунікативного прийняття описує складність та трудозатратність взаємодії зі спільнотою у різних комунікативних завданнях, у тому числі і завданнях державної безпеки.

Визначимо для даного показника наступні орієнтовні значення. Крайнє значення «-1» відповідає найвищому рівню критичності спільноти – вона є ворожою щодо держави та має консолідовану позицію. Крайнє значення «1» відповідає найвищому рівню прийняття державних ідей спільнотою – вона є продержавною і має консолідовану позицію. Значення «0» відповідає спільнотам, у яких, попри наявність тих чи інших настроїв, відсутня внутрішня самоорганізація та керованість.

Чим нижчий показник, тим складніше досягати в межах спільноти поставлених цілей. Даний показник пропонується визначати у наступний спосіб:

$$CmA_i = \frac{1}{3} CmL_i (CCAgr_i * VC^{(CCAgr)} + CCMod_i * VC^{(CCMod)} + CCCtrl * VC^{(CCCtrl)}), (3.6)$$

де $VC^{(xx)}$ – відповідні вагові коефіцієнти, які як і для показника комунікативної цінності лежать в діапазоні [0;1] і в сумі дають 1. Для визначення характеру критичності (позитивна для держави чи негативна) у вираз у якості множника уведений вище показник лояльності спільноти.

Низький рівень показника свідчить про потенційну загрозу для представників влади чи політиків: вони можуть бути скомпроментовані згідно з засадою оцінювання суспільством особистості на основі кола спілкування. Відповідно, поява у таких спільнотах відповідальних посадовців та лідерів думок повинна супроводжуватися попередньою спеціальною підготовкою з підвищення психокомунікативних навичок та риторики, і потім супроводжуватися систематичним моніторингом результатів їхньої діяльності.

3.1.3. Показники близькості завданням державної безпеки

Показник релевантності вказує на близькість спільноти завданням захисту та безпеки інформаційного простору держави. Його практичне визначення може змінюватися при зміні самих завдань (захист, контрнаступ, зовнішня інформаційна діяльність тощо). Таким чином в межах показника релевантності інкапсулюється значна частина особливостей конкретного практичного завдання, що забезпечує незмінність моделі та базованого на ній інстументарію для широкого спектру завдань. Сам показник обчислюватимемо наступним чином:

$$\begin{aligned} CmRel_i = CmRel\_lang_i * CmRel\_Reg_i * CmRel\_Age_i * \\ * CmRel\_Act_i * CmRel\_Int_i * CmRel\_Th_i * CSTD_i \end{aligned}, \qquad (3.7)$$

де $CmRel\_lang_i$ та інші множники – атомарні релевантності за кожним з напрямків, визначаються експертом у діапазоні [0;1].

Для показника $CmRel\_Th_i$ можливим варіантом визначення є обчислення частки релевантних термінів у описі тематики спільноти до загального числа ключових слів:

$$CmRel\_Th_i = \frac{Count\_rel(CCTh_i)}{Count(CCTh_i)}, \qquad (3.8)$$

де $Count\_rel(CCTh)$ – число релевантних термінів; $Count(CCTh)$ – число усіх термінів.

У випадку зміни завдань з захисту інформпростору змінюються визначення окремих релевантностей. Переважно якийсь з показників є неважливим. У такому разі відповідна йому релевантність визначається рівною 1. Наприклад, якщо в конкретних завданнях не має значення вікова характеристика спільноти, то $CmRel\_Age_i = 1$.

Показник лояльності віртуальної спільноти дозволяє формально описати узагальнене ставлення спільноти до системи державних цінностей та класифікувати її як дружню, по відношенню до держави, чи ворожу.

Як і попередні показники він може виводитися з базових, зокрема з показників груп «рівня державного впливу» та «напрямку інформаційної діяльності в сфері безпеки». Можливим є використання наступного виразу:

$$CmL_i = \frac{1}{7}(CSGP_i * VC^{(CSGP)} + CSGJ_i * VC^{(CSGJ)} + CSGR_i * VC^{(CSGR)} - \\ - CSFR_i * VC^{(CSFR)} + CSSR_i * VC^{(CSSR)} + CSGR_i * VC^{(CSGR)} + CSCV_i * VC^{(CSCV)}), \quad (3.9)$$

де $VC^{(xx)}$ – відповідні вагові коефіцієнти, які як і для показника комунікативної цінності лежать в діапазоні [0;1] і в сумі дають 1.

При такому визначенні значення показника лояльності лежить в діапазоні [-1;1] – від «абсолютно ворожа спільнота» до «повністю лояльна спільнота».

Важливо відзначити, що визначення даного показника в діапазоні [-1;1] може здійснюватися не лише шляхом обчислень, але експерною (політологічною) оцінкою. Зокрема, формальний, запропонований вище, спосіб за певних умов може не відповідати окремим політичним аспектам організації суспільства та засадами державної безпеки.

Незалежно від способу визначення показника лояльності, формалізація дозволяє включати його в методи та алгоритми захисту інформаційного простору держави.

Для подальщого відбору спільнот у процесах захисту інформаційного простору формалізуємо поняття «*шкідлива спільнота*» та «*корисна спільнота*».

Шкідливою вважатимемо спільноту, для якої:

$$CmL_i \le C_{Enemy}^{(CmL)}, \tag{3.10}$$

де $C_{Enemy}^{(CmL)}$ – константа, що визначає порогове значення ворожості для показника *CmL* «*Лояльність*». На практиці значення константи доцільно вибирати з діапазону [-1;-0,75].

Корисною вважатимемо спільноту, для якої:

$$CmL_i \ge C_{Friend}^{(CmL)}, \tag{3.11}$$

де $C_{Friend}^{(CmL)}$ – константа, що визначає порогове значення ворожості для показника *CmL* «*Лояльність*». На практиці значення константи доцільно вибирати з діапазону [0,75;1].

3.1.4. Застосування системи зведених показників спільнот

Отримані вище показники можуть використовуватися в широкому спектрі завдань з інформаційної взаємодії та протиборства в соціальних середовищах Інтернету. Зокрема, це наступні задачі.

Пріоретизація спільнот за окремим показником. Найчастіше, за важливістю (відносною чи абсолютною) з врахуванням релевантності.

Фільтрація спільнот за доцільністю. Найчастіше за ознаками лояльності та релевантності.

Фільтрація спільнот за складністю. Найчастіше за показниками комфортності спілкування.

Ідентифікація суб’єктів інформаційної діяльності. Використовуються для виявлення значущості лідерів думок, модераторів та інших суттєвих користувачів з точки зору інформаційної безпеки.

Формування плану ресурсної підтримки. Використовуються співвідношення різних показників між собою, зокрема з врахуванням лояльності, важливості, комфорту.

Формування плану заходів із нейтралізації. Використовуються співвідношення різних показників між собою, зокрема з врахуванням лояльності, важливості, комфорту.

Детальніше наведені прикладні задачі та шляхи їхнього науково-практичного вирішення описано далі.

3.2. Планування заходів із захисту інформаційного простору держави

Ефективний захист інформаційного простору держави вимагає планування комплексу взаємозалежних заходів та їхнього ресурсного забезпечення з кожного визначеного тематичного напрямку. Окремі заходи повинні відбуватися в певній послідовності або одночасно, паралельно. Ресурсне забезпечення повинне відображати необхідність задіяння осіб, здатних за кваліфікацією, можливостями та світоглядними засадами виконувати різноманітні оперативні завдання.

3.2.1. Загальний інформаційно-технологічний алгоритм організації заходів у віртуальних спільнотах

Проведення заходів із захисту інформаційного простору держави у спільнотах не може бути ефективним без проведення цілого комплексу дій, які далі систематизовано у вигляді спеціального алгоритму, здійснення якого розподілене між різними виконавцями. Такими виконавцями є:

- менеджери соціальних комунікацій – відповідальні особи, що володіють компетенціями та наділені повноваженнями з управління процесами соціальних комунікацій з метою захисту інформаційного простору

держави, представники відповідних органів влади чи правоохоронних органів, керівники громадських організацій;

- інформаційні аналітики – компетентні особи, що володіють навиками та ресурсами з аналізу соціальних середовищ Інтернету, зокрема спільнот на платформах соціальних мереж та Веб-форумів, представники відповідних органів влади чи правоохоронних органів, активісти громадських організацій;
- оперативні виконавці - компетентні особи, що володіють навиками та ресурсами з діяльності в соціальних середовищах Інтернету, переважно активісти громадських організацій та представники правоохоронних органів.

Далі пропонується загальний розподілений алгоритм типового процесу організації заходів у віртуальних спільнотах (див. рис.3.1).

На етапі «*Формалізація завдань у формі ключових слів*» визначається опис предметної області у межах якої здійснюватимуться заходи з захисту. За допомогою визначених термінів здійснюється також відповідна тематична проєкція (див. розд. 2.1.6 «Тематична проекція активності користувача»).

На наступному етапі визначаються параметри лінійних згорток у ряді виразів для обчислення зведених показників суб’єктів, зокрема у виразах (3.1)-(3.3), (3.5)-(3.7), (3.9). Оптимальним підходом для визначення (враховуючи трудомісткість) є «запозичення» цих параметрів з аналогічних попередніх завдань, з уточненням, за необхідністю, окремих параметрів.

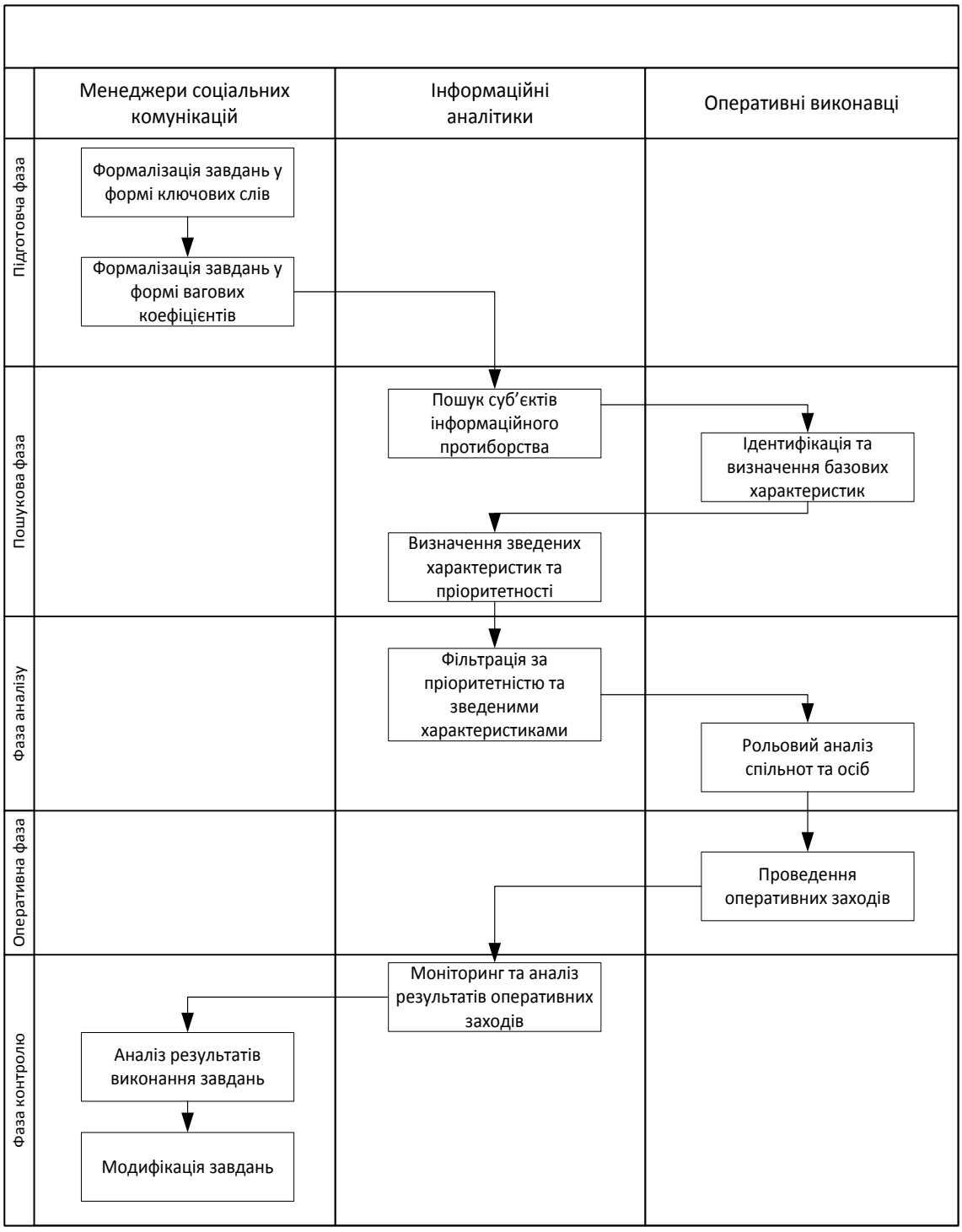

Рис. 3.1. Інформаційно-технологічний алгоритм організації заходів у ВС

Етап «*Пошук суб'єктів інформаційного протиборства*» передбачає виявлення потенційно важливих для інформаційного простору осіб та спільноти, конкретні базові характеристики яких визначаються уже на

наступному етапі «*Ідентифікація та визначення базових характеристик*» у результаті інформаційно-пошукових робіт волонтерами.

На наступних етапах отримані базові характеристики опрацьовуються аналітиками для визначення зведених характеристик та визначенні пріоритетності, фільтрації списку суб'єктів для усунення з розгляду малозначимих (з метою оптимізації використання ресурсів).

На етапі «*Рольовий аналіз спільнот та осіб*» для відібраних суб'єктів визначаються їхні ролі у процесах інформаційного протиборства, зокрема визначаються ролі окремих впливових користувачів (див. розд. 2.1.7 «Спеціальні ролі користувачів у процесах соціокомунікативного протиборства в інформаційному просторі»).

Етап «*Проведення оперативних заходів*», на відміну від попередніх, передбачає безпосередню комунікаційну взаємодію з суб'єктами інформаційного протиборства і здійснюється впродовж певного періоду (тривалість залежить від загальної характеристки завдання: надзвичайне, термінове, стратегічне тощо). Взаємодія здійснюється з використанням пропонованих далі у роботі методів (див. розділ 3.3 «Методи та алгоритми виконання окремих оперативних завдань із захисту інформаційного простору держави»).

На завершальних етапах аналітики і, після їхнього опрацювання, менеджери здійснюють аналіз результатів оперативної діяльності та приймають керівні рішення щодо подальших дій. Зокрема, можливі рішення можуть носити наступний характер:

- продовжувати діяльність з уточенням завдань – починається новий цикл виконання даного алгоритму з самого початку;
- продовжувати діяльність без змін – новий цикл без попередніх етапів, зразу з етапу проведення оперативних заходів;

- завершити виконання завдання – припинити виконання завдання, зберігаючи накопичені дані (особливо щодо ідентифікації суб’єктів) у архівній БД.

3.2.2. Алгоритм персоналізації суб’єктів інформаційної діяльності

Одним із ключових завдань раннього етапу діяльності з захисту інформаційного простору держави є формування каталогу значущих персоналій, які є в соціальних середовищах Інтенету. У такий каталог обов’язково повинні потрапляти впливові особи різних ролей (див. розділ 2.1.7 «Спеціальні ролі користувачів у процесах соціокомунікативного протиборства в »), проте, крім них, у даний каталог доцільно включати усіх ідентифікованих користувачів ССІ. При сучасному рівні розвитку комп’ютерних платформ та технологій баз великих даних така задача є достатньо реальною для практичного вирішення.

Структурування каталогу, його модель даних, повинна базуватися на формальній моделі користувача ССІ, що запропонована у розділі 2.1 «Формалізація користувачів соціальних середовищ Інтернету з точки зору безпеки інформаційного простору держави» і відображати наведені там базові та зведені характеристики. Саме в цьому є принципова відмінність даного алгоритму від ряду існуючих на сьогодні [5, 23, 94, 99].

Далі наведено загальний алгоритм типового процесу організації заходів у віртуальних спільнотах (див. рис. 3.2).

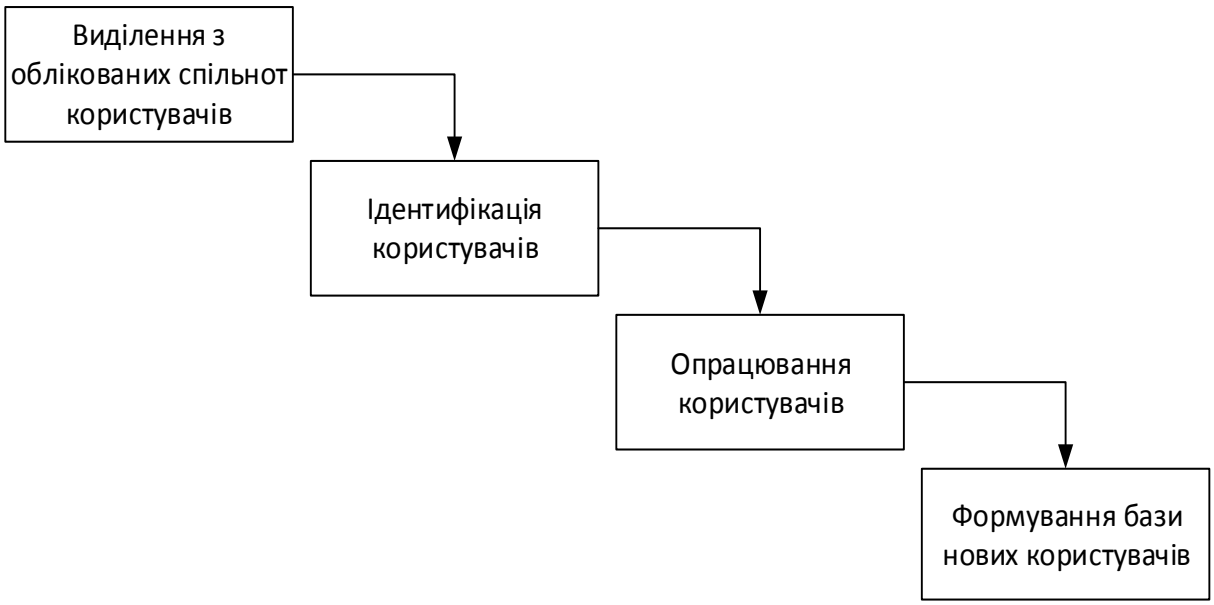

Рис. 3.2. Типовий процес організації заходів у ВС.

Розглянемо етапи наведеного алгоритму детальніше.

Виділення з облікованих спільнот передбачає автоматизований або напівавтоматизований аналіз їх наповнення з метою формування попереднього списку записів можливих мережевих ідентифікацій осіб – учасників спільнот.

Ідентифікація користувачів передбачає дії з визначення конкретних особистостей:

- відсів помилкових записів, які не є записами про користувачів;
- безпосереднє виявлення нових користувачів на основі мережевих ідентифікацій з попереднього етапу;
- виставлення для користувачів унікальних ідентифікаторів UIId, хоча би одної мережевої ідентифікації;
- внесення у базу даних користувачів.

Опрацювання користувачів полягає у визначенні всього набору характеристик користувача (див. розділ 2.1 «Формалізація користувачів соціальних середовищ Інтернету з точки зору безпеки інформаційного простору держави») та виявленні можливих повторів одних і тих самих

фізичних користувачів із різними мережевими ідентифікаціями. Даний етап реалізується окремим алгоритмом, що наведений на рис. 3.3.

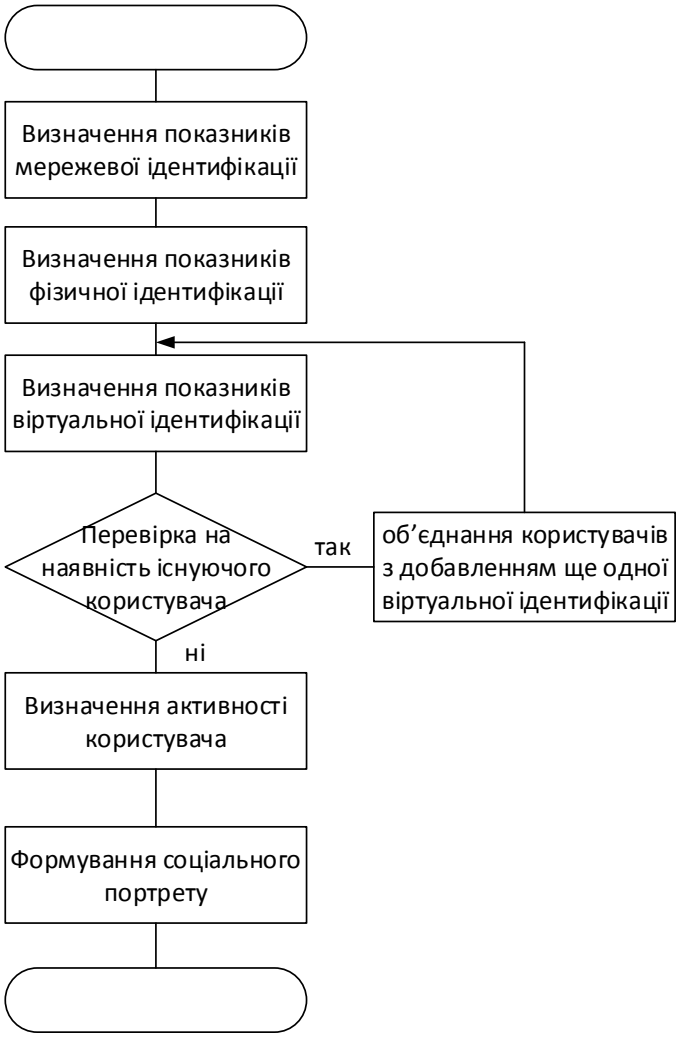

Рис. 3.3. Блок-схема алгоритму опрацювання окремого користувача

Формування бази нових користувачів є фактично початком нового циклу загального алгоритму, що забезпечує його рекурсивність. У значній мірі даний етап дублює функціональність етапу «*Виділення користувачів із спільнот*», проте на цьому етапі користувачі виділяються не з спільнот, а з соціального портрета, фактично з кожного користувача вибираються його «читачі» та «постачальники контенту» (див. розділ 2.1.5 «Формальний опис соціального портрету користувача»), які розглядаються як вхідні дані для другого етапу «Ідентифікація користувачів».

3.3. Методи та алгоритми виконання окремих оперативних завдань із захисту інформаційного простору держави

Запроновані вище методи дозволяють сформувати узагальнені показники суб'єктів інформаційної діяльності та на їхній основі побудувати загальну систему заходів із захисту інформаційного простору держави.

Далі у розділі досліджуються питання виконання окремих оперативних завдань, що постають у процесі реалізації такого плану. Зокрема, пропонуються методи виявлення користувачів певних ролей, шкідливих для держави з визначенням можливих шляхів ефективної протидії.

3.3.1. Виявлення лідерів думки, що здійснюють вплив в інформаційному просторі держави

Одним з найефективніших видів організації шкідливих впливів у інформаційному просторі держави є формування, популяризація та ресурсна підтримка лідерів думок із відповідним антидержавним спрямуванням. Лідери думок із певним рівнем впливу здатні впровадити широкий спектр ідей, здійснювати психологічні та ідеологічні диверсії, маніпулювати громадською думкою.

Як свідчать матеріали щодо розслідування російських впливів на політичні через соціальні мережі у США та країнах ЄС, є тенденція до формування цілої системи лідерів думок з прихованими мотиваціями та завданнями [1].

Ідентифікація таких користувачів дозволяє здійснювати ряд заходів інформаційного та оперативного характеру, нівелюючи їхній вплив на масову свідомість.

У роботі пропонується застосовувати термін «лідери думок» до певного класу користувачів на основі поведінкових ознак. Часто даний

термін (особливо його англомовний варіант «*opinion leader*») застосовують до різних користувачів із великою аудиторією споживачів контенту. Проте такий підхід має ряд недоліків:

- не врахування поведінкових характеристик неминуче веде до зниження ефективності комунікаційних методів протидії;
- виявляються лише особистості з великими обсягами аудиторії, що ускладнює силові методи (поширюється негатив в суспільстві);
- значна частина шкідливих впливів по факту уже відбулася, суспільство відреагувало на них у небажаній формі (особливо актуальна проблема у випадку стрімкої ескалації напруги).

Поведінкове визначення лідера думок дозволяє виділити наступні взаємодоповнювальні задачі:

- раннє **виявлення потенційних лідерів думок** – дозволяє реалізувати поставлені цілі щодо лідера думок з високою ефективністю та відносно невеликими ризиками та ресурсами, проте охоплює велику кількість користувачів;
- виявлення **динамічних лідерів думок** (зі швидким зростанням популярності) – охоплює доволі вузьку множину потенційних лідерів думок, для яких простежується висока динаміка збільшення популярності, відповідно є можливість задіяння широкого спектру заходів;
- виявлення **популярних лідерів думок** (з високим суспільним значенням) – охоплює лише незначну кількість, проте, як було сказано вище, супроводжується додатковими ризиками, вимагає комплексного підходу.

Розглянемо детальніше ці завдання. Розподіл між потенційними, динамічними та популярними здійснюватимемо на основі **показника популярності користувача**.

Найпростішим способом визначення популярності лідера думки є кількість споживачів його контенту:

$$UserPop(User_i) = Count(UF_i). \quad (3.12)$$

Можливими є інші, складніші ніж (3.12), способи визначення даного показника, зокрема такі, що враховують графову модель соціальних зв'язків та цитування матеріалів, проте з точки зору подальших підходів, це не є принциповим. Імовірно, що складніші визначення популярності є повністю корельованими з наведеним, проте є значно складнішими в обчисленні та зборі інформації.

Популярним лідером думки вважатимемо користувача, який відповідає сильній ознаці (2.17) та ознаці високої популярності:

$$UserPop(User_i) \geq \overline{C}_{UP}^{(OL)}, \quad (3.13)$$

де $\overline{C}_{UP}^{(OL)}$ – константа, визначає мінімальне число споживачів контенту для популярного лідера думки.

Потенційним лідером думки вважатимемо користувача, який відповідає сильній ознаці (2.17), ознаці активності (2.19) та має мінімальну допустиму популярність:

$$UserPop(User_i) \geq \underline{C}_{UP}^{(OL)}, \quad (3.14)$$

де $\underline{C}_{UP}^{(OL)}$ – константа, визначає мінімальне число споживачів контенту для потенційного лідера думки.

Динамічним лідером думки вважатимемо користувача, який відповідає одній з ознак (2.17) або (2.18), ознаці (3.14) на кінець періоду та має високий приріст популярності за певний період:

$$UserPop(User_i, T + \Delta T) - UserPop(User_i, T) \geq C_{Dyn}^{(OL)}, \quad (3.15)$$

де $C_{Dyn}^{(OL)}$ – мінімальний приріст популярності за період, T – початок періоду, ΔT - визначений проміжок часу моніторингу (на практиці місяць

або тиждень у залежності від динамічності та напруженості ситуації в суспільстві).

У якості кінця періоду в більшості оперативних завдань доцільно брати біжучий момент часу. Виявлення указаних типів лідерів думок доцільно здійснювати послідовно, з врахуванням попередніх результатів. Пропонується алгоритм, наведений на рис. 3.4.

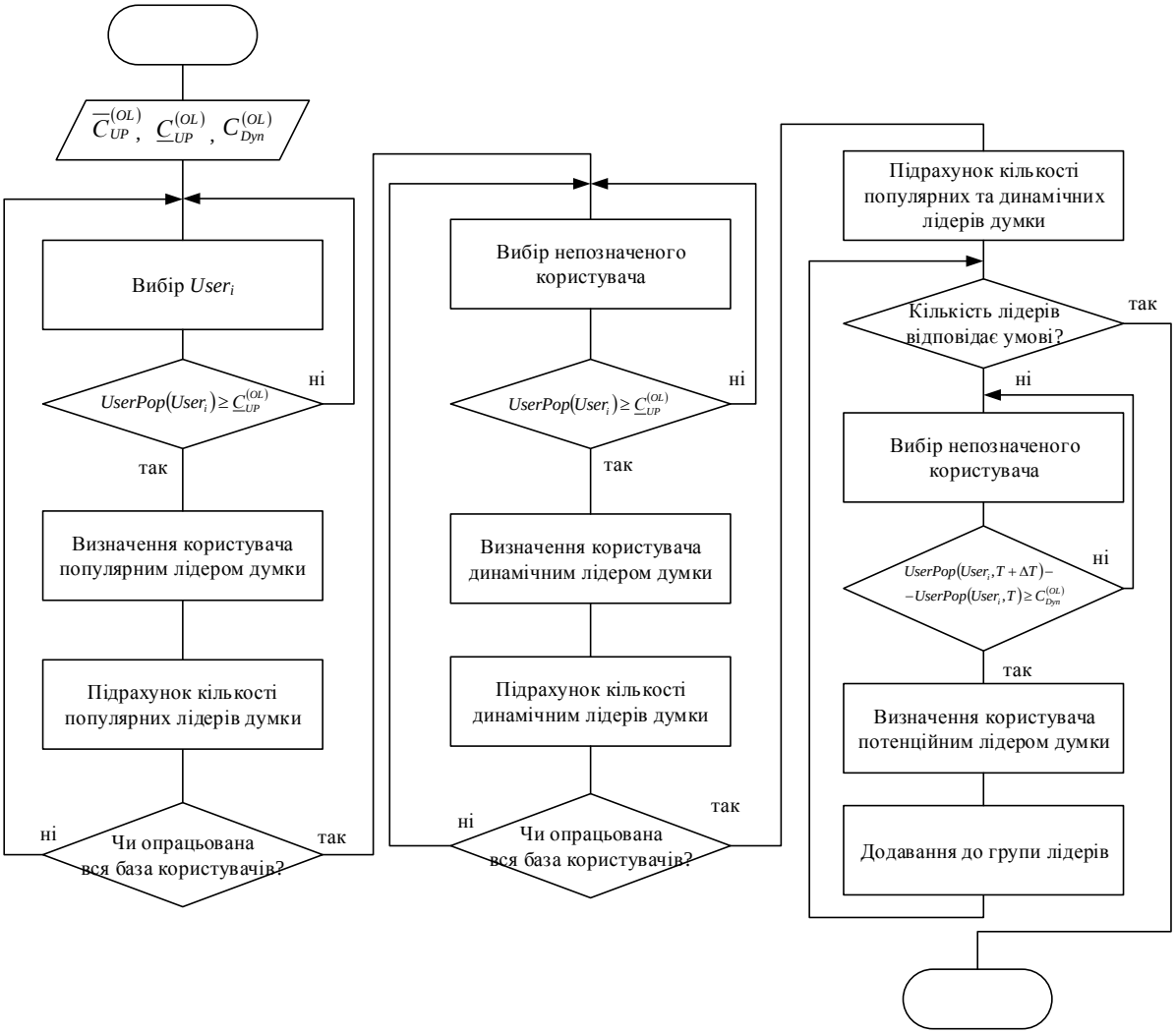

Рис. 3.4. Блок-схема алоритму формування бази лідерів думок

Шукати з метою подальшої протидії потенційних лідерів доцільно за умови відсутності належного числа популярних та динамічних лідерів. Це обумовлено не низьким значенням потенційних лідерів, а тим, що при

великій кількості реальних лідерів для них малоймовірним є перехід у «вищу» категорію.

Враховуючи тимчасовий характер динамічного лідерства важливо, щоби алгоритм відпрацьовувався достатньо часто, не рідше $\frac{\Delta T}{2}$ (див. (3.15)).

3.3.2. Протидія лідерам думки, що здійснюють шкідливі впливи в інформаційному просторі держави

Лідери думок можуть здійснювати різні впливи в інформаційному просторі держави. В окремих випадках лідери думок можуть цілеспрямовано або ненавмисно здійснювати шкідливу діяльність (ворожа пропаганда, розпалювання ворожнечі, створення панічних настроїв тощо). Критично важливо ефективно протидіяти таким суб'єктам, з врахуванням їхніх актуальних характеристик.

Такими, що здійснюють шкідливі впиви, вважатимемо тих лідерів думок, для яких виконується умова:

$$USG_i \le C_{Enemy}^{(USG)}, \qquad (3.16)$$

де $C_{Enemy}^{(USG)}$ – константа, що визначає порогове значення ворожості для показника *USG* «*Ставлення до держави*». На практиці значення константи доцільно вибирати з діапазону [-1;-0,75].

Далі визначимо наступні методи протидії кожній з категорій лідерів думок, що здійснюють шкідливу для держави діяльність згідно (3.16).

Відзначимо, що важливо застосовувати методи протидії лише проти тих лідерів думок, щодо яких не може бути застосована звичайна публічна політична дискусія з можливістю досягнення взаєморозуміння та усунення антидержавних дій. Для цього доцільно використати запропоновані показник гнучкості позиції користувача та ставлення до держави (див. табл. 2.2 та вираз (2.4)).

Динамічні лідери якраз являють собою користувачів, які переходять з нижчої в вищу категорію. На цьому етапі вони є достатньо вразливі (як потенційні лідери), але їхнє значення наближається до популярних. У такому разі боротьба з шкідливими динамічними лідерами є одним з найважливіших завдань з огляду на ефективність процесу (див. рис. 3.5).

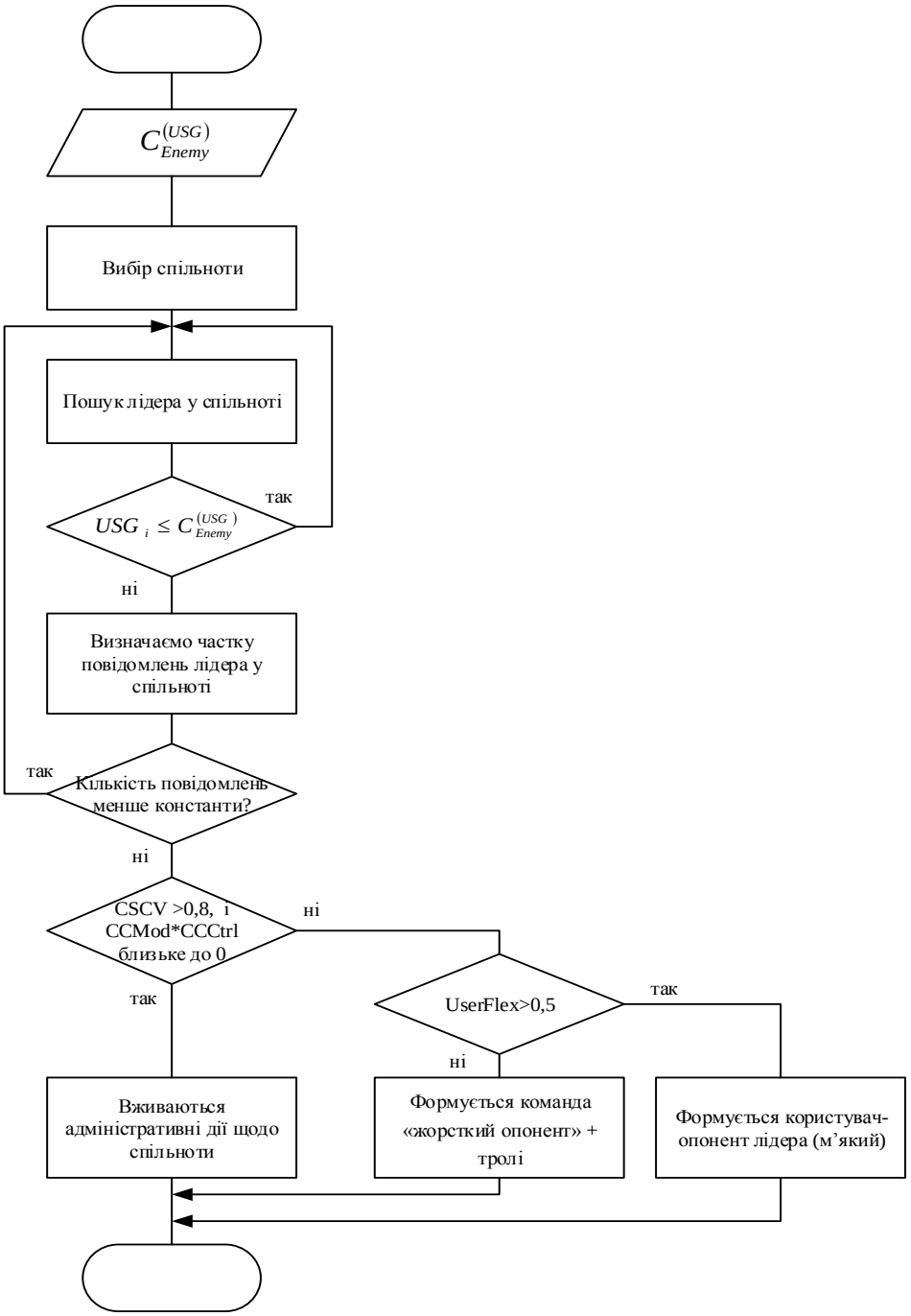

Рис. 3.5. Блок-схема алгоритму комунікаційної протидії потенційному лідеру думки

Основними комунікаційними інструментами протидії динамічним та потенційним лідерам є використання кваліфікованих опонентів та пониження показників популярності спільнот у яких вони діють. На рис. 3.5 наведений відповідний алгоритм.

Для динамічних лідерів поданий алгоритм повністю зберігає актуальність, лише відрізняються вимоги до дій опонентів. Опоненти повинні бути більше активними та проактивними, враховуючи динаміку лідера. Доцільним також є залучення тролів для пониження статусу і мотивації трансляторів матеріалів динамічного лідера думки.

Дії щодо спільнот, що згадані в алгоритмі, досліджено далі в роботі.

Крім комунікаційної протидії протенційним і динамічним лідерам, ефективними є й інші форми впливів, у першу чергу, організаційні та правові. Лідери, які ще не мають значного суспільного впливу, часто проводять шкідливу діяльність необдумано або під впливом інших осіб та, не усвідомлюючи в повній мірі наслідків діяльності. Як результат, ефективними можуть бути співбесіди, попередження, юридичні інструменти, проте їхнє застосування виходить за межі даної роботи.

Нейтралізація впливу популярних лідерів думок є складнішим завданням, проте обов’язковим для вирішення у випадку реальної загрози національній безпеці. Незалежно від інших інструментів, важливим є аспект комунікативної протидії. Популярні лідери думок характеризуються:

- авторським характером матеріалів;
- високою популярністю;
- достатньою активністю підготовки матеріалів.

У загальному зміст комплексу характеристик зводиться до того, що лідер думок в сучасних умовах конкурентної діяльності потребує суттєвого ресурсного забезпечення, і це робить його вразливим. Це відкриває можливість для протидії, яка зведена далі у таблиці 3.1.

Таблиця 3.1. Напрямки протидії популярним шкідливим лідерам думок

Характеристика	**Вразливість лідера**	**Можливості використання**
Авторський матеріал	Недостовірні дані	Критика опонента з ретрансляцією
	Суб'єктивність	Критика опонента з ретрансляцією
	Недостатня культура	Критика опонента, тролінг
	Погана стилістика	Тролінг
Висока популярність	Широкий спектр читачів	Поширення власної інформації в коментарях, контрпропраганда
	Низька критичність	Проведення спецоперацій комунікативно-психологічного характеру
	Конкуренція з іншими лідерами	Використання площадки для компроментації інших шкідливих лідерів
Активність підготовки	Брак контенту	Можливіть впливу на тематику та зміст повідомлень лідера думки
	Матеріальне забезпечення	

Для певних лідерів, у силу обставин, окремі позиції у таблиці можуть бути більше або менше актуальні, що відповідно впливає на стратегію взаємодії з лідером.

3.3.3. Виявлення тролів та опонентів, що діють згідно визначеного плану та завдання

Поширеним елементом інформаційного протистояння в соціальних мережах є залучення користувачів із спеціальними комунікативними навичками до деструктруктивної діяльності щодо лідерів думок та спільнот. Формально, такі користувачі рідко порушують законодавство, проте на практиці можуть нівелювати позитивний вплив авторитетних у суспільстві особистостей, і, що ще гірше, зруйнувати патріотично налаштовану спільноту, ліквідувавши таким чином певний суспільний ресурс, доступний для підтримки державних інтересів. Руйнуванню можуть підлягати великі спільноти, які охоплюють десятки та сотні тисяч громадян. Результатом є або деградація спільноти, або втрати учасниками

мотивацій до суспільно корисних дій (волонтерство, взаємодопомога, інформаційна підтримка тощо).

Методи виявлення тролів базуються на запропованих у роботі ознаках (2.27), (2.28), (2.29), (2.30), а також гіпотезі, що троль, виконуючи завдання, певною мірою є «прив'язаним» до окремих користувачів з ролями «*лідер думки*», «*модератор*», «*транслятор*».

Окрім того, виявлення шкідливих тролів на відміну від виявлення шкідливих лідерів думок має сенс лише в контексті захисту наперед визначених спільнот та користувачів, що є важливими для завдань захисту держави.

Таким чином, отримуємо наступний алгоритм виявлення шкідливих тролів (див. рис. 3.6.).

Як і лідери думок, тролі можуть мати різну ступінь популярності серед користувачів, проте на психологічному рівні користувачі розуміють технічне значення тролів, що призводить до невисокого суспільного авторитету. Таким чином, для протидії тролям може застосовуватися увесь спектр заходів як комунікаційних, так і правових. Вразливість тролів до комунікаційних заходів, як правило, підвищується через їхню анонімність або недостовірність персональних даних.

Ефективним методом протидії також є підвищення комунікативних навичок та запровадження спеціальних комунікативних стратегій для лідерів думок та спільнот, цінних для державної безпеки. *У такому разі, зусилля шкідливих тролів можуть витрачатися намарно або взагалі діяти в руслі державних інтересів, виникає можливість* ***експлуатації ворожих користувачів в інтересах держави***.

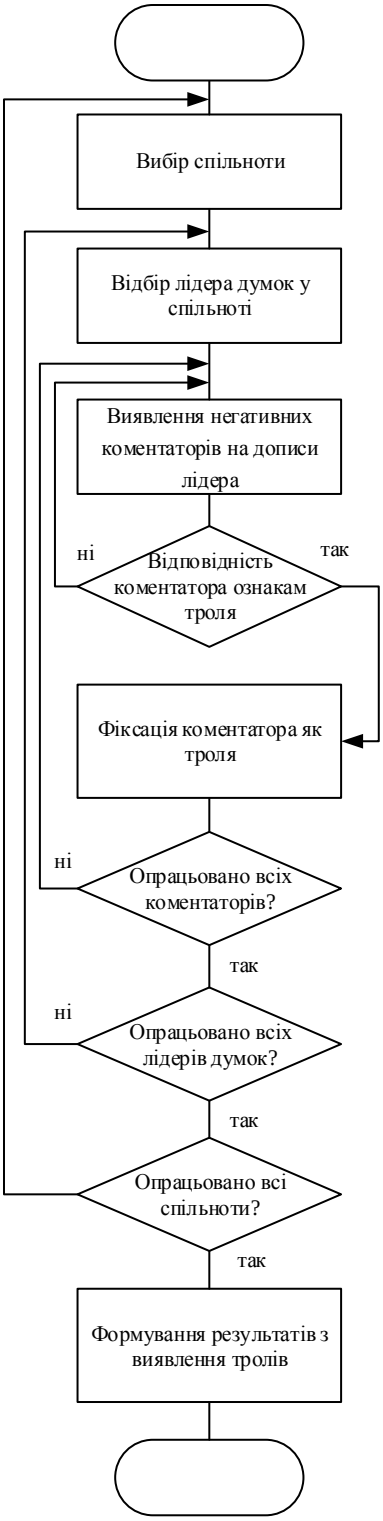

Рис. 3.6. Блок-схема алгоритму виявлення шкідливих тролів

Ключовим елементом таких стратегій є гіпотеза про матеріальне або інше зацікавлення троля та його підзвітність керівництву. *На цьому базується* ***метод непрямої протидії****, наведений далі*:

1) підведення троля до межі порушення правил спілкування - за необхідності правила спілкування повинні бути відповідним чином підсилені;
2) поставлення його перед фактом практично неминучого блокування – виникає загроза невиконання тролем завдань;
3) неблокування його, проте розкриття його поведінки як троля, – троль змушений формально коректувати поведінку і діяти в межах спільноти.

При належному виконанні указаних дій ресурси троля спрямовуються на інтенсифікацію спілкування в межах спільноти, що дозволяє усунути одну з ключових проблем більшості спільнот – низьку активність користувачів у створенні контенту. Окрім того, отримуються інші, додаткові, переваги (можливість «живої» демонстрації карикатурної поведінки шкідливих тролів в спільнотах тощо).

Відзначимо, що на сьогодні в соціальних середовищах Інтернету наявний певний поділ тролів на «товстих» та «тонких». До першої категорії відносяться користувачі даної ролі з низькими комунікативними навиками та якістю матеріалу, до другої – з високими. Пропонований вище метод непрямої протидії доцільно використовувати лише проти «тонких» тролів. ***Окрім того, указаний підхід доцільно також застосовувати і до шкідливих користувачів ролі «опонент»****, враховуючи той факт, що «тонкий троль» і «опонент» є доволі близькими і відрізняються лише характером впливу (психологічний та інформаційний).*

3.3.4. Виявлення модераторів, що здійснюють ресурну підтримку шкідливих впливів

Виявлення модераторів, шкідливих для інформаційної безпеки держави базується на аналізі акцій впливу (див. розділ 2.1.4 «Формальний опис активності користувача»), враховуючи характер змін видимості та

характер контенту, до якого він застосовується. Визначимо наступні види ознак, що дозволяють ідентифікувати модератора як шкідливого:

- ознака контрольованих ресурсів;
- строгість до патріотичних лідерів думок;
- поблажливість до ворожих лідерів думок.

Найпростішою є ознака контрольованих ресурсів. Тобто шкідливим є модератор, який керує спільнотою, визначеною визначенням як шкідлива (див. розділ 2.2.6 «Характеристики державної безпеки»), тобто повинна виконуватися хоча б одна з двох умов:

- $CmL_i \le C_{Enemy}^{(CmL)}$ – шкідливий за ознакою лояльності або
- $CmA_i \le C_{Enemy}^{(CmA)}$ – шкідливий за ознакою комунікативного спрямування хоча би для одної спільноти, у якій користувач виконує функції модератора.

Дана ознака дозволяє виділити модераторів, які явно підтримують розвиток спільнот шкідливого для держави спрямування. Проте, на практиці шкідлива діяльність може здійснюватися і в менш очевидний спосіб. Модератор може формально адмініструвати політично нейтральну спільноту з представленим широким спектром думок (показник CmL_i близький до нуля), проте здійснювати політику модерування у такий спосіб, що лідери думок патріотичного спрямування опиняються в програшній ситуації. Зокрема, можуть здійснюватися наступні дії.

Надміру строге застосування правил до патріотичних лідерів думок, тобто показник його особистого комфорту є значно нижчим, ніж загальний:

$$CmComf_i > CmComf_i^* \ , \qquad (3.17)$$

де $CmComf_i^*$ – показник комфорту для патріотично налаштованих лідерів думок.

Недостатньо строге застосування правил до шкідливих користувачів, створення їм комфортних умов

$$CmComf_i < CmComf_i^{**}, \quad (3.18)$$

де $CmComf_i^{**}$ – показник комфорту для шкідливих лідерів думок, опонентів та тролів.

Виконання хоча б однієї з указаних ознак дозволяють віднести модератора спільноти до таких користувачів, які здійснюють шкідливу для безпеки держави діяльність.

3.4. Організація ресурсної підтримки заходів із підтримки та нейтралізації суб'єктів інформаційної діяльності

Ключовим елементом заходів із захисту інформаційного простору держави є взаємодія з суб'єктами, які мають суттєвий вплив на інформаційні процеси [7, 60, 61, 91, 93, 97].

Окрім протидії шкідливим суб'єктам, іншою складовою заходів з зміцнення безпеки інформаційного простору держави в соціальних середовищах Інтернету є організація та підтримка суб'єктів, що виконують корисні для держави функції. До таких суб'єктів віднесемо як окремих користувачів (як правило, що відповідають окремим визначеним вище ролям), так і спільноти з відповідними показниками груп *CC* та *CS* (див. табл. 2.7 та табл. 2.8).

Корисними для безпеки інформаційного простору вважатимемо користувачів, для яких (за аналогією з (3.16)) виконується наступна умова:

$$USG_i \geq C_{Friend}^{(USG)}, \quad (3.19)$$

де $C_{Friend}^{(USG)}$ – константа, що визначає порогове значення патріотичності для показника *USG* «*Ставлення до держави*». На практиці значення константи доцільно вибирати з діапазону [0,75;1].

3.4.1. Використання дисбалансу для ідентифікації ресурсних потреб лідерів думок

Для кожного користувача, що проводить активні інформаційні дії в соціальних середовищах Інтернету є певний характерний стиль спілкування, що базується як на особистих характеристиках, так і на наявних ресурсах користувача. Для рольових користувачів визначено певні цілі їхньої діяльності, відповідно це дає можливість досліджувати питання ефективності використання ресурсів згідно певної моделі поведінки та цілей.

Ресурсна підтримка користувача може забезпечити суттєве або визначальне збільшення його впливу на інформаційний простір, проте на практиці такі ресурси часто витрачаються безсистемно, що не дозволяє досягати очікуваних результатів.

Типи ресурсів та їхнього забезпечення залежать від цілей (і відповідно ролей), які поставлені перед користувачами. Далі дослідимо їх детальніше.

Для лідерів думок ціль – формування громадської думки, відповідно, результати діяльності можна звести до таких основних факторів:

- **обсяги аудиторії** – показник *UserPop,* що був уведений вище (див. розділ 3.3.1 «Виявлення лідерів думки, що здійснюють вплив в інформаційному просторі держави»);
- **кількість створеного контенту** – показник *UserContentCount*, у якості якого вибирається $Count(UAIC_i)$ *або* $Count(UAIUC_i)$ (див. розділ 2.1.7 «Спеціальні ролі користувачів у процесах соціокомунікативного протиборства в »)
- **якість створеного контенту** – показник *UserQuality,* як певна інтегральна характеристика, що описує вплив, достовірність, стилістику контенту на аудиторію.

Визначимо, що значення характеристики **якість створеного контенту** лежить в діапазоні [0,1]. Можливим трактуванням показника є імовірність того, що контент мав суттєвий планований автором вплив на думку читача. Визначення показника здійснюється експертним шляхом.

Введемо інтегрований показник впливовості контенту як добуток:

$$UserImpact(User_i) = UserPop(User_i) * UserQuality(User_i). \quad (3.20)$$

Таким чином, отримуємо дві характеристики, що описують результативність діяльності літера думок: продуктивість (кількість створеного контенту) та впливовість контенту.

Очевидно, що для різних користувачів як значення цих показників, так і співвідношення між ними відрізняються, проте в силу однотипності комунікаційних процесів можна вважати, що в кожній тематиці існує певне еталонне співвідношення «впливовість/продуктивність». У якості такого еталону може виступати лідер думки в предметній галузі, який відрізняється такими суб'єктивним характеристиками, як успішність, авторитетність, незалежність від обставин. Тоді $\frac{UserImpact(User_*)}{UserContentCount(User_*)}$ – еталонне співвідношення, де $User_*$ – еталонний лідер думки.

Автори думок, для яких указане співвідношення суттєво відрізняється від еталонних, знаходяться або в зоні ризику втрати позиції, або недостатньо реалізовують свій потенціал. Самого еталонного лідера необхідно визначати експертним шляхом на основі актуального стану соціальних середовищ.

Далі на рис. 3.7 наведено можливі варіанти дисбалансу у показниках.

Розглянемо детальніше пропоновану схему співвідношення показників.

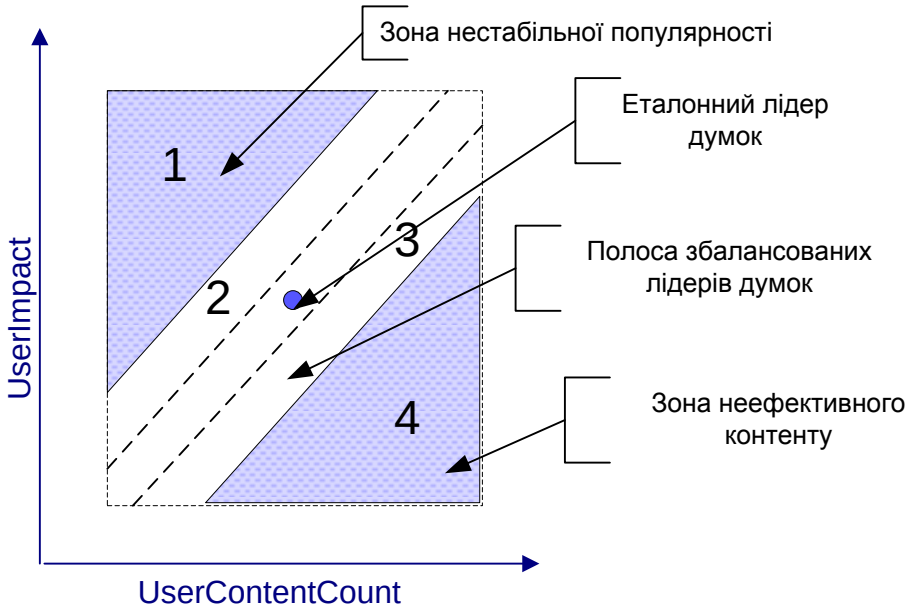

Рис. 3.7. Баланс показників лідерів думок

У кожному з варіантів дисбалансу виникають певні можливості з його усунення і, відповідно, підвищення показників діяльності лідера думок. Розглянемо їх далі.

У зонах 1 та 2, тобто у випадку, коли $\frac{UserImpact(User_i)}{UserContentCount(User_i)} > \frac{UserImpact(User_*)}{UserContentCount(User_*)}(1+\Delta)$ знаходяться ті лідери думок, які користуються великою популярністю, проте продуктивність інформаційної діяльності є низькою. Така ситуація виникає у випадках відсутності творчих ідей або низької інтенсивності створення матеріалів. Популярність досягається за рахунок окремих психологічних, комунікаційних навичок, вдалої відповідності суспільним настроям, проте в середньо та довготерміновій перспективі є нестабільною і, швидше за все, автор буде витіснений іншими, більш конкурентними.

Для підтримки діяльності корисних лідерів думок даної зони доцільно залучати ресурси для компенсації дисбалансу:

- помічників для формування нового контенту, копірайтерів та аналітиків;

- редакторів, верстальників, фоторедакторів для виконання рутинних робіт із оформлення матеріалу.

Для протидії шкідливим лідерам даної зони доцільно залучати ресурси для використання нестабільності, що породжує дисбаланс:

- залучати опонентів для підкреслення слабкості позиції лідера думки;
- формувати нових конкурентних лідерів думок, корисних для держави, які формуватимуть аудиторію на основі аудиторії шкідливого лідера.

Відмінність між зонами 1 і 2 лежить в мірі обов'язковості застосування заходів. Чим віддаленіша позиція лідера думки від зони балансу, тим вища імовірність руйнування його впливу. Відповідно для зони 1 заходи є обов'язковими, зони 2 – рекомендованими (якщо прийняте рішення про ресурсну підтримку лідера думки).

У зонах 4 та 3, тобто у випадку, коли $\frac{UserImpact(User_i)}{UserContentCount(User_i)} < \frac{UserImpact(User_*)}{UserContentCount(User_*)}(1-\Delta)$ знаходяться ті лідери думок, які проводять активну та якісну інформаційну діяльність, проте не користаються високою впливовістю (популярністю або переконливістю). Така ситуація виникає у випадках надто формального подання матеріалів, поганого стилістичного подання матеріалів, слабкої аргументаційної частини, слабких компетенцій з Інтернет-реклами, поганих комунікаційних навичок, окремих акцентуацій характеру автора. Фактично, можна сказати, що потенціал автора використовується не в повній мірі, марнуються його зусилля. У довгостроковій перспективі автор втрачатиме інтерес до творчості, не маючи належної аудиторії.

Підтримки діяльності корисних лідерів думок даної зони дозволяє з невеликою затратою ресурсів отримати значний результат. Ресурсами для компенсації дисбалансу є:

- фахівці з реклами, рекламна підтримка, нові площадки для поширення матеріалів;

- редактори, стилісти для підвищення переконливості матеріалів (за необхідності);
- транслятори матеріалів для збільшення зони поширення.

Для протидії шкідливим лідерам даних зон доцільно залучати ресурси для використання неефективності, що породжує дисбаланс:

- залучати тролів для руйнування площадок і дискусій, де поширює матеріали лідер думки (опонування є недоцільним, так як воно збільшуватиме популярність);
- звертати увагу на відсутність суспільного інтересу до лідера думки;
- впливати на зміст матеріалів лідера думок, мотивуючи можливостями збільшення популярності.

Відмінність між зонами 4 і 3 аналогічно лежать в мірі обов'язковості застосування заходів.

У полосі збалансованих знаходяться ті лідери думок, які мають схоже з еталонним співвідношення між впливовістю та популярністю, проте вони можуть суттєво відрізнятися від еталонного масштабами суспільного впливу.

Підтримка та протидія лідерам думок з цієї зони здійснюється усіма наведеними інстументами обох груп, але без надання суттєвих переваг котрійсь ціз груп.

3.4.2. Використання дисбалансу для ресурсної взаємодії з спільнотами

Поняття дисбалансу, як відхилення від еталонного співвідношення окремих показників, може бути використане не лише для визначення сильних та слабких місць лідерів думок, як це запропоновано у попередньому підрозділі, але для інших завдань, пов'язаних із взаємодією в соціальних середовищах Інтернету.

Однією з таких задач є взамодія з різними цілями (підтримки корисних, нейтралізації ворожих) зі спільнотами в соціальних мережах.

Визначимо наступні види дисбалансів для віртуальних спільнот:

- дисбаланс «популярність/активність» - оцінка якості комунікативних процесів і піару спільноти;
- дисбаланс «популярність/значимість» - оцінка якості контенту спільноти та її піару.

Визначення указаних дисбалансів здійснюється на основі показників, що описані у розділах 2.2.3 «Показники аудиторії віртуальних спільнот», 2.2.4 «Показники суспільної значимості».

Як і для лідерів думок уведемо поняття «еталонна спільнота», у якості якої екперт повинен вибрати спільноту, що відповідає таким ознакам: самодостатність (незалежність від зовнішнього ресурсного забезпечення), тривале існування (не менше 2-років), наявність високих показників популярності та авторитетності.

У якості контрольного для дисбалансу «популярність/активність» виберемо співідношення $\frac{Popular(Cm_i)}{CAAM_i}$ для *i*-ї спільноти, де $Popular(Cm_i)$ – зведений показник популярності спільноти (див. вираз (3.1)). Еталонне співвідношення відповідно буде – $\frac{Popular(Cm_*)}{CAAM_*}$.

У випадку реалізації спільноти на платформі соціальних мереж замість показника *Popular* доцільно вибирати показник *CAAF*, як такий, що значно простіше ідентифікується. Відповідно, змінюються і вирази для визначення балансу.

Аналогічно до поділу на зони лідерів думок виділимо зони для балансу спільнот за показниками «популярність/активність» (див. рис. 3.8).

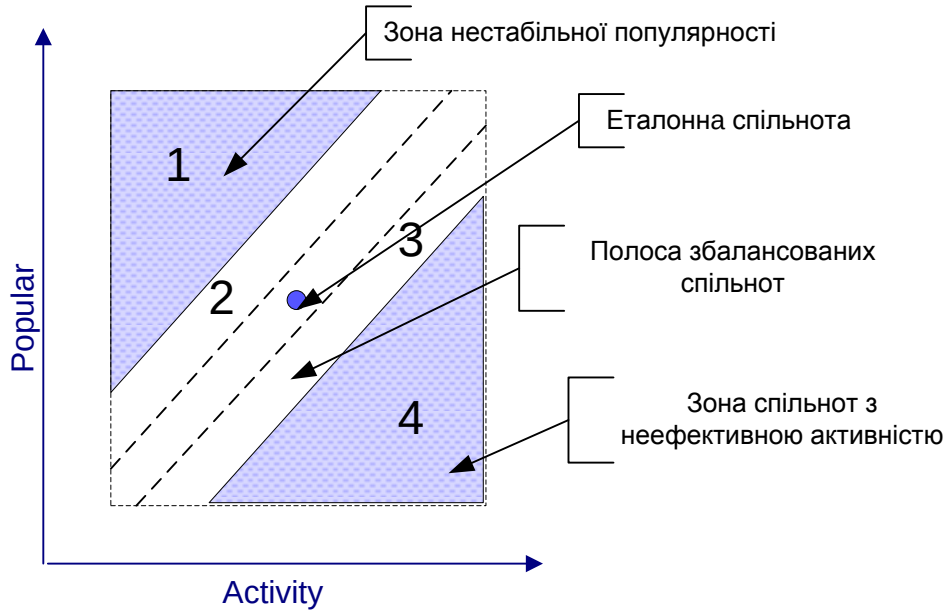

Рис. 3.8. Баланс спільнот «популярність/активність»

У зонах 1 та 2, тобто у випадку, коли $\frac{Popular(Cm_i)}{CAAM_i} > \frac{Popular(Cm_*)}{CAAM_*}(1+\Delta)$ знаходяться ті спільноти, які користуються великою популярністю, проте кількість активних учасників є недостатньою для тривалого самодостатнього функціонування. Такі спільноти, зазвичай, грунтуються на високій активності та мотивації невеликої групи учасників та на суттєвій зовнішній ресурсній підтримці. Популярність досягається за рахунок вдалої стилістики матеріалів та спілкування, відповідності суспільним настроям, проте в середньо та довготерміновій перспективі такі спільноти легко витісняються більш конкурентними.

Для підтримки корисних спільнот даної зони доцільно:

- знаходити активістів для збільшення обсягів активної спільноти та реалізовувати системи персональної матеріальної винагороди;
- змінити формальні правила та традиції спільноти з метою простішого входження новачків;

- здійснювати експлуатацію ворожих опонентів та тролів (див. розділ 3.3.3 «Виявлення тролів та опонентів, що діють згідно визначеного плану та завдання»).

Для протидії шкідливим спільнотам зони доцільно залучати ресурси для використання нестабільності, що породжує дисбаланс:

- залучати тролів для пониження якості наявних матеріалів;
- формувати нові спільноти корисні для держави, які формуватимуть аудиторію на основі шкідливої.

В окремих випадках (наявності незаангажованого адміністрування та технічних інструментів самодерації – характерно для певних типів Веб-форумів та Вікі-спільнот) - доцільно опрацьовувати варіант «захоплення» спільноти. Відносно невелика кількість учасників може не протистояти зростанню спільноти новим з іншою системою цінностей.

Відмінність між зонами 1 і 2 лежить в мірі обов'язковості застосування заходів.

У зонах 4 та 3, тобто у випадку, коли $\frac{Popular(Cm_i)}{CAAM_i} < \frac{Popular(Cm_*)}{CAAM_*}(1-\Delta)$ знаходяться ті спільноти, які мають велике число активних користувачів, проте не користаються високою популярністю. Така ситуація виникає у випадках низької якості матеріалів, надмірної фамільярності в межах спільноти, домінування тем особистого характеру. Фактично, зусилля спільноти на створення контенту витрачаються неефективно, не отримуючи суспільного ефекту. У довгостроковій перспективі спільнота приречена на деградацію.

Підтримки діяльності корисних спільнот даної зони дозволяє з невеликою затратою ресурсів отримати значний результат. Для цього необхідно:

- рекламна підтримка спільноти;

- модифікація формальних правил та традицій спільноти щодо вибору тем та характеру спілкування;
- транслятори матеріалів для збільшення зони поширення.

Щоб протидіяти шкідливим спільнотам даних зон доцільно залучати ресурси для використання неефективності, що породжує дисбаланс:

- залучати тролів (у першу чергу «товстих») для руйнування активної аудиторії шляхом втрати комунікаційного комфорту;
- звертати увагу на відсутність суспільного інтересу до спільноти, акцентуючи увагу на певному «сектанстві» спільноти.

Патріотично налаштованим користувачам доцільно рекомендувати покинути спільноту, у зв'язку з низькою ефективністю їхньої діяльності в ній (матеріали є мало затребуваними в суспільстві). Це призводить до пониження інтелектуального рівня дискусій та, відповідно, подальшої втрати суспільного інтересу до спільноти і її неминучої деградації, врешті-решт і залучення кваліфікованих користувачів-«опонентів» до участі в таких спільнотах є небажаним.

Відмінність між зонами 4 і 3 аналогічно лежить в мірі обов'язковості застосування заходів.

Коротко розглянемо далі другий вид дисбалансу - дисбаланс «популярність/значимість».

У якості контрольного для дисбалансу «популярність/значимість» виберемо співвідношення одного з показників популярності (*Popular(CM$_i$)* або *CAAM$_i$*) для *i*-ї спільноти (див. вище), а для показника значимості – один з показників, що наведені у табл. 2.6 (наприклад *CICC$_i$* – найпростіший для автоматизованого визначення у нинішніх умовах).

Розподіл між зонами, певною мірою, є аналогічним до попереднього випадку.

У зонах 1 та 2 знаходяться ті спільноти, які користуються великою популярністю, проте суспільне значення є невисоким. Популярність

досягається за рахунок вдалої стилістики матеріалів та інтенсивній рекламі, проте в перспективі такі спільноти легко витісняються більш конкурентними.

Для підтримки корисних спільнот даної зони доцільно:

- підвищувати якість матеріалів, залучаючи дружніх лідерів думок;
- здійснювати експлуатацію ворожих опонентів.

Щоб протидіяти шкідливим спільнотам зони доцільно залучати ресурси для використання нестабільності, що породжує дисбаланс, у першу чергу, формувати нові спільноти корисні для держави, які формуватимуть аудиторію на основі шкідливої.

У зонах 4 та 3 знаходяться ті спільноти, які мають велику кількість згадувань, проте не користуються високою популярністю. Така ситуація виникає у випадках високої якості матеріалів, які мають надто формальний характер. Серед спільнот даних зон слід виділити спеціалізовані спільноти формування баз знань, таких як Вікіпедія. Головною проблемою таких спільнот є система мотивації користувачів, проте у довгостроковій перспективі вони мають критично важливе значення для безпеки інформаційного простору держави.

Підтримки діяльності корисних спільнот даної зони зводиться до:

- ресурсної підтримки користувачів;
- забезпечення поширення матеріалів, зокрема за допомогою трансляторів;

Для протидії шкідливим спільнотам даних зон доцільно:

- залучати тролів (у першу чергу «товстих») для руйнування активної аудиторії шляхом втрати комунікаційного комфорту важливого для лідерів думок;
- реалізовувати сценарії «захоплення спільноти» (актуально для вікі-спільнот з акцентованою саморегульованістю).

Відзначимо, що вибір дій щодо дружніх чи ворожих спільнот повинен здійснюватися на результатах аналізу обох видів дисбалансу спільнот та дисбалансу лідерів думок, навколо яких сформована спільнота.

3.5. Висновки до розділу

У третьому розділі дисертаційної роботи розроблено ряд спеціальних методів та алгоритмів, покликаних підвищити якість та ефективність діяльності з захисту інформаційного простору держави.

Розроблено методи визначення ряду зведених показників віртуальних спільнот, зокрема показники комунікативного комфорту та близькості завданням державної безпеки. Показано їхнє застосування для пріоритезації спільнот у відповідних завданнях.

Далі у розділі наведено методи планування заходів із захисту інформаційного простору, зокрема: загальний алгоритм організації заходів у спільнотах; алгоритм персоналізації суб’єктів інформаційної діяльності, методи виявлення впливових лідерів думок; методи продидії шкідливим лідерам думок та модераторам; виявлення тролів та опонентів, що провадять наперед плановану діяльність.

На завершення розділу запроновано підхід до організації ефективної ресурсної підтримки корисних заходів, що базуються на понятті дисбалансу у співвідношеннях між окремими показниками.

Розділ 4. Побудова комплексної системи управління заходами з протидії пропаганді в ССІ

Розроблені в роботі методи та засоби захисту інформаційного простору держави є повністю орієнтованими на сучасні інформаційні технології і потребують програмно-технічної підтримки. Ефективною така підтримка може бути за умови компексного підходу, коли розв'язання окремих задач здійснюється узгоджено, на основі єдиної інформаційної платформи.

У якості такої платформи доцільно використати розроблені в другому розділі дисертаційної роботи формальні моделі користувачів та спільнот, а функціональність системи базувати на відповідних методах та алгоритмах.

Далі у розділі буде розглянуто архітектуру та приниципи реалізації пропонованого програмного комплексу, модель її бази даних та функціональні особливості окремих компонент.

Основні результати розділу опубліковано в роботах [27, 50, 52, 126].

4.1. Архітектура програмного комплексу

Загальну архітектуру програмного комплексу наведено далі на рис. 4.1. У розробці архітектури системи використано результати теоретичних розділів роботи та загальні підходи до розробки систем аналогічних класів, викладені, зокрема, в роботах [61, 63, 96, 100, 101].

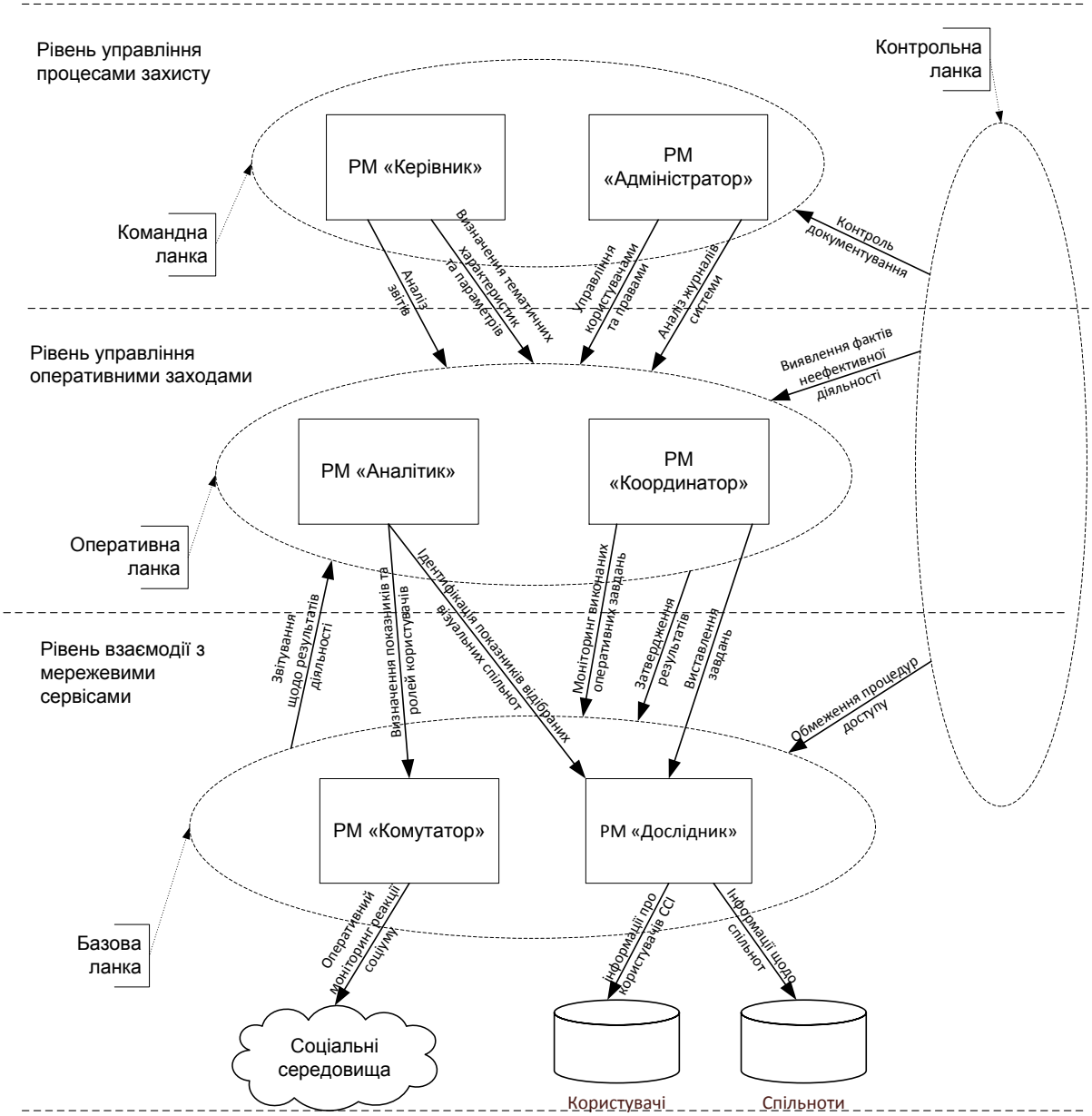

Рис. 4.1. Загальна архітектура програмного комплексу

Користувачами системи є:

- **командна ланка** – відповідальні за безпеку інформаційного простору за напрямками, з числа осіб з високою кваліфікацією та компетенціями;
- **оперативна ланка -** оперативні працівники середньої ланки, відповідальні за безпеку за окремими проектами або об’єктами;
- **базова ланка -** виконавці з числа оперативних працівників базової ланки або волонтерів;

- **контрольна ланка** – виконавці з числа фахівців кібезбезпеки та безпеки прикладних інформаційних систем, адміністратори.

Дані категорії користувачів визначено на основі алгоритму, наведеного в розділі 3.2.1 «Загальний інформаційно-технологічний алгоритм організації заходів у віртуальних спільнотах».

В архітектурі наявно два програмні рівні системи, рівень інфраструктури та середовище розділеного безпечного доступу, які відповідають ланкам користувачів.

- **1-й рівень** – рівень управління процесами захисту. На даному рівні наявні компоненти, за допомогою яких проводиться контроль та керування заходами у цілому, призначений для командної ланки.
- **2-й рівень** – рівень управління оперативними заходами. На даному рівні наявні компоненти, за допомогою яких проводиться управління оперативних завдань, що передаються на виконання оперативним працівникам та волонтерам. Призначений для оперативної ланки.
- **Інфраструктурний рівень** – рівень взаємодії з мережевими сервісами, які реалізують соціальні середовища Інтернету та засоби для автоматизації рутинних дій. Цей рівень призначений для виконання оперативних функцій працівниками та волонтерами, технічна реалізація є доволі автономною в контексті комплексу.

З точки зору базового програмного забезпечення система реалізується засобами, орієнтованими на опрацювання великих масивів даних. З програмно-технічної точки зору система реалізується на комплексі технологій, орієнтованих на системи з відкритим кодом. У якості операційної системи необхідно використовувати одну з корпоративних версій Linux з підтримкою кластерів та хмарних обчислень. Для збереження та опрацювання даних доцільно використати СКБД Oracle Enterprise Server. Для реалізації повноцінного текстового пошуку з врахуванням нечіткостей та лексичних слоформ доцільно

використати одну з систем текстового пошуку в локальному варіанті (наприклад систему MnogoSearch), або використати розширені можливості СКБД Oracle з опрацювання природномовних текстів (опція Oracle Text). Причому, враховуючи необхідність врахування фактора обмеженого доступу до даних, доцільнішим є використання інтегрованих в СКБД опцій.

Для організації безперебійної надійної роботи комплексу в умовах накопичення великих даних доцільно використати хмарні технології розподілення даних та обчислень, проте з міркувань безпеки використання наявних хмарних сервісів (таких як Amazon чи Oracle Cloud) є сумнівним.

Оптимальним рішенням є розгортання власної хмари з обмеженим доступом на мережевому рівні та системою багатоетапної аутентифікації і розділенням доступу до первинних даних (див. далі).

4.2. Модель бази даних програмного комплексу

Модель бази даних системи базується на формальній моделі предметної області, що наведено у розд. 2 «Побудова формальних моделей ССІ з врахуванням безпекового фактору». База даних системи може бути реалізована як єдина БД, з фізичної точки зору, проте її опис наведено покомпонентно з метою підвищення ілюстративності.

4.2.1. База даних «Користувачі»

БД «Користувачі» охоплює базові масиви даних про користувачів соціальних мереж, що обліковуються. Це зокрема: ідентифікаційні дані користувача (включно з мережевою ідентифікацією), ролі користувача, якщо вони визначені для нього, характеристки державної безпеки (див. рис. 4.2).

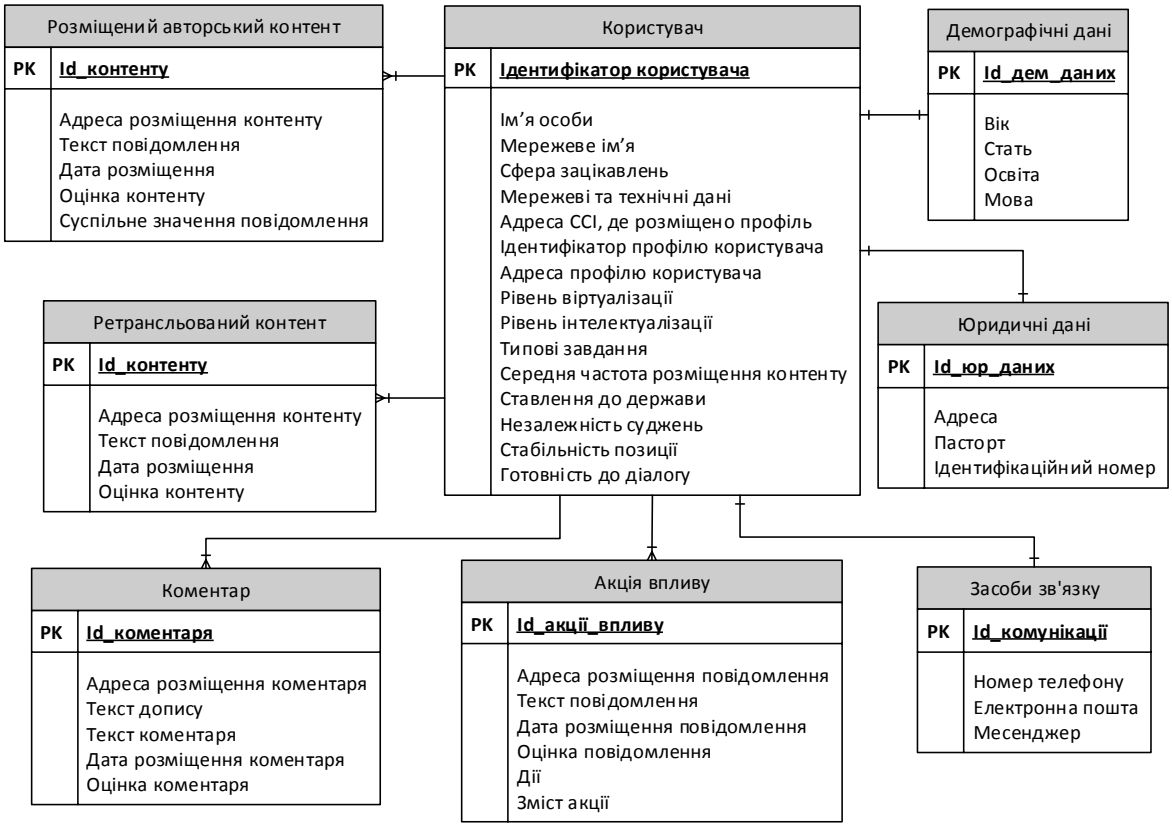

Рис. 4.2. Інформаціна модель користувача соціальних середовищ Інтернету

Дана компонента бази даних може використовуватися автономно, або в складі інших аналогічних систем для базового обліку користувачів соціальних мереж у цілому (якщо поставлена таке завдання), або для обліку окремих, значущих для безпеки інформаційного простору держави, персоналій.

4.2.2. База даних «Активність користувачів»

БД «Активність користувачів» документує дії користувачів соціальних мереж, зокрема зі створення нового контенту.

Дана компонента бази даних може використовуватися лише в поєднанні з базовою компонентою «Користувачі» для поглибленого обліку окремих, значущих для безпеки інформаційного простору держави, персоналій, а також у прикладних психологічних завданнях, пов'язаних із поглибленим аналізом поведінки користувачів у глобальній мережі.

4.2.3. База даних «Соціальний портрет користувача»

БД «Соціальний портрет користувача» документує стосунки користувачів з іншими користувачами та спільнотами.

Дана компонента бази даних може використовуватися лише в поєднанні з базовою компонентою «Користувачі» для поглибленого обліку окремих, значущих для безпеки інформаційного простору держави, персоналій або ж у прикладних соціологічних задачах аналітичного опрацювання системи соціальних зв'язків (social graph) за умови наявності відповідного достатньо повного масиву даних та обчислювальних ресурсів.

4.2.4. База даних «Спільноти»

БД «Спільноти» містить базові масиви даних про спільноти соціальних мереж, що обліковуються (див. рис. 4.3). Це зокрема: технічні характеристики, показники аудиторії, показники суспільної значимості, характеристики змісту та комунікації, характеристики державної безпеки.

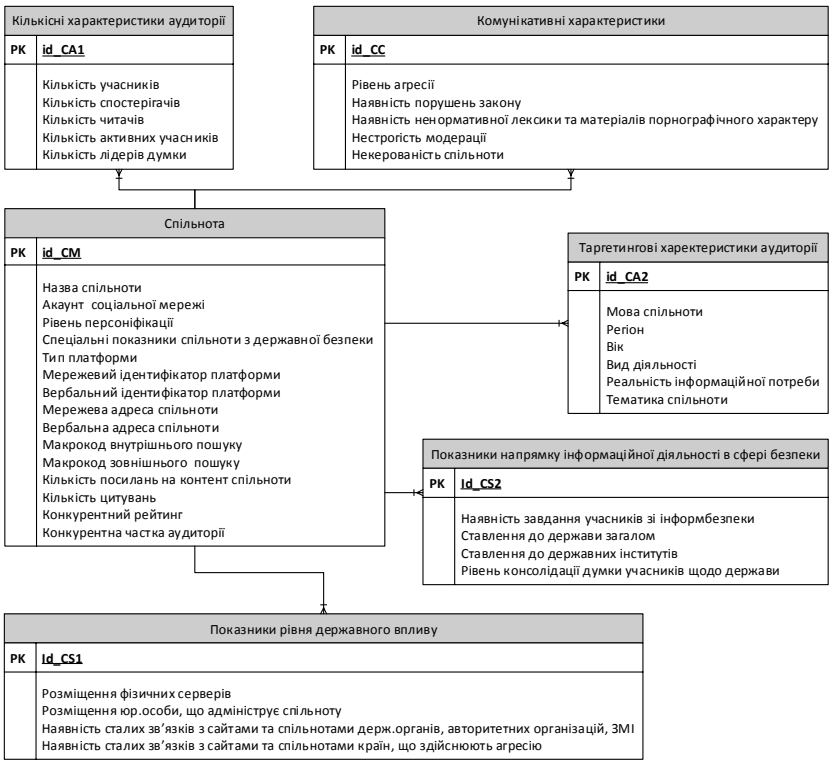

Рис. 4.3. Інформаційна модель соціальних середовищ Інтернету

Дана компонента бази даних може використовуватися автономно, або в складі інших аналогічних систем для базового обліку спільнот, які формують важливі сегменти з точки зору безпеки інформаційного простору держави.

4.3. Компоненти системи

4.3.1. Компоненти командного рівня

Компоненти командного рівня призначені для загального управління системою та процесами захисту інформаційного простору. Такими компонентами є:

- компонента «Адміністратор»;
- компонента «Керівник».

Компонента «Адміністратор» призначена для виконання типових функцій системного адміністратора, зокрема:

- конфігурування та моніторинг системи;
- аналіз журналів системи;
- управління користувачами та правами.

Компонента «Керівник» призначена для стратегічного управління діяльністю, відповідно серед її функцій є:

- визначення тематичних характеристик для подальших фільтрів суб’єктів за релевантністю;
- визначення конкретних значень вагових параметрів, що визначають характер інформаційної діяльності і є введеними у розгляд в попередніх розділах;
- аналіз звітів оперативних виконавців, координаторів та аналітиків;
- підтвердження повноважень користувачів.

4.3.2. Компоненти оперативного рівня

Компоненти даного рівня забезпечують можливість виконання завдань з підвищеною відповідальністю, зокрема, завдань оперативного управління та комплексного аналізу (див. рис. 4.4).

Компонентами оперативного рівня є:

- компонента «Аналітик»;
- компонента «Координатор».

Завданням «Аналітика» є аналіз даних щодо комунікативних процесів у ССІ, зокрема ідентифікація можливих напрямків оперативної діяльності.

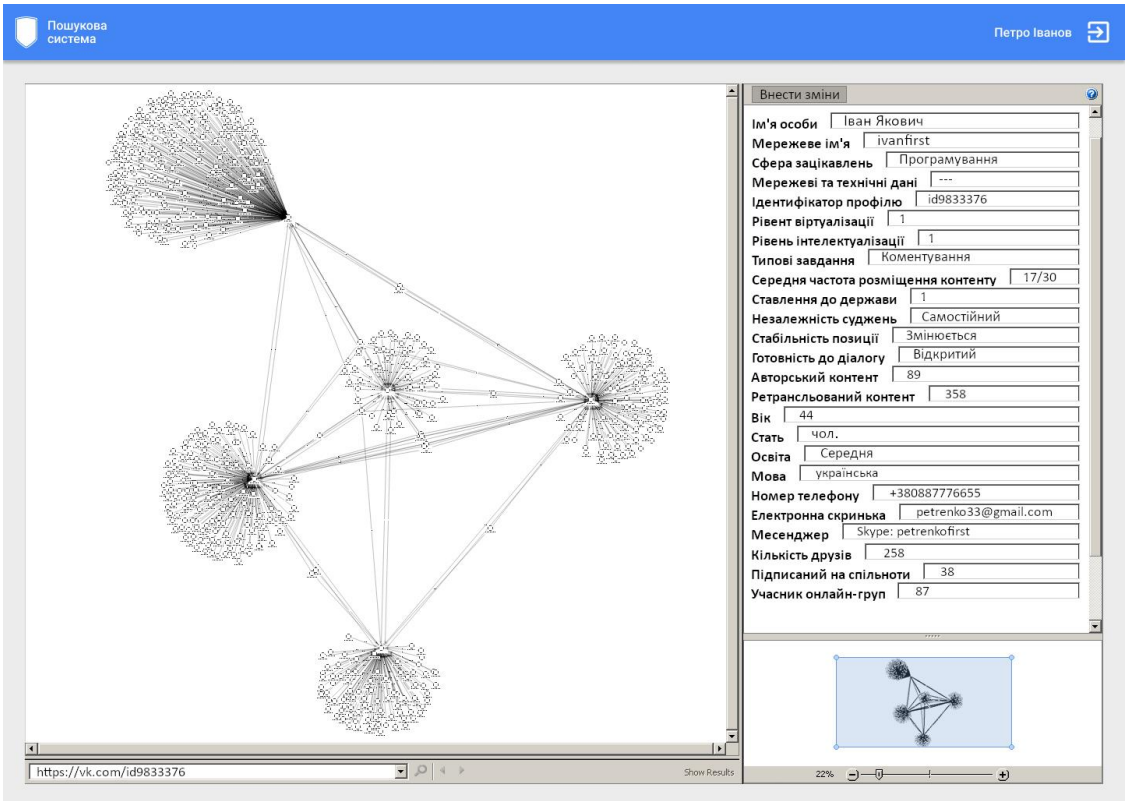

Рис. 4.4. Інтерфейс робочого місця «Аналітик»

Основні функції:

- ідентифікація показників відібраних віртуальних спільнот – згідно до моделі, наведеної в роз. 2.2 «Побудова формальної моделі віртуальних спільнот як середовища соціокомунікативного протиборства» та розд.

3.1 «Зведені показники віртуальних спільнот та пріоритезація спільнот з точки зору державної безпеки»;

- визначення показників та ролей окремих відібраних користувачів згідно до відповідних моделей (див. 2.1 «Формалізація користувачів соціальних середовищ Інтернету з точки зору безпеки інформаційного простору держави»);
- визначення пріоритетності напрямків впливу 3.2 (див. розділ «Планування заходів із захисту інформаційного простору держави»).

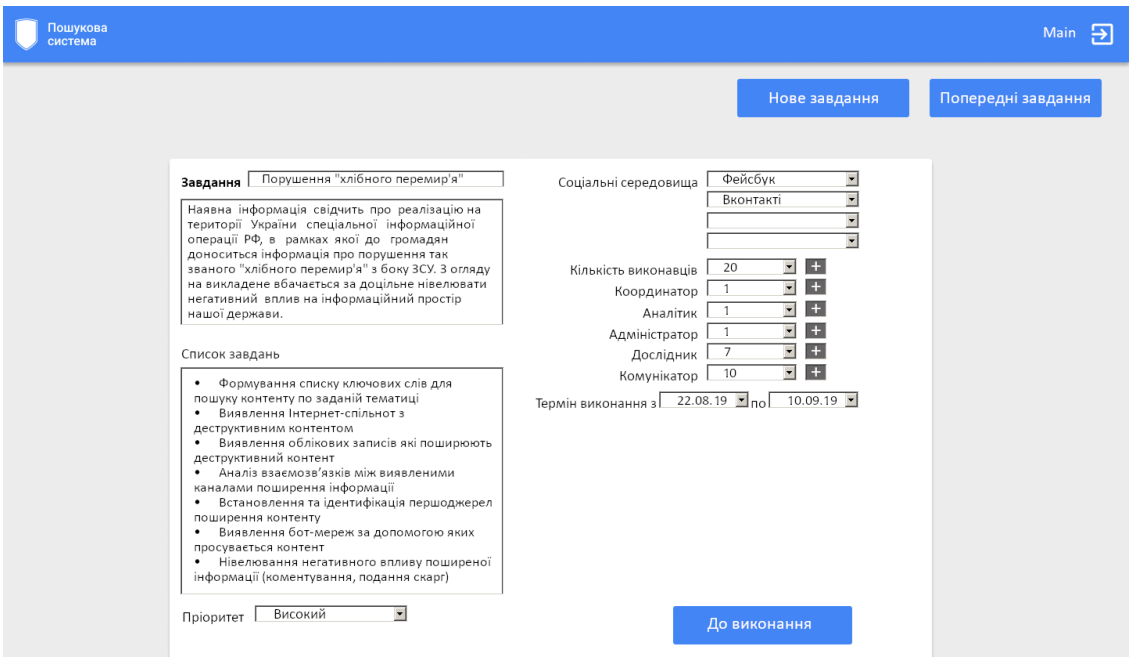

Рис. 4.5. Інтерфейс робочого місця «Координатор»

Завданням «Координатора» є організація скоординованих дій волонтерів із виконання оперативних завдань (див. рис. 4.5). Це передбачає:

- виставлення завдань – внесення в базу даних інформації про нові завдання у формі «профіль, спільнота або дискусія» + «оперативна задача».;
- моніторинг виконання оперативних завдань – швидкий доступ до профілів, спільнот та дискусій, щодо яких виконуються завдання, з відображенням текстових слідів діяльності;

- затвердження результатів – валідація їх та зміну статусу в базі даних системи.

Перелік можливих завдань формується з врахуванням запропонованих методів у розд . 3 «Методи та алгоритми»

4.3.3. Компоненти інфраструктурного рівня

Компоненти інфраструктурного рівня призначені для спрощення дій оперативних працівників із взаємодією з сервісами Інтернету, у першу чергу, з соціальними середовищами та з глобальними пошуковими системами. З технологічної точки зору дане ПЗ в певній мірі імітує роботу класичного Веб-браузера. Як наслідок, його реалізацію доцільно здійснювати як надбудову над одним зі стандартних браузерних ядер. Найбільш перспективним виглядає використання в якості такого ядра браузера з відкритим кодом Chromium. Надбудова над цим ядром покликана автоматизувати ряд окремих дій, виконання яких може забирати багато часу та зусиль виконавця.

ПЗ даного рівня може володіти певними інтелектуальними характеристиками (зокрема валідації тексту тощо), але через складність завдань та області використання, чутливість середовища до помилкових вчинків, довготривалість наслідків, не доцільно розглядати варіанти повністю автоматизованого ПЗ, хоча значну частину рутинних дій автоматизувати доцільно.

Компонентами інфраструктурного рівня є:

- компонента «Дослідник» (див. рис. 4.6);
- компонента «Комунікатор».

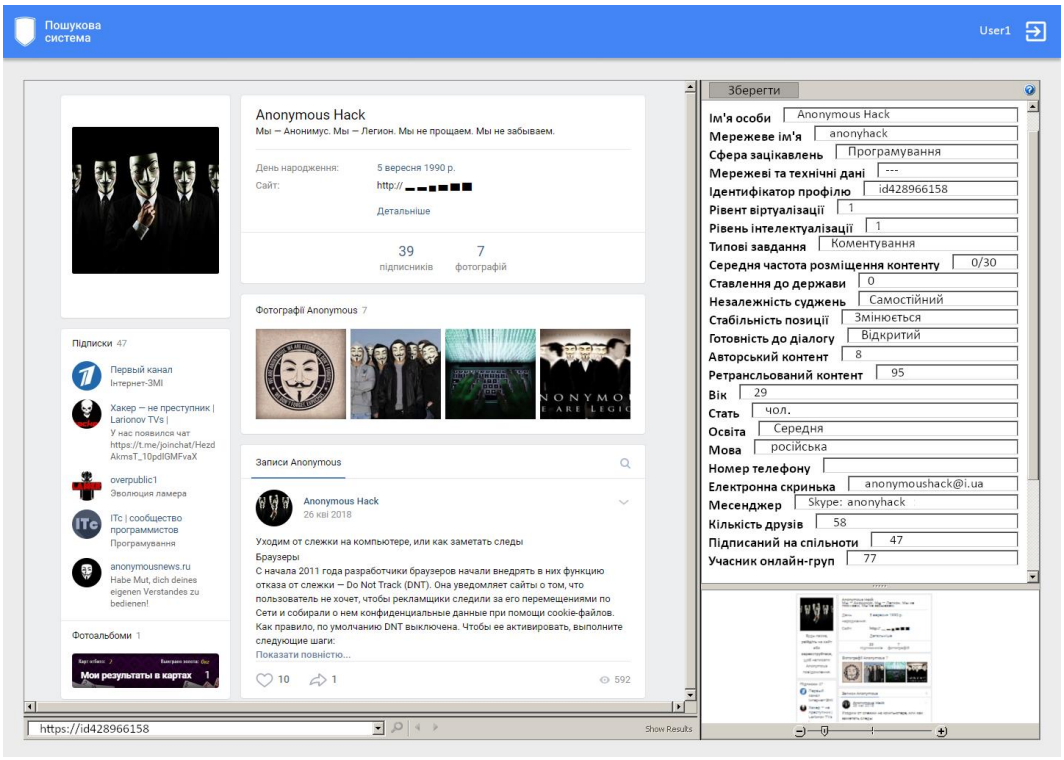

Рис. 4.6. Інтерфейс робочого місця «Дослідник»

Завданням компоненти «Дослідник» є збір первинних даних щодо суб'єктів комунікативних процесів у ССІ, зокрема ідентифікація фізичних осіб та спільнот, релевантних проблемам безпеки інформаційного простору. Основні функціональні можливості:

- внесення в БД «Користувачі» інформації про користувачів ССІ, визначення їхньої мережевої та фізичної ідентифікації;
- внесення в БД «Каталог» інформації щодо спільнот, визначення базових характеристик;
- внесення в БД «Активність користувачів» інформації щодо актуальних дискусій, важливих, з точки зору, державної безпеки.

Завданням компоненти «Комунікатор» є здійснення активної інформаційної діяльності в ССІ згідно визначених завдань в межах компоненти «Координатор» (див. рис. 4.7).

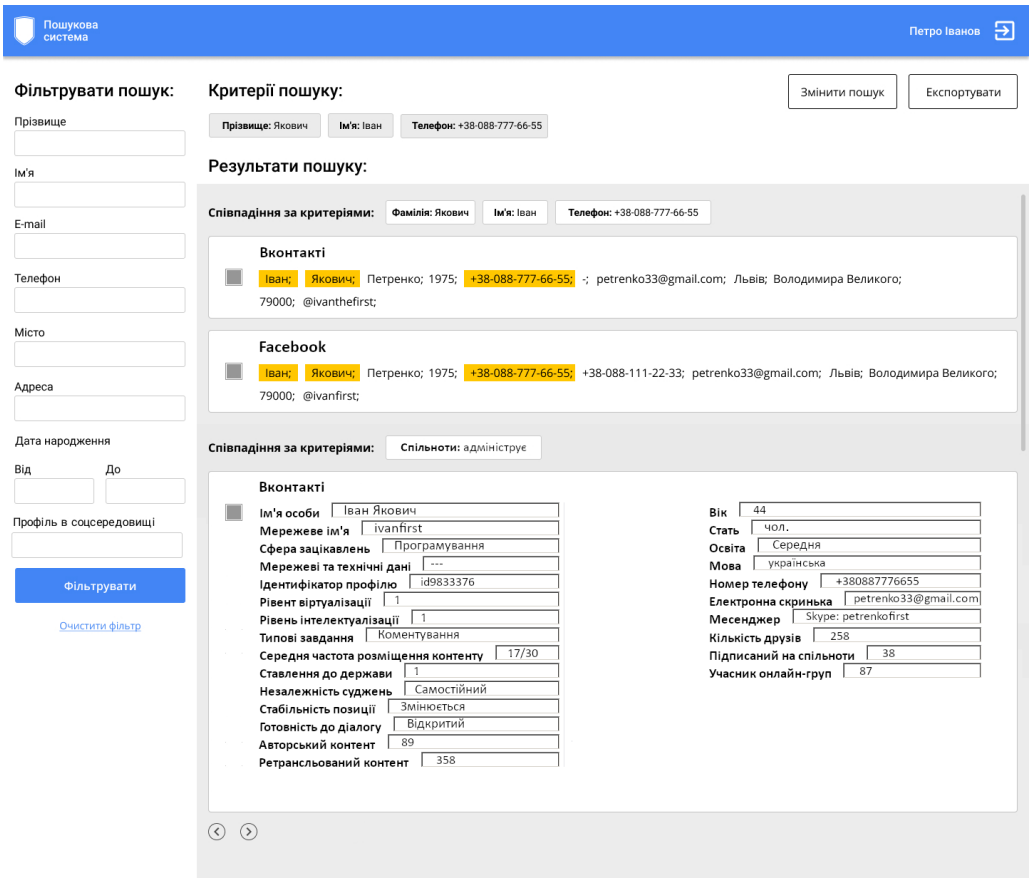

Рис. 4.7. Інтерфейс робочого місця «Координатор»

Основні завдання полягають в:

- здійсненні цілеспрямованої системної комунікації (написання текстів, коментування, реагування) у відповідності з пропонованими в роботі методами інформаційного протиборства;
- оперативний моніторинг реакції соціуму;
- звітуванні щодо результатів діяльності.

4.3.4. Компонента захисту або рівень безпеки

Компонента захисту орієнтована на комплексне забезпечення надійності комунікативних процесів і включає:

- функцію строгого розділення до масивів даних як за вертикальним, так і за горизонтальним принципом, що передбачає обмеження не лише на рівні інтерфейсів та процедур доступу, але й на рівні СКБД і для цього

використовується підхід параметризованих запитів (views) з обмеженням по користувачу, запронований у роботах [120, 125] ;

- виявлення фактів неефективної або шкідницької діяльності окремих виконавців – інтелектуальне опрацювання задокументованих дій оперативних виконавців на предмет виявлення таких дій, які є шкідливими для поставлених завдань;
- ідентифікація нових загроз із боку CCI – аналіз різних узгоджених змін у настроях чи діях окремих користувачів у межах одної або різних облікованих спільнот.

Враховуючи критичну важливість безпеки комплексу, опрацювання фактів обмежень та виявлення загроз повинні відбуватися в «тихому» для користувачів режимі, з документуванням, доступним лише адміністратору системи. Окремі незручності, що виникатимуть у роботі з системою, у такому разі компенсуються вищим рівнем захисту від несанкціонованого втручання. Критичним є не стільки комфортне для користувача опрацювання системних обмежень та повідомлень про них, скільки безумовне їх дотримання, документування та відсутність деталізації проблеми (як фактор зменшення загроз, пов’язаних з ін’єкцією різного виду кодів).

Важливість такого підходу та компоненти у цілому підсилюється тим фактом, що можливими користувачами є не лише представники правоохоронних органів, які несуть підсилену відповідальність за свої дії та пройшли відповідну кадрову перевірку, але й звичайні мережеві активісти, на яких така практика не поширюється і, відповідно, породжують загрози гуманітарного характеру.

4.3.5. Вимоги до інтерфейсів користувача системи

Головними вимогами до інтерфейсу системи з точки зору користувача є:

- професійний характер інтерфейсу – не передбачається використання системи непідготовленими користувачами;
- зручність використання на різних типах техніки – можливе використання з різних вузлів мережі, у тому числі на мобільних клієнтах;
- доступ до даних за запитом, доставлення даних окремими пакетами – для ефективної роботи з великими даними;
- передача даних повинна здійснюватися з максимальним рівнем захисту – можлива передача даних через публічні мережі.

4.4. Результати впровадження системи

У межах впровадження підходів, що зпропоновано у дисерційній роботі, громадськими активістами здійснюється ряд системних заходів у соціальних мережах «Фейсбук» та «Вконтакті», на інших мережевих площадках. Діяльність активістів здійснюється з використанням методів наведених у розд. 3.2 «Протидія лідерам думки, що здійснюють шкідливі впливи в інформаційному просторі держави», 3.3.3 «Виявлення тролів та опонентів, що діють згідно визначеного плану та завдання» з занесенням результатів в БД наведеної вище структури.

Далі (див. рис. 4.8) наведено результати дворічної діяльності з захисту інформаційного простору України мережевими активістами, що діяли за зазначеною схемою. Такі дії проводилися в окремих, критично важливих для національної безпеки, спільнотах. Визначення таких спільнот здійснювалося, зокрема, з використанням запропонованих у роботі підходів (див. розд. 2.2.4 «Показники суспільної значимості»).

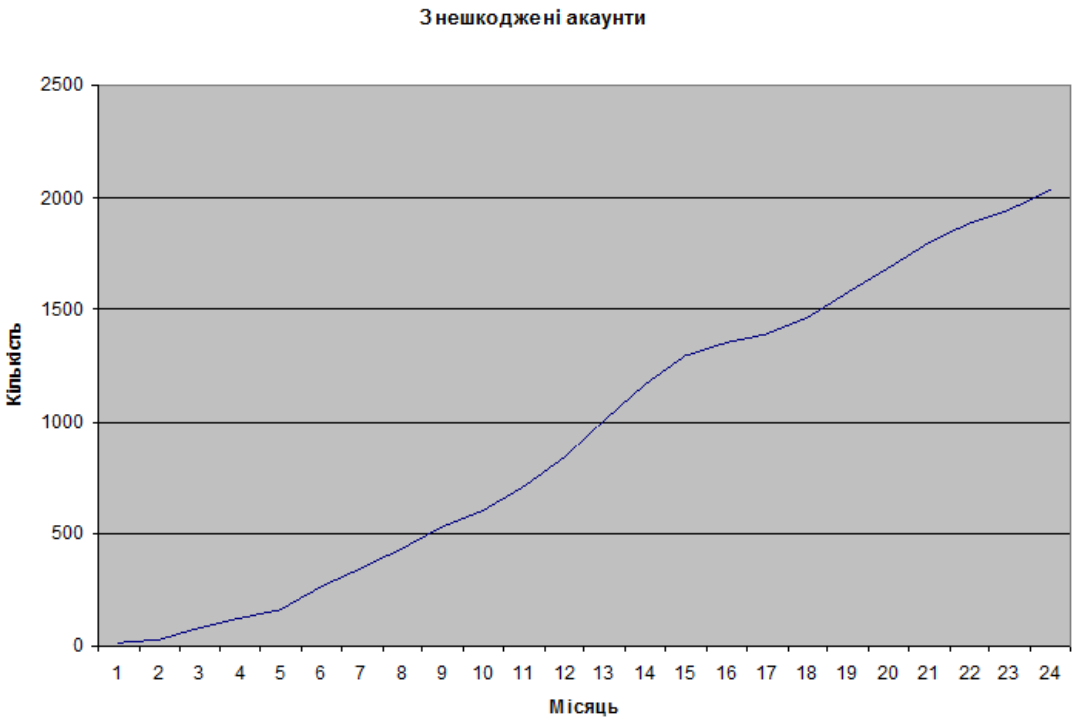

Рис. 4.8. Кількість знешкоджених акаунтів

На графіку наведено дані про кількість знешкоджених акаунтів, тролів та трансляторів, які ідентифіковано як шкідливі в спільнотах, що підлягають моніторингу . Знешкодженими вважаються транслятори, які у середньому проявляють мережеву активність не частіше разу на тиждень або у випадку блокування акаунту, ліквідації чи самоліквідації акаунту.

На графіку можна простежити окремі етапи інформаційної діяльності з виявлення шкідливих акаунтів. Повільне зростання перших 6-ти місяців обумовлене поступовим накопиченням даних про спільноти, наповненням базових інформаційних масивів, початкове виявлення шкідницьких акаунтів, які необхідно нейтралізувати. У подальшому спостерігається доволі рівномірний процес знешкодження акаунтів, окремі зміни в динаміці обумовлені не особливостями експлуатації системи, а змінами в інтенсивності агресивних дій в інформаційному просторі України.

На іншому графіку (див. рис. 4.9) наведено динаміку зміни частки лідерів думок, що здійснюють шкідливу діяльність щодо України у

загальній кількості лідерів думок. У даному випадку моніторингу підлягали користувачі, що здійснювали активну діяльність в ряді визначених наперед важливих для національної безпеки спільнотах.

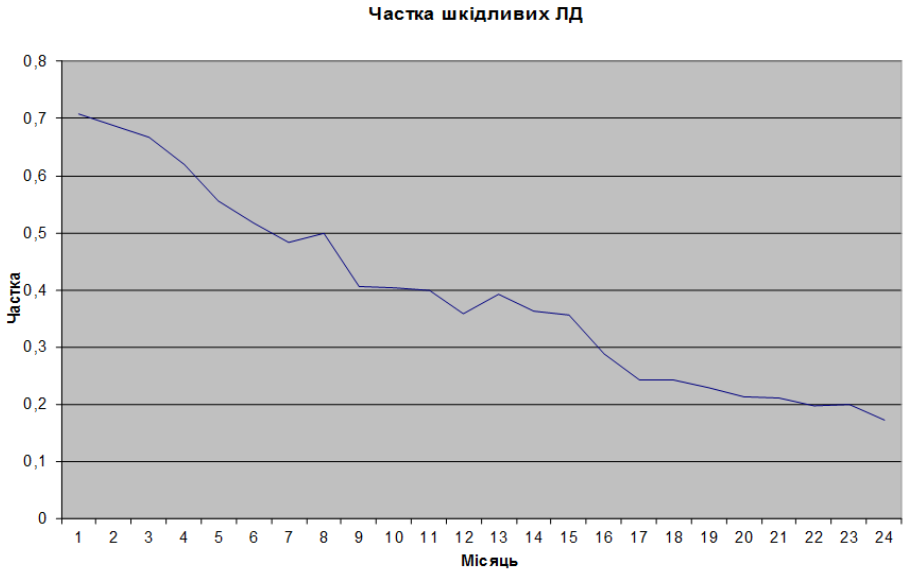

Рис. 4.9. Динаміка зміни частки шкідливих лідерів думок

В абсолютних величинах кількість лідерів думок у спільнотах, що знаходилися під моніторингом, збільшилася з 20-ти до 44-х, переважно за рахунок патріотично налаштованих користувачів.

Співставлення надходження даних про нових лідерів думок та зміни числа активних лідерів думок, що проводили деструктивну діяльність, дозволяють стверджувати, що більшість шкідливих впливів нейтралізувалися й ідентифіковані як шкідливі користувачі, припиняли свою активність, втративши можливість ефективно проводити агресивні дії.

4.5. Висновки до розділу

У четвертому розділі дисертаційної роботи наведено практичні результати дисертаційної роботи, втілені в комплексній системі захисту інформаційного простору держави.

Описано багаторівневу архітектуру програмного комплексу, в розробленні якої використано результати теоретичних розділів роботи та загальні підходи до розробки систем аналогічних класів. Визначено категорії користувачів системи: командна ланка, оперативна ланка, базова ланка, контрольна ланка. З програмно-технічної точки зору система реалізується на комплексі технологій, орієнтованих на системи з відкритим кодом та засобами, орієнтованими на опрацювання великих масивів даних. Далі у розділі наведено орієнтовну структуру бази даних комплексу в ERD нотації, яка базується на формальних моделях, розроблених у попередніх розділах.

У розділі також описано функції компонент системи за її рівнями. Відзначено методи та алгоритми, розроблені у роботі, на яких базуються відповідні компоненти, визначено основні вимоги до користувальницького інтефейсу системи.

На завершення розділу подано окремі результати практичної апробації дисертаційних досліджень у інформаційному просторі України.

Висновки

У дисертаційній роботі вирішено важливе наукове завдання – підвищення рівня захисту інформаційного простору держави за допомогою розроблення математичного та програмного забезпечення протидії інформаційній пропаганді в соціальних середовищах Інтернету та їхнього практичного втілення. Зокрема, отримано такі результати:

- проаналізовано розвиток та функціонування соціальних середовищ Інтернету, що підтвердило актуальність наукового завдання із розроблення методів та засобів протидії інформаційній пропаганді;
- набули подальшого розвитку формальні моделі користувачів соціальних середовищ Інтернету з уведенням спеціальних характеристик мережевого, інформаційного, соціокомунікаційного змісту, орієнтованих на завдання захисту інформаційного простору, що дало змогу формалізувати та вирішити важливі завдання організації ефективної взаємодії із користувачами соціальних середовищ Інтернету;
- удосконалено формальні моделі віртуальних спільнот з описом їх як середовища інформаційного протиборства з характеристиками аудиторії, суспільної значущості, змісту, комунікації, державної безпеки, що стало основою для побудови інформаційної моделі системи управління заходами із захисту інформаційного простору;
- уперше побудовано метод оцінювання віртуальних спільнот за допомогою зведених показників, орієнтованих на завдання захисту інформаційного простору держави на підставі базових характеристик формальної моделі цих спільнот, яка стала основою для розроблення низки прикладних методів протидії інформаційній пропаганді;
- уперше розроблено методи планування заходів із протидії інформаційній пропаганді у соціальних середовищах Інтернету, що грунтуються на запропонованих формальних моделях користувачів і

спільнот та їхніх зведених показниках, і забезпечують можливість організації неперервної системної протидії комплексним загрозам для безпеки національного інформаційного простору;

- побудовано алгоритми виявлення окремих груп користувачів (та протидії їм), які ведуть деструктивну діяльність в інформаційному просторі держави, що грунтуються на уведених у роботі спеціальних ролях користувачів, а це уможливлює ефективне виконання оперативних завдань з інформаційного протиборства;
- розроблено підхід до організації ресурсної підтримки заходів із протидії інформаційній пропаганді з використанням апарату дисбалансів у показниках користувачів та віртуальних спільнот соціальних середовищ Інтернету;
- розроблено комплексну систему управління заходами з протидії пропаганді, яка основана на запропонованих у роботі формальних моделях, методах та алгоритмах і забезпечує автоматизацію та ефективне виконання основних завдань організації та координації дій відповідальних осіб і волонтерів щодо захисту інформаційного простору держави;
- апробовано запропоновані методи і засобів протидії інформаційній пропаганді у соціальних середовищах Інтернету з використанням їх в окремих, важливих для національної безпеки, спільнотах.

Література

1. Bottery M. The End of Citizenship? The Nation State, Threats to its Legitimacy, and Citizenship Education in the Twenty-first // Cambridge Journal of Education. 2003. Vol. 33. No 1. pp. 101–122.
2. Carley, K. , Lee, J., Krackhardt D. Destabilizing networks. Connections, 2002. – Vol. 24, Issue 3. – P. 79–92.
3. Fedushko S., Development of verification system of socio-demographic data of virtual community member, Radio Electronics Computer Science Control, Article no. 3, pp. 87-92, 2016.
4. Fedushko, S., Development of a software for computer-linguistic verification of socio-demographic profile of web-community member, Webology. - Iran: Webology Center, 2014. – Vol. 11. — No. 2, Article 126. – 14 p. Available at: http://www.webology.org/2014/vl ln2Zal26.pdf
5. Ferrara, E. Disinformation and Social Bot Operations in the Run Up to the 2017 French Presidential Election. First Monday 22, 8 (2017).
6. Flynn, L., Goldsmith, R., Eastman, J,. Opinion Leaders and Opinion Seekers: Two New Measurement Scales, Journal of the Academy of Marketing Science . – 1996. – 24. – P.137-147.
7. Hryshchuk, R., & Molodetska, K. (2017). Synergetic Control of Social Networking Services Actors' Interactions. Szewczyk, R., &Kaliczyńska, M. (Eds). Recent Advances in Systems, Control and Information Technology, 543, 34-42. Retrieved from https://link.springer.com/chapter/10.1007%2F978-3-319-48923-0_5.
8. Im, J., Chandrasekharan, E., Sargent, J., Lighthammer, P., Denby, T., Bhargava, A., Hemphill, L., Jurgens, D., & Gilbert, E. (2019). Still out there: Modeling and Identifying Russian Troll Accounts on Twitter. CoRR, abs/1901.11162

9. Information operation roadmap [Text] / DoD US, 30 october 2003. – 78p. http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap .pdf
10. Karlsen R. Followers are opinion leaders: The role of people in the flow of political communication on and beyond social networking sites, European Journal of Communication. – 2015. – Vol 30, Issue 3. – P.301-318.: https://doi.org/10.1177/0267323115577305.
11. Kohring, M. & Matthes, J., Trust in news Media: Development and validation of a multidimensional scale, Communication Research, 2007, vol. 34, no. 2, pp. 231-252.
12. Korzh, R., Peleschyshyn, A., Syerov, Y., S. Fedushko, The cataloging of virtual communities of educational thematic Webology. – 2014. – Vol. 11. – № 1. – P. 1–16.
13. Lawson, S., Putting the "war" in cyberwar: Metaphor, analogy, and cybersecurity discourse in the United States, *First Monday*, 2012, vol. 17, no. 7.
14. Lazo, M., Batlle, F., Information quality and trust: From traditional media to cybermedia. Communication: Innovation & Quality, 2019
15. Markovets, O., Peleschyshyn, A., Modeling of Citizen Claims Processing by Means of Queuing System, International Journal of Computer Science and Business Informatics (IJCSBI), Vol. 15, No. 1. January 2015. – P. 36-46.
16. Mondal, M., Messias, J., Ghosh, S., Gummadi K., Kate, Aniket., Forgetting in Social Media: Understanding and Controlling Longitudinal Exposure of Socially Shared Data. In Twelfth Symposium on Usable Privacy and Security, SOUPS 2016, Denver, CO, USA, June 22-24, 2016. – P. 287-299.
17. Mousavizadeh, M., Hazarika, B. & Rea, A. 2018, A study of news credibility and trust on social media - A multi-cultural evaluation, *Americas*

Conference on Information Systems 2018: Digital Disruption, AMCIS 2018.

18. Peleshchyshyn A., Markovets O., Vus V., Albota S. Identifying specific roles of users of social networks and their influence methods // Комп'ютерні науки та інформаційні технології (CSIT-2018) : матеріали XIII Міжнар. наук.-техн. конф., Львів, 11–14 верес. 2018 р. Львів, 2018. С. 39–42.
19. Peleshchyshyn A., Vus V., Albota S., Markovets O. A formal approach to modeling the characteristics of users of social networks regarding information security issues // Advances in Intelligent Systems and Computing. 2019. Vol. 902 : Advances in artificial systems for medicine and education II. The second international conference of artificial intelligence, medical engineering, education (AIMEE2018), 6–8 Oct. 2018, Moscow, Russia. P. 485–494.
20. Robinson, N. and Lance Holbert, r., 2018. Taking sides in the war on news: exploring curvilinear associations and group differences related to perceptions of news media as threat. Journal of Applied Communication Research, 46(6), pp. 684-702.
21. Russell M., Klassen M. Mining the Social Web: Data Mining Facebook, Twitter, LinkedIn, Google+, GitHub, and More, 3rd Edition. – O'Reilly Media, 2018. – 423 p.
22. Spangher, A., Ranade, G., Nushi, B., Fourney, A., Horvitz, E.: Analysis of Strategy and Spread of Russia-sponsored Content in the US in 2017. arXiv preprint arXiv:1810.10033 (2018).
23. Stewart, L.G., Arif, A., & Starbird, K. (2018). Examining Trolls and Polarization with a Retweet Network. https://faculty.washington.edu/kstarbi/examining-trolls-polarization.pdf

24. Stohl C., Stohl M.. Networks of Terror: Theoretical Assumptions and Pragmatic Consequences // Communication Theory. – 2007. – Vol. 17, Issue 2. – P. 93–124. doi: 10.1111/j.1468-2885.2007.00289.x
25. Stohl, C., Stohl M., Networks of Terror: Theoretical Assumptions and Pragmatic Consequences , Communication Theory. – 2007. – Vol. 17, Issue 2. – P. 93–124. doi: 10.1111/j.1468-2885.2007.00289.x 3
26. Thomas, K., Grier, C., & Paxson, V. Adapting social spam infrastructure for political censorship. In Proceedings of the 5th USENIX conference on Large-Scale Exploits and Emergent Threats. USENIX Association, 2012.
27. Trach O., Vus V., Tymovchak-Maksymets O. Typical algorithm of stage completion when creating a virtual community of a HEI // Сучасні проблеми радіоелектроніки, телекомунікацій, комп'ютерної інженерії (TCSET'2016) : матеріали XIII Міжнар. конф., Львів, Славське, 23–26 лют. 2016 р. Львів : Вид-во Львів. політехніки, 2016. С. 849–851.
28. Traylor, T., Straub, J., Gurmeet & Snell, N. 2019, "Classifying Fake News Articles Using Natural Language Processing to Identify In-Article Attribution as a Supervised Learning Estimator", Proceedings – 13th IEEE International Conference on Semantic Computing, ICSC 2019, pp. 445.
29. Turcotte, J., York, C., Irving, J., Scholl, R., Pingree, R., News Recommendations from Social Media Opinion Leaders: Effects on Media Trust and Information Seeking. Journal of Computer-Mediated Communication, Volume 20, Issue 5, 1 September 2015, Pages 520–535, https://doi.org/10.1111/jcc4.12127.
30. Valente T. Identifying Opinion Leaders to Promote Behavior Change / Thomas W. Valente, Patchareeya Pumpuang // Health Education & Behavior. – December 2007. – 34, Issue 6. – P.841–845.
31. Veale T., Cook M. Twitterbots: Making Machines that Make Meaning / Massachusetts Institute of Technology. – The MIT Press, 2018.

32. Vus V., Albota S., Dobrovolska V. The analysis of online communities as platforms for informational influences. Journal of Scientific and Engineering Research. 2019. Vol. 6, is. 2. P. 72–78.
33. Yatsko, V. Starikov, M., Butakov A., Automatic genre recognition and adaptive text summarization , Automatic Documentation and Mathematical Linguistics. – 2010. – Vol. 44, Issue 3. – P. 111–120.
34. Yoon, I. Why is it not just a joke? Analysis of Internet memes associated with racism and hidden ideology of colorblindness (2016) Journal of Cultural Research in Art Education, 33, pp. 92-123
35. Zannettou, S., Caulfield, T., Setzer, W.N., Sirivianos, M., Stringhini, G., & Blackburn, J. Who Let The Trolls Out? Towards Understanding State-Sponsored Trolls WebSci '19 Proceedings of the 10th ACM Conference on Web Science Pages 353-362,Boston, Massachusetts, USA — June 30 – July 03, 2019. https://arxiv.org/pdf/1811.03130.pdf.
36. Zheng, Y., Zhong, B. & Yang, F., When algorithms meet journalism: The user perception to automated news in a cross-cultural context, Computers in Human Behavior, 2018, vol. 86, pp. 266-275.
37. Асадова З. А. Состояние и стратегии обеспечения информационной безопасности в странах Центральной Азии на примере Республики Казахстан , Вестник МГИМО-Университета. – 2016. – № 6. – С. 92–96.
38. Бадер А. В. Вплив інформаційної складової збройного насилля на політичний процес в Україні , Гілея: зб. наук. праць. – № 116 – 2017. – С. 302–305.
39. Березко О. Л. Алгоритм активної реферальної персоніфікації інформаційного наповнення World Wide Web, Науковий вісник Національного лісотехнічного університету України : зб. наук.-техн. праць. – Львів : РВВ НЛТУ України, 2010. – Вип. 20.4. – С. 281–285.
40. Березко О. Л. Формальні моделі Веб-сторінки та історії її інформаційного наповнення, Східно-Європейський журнал передових

технологій. – Харків : Технологічний центр, 2009. – № 5/2 (41). – С. 26-32.

41. Березко О. Л. Каталог Веб-особистостей, Вісник Національного університету “Львівська політехніка” : Комп’ютерні системи та мережі. – Львів : Видавництво Львівської політехніки, 2008. – № 630. – С.12–16.
42. Березко О. Л. Персоніфікаційна класифікація Веб-сайтів, Східно-Європейський журнал передових технологій. – Харків : Технологічний центр, 2009. – № 4/2 (40). – С. 27–32.
43. Березко О.Л. Методи та засоби персоніфікації інформаційного наповнення у глобальній системі World Wide Web: автореф. дис. канд. техн. наук : 01.05.03,; Нац. ун-т "Львів. політехніка". – Л., 2011. – 20 с.
44. Бидюк П.И., Коваленко И.И., Баклан И.В. Системный анализ и информационные технологии в управлении проектами // Київ: Экономика и право. 2001. С. 270.
45. Брандман Э. М. Глобализация и информационная безопасность общества: монография, М-во образования и науки Российской Федерации, Московский гос. обл. ун-т, Тюменский гос. нефтегазовый ин-т, Ямальский нефтегазовый ин-т (фил.). – Москва : Изд-во ГПИБ России, 2007. – 173 с.
46. Булатова Е. И. Информационные войны: от теории к практике, Вестник электронных и печатных СМИ. – 2016. – № 1. – С. 23–29.
47. Бухарин С.Н., Циганов В.В. Методы и технологии информационных войн // Академический Проект. 2007. С. 384.
48. Бушуева Н.С., Бушуев С.Д., Бабаев И.А. Креативные технологии управления проектами и программами : Монография // Київ: Саммит-Книга. 2010. С. 768.
49. Воронцова Л., Фролов Д., История и современность информационного противоборства / Л. В. Воронцова,. – Москва, 2004. – 192 с.

50. Вус А. Аналіз форм публічної інформаційної діяльності в соціальних середовищах Інтернету // Інформація, комунікація, суспільство (ICS-2019) : матеріали 8-ої Міжнар. наук. конф., 16–18 травня 2019 р., Чинадієво. Львів : Вид-во Львів. політехніки, 2019. С. 41–43.
51. Вус А. Соціальні мережі як інструмент інформаційного протиборства // Інформація, комунікація, суспільство (ICS-2015) : матеріали 4-ої Міжнар. наук. конф., 20–23 трав. 2015 р., Львів, Славське. Львів : Вид-во Львів. політехніки, 2015. С. 28–29.
52. Вус В. А., Пелещишин А. М. Аналіз проблеми створення спеціального програмного забезпечення для протидії пропаганді в соціальних мережах // Інформація, , суспільство (ICS-2016) : матеріали 5-ої Міжнар. наук. конф., 19–21 трав. 2016 р., Львів, Славське. Львів : Вид-во Львів. політехніки, 2016. С. 38–39.
53. Вус В. А., Пелещишин А. М. Зведені показники віртуальних спільнот та пріоритезація спільнот з точки зору державної безпеки. Стандартизація, сертифікація, якість. 2019. № 2 (114). С. 73–80.
54. Вус В. Аналіз основних класів соціальних середовищ // Інформація, комунікація, суспільство (ICS-2018) : матеріали 7-ої Міжнар. наук. конф., 17–19 трав. 2018 р., Чинадієво. Львів : Вид-во Львів. політехніки, 2018. С. 39–40.
55. Гапеєва О. Л. Актуальні проблеми інформаційної безпеки: досвід ОДКБ, Матеріали міжнародної науково-практичної конференції «Інформаційний вимір гібридної війни: досвід України» – Київ, 11 травня 2017 р., – С. 102–107.
56. Гапеєва О. Л. Деякі питання забезпечення інформаційної безпеки в Україні, Військово-історичний вісник. – 2017. – № 3. – С. 31–39.
57. Гапеєва О. Л. Інформаційна безпека на пострадянському просторі: системно-історичний аналіз, Грані: науково-теоретичний альманах. – 2016. – № 140. – С. 93–99.

58. Горбулін, В., Додонов, О., ЛандеД., Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія. – Київ: Інтертехнологія, 2009. – 164 с.
59. Грищук Р.В., Мамарєв В.М., Молодецька-Гринчук К.В., “Класифікація профілів інформаційної безпеки акторів в соціальних інтернет-сервісах (на прикладі мікроблогу Twitter)”, Інформаційні технології та комп’ютерна інженерія,No2, с.12–19, 2017.
60. Грищук Р.В., Молодецька-Гринчук К.В. “Концепція синергетичного управління процесами взаємодії агентів у соціальних інтернет-сервісах”, Безпека інформації, т.21, No2, с.123–130, 2015.
61. Грищук Р.В., Молодецька-Гринчук К.В., “Постановка проблеми забезпечення інформаційної безпеки держави у соціальних інтернет-сервісах”, Сучасний захист інформації, No3(31), с.86–96, 2017.
62. Грищук Р.В., Молодецька-Гринчук К.В.,“Метод прогнозування динаміки поширення контенту й запитів на нього за даними контент-аналізу повідомлень у соціальних інтернет-сервісах”, Системи управління, навігації та зв’язку, No4(36), с.60–65, 2015.
63. Грищук Р.В., Молодецька-Гринчук К.В.,“Методологія побудови системи забезпечення інформаційної безпеки держави у соціальних інтернет-сервісах”, Захист інформації, т.19, No4, с.254–262, 2017.
64. Гумінський Р. В. Віртуальні спільноти як суб'єкт інформаційної безпеки держави, Захист інформації. – 2012. – № 3. – С. 18-25.
65. Гумінський Р. В. Методика прийняття рішення щодо протидії інформаційним загрозам віртуальних спільнот, Вост.-Европ. журн. передовых технологий. – 2015. – № 2/2. – С. 4-8.
66. Гумінський Р. В., Пелещишин А. М., Визначення рекомендацій щодо інформаційного впливу на структуру віртуальної спільноти, Безпека інформації. – 2014. – 20, № 3. – С. 264-273.

67. Гумінський Р. В., Пелещишин А. М., Загрози інформаційної безпеки держави в соціальних мережах, Наука і техніка Повітр. сил Збройн. сил України. – 2013. – № 2. – С. 192-199.
68. Гумінський Р. В., Пелещишин А. М., Модель інформаційного середовища віртуальної спільноти, Вост.-Европ. журн. передовых технологий. – 2014. – № 2/2. – С. 10-16. - Бібліогр.: 10 назв. - укр.
69. Добровольська В. В., Пелещишин А. М., Вус В. А. Фактор соціальних мереж у завданнях захисту суспільного інформаційного образу закладів культури. Вісник Національної академії керівних кадрів культури і мистецтв. 2018. № 4. С. 132–137.
70. Домарева, В. В. Безопасность информационных технологий. Системный подход [Текст] / В. В. Домарева. – К.:Изд. «Диасофт», 2004. – 992 с.
71. Згуровский М. З., Доброногов А. В. , Померанцева Т. Н. Исследование социальных процессов на основе методологии системного анализа // Национальная академия наук Украины. Киев : Наукова думка. 1997. С. 221.
72. Згуровський М. З., Гавриш О. А. , Войтко С. В. Розробка методики визначення рівня загроз сталому економічному розвитку України // Економічний вісник НТУУ «КПІ» : збірник наукових праць. 2011. № 8. С. 26–33.
73. Згуровський М.З., Петренко А.І. Е-наука на шляху до семантичного Грід. Частина 1: Об’єднання Web- і Грід-технологій // Систем. дослідж. та інформ. технології. 2010. № 1. С. 26–38.
74. Згуровський М.З., Петренко А.І. Е-наука на шляху до семантичного Грід. Частина 2: Семантичний Web- і семантичний Грід // Систем. дослідж. та інформ. технології. 2010. № 2. С. 7–25.
75. Зелинский С. А. Информационно-психологические войны (Современные психотехнологии манипулирования) / С. А. Зелинский

[Електронний ресурс] – Режим доступа: http://psyfactor.org/lib/zln3.htm/.

76. Інформаційна безпека України: блогери в гібридній війні [Електронний ресурс]. – Режим доступу: http://voi.com.ua/news/775988/.
77. Історія інформаційно-психологічного протиборства: підруч. / [Я. М. Жарков, Л. Ф. Компанцева, В. В. Остроухов, В. М. Петрик, М. М. Присяжнюк, Є. Д. Скулиш]; за заг. ред. д.ю.н., проф., засл. юриста України Є. Д. Скулиша. – Київ: Наук.-вид. відділ НА СБ України, 2012. – 212 с.
78. Корж Р.О. Формальний опис агресії в соціальних середовищах інтернету // Вісник інженерної академії України. 2018. Вип. № 1. С.70-74.
79. Короткий Т. Р. Понятие информационной войны в международном праве / Т. Р. Короткий, Д. А. Коваль // Альманах Международного права. – 2010. – Выпуск 2. – С. 331–343.
80. Ланде Д.В., Фурашев В.М. Системи моніторингу, витягу фактів, побудови зв’язків на основі аналізу неструктурованих текстів // Правова інформатика. К.: Науково-дослідний центр правової інформатики. 2010. № 2(26). С. 3–9.
81. Ланко Д. А., Левченко О. В. Форми ведення інформаційної боротьби: практичний підхід до понятійного апарату, Наука і оборона. – 2013. – № 3. – С. 21–27.
82. Левикін В. М., Костенко О. П., Петріченко О. В. Розробка комплексного методу пошуку і оцінки проектних рішень для маркетингових інформаційних систем // Математичні машини і системи. 2012. № 4. С. 84-93. Режим доступу: http://nbuv.gov.ua/UJRN/MMS_2012_4_11.

83. Левикін В.М., Костенко О.П., Хміль-Чуприна В.В. Розробка моделей просторово-траєкторного підходу до до моделювання процесу проектування маркетингових інформаційних систем // Математичні машини і системи. 2012. №2. С.126-135.
84. Левикін В.М., Костенко О.П., Зінченко Є.Г., Оліфіренко О.Л. Розробка моделей функціональної структури та модульної архітектури маркетингової інформаційної системи // Проблеми інформаційних технологій. 2011. № 2. С. 124-131. Режим доступу: http://nbuv.gov.ua/UJRN/Pit_2011_2_19.
85. Литвинов Д., Крикунов А. Социальные сети как поле арены информационного противоборства, Дипломатика: спецвыпуск. – С. 139–145.
86. Лызь Н., Веселов, Г., Лызь А., Информационно-психологическая безопасность в системах безопасности человека и информационной безопасности государства, Известия Южного Федерального университета . – 2014. – № 8. – С. 58–66.
87. Макаров В. Концептуальные основы научного обеспечения изучения глобального информационного пространства / В. Макаров, В. Гусев // Российский гуманитарный журнал. – 2014. – № 4. – С. 282–288.
88. Макаров В.Е. Политические и социальные аспекты информационной безопасности – Таганрог, 2015. – 349 с.
89. Марковець О.В., Пелещишин А.М., Хміль І.О., Реалізація системи опрацювання звернень громадян до органів влади у гетерогенних веб-середовищах, Наукові праці Донецького національного технічного університету Серія: “Інформатика, кібернетика та обчислювальна техніка”.- Красноармійськ, 2015 №1 (20), С.169-175.
90. Мастикаш О., Федушко С., Автоматизація збору персональних даних з соціальних мережах, Інформаційне суспільство: тенденції регіонального розвитку : матеріали міжнародної науково-практичної

конференції ISRDT-2016,. – Львів : Видавництво «Редакція «УП», 2016. – С. 46–47.

91. Молодецька К.В., Синтез синергетичного управління попитом агентів на контент у соціальних інтернет-сервісах, Інформатика та математичні методи в моделюванні, т.5, No4, с.330–338, 2015.
92. Молодецька К.В., Соціальні інтернет-сервіси як суб'єкт інформаційної безпеки держави, Information technology and security, vol.4, No1(6), с.13–20, 2016.
93. Молодецька К.В., Спосіб підтримання заданого рівня попиту акторів соціальних інтернет-сервісів на контент, Радіоелектроніка, інформатика, управління, No4(35), с.113–117, 2015.
94. Молодецька К.В., Технологія виявлення організаційних ознак інформаційних операцій у соціальних інтернет-сервісах, Проблеми інформаційних технологій, No20, с.84–93, 2016.
95. Молодецька К.В.,Методика вибору атрактора для управління динамікою процесів взаємодії акторів у соціальних інтернет-сервісах, Інформаційна безпека, No3(15),4(16),с.146–151, 2014.1
96. Молодецька-Гринчук К.В., Аналіз впливу загроз інформаційній безпеці держави у соціальних-інтернет сервісах на сфери суспільної діяльності, Управління розвитком складних систем, No30, с.121–127, 2017.
97. Молодецька-Гринчук К.В., Метод виявлення ознак інформаційних впливів у соціальних інтернет-сервісах за змістовними ознаками, Радіоелектроніка, інформатика, управління, No2(41), с.117–126, 2017.
98. Молодецька-Гринчук К.В., Метод оцінювання ознак загроз інформаційній безпеці держави у соціальних інтернет-сервісах, Автоматизація технологічних і бізнес-процесів, vol.9, is.2, с.36–42, 2017.

99. Молодецька-Гринчук К.В., Метод побудови профілів інформаційної безпеки акторів соціальних інтернет-сервісів, Інформаційна безпека, No1(25), 2(26), с.104–110, 2017.
100. Молодецька-Гринчук К.В., Модель системи підтримки прийняття рішень для виявлення ознак загроз інформаційній безпеці держави у соціальних інтернет-сервісах та оцінювання їх рівня, Безпека інформації, т.23, No2, с.136–144, 2017.
101. Молодецька-Гринчук К.В., Прототип програмного комплексу виявлення ознак загроз інформаційній безпеці держави у соціальних інтернет-сервісах та оцінювання їх рівня, Системи обробки інформації, No5(151), с.122–129, 2017.
102. Панарин И. Н. Информационная война и геополитика,– Москва: Поколение, 2006. – 560 с.
103. Панарин И., Панарина Л., Информационная война и мир, – Москва: Олма-Пресс, 2003. – 384 с.
104. Пелещишин А. М. Гумінський Р. В., Тимовчак-Максимець О. Ю. Пошук сторінок дискусій в соціальних мережах глобальними пошуковими системами, "Безпека інформації" наук.-практ. журнал. – Київ, 2013 – № 3 (19). – С. 181 – 187.
105. Пелещишин А. М., Вус В. А. Особливі категорії користувачів соціальних середовищ Інтернету, що впливають на безпеку інформаційного простору держави // Освіта і наука у сфері національної безпеки: проблеми та пріоритети розвитку : зб. наук. пр. за матеріалами міжнар. наук.-практ. конф., Острог, 1 груд. 2017 р. Острог : Вид-во Нац. ун-ту «Остроз. акад.», 2017. С. 27–29.
106. Пелещишин А. М., Вус В. А. Показники віртуальної спільноти, що впливають на безпеку національного інформаційного простору // Стан та перспективи реформування сектору безпеки і оборони України :

матеріали міжнар. наук.-практ. конф., Київ, 24 листоп. 2017 р. Київ, 2017. Т. 1. С. 320–322.

107. Пелещишин А. М., Вус В. А. Фактори соціальних середовищ інтернету в системі національної безпеки. Вісник інженерної академії України. 2018. № 2. С. 78–82.
108. Пелещишин А. М., Вус В. А., Марковець О. В. Побудова формальної моделі віртуальних спільнот як середовища соціокомунікативного протиборства. Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Технічні науки. 2018. Т. 29 (68), № 4, ч. 1. С. 201–207.
109. Пелещишин А. М., Вус В. А., Тимовчак-Максимець О. Ю. Спеціальна безпекова модель користувача соціальних середовищ Інтернету. Безпека інформації. Ukrainian Scientific Journal of Information Security. 2018. Т. 24, № 1. С. 62–68
110. Пелещишин А. М., Тимовчак-Максимець О. Ю., Аналіз комунікативної взаємодії учасників спільнот Веб-форумів, Вост.-Европ. журн. передовых технологий. – 2010. – № 6/8. – С. 44-49..
111. Пелещишин А., Тимовчак-Максимець О., Вус В. Характеристики формальної моделі віртуальних спільнот як середовища поширення інформаційної агресії // Безпекові виклики у геополітиці XXI століття : матеріали міжнар. наук.-практ. конф., Львів, 23–24 листоп. 2017 р. Львів, 2017. С. 149.
112. Пелещишин А.М. Сєров Ю. О., Березко О. Л., Пелещишин О. П., Тимовчак-Максимець О. Ю. Процеси управління інтерактивними соціальними комунікаціями в умовах розвитку інформаційного суспільства : монографія; МОНМС України, Нац. ун-т "Львів. політехніка". – Л., 2012. – 365 с.
113. Пелещишин А. М., Сєров Ю.О., Слобода К.О., Виявлення та усунення конфліктів між учасниками спільнот середовища Веб 2.0 на прикладі

Веб-форумів, Східно-Європейський журнал передових технологій. – Харків, 2009. – №6/3 (42) / 2009 – С.55–59.

114. Почепцов Г., Сегодня не информационная, а пропагандистская война [Електронний ресурс]. – Режим доступа: http://hvylya.net/analytics/society/georgiy-pocheptsov-segodnya-ne-informatsionnaya-a-propagandistskaya-voyna.html.
115. Сєров Ю., Відстеження появи небезпечного контенту онлайн спільнот як ключовий аспект інформаційно-психологічної безпеки онлайн-користувачів. Безпека інформації. 2017. Т.23, № 2. С. 113–121.
116. Сєров Ю., Методи та засоби побудови ефективних віртуальних спільнот на основі Веб-форумів: автореф. дис. ... канд. техн. наук : 01.05.03; Нац. ун-т "Львів. політехніка". — Л., 2010. — 20 с. — укр.
117. Сєров Ю.О., Кравець Р.Б., Пелещишин А. М., Методи аналізу ефективності Веб-форумів, Інформаційні системи та мережі : Вісник Національного університету «Львівська політехніка». – 2009. – № 653. – С.197–206.
118. Сєров Ю. О. Моделювання поведінки та класифікація учасників Веб-спільнот на основі нечітких множин, Інформаційні системи та мережі : Вісник Національного університету «Львівська політехніка». – 2008. – № 610. – С.218–228.
119. Сєров Ю. О., Кравець Р. Б. Використання нечітких множин для моделювання активності учасників Веб-спільнот, Автоматизированные системы управления и приборы автоматики: Всеукраинский межведомственный научно-технический сборник. – Харків, 2007. – № 141. – С.113–118.
120. Тарасов Д. О. Формальні моделі систем захисту інформації реляційних баз даних, Вісник Національного університету "Львівська політехніка". – 2003. – № 489 : Інформаційні системи та мережі. – С. 296-306.

121. Тимовчак-Максимець О. Ю. Комп'ютерно-лінгвістичні методи та засоби виявлення споживацького досвіду на веб-форумах : автореф. дис. канд. техн. наук : 10.02.21; Нац. ун-т "Львів. політехніка". – Л., 2013. – 20 с.
122. Тимовчак-Максимець О. Ю. Методи використання розширених можливостей глобальних пошукових систем в задачі пошуку споживацького досвіду в онлайн середовищах, Вісн. Нац. ун-ту "Львів. політехніка". – 2011. – № 715. – С. 333-342.
123. Тимовчак-Максимець О. Ю. Моделювання оцінних суджень у дописах учасників веб-форумів, Вісн. Нац. ун-ту "Львів. політехніка". – 2010. – № 673. – С. 374-383.
124. Тимовчак-Максимець О. Ю. Пелещишин А. М., Місце та роль споживацького досвіду в інформаційному середовищі, Вост.-Европ. журн. передовых технологий. – 2012. – № 2/11. – С. 39-45.
125. Томашевський В.М., Яцишин А.Ю. Математична модель задачі проектування гібридних сховищ даних з врахуванням структур джерел даних // НТУУ «КПІ». Вісник НТУУ «КПІ». Київ: Век+. 2011. С. 53.
126. Трач О. Р., Вус В. А. Визначення параметрів показників організації життєвого циклу віртуальних спільнот. Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Технічні науки. 2019. Т. 30 (69), № 1, ч. 1. С. 143–148.
127. Федушко С.С., Білущак Г. І. Формування системи лінгво-комунікативних індикаторів соціально-демографічних характеристик web-учасників // Збірник наукових праць "Управління розвитком складних систем" Київського національного університету будівництва і архітектури. 2014. Випуск 18. с. 112-122.
128. Форкун Ю.В. Методика оцінки діяльності розробників інформаційно-довідкового забезпечення суспільних комунікаційних систем //

Технологічний аудит та резерви виробництва. 2012. Т. 4, №6/4. с. 45-46

129. Форкун, Ю. В. Пелещишин А. М. Сучасні підходи технології розроблення та формування інформаційно-довідкового забезпечення суспільних комунікаційних систем, СхідноЄвропейський журнал передових технологій, №2/2(56)2012 – С. 3-12.
130. Халилов Д. Маркетинг в социальных сетях, Москва: Манн, Иванов и Фербер. 2013. С. 240.
131. Ших К. Эра Facebook. Как использовать возможности социальных сетей для развития вашего бизнеса [Текст] // Москва: Манн, Иванов и Фербер. 2010. С.304.

Додаток А. Акти використання результатів дисертаційного дослідження

«ЗАТВЕРДЖУЮ»
Голова ГО «Варта 1»

_____ Зінкевич І. В.

«___» червня 2019р.

Акт
про впровадження результатів наукових досліджень
Вуса Володимира Антоновича

Комісія у складі учасників ГО «Варта 1» Зінкевича Ігоря Володимировича, Романчака Андрія Олександровича та Зінкевич Ольги Володимирівни склала цей акт про розгляд результатів наукових досліджень Вуса Володимира Антоновича на тему «Математичне та програмне забезпечення протидії інформаційній пропаганді в соціальних середовищах Інтернету», а саме:

- аналіз сучасних підходів до інформаційного протиборства та протидії пропаганді;
- побудова формальних моделей соціальних середовищ Інтернету з врахуванням безпекового фактору;
- методи та алгоритми ефективної протидії інформаційній пропаганді;
- побудова комплексної системи управління заходами з протидії пропаганді в соціальних середовищах Інтернету.

Впровадження вказаних результатів дисертаційної роботи Вуса Володимира Антоновича дозволило підвищити ефективність процесів по виявленню бот-мереж з числа активних дописувачів віртуальної спільноти громадської організації та протидії загрозам інформаційній безпеці регіону, а саме:

- підвищення ефективності управління заходами з протидії пропаганді с соціальних середовищах Інтернету;
- формування обгрунтованих рекомендацій щодо прийняття рішення по протидії інформаційним загрозам віртуальній спільноті громадської організації та стратегій нівелювання інформаційних впливів пропаганди в соціальних мережах.

_____ Зінкевич І. В.
_____ Романчак А. О.
_____ Зінкевич О. В.

"ЗАТВЕРДЖУЮ"
Проректор з наукової роботи
Національного університету
"Львівська політехніка"
_____ проф. Н. І. Чухрай
"___" _____ 2019 р.

А К Т

про використання результатів дисертаційної роботи "Математичне та програмне забезпечення протидії інформаційній пропаганді в соціальних середовищах Інтернету" аспіранта кафедри соціальних комунікацій та інформаційної діяльності Вуса Володимира Антоновича, представленої на здобуття наукового ступеня кандидата технічних наук, при виконанні науково-дослідних робіт Національного університету "Львівська політехніка"

Ми, що нижче підписались, начальник НДЧ, к.т.н., доц. Жук Л.В. та члени комісії: завідувач відділу науково-організаційного супроводу наукових досліджень, к.т.н. Лазько Г.В.; заступник начальника планово-фінансового відділу Чулой Т.М. та завідувач кафедри соціальних комунікацій та інформаційної діяльності, д.т.н., професор Пелещишин А.М. цим актом підтверджуємо, що результати дисертаційної роботи аспіранта кафедри соціальних комунікацій та інформаційної діяльності Вуса В.А. використано під час виконання науково-дослідної роботи кафедри соціальних комунікацій та інформаційної діяльності Національного університету "Львівська політехніка": "Соціальні комунікації в глобальному інформаційному просторі" (№ державної реєстрації 0115U000460).

Вус В.А. провів системний аналіз розвитку та функціонування соціальних середовищ Інтернету як середовища інформаційного протиборства та пропаганди; здійснив побудову формальної моделі користувачів соціальних середовищ Інтернету, яка орієнтована на опис та вирішення завдань захисту інформаційного простору і охоплює загальну формалізацію характеристик мережевого, інформаційного, соціокомунікаційного змісту; розробив методи загального планування заходів із захисту інформаційного простору держави та виконання окремих оперативних заходів із протидії інформаційній пропаганді у соціальних середовищах Інтернету.

Начальник НДЧ,
к.т.н., доцент — Л.В. Жук

Члени комісії:
Зав. відділу НОСНД,
к.т.н. — Г.В. Лазько

Заст. начальника ПФВ — Т.М. Чулой

Зав. кафедри СКІД,
д.т.н., професор — А.М. Пелещишин

«ЗАТВЕРДЖУЮ»
ТВО начальника Управління СБУ
у Львівській області
полковник Чигрик В. І.

«12» червня 2019р.

Акт
про впровадження результатів дисертаційних досліджень
Вуса Володимира Антоновича

Комісія у складі:
голова комісії: Івануса Олександр Володимирович
члени комісії: Чайка Тарас Іванович
Овчаренко Антон Валерійович
Касьяненко Станіслав Ігорович
секретар комісії: Колупаєва Антоніна Альбертівна

склала цей акт про розгляд результатів дисертаційних досліджень Вуса В. А. на тему «Математичне та програмне забезпечення протидії інформаційній пропаганді в соціальних середовищах Інтернету», а саме:

- формалізація користувачів соціальних середовищ Інтернету з точки зору безпеки інформаційного простору держави;
- побудова формальної моделі віртуальних спільнот як середовища соціокомунікативного протиборства;
- методи та алгоритми ефективної протидії інформаційній пропаганді;
- планування заходів з захисту інформаційного простору держави
- методи та алгоритми виконання окремих оперативних завдань з захисту інформаційного простору держави;
- організація ресурсної підтримки заходів з підтримки та нейтралізації суб'єктів інформаційної діяльності;
- побудова комплексної системи управління заходами з протидії пропаганді в соціальних середовищах Інтернету.

Впровадження указаних результатів дисертаційної роботи Вуса В. А. дозволило підвищити ефективність процесів по виявленню та протидії загрозам інформаційній безпеці України, а саме:

- підвищення ефективності пошуку контенту, який може впливати на інформаційну безпеку держави, а також каналів поширення інформації в загальнодоступних та соціально-орієнтованих електронних ресурсах;

- формування обгрунтованих рекомендацій щодо прийняття рішення по протидії інформаційним загрозам та стратегій інформаційного впливу на віртуальні спільноти в соціальних мережах.

Голова комісії: _____ Івануса О. В.

Члени комісії: _____ Чайка Т. І.

_____ Овчаренко А. В.

_____ Касьяненко С. І.

Секретар комісії: _____ Колупаєва А. А.

р. №62/30-1489к

Додаток Б. Список публікацій здобувача за темою дисертації та відомості про апробацію результатів дисертації

1. Добровольська В. В., Пелещишин А. М., Вус В. А. Фактор соціальних мереж у завданнях захисту суспільного інформаційного образу закладів культури. Вісник Національної академії керівних кадрів культури і мистецтв. 2018. № 4. С. 132–137. (Особистий внесок здобувача: запропоновано концепцію переходу до суспільноактивної діяльності в соціальних мережах)
2. Vus V., Albota S., Dobrovolska V. The analysis of online communities as platforms for informational influences. Journal of Scientific and Engineering Research. 2019. Vol. 6, is. 2. P. 72–78. (Особистий внесок здобувача: описано види спілкування в онлайн-спільнотах та їхні характеристики)
3. Пелещишин А. М., Вус В. А., Тимовчак-Максимець О. Ю. Спеціальна безпекова модель користувача соціальних середовищ Інтернету. Безпека інформації. Ukrainian Scientific Journal of Information Security. 2018. 24 (1). С. 62–68. (Особистий внесок здобувача: опис формальної моделі користувача соціальних середовищ Інтернету)
4. Пелещишин А. М., Вус В. А., Марковець О. В. Побудова формальної моделі віртуальних спільнот як середовища соціокомунікативного протиборства. Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Технічні науки. 2018. Т. 29 (68), № 4, ч. 1. С. 201–207. (Особистий внесок здобувача: визначення правил формування контенту у соціальних середовищ Інтернету, визначення характеристик віртуальних спільнот)
5. Пелещишин А. М., Вус В. А. Фактори соціальних середовищ інтернету в системі національної безпеки. Вісник інженерної академії України. 2018. № 2. С. 78–82. (Особистий внесок здобувача: визначено фактори соціальних середовищ Інтернету як середовища, у яких здійснюється як корисна так і шкідлива інформаційна діяльність та типи соціальних середовищ з точки зору системної організації процесу комунікації.)
6. Трач О. Р., Вус В. А. Визначення параметрів показників організації життєвого циклу віртуальних спільнот. Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Технічні науки. 2019. Т. 30 (69), № 1, ч. 1. С. 143–148. (Особистий внесок здобувача: розподіл ролей користувачів соціальних середовищ Інтернету)
7. Вус В. А., Пелещишин А. М. Зведені показники віртуальних спільнот та пріоритезація спільнот з точки зору державної безпеки. Стандартизація, сертифікація, якість. 2019. № 2 (114). С. 73–80. (Особистий внесок здобувача: визначення зведених показників віртуальних спільнот, орієнтованих на завдання захисту інформаційного простору держави)

8. Вус В. Соціальні мережі як інструмент інформаційного протиборства // Інформація, комунікація, суспільство (ICS-2015) : матеріали 4-ої Міжнар. наук. конф., 20–23 трав. 2015 р., Львів, Славське. Львів : Вид-во Львів. політехніки, 2015. С. 28–29.

9. Вус В. А., Пелещишин А. М. Аналіз проблеми створення спеціального програмного забезпечення для протидії пропаганді в соціальних мережах // Інформація, , суспільство (ICS-2016) : матеріали 5 Міжнар. наук. конф., 19–21 трав. 2016 р. Львів : Вид-во Львів. політехніки, 2016. С. 38–39. (Особистий внесок здобувача: визначено основні завдання для програмного забезпечення протидії пропаганді в соціальних мережах)

10. Trach O., Vus V., Tymovchak-Maksymets O. Typical algorithm of stage completion when creating a virtual community of a HEI // Сучасні проблеми радіоелектроніки, телекомунікацій, комп'ютерної інженерії (TCSET'2016) : матеріали XIII Міжнар. конф., 23–26 лют. 2016 р. Львів : Вид-во Львів. політехніки, 2016. С. 849–851. (Особистий внесок здобувача: визначено етапи створення віртуальної спільноти).

11. Пелещишин А. М., Вус В. А. Показники віртуальної спільноти, що впливають на безпеку національного інформаційного простору // Стан та перспективи реформування сектору безпеки і оборони України : матеріали Міжнар. наук.-практ. конф., 24 листоп. 2017 р. Київ, 2017. Т. 1. С. 320–322. (Особистий внесок здобувача: характеристики показників віртуальної спільноти).

12. Пелещишин А., Тимовчак-Максимець О., Вус В. Характеристики формальної моделі віртуальних спільнот як середовища поширення інформаційної агресії // Безпекові виклики у геополітиці XXI століття : матеріали Міжнар. наук.-практ. конф., 23–24 листоп. 2017 р. Львів, 2017. С. 149. (Особистий внесок здобувача: описано показники рівня державного впливу у формальної моделі віртуальних спільнот).

13. Пелещишин А. М., Вус В. А. Особливі категорії користувачів соціальних середовищ Інтернету, що впливають на безпеку інформаційного простору держави // Освіта і наука у сфері національної безпеки: проблеми та пріоритети розвитку : зб. наук. пр. за матеріалами Міжнар. наук.-практ. конф., Острог, 1 груд. 2017 р. Острог : Вид-во Нац. ун-ту «Остроз. акад.», 2017. С. 27–29. (Особистий внесок здобувача: визначення категорій користувчів у соціальних середовищах Інтернету).

14. Вус В. Аналіз основних класів соціальних середовищ // Інформація, комунікація, суспільство (ICS-2018) : матеріали 7 Міжнар. наук. конф., 17–19 трав. 2018 р., Чинадієво. Львів : Вид-во Львів. політехніки, 2018. С. 39–40.

15. Peleshchyshyn A., Markovets O., Vus V., Albota S. Identifying specific roles of users of social networks and their influence methods // Комп'ютерні науки та інформаційні технології (CSIT-2018) : матеріали XIII Міжнар. наук.-техн. конф., Львів, 11–14 верес. 2018 р. Львів, 2018. С. 39–42. (Особистий внесок здобувача: формальний опис активності користувача

соціальних середовищах Інтернету).

16. Peleshchyshyn A., Vus V., Albota S., Markovets O. A formal approach to modeling the characteristics of users of social networks regarding information security issues // Advances in Intelligent Systems and Computing. 2019. Vol. 902 : Advances in artificial systems for medicine and education II. The second international conference of artificial intelligence, medical engineering, education (AIMEE2018), 6–8 Oct. 2018. Springer, 2019. P. 485–494. (Особистий внесок здобувача: описано структуру бази даних користувачів соціальних середовищах Інтернету).

17. Вус В. Аналіз форм публічної інформаційної діяльності в соціальних середовищах Інтернету // Інформація, комунікація, суспільство (ICS-2019) : матеріали 8 Міжнар. наук. конф., 16–18 травня 2019 р., Чинадієво. Львів: Вид-во Львів. політехніки, 2019. С. 41–43.

Апробація результатів дисертації. Основні результати дисертаційного дослідження неодноразово висвітлювалися на міжнародних та всеукраїнських наукових конференціях, зокрема: на XIII Міжнародній конференції Сучасні проблеми радіоелектроніки, телекомунікацій, комп'ютерної інженерії (TCSET'2016) (Львів, Славське,2016); XIII Міжнародній науково-технічній конференції «Комп'ютерні науки та інформаційні технології» CSIT'2018 (Львів, 2018); 4, 5, 7, 8 Міжнародних наукових конференціях «Інформація, комунікація, суспільство» (Львів, 2015, 2016, 2018, 2019); Міжнародній науково-практичній конференції «Стан та перспективи реформування сектору безпеки і оборони України», (Київ, 2017); Міжнародній науково-практичній конференції «Безпекові виклики у геополітиці XXI століття» (Львів, 2017), Міжнародній науково-практичній конференції «Освіта і наука у сфері національної безпеки: проблеми та пріоритети розвитку» (Острог, 2017). Про результати дисертаційних досліджень автор регулярно доповідав на наукових семінарах кафедри соціальних комунікацій та інформаційної діяльності Національного університету «Львівська політехніка» (2015, 2017-2019).