Міністерство освіти і науки України

Національний університет "Львівська політехніка"

ВУС ВОЛОДИМИР АНТОНОВИЧ

УДК 004.652.4004.738.5:001.102-049.5:351.862.4(043)

МАТЕМАТИЧНЕ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ ІНФОРМАЦІЙНІЙ ПРОПАГАНДІ В СОЦІАЛЬНИХ СЕРЕДОВИЩАХ ІНТЕРНЕТУ

Спеціальність 01.05.03 – Математичне та програмне забезпечення обчислювальних машин і систем

АВТОРЕФЕРАТ

дисертації на здобуття наукового ступеня кандидата технічних наук

Львів – 2019

Дисертацією є рукопис.

Робота виконана у Національному університеті "Львівська політехніка" Міністерства освіти і науки України.

Науковий керівник — доктор технічних наук, професор
Пелещишин Андрій Миколайович,
Національний університет «Львівська політехніка»,
завідувач кафедри соціальних комунікацій та інформаційної діяльності

Офіційні опоненти — доктор технічних наук, професор
Бідюк Петро Іванович,
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»,
ННК «Інститут прикладного системного аналізу»,
професор кафедри математичних методів системного аналізу

доктор технічних наук, доцент
Молодецька Катерина Валеріївна,
Житомирський національний агроекологічний університет,
керівник навчально-наукового центру інформаційних технологій

Захист відбудеться 12 грудня 2019 р. о 16^{00} годині на засіданні спеціалізованої вченої ради Д 35.052.05 у Національному університеті "Львівська політехніка" (79013, м. Львів, вул. С. Бандери, 12, ауд. 226 головного корпусу).

З дисертацією можна ознайомитися у науково-технічній бібліотеці Національного університету "Львівська політехніка" (79013, м. Львів, вул. Професорська, 1).

Автореферат розісланий "11" 11 2019 р.

Учений секретар
спеціалізованої вченої ради,
доктор технічних наук, професор Р. А. Бунь

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

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-пропагандистської діяльності (аж до нових форм інформаційних війн), а також до захисту держави та громадян від таких шкідливих впливів.

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.

Окремі дослідження у сфері моделювання та забезпечення соціально-інформаційних процесів у Інтернеті здійснювались у напрямах: моделювання соціальних мереж та спільнот, розроблення методів проєктування та управління (К.В. Молодецька, Р.В. Грищук, Ю.О. Сєров), моделювання процесів накопичення даних та знань у глобальних мережах (В.М. Левикін, О.П. Костенко, О.В. Петріченко), інформаційний пошук у соціальних середовищах (Д.В. Ланде, В.М. Фурашев, M. Russell, M. Klassen), виявлення та опрацювання суб'єктивно поданої інформації (E. Ferrara, R. Karlsen, T. Valente, О.Ю. Тимовчак-Максимець), ідентифікація та класифікація користувачів соціальних мереж та спільнот, визначення окремих ролей та класів (О.Л. Березко, О.П. Пелещишин, С.С. Федушко), комерціалізація соцмереж та спільнот, піар та реклама (Д. Халилов, К. Ших), інтеграція суспільних та державних інституцій, соціальних середовищ Інтернету, зокрема в електронне урядування та демократію, електронну освіту (M. Bottery, Н.С. Бушуєва, М.З. Згуровський, В. Макаров, О.В. Марковець), ідентифікація спаму, оцінювання значущості інформації (Ю. В. Форкун). Проте їхні дослідження не охоплюють фактора захисту інформаційного простору держави та прикладного застосування інформаційного протиборства в соціальних середовищах інтернету (ССІ), що зумовлює актуальність створення програмного забезпечення протидії інформаційній пропаганді в ССІ.

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 і передбачають опис суспільної значущості та характеристик для державної безпеки;
- побудова методів та алгоритмів планування заходів із захисту інформаційного простору держави, виявлення та протидії окремим деструктивним групам користувачів ССІ;
- 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;
- апробація запропонованих методів і засобів протидії інформаційній пропаганді у ССІ з використанням їх у окремих, критичних для національної безпеки, спільнотах.

Об'єктом дослідження є процеси інформаційного впливу у ССІ.

Предметом дослідження є моделі та методи математичного і програмного забезпечення протидії інформаційній пропаганді в ССІ.

Методи дослідження. Під час вирішення завдань моделювання користувачів ССІ 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 полягає у науковому обґрунтуванні та вирішенні наукового завдання розроблення нових методів та засобів протидії інформаційній пропаганді в СС І. Отримано такі наукові результати:

- набули подальшого розвитку формальні моделі користувачів СС І 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 СС І;
- 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 СС І, 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 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 СС І;
- 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 дисертаційних досліджень 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: [1] – запропоновано концепцію переходу до суспільно активної діяльності в соцмережах; [2] – описано види спілкування в онлайн-спільнотах; [3] – описано формальну модель користувача ССІ; [4] – визначено правила формування контенту в ССІ, характеристики веб-спільнот; [5] – виділено фактори ССІ як середовищ з корисною та шкідливою інформаційною діяльністю та типи соціальних середовищ з погляду системної організації процесу комунікації; [6] – проаналізовано розподіл ролей користувачів ССІ; [7] – визначено зведені показники веб-спільнот, орієнтованих на завдання захисту інформаційного простору держави; [9] – встановлено основні завдання для програмного забезпечення протидії пропаганді в соцмережах; [10] – виокремлено етапи створення веб-спільноти; [11] – описано характеристику показників веб-спільноти; [12] – описано показники рівня державного впливу в формальній моделі веб-спільнот; [13] – визначено категорії користувачів у ССІ; [15] – виконано формальний опис активності користувача ССІ; [16] – описано структуру бази даних користувачів ССІ.

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 та 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.

Структура та обсяг роботи. Дисертаційна робота складається зі вступу, чотирьох розділів, висновків, списку літератури зі 131 найменування та двох

додатків. Загальний обсяг дисертації становить 183 сторінки, з них 132 сторінки основного тексту, який містить 18 рисунків та 10 таблиць.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі обґрунтовано актуальність теми, сформульовано мету та основні завдання досліджень, показано зв'язок із науковими програмами, планами, темами, сформульовано наукову новизну. Висвітлено практичну цінність, реалізацію і впровадження результатів роботи. Наведено дані про особистий внесок здобувача, апробацію роботи та публікації.

У першому розділі дисертації проаналізовано особливості функціонування соціальних середовищ Інтернету як джерела позитивних та негативних впливів у системі національної безпеки. Виділено основні класи соціальних середовищ: веб-форумів та standalone-блогів; електронних ЗМІ та колективних блогів; самомодерованих енциклопедій; сервісів соціальних мереж. Проаналізовано особливості кожної з платформ ССІ та правила організації контенту, виявлено спільні риси цих соціальних середовищ, зокрема – організацію за схемою «стаття + обговорення» тощо. Проаналізовано форми публічної інформаційної діяльності у виділених класах соціальних середовищ, здійснено їхню класифікацію за ознаками «колективність» та «контрольованість» результатів діяльності. Технології інформаційної та маркетингової діяльності в ССІ, які за змістом та характером суміжні із завданнями захисту інформаційного простору, є важливими орієнтирами для наукових досліджень у цій сфері. Проаналізовано окремі тенденції онлайн-маркетингу, зокрема: залучення лідерів думок для формування громадської думки; використання веб-спільнот як інструменту для PR, окремі питання взаємодії із користувачами соціальних середовищ.

У другому розділі дисертації розроблено низку формальних моделей суб'єктів інформаційної діяльності. На сьогодні існує ряд підходів до класифікації користувачів ССІ, проте пропоновані класифікації зосереджені на проблематиці організації ефективного функціонування віртуальних спільнот. Наведена в розділі модель користувача охоплює широкий спектр характеристик, об'єднаних у такі групи: ідентифікатор та персональні дані (*UI*); характеристики державної безпеки (*US*); активність (*UA*); читачі контенту (*UF*); постачальники контенту (*UH*); спільноти користувача (*UC*). Користувача описуємо кортежем:

$$User_i = \langle UI_i, US_i, UA_i, UF_i, UH_i, UC_i \rangle, \quad (1)$$

де елементами кортежу є відповідні складові моделі.

У зв'язку з тим, що одна особа може бути представлена декількома учасниками ССІ, ідентифікація користувача зведена до ідентифікації фізичної особи. Тому серед показників ідентифікації окремо виділено: показники фізичної ідентифікації (*UIR*) – для описання персональних даних; показники віртуальної ідентифікації (*UIV*) – для описання узагальнених характеристик поведінки в ССІ; мережевої (*UIS*) – щодо специфічних для мережі ідентифікаційних даних. Важливо, що набір показників мережевої ідентифікації для кожного користувача не є єдиним. Цей розділ характеристик є множиною кортежів з елементами

указаного типу. Тобто для однієї особи може бути визначено декілька записів з адресою профілю, ідентифікатором, псевдонімом тощо. Отже:

$$UI_i = \langle UIID_i, UIS_i, UIR_i, UIV_i \rangle, \quad (2)$$

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.

У багатьох завданнях аналізу соціальної структури Інтернету первинною є інформація щодо мережевої, а не фізичної ідентифікації, тому важливою є така множина:

$$UIS = \bigcup_{i=1}^{N^{(UI)}} \left\{ \langle UISN_{ij}, UISNId_{ij}, UISA_{ij}, UISName_{ij} \rangle \right\}_{j=1}^{N_i^{(UIS)}}, \quad (3)$$

де $N^{(UI)}$ – кількість фізичних користувачів, *UISN* - адреса ССІ, *UISNId* - ідентифікатор профілю користувача, *UISNA* - адреса профілю користувача, *UISName* - мережеве ім'я.

Множина *UIS* являє собою множину усіх мережевих ідентифікацій (умовно – множину віртуальних особистостей у ССІ). Під час формування бази даних користувачів у завданнях захисту інформаційного простору вкрай важливий облік його окремих спеціальних характеристик, пов'язаних із державною безпекою. Показники цієї групи складно визначати, з розвитком технологій штучного інтелекту в сфері опрацювання природномовних текстів на предмет оцінювання суджень та виявлення почуттів, їх можна буде опрацьовувати автоматизовано. Для зменшення затрат праці на ручне опрацювання показники цієї групи (*US*) пропонуємо визначати лише для користувачів певного рівня значущості або за наявності ролей.

На базовому рівні ознаки розділено з міркувань простішого автоматизованого визначення. Так *USSt* «Стабільність позиції» відстежують, аналізуючи зміни лексики протягом тривалого часу, *USIn* «Незалежність суджень» ідентифікується як відсутність кореляції між тональністю співрозмовників та тональністю автора в близькі моменти часу. Ознаку *USDl* «Готовність до діалогу» в автоматизованому режимі ідентифікувати найпростіше, аналізуючи лексику на предмет відсутності та наявності відповідних лінгвістичних маркерів (зокрема, лайків, увічливих звертань тощо).

Інтегрований показник гнучкості позиції користувача визначаємо так:

$$UserFlex(User_i) = USIn_i * USSt_i * USDl_i. \quad (4)$$

Цей показник відображає здатність користувача сприймати думку опонентів у дискусіях, змінювати свої погляди під час аргументованої дискусії.

Сьогодні конкретні форми активності користувача ССІ проявляються по-різному. Узагальнюючи їх на основі типових функцій соцмереж, визначимо такі форми активності з формування контенту: публікація нового контенту; публікація коментаря; ретрансляція контенту; оцінювання контенту; акція впливу – спеціальний вид дії, спрямований не на контент безпосередньо, а на регулювання дій інших користувачів. Наприклад, модерація контенту та користувачів, запрошення нових користувачів, ресурсне забезпечення. Указану

активність відображено в групі UA відповідних показників. На основі теоретико-множинного підходу в роботі формально описано кожен із видів контенту.

Кожен користувач ССІ характеризується не лише власним контентом, але і системою соціальних зв'язків з іншими користувачами. У роботі їх формалізовано в соціальний портрет користувача ССІ. Складовими соціального портрета є читачі (споживачі) контенту, постачальники контенту, спільноти з правом перегляду, спільноти з правом публікації, контрольовані ресурси. Визначено спеціальні ролі користувачів ССІ, важливі з погляду державної безпеки: лідери думок, модератори, транслятори, опоненти, тролі, боти. Уведено формальні порівняльні ознаки окремих показників із встановленим для кожної ролі пороговим значенням. Визначають ці константи, формуючи комплексне завдання із захисту інформаційного простору в певному тематичному напрямку з урахуванням актуальних характеристик середовищ. Основна функція лідерів думок – формування нового процесу з поширення певного суспільно значущого авторського контенту (*UAIC*), зокрема нових трактувань фактів, аналітичних оглядів та проголошення ідей. Визначено таку ознаку лідера думки:

$$\frac{Count\left(UAIC_i\right)}{Count\left(Content_i\right)} \geq C_C^{(OL)}, \tag{5}$$

де $Content_i = UAUC_i \cup UACom_i \cup UART \cup UAIA_i$ – весь змістовий контент користувача (без оцінок контенту); $C_C^{(OL)} \in [0;1]$ – константа, що визначає необхідну для лідера думок частку авторських матеріалів.

Для лідера думки повинна виконуватися ознака достатньої активності (середня частота розміщення контенту *UACF*):

$$UACF_i \geq C_F^{(OL)}. \tag{6}$$

Для інших ролей аналогічно встановлено основні характеристики та порівняльні ознаки, що дають змогу визначити ролі конкретних користувачів ССІ, важливих для інформаційного протиборства. Розроблено спеціальну модель віртуальних спільнот як середовища протиборства в інформаційному просторі. Визначено перелік характеристик, які об'єднано у такі групи: технічна (*CT*), аудиторна (*CA*), суспільної значущості (*CI*), змісту та комунікації (*CC*), державної безпеки (*CS*).

Формально віртуальна спільнота Cm_i у цьому разі описується кортежем:

$$Cm_i = \langle CT_i, CA_i, CI_i, CC_i, CS_i \rangle, \tag{7}$$

де елементами кортежу є наведені вище групи характеристик.

Технічні показники характеристики віртуальних спільнот відображають способи забезпечення її функціонування в мережевому середовищі: засоби хостингу, програмні засоби, мови розмітки, оформлення розміщених матеріалів, їх доступність зовні спільноти та для автоматизованих сервісів збирання даних. Показники аудиторії віртуальних спільнот характеризують популярність спільноти серед користувачів Інтернету та її обсяги в різних аспектах. Ці показники є важливим фактором для оцінювання важливості спільноти як середовища інформаційної взаємодії та протистояння агресії. У моделі запропоновано розмежовувати поняття «спостерігач» та «читач». До

спостерігачів належать ті користувачі Інтернету, які використовують примусове доставлення нового контенту або його анонсів (push-технології). Читачами вважатимемо користувачів Інтернету, які доступаються до контенту епізодично, без підписки, коли їх щось зацікавило, але не рідше ніж раз на місяць.

Показники суспільної значущості відображають вплив спільноти на зовнішнє середовище. Виділено такі показники цієї групи: кількість посилань на контент спільноти (*CILC*); кількість цитувань (*CICC*); конкурентний рейтинг (*CICR*); конкурентна частка аудиторії (*CICP*). Показник *CICR* «Конкурентний рейтинг», на відміну від частки аудиторії, описує лише умовну позицію серед конкурентів («головний», «другий» тощо). Показник доволі легко встановлює експерт. Основна цінність цього показника – можливість оцінити частку цільової аудиторії, яку охоплює спільнота, та її кількісні характеристики, якщо відсутні надто трудомісткі інші способи. Для цього використаємо гіпотезу про те, що аудиторія розподілена між рейтингованими спільнотами згідно із законом Зіпфа. У такому разі приблизна оцінка кількості читачів (*CAAR*):

$$CAAR_i = \frac{CAAR\left(\overline{Cm}\right)}{CICR_i}, \tag{8}$$

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

Характеристики змісту та комунікації описують характер спільноти, її спрямування та призначення і, отже, визначають вибір щодо неї завдань із захисту інформаційного простору держави.

Для вирішення завдань захисту інформаційного простору держави необхідно ввести в модель окремі вузькоспеціалізовані показники, а саме показники групи «Характеристики державної безпеки». Якщо наведені вище характеристики можна використовувати в ширшому спектрі завдань, пов’язаних із віртуальними спільнотами, то група характеристик спільнот вужче спеціалізована, орієнтована власне на завдання зі сфери соціокомунікаційної безпеки й охоплює дві підгрупи: показники рівня державного впливу; показники напряму інформаційної діяльності в сфері безпеки.

<u>У третьому розділі</u> сформовано спеціальні методи та алгоритми, покликані поліпшити якість та підвищити ефективність діяльності із захисту інформаційного простору держави. Формалізація показників віртуальних спільнот уможливлює побудову інтегрованих показників – основи для процедур прийняття рішень в окремих завданнях інформаційного захисту. Уведено низку інтегрованих показників, актуальних для завдань соціокомунікаційної безпеки. Враховуючи значну кількість показників та складність взаємозв'язків між ними, їх систематизовано у певні групи.

Показники впливовості доволі універсальні й застосовуються у широкому спектрі завдань з інформування населення, рекламно-маркетингової діяльності тощо. До цієї групи належить показник популярності спільноти як узагальнення базових показників групи «Популярність» за допомогою лінійної згортки

$$Popular\left(CM_i\right) = CAM_i * VC^{(P)}_{(CAM)} + CAAF_i * VC^{(P)}_{(CAAF)} + CAAR_i * VC^{(P)}_{(CAAR)}, \tag{9}$$

де *CAM* – кількість учасників, *CAAF* – кількість спостерігачів, *CAAR* – кількість читачів, $VC_{(CAM)}^{(P)}, VC_{(CAAF)}^{(P)}, VC_{(CAAR)}^{(P)}$ – вагові коефіцієнти відповідних базових показників.

Популярність спільноти – важливий показник, який характеризує обсяги аудиторії, що споживає інформацію, і застосовний у широкому спектрі завдань, пов'язаних із інформуванням населення, разом із маркетинговими, промоційними завданнями і завданнями інформаційного протиборства.

Рівень впливу інформації на споживача визначається авторитетністю джерела, що її поширює. Доцільно ввести до розгляду показник авторитетності спільноти. Базовою авторитетністю є рівень впливу спільноти на думку наявної аудиторії. Показник формують лінійною згорткою кількох показників спільнот:

$$AuthBase(CM_i) = CCInt_i * \left(\frac{CAAM_i}{CAM_i} * VC_{(CAAM)}^{(AB)} + \frac{CAOL_i}{CAM_i} * VC_{(CAOL)}^{(AB)} + CICP_i * VC_{(CICP)}^{(AB)} \right), \quad (10)$$

де *CCInt* – реальність інформаційної потреби, *CAAM* – кількість активних учасників, *CAOL* – кількість лідерів думки, $VC_{(CAAM)}^{(AB)}, VC_{(CAOL)}^{(AB)}, VC_{(CICP)}^{(AB)}$ – вагові коефіцієнти лінійної згортки, підібрані так, щоби $0 \le AuthBase(CM_i) \le 1$.

Показник абсолютної важливості віртуальної спільноти відображає у певних абсолютних одиницях важливість спільноти з погляду безпеки держави. Це дає змогу ранжувати спільноти однієї категорії за пріоритетом, для оптимізації використання наявних в органах безпеки ресурсів під час виконання завдань у межах однієї цільової аудиторії. За розмірністю цей показник відповідає показнику аудиторії сайта і формується з обчисленого показника популярності та базових показників суспільної значущості.

Показник важливості обчислюватимемо за такою формулою:

$$CmAI_i = \frac{1}{3} AuthBase(CM_i) * \left(Popular(CM_i) * VC_{(Pop)}^{(CAI)} + CILC_i * VC_{(CILC)}^{(CAI)} + CICC_i * VC_{(CICC)}^{(CAI)} \right), \quad (11)$$

де $VC_{(Pop)}^{(CAI)}, VC_{(CILC)}^{(CAI)}, VC_{(CICC)}^{(CAI)}$) – відповідні вагові коефіцієнти.

Показник відносної важливості віртуальної спільноти забезпечує порівняння між собою спільнот різних типів та тематик, даючи змогу сумістити їх під час вибору та пріоритезації для виконання різних комплексних завдань, які охоплюють різні цільові аудиторії. Обчислюватимемо її так:

$$CmRI_i = \frac{CmAI_i}{CmAI(\overline{Cm})}, \quad (12)$$

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

Показники комфортності спілкування також універсальні й описують трудомісткість і складність процесу спілкування, визначаючи можливість широкого залучення користувачів до виконання комунікативних завдань.

Показник комунікативного комфорту віртуальної спільноти вказує на якість спільноти з погляду стилю її спілкування, що проявляється у якості її контенту. Вплив спільноти з високою комфортністю спілкування на суспільну думку

потенційно вищий, у них значний потенціал росту, за необхідності їх можна збільшити без надмірних зусиль і залучення спеціальних фахівців.

Вплив спільнот із низькою комфортністю навіть за умови великих обсягів аудиторії не є стабільно високим, його можна нівелювати, не витрачаючи значних ресурсів. Цей показник обчислюватимемо так:

$$CmComf_i = \frac{1}{4}\left(CCAggr_i * VC_{(CCAggr)}^{(Comf)} + CCMod_i * VC_{(CCMod)}^{(Comf)} + CCPL_i * VC_{(CCPL)}^{(Comf)} + CCAdult_i * VC_{(CCAdult)}^{(Comf)}\right), \quad (13)$$

де *CCAgr* – рівень агресії, *CCMod* – нестрогість модерації, *CCPL* – рівень персоніфікації, *CCAdult* – наявність ненормативної лексики, $VC_{(CCAggr)}^{(CV)}, VC_{(CCMod)}^{(CV)}, VC_{(CCPL)}^{(CV)}, VC_{(CCAdult)}^{(CV)}$ – вагові коефіцієнти при відповідних показниках у діапазоні [0;1], причому $VC_{(CCAggr)}^{(Comf)} + VC_{(CCMod)}^{(Comf)} + VC_{(CCPL)}^{(Comf)} + VC_{(CCAdult)}^{(Comf)} = 1$.

Значення показника комунікативної цінності лежать у діапазоні [0;1].

Показник комунікативного прийняття описує складність та затрати праці на взаємодію зі спільнотою. Що нижчий показник, то складніше досягати в межах спільноти поставлених цілей. Цей показник визначаємо у такий спосіб:

$$CmA_i = \frac{1}{3} CmL_i (CCAgr_i * VC^{(CCAgr)} + CCMod_i * VC^{(CCMod)} + CCCtrl * VC^{(CCCtrl)}), \quad (14)$$

де *CCCtrl* – некерованість спільноти, *VC(xx)* – відповідні вагові коефіцієнти, які, як і для показника комунікативної цінності, лежать у діапазоні [0;1] і в сумі дають 1.

Показники близькості завданням державної безпеки є спеціальними і проблемними й визначають політику щодо спільноти.

Показник релевантності вказує на близькість спільноти до завдань захисту та безпеки інформаційного простору держави. Обчислюватимемо його так:

$$\begin{aligned} CmRel_i = {} & CmRel\_lang_i * CmRel\_Reg_i * CmRel\_Age_i * \\ & * CmRel\_Act_i * CmRel\_Int_i * CmRel\_Th_i * CSTD_i \end{aligned}, \quad (15)$$

де $CmRel\_lang_i$ та інші множники – атомарні релевантності за кожним з напрямів, визначає їх експерт у діапазоні [0;1].

Можливим варіантом визначення показника *CmRel_Thi* є обчислення частки релевантних термінів у описі тематики спільноти до загальної кількості ключових слів:

$$CmRel\_Th_i = \frac{Count\_rel(CCTh_i)}{Count(CCTh_i)}, \quad (16)$$

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

Якщо змінюються завдання із захисту інформаційного простору, змінюються і визначення окремих релевантностей. Переважно якийсь із показників є неважливим. У такому разі вважають, що відповідна йому релевантність дорівнює 1. Наприклад, якщо для конкретного завдання не має значення вікова характеристика спільноти, то $CmRel\_Age_i = 1$.

Показник лояльності веб-спільноти дає змогу формально описати узагальнене ставлення спільноти до системи державних цінностей та

класифікувати її як дружню щодо держави чи ворожу. Цей показники виводимо з базових, зокрема з показників груп «рівня державного впливу» та «напряму інформаційної діяльності в сфері безпеки». Можна скористатись таким виразом:

$$CmL_i = \frac{1}{7}(CSGP_i * VC^{(CSGP)} + CSGJ_i * VC^{(CSGJ)} + CCSG_i * VC^{(CSGR)} - \\ - CSFR_i * VC^{(CSFR)} + CSSR_i * VC^{(CSSR)} + CSGR_i * VC^{(CSGR)} + CSCV_i * VC^{(CSCV)}), \quad (17)$$

де *CSGP* – розміщення фізичних серверів, *CSGJ* – розміщення юр.особи, що адмініструє спільноту, *CSFR* – наявність сталих зв'язків з сайтами та спільнотами країн, що здійснюють агресію, *CSSR* – ставлення до держави загалом, *CSGR* – ставлення до державних інститутів, *CSCV* – рівень консолідації думки учасників щодо держави, *VC(xx)* – відповідні вагові коефіцієнти, що, як і для показника комунікативної цінності, лежать у діапазоні [0;1] і в сумі дають 1. За такого визначення значення показника лояльності міститься у діапазоні [-1;1] – від «абсолютно ворожа спільнота» до «повністю лояльна спільнота».

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

Шкідливою вважатимемо спільноту, для якої:

$$CmL_i \le C_{Enemy}^{(CmL)}, \quad (18)$$

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

Корисною вважатимемо спільноту, для якої:

$$CmL_i \ge C_{Friend}^{(CmL)}, \quad (19)$$

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

Указані зведені показники використовують у спектрі завдань з інформаційної взаємодії та протиборства в ССІ. Це завдання: пріоритезації спільнот; фільтрація спільнот за доцільністю; фільтрація спільнот за складністю; ідентифікація суб'єктів інформаційної діяльності; формування плану ресурсної підтримки. Наведено також розроблені методи й алгоритми планування заходів з протидії пропаганді, зокрема загальний розподілений інформаційно-технологічний алгоритм організації заходів у веб-спільнотах. Одним із ключових завдань раннього етапу діяльності із захисту інформаційного простору держави є формування каталогу значущих персоналій, які є в ССІ. Щоб вирішити його, сформовано алгоритм персоналізації суб'єктів інформаційної діяльності. Для деталізації одного з його етапів розроблено алгоритм опрацювання окремого користувача, який забезпечує збирання і систематизацію даних щодо користувача згідно із запропонованою формальною моделлю. Досліджено виконання окремих оперативних завдань, що постають під час реалізації такого плану. Запропоновано методи виявлення користувачів, які виконують шкідливі для держави ролі, з визначенням можливих способів ефективної протидії. Розроблено метод виявлення лідерів думки, впливових в інформаційному

просторі держави. Запропоновано застосовувати термін «лідери думок» щодо певного класу користувачів на основі поведінкових ознак. Поведінкове визначення лідера думок дає змогу вирішити взаємодоповнювальні завдання виявлення лідерів думок: потенційних, динамічних, популярних, на основі заданих порогових значень. Відповідний алгоритм наведено на рис. 1.

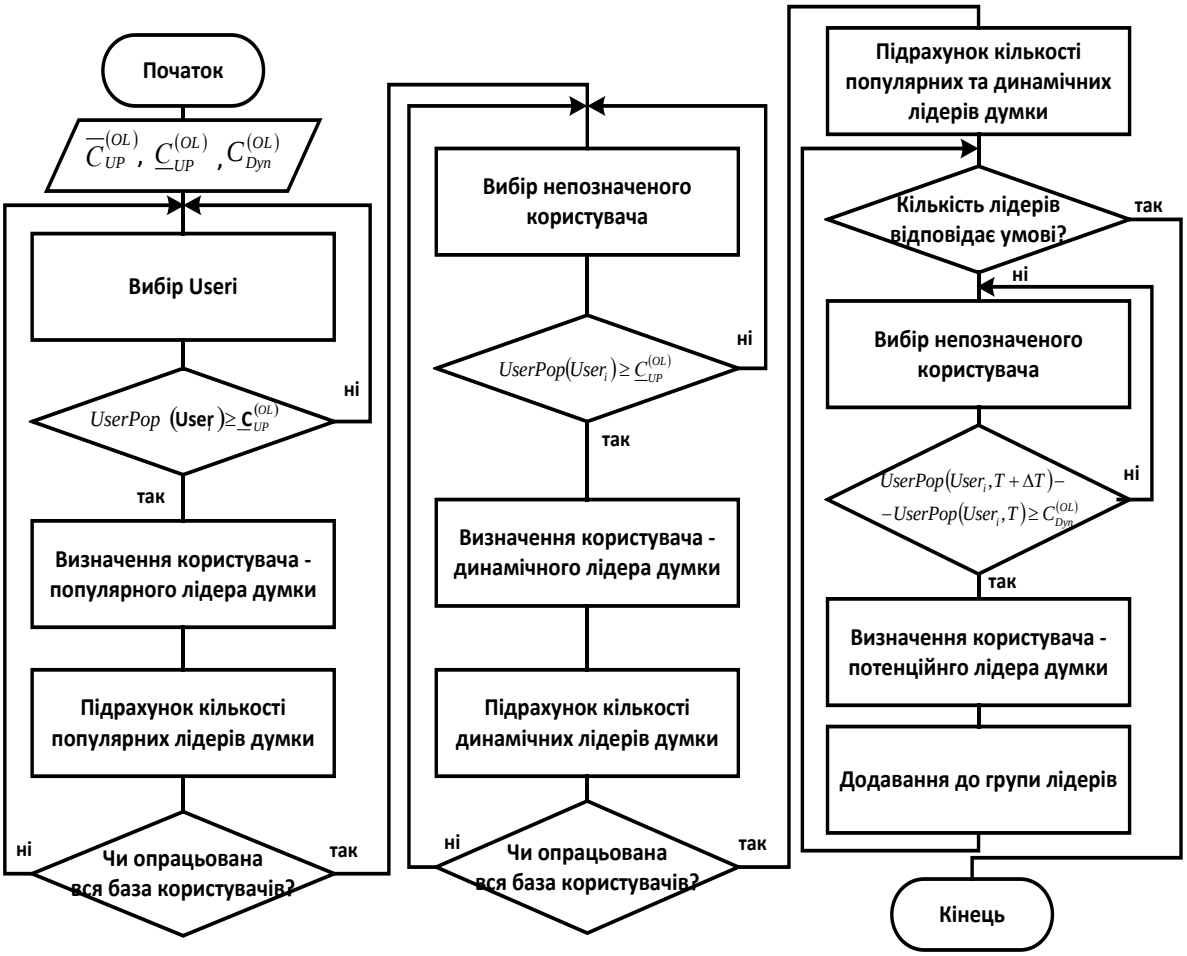

Рис. 1. Блок-схема алгоритму формування бази лідерів думок

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 урахуванням їхніх актуальних характеристик. Вважатимемо, що здійснюють шкідливі впливи ті лідери думок, для яких виконується умова:

$$USG_i \leq C_{Enemy}^{(USG)}, \tag{20}$$

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].

Основними комунікаційними інструментами протидії динамічним та потенційним лідерам є залучення кваліфікованих опонентів, пониження показників популярності спільнот. Відповідний алгоритм наведено на рис. 2.

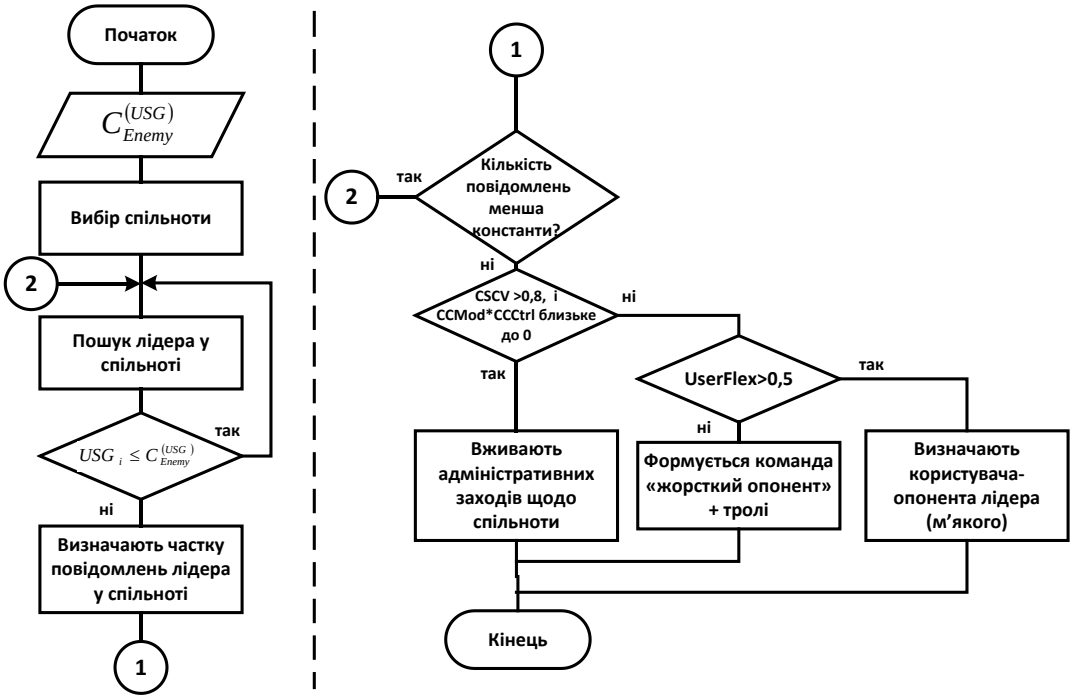

Рис. 2. Блок-схема алгоритму комунікаційної протидії потенційному лідеру думки

Нейтралізація впливу популярних лідерів думок є складнішим завданням, яке необхідно вирішувати у випадку реальної загрози національній безпеці. Запропоновано методи виявлення тролів та опонентів. Такі користувачі здатні зруйнувати патріотично налаштовану спільноту, ліквідувавши суспільний ресурс, здатний підтримати державні інтереси. Методи виявлення тролів ґрунтуються на запропонованих ознаках та гіпотезі, що троль, виконуючи завдання, певною мірою «прив'язаний» до користувачів з ролями «лідер думки», «модератор», «транслятор». Запропоновано підхід до виявлення модераторів, що є основаним на застосуванні формальної моделі користувача та оцінюванні суб'єктивності дотримання модератором правил спільноти. Подано підходи до організації ресурсної підтримки заходів із підтримки та нейтралізації суб'єктів інформаційної діяльності: лідерів думок та веб-спільнот. Указані підходи основані на використанні інструментарію виявлення дисбалансів між певними суб'єктами.

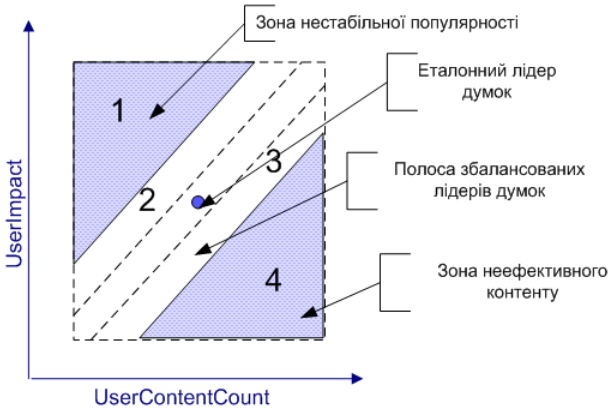

Рис. 3. Баланс показників лідерів думок

На рис. 3 наведено приклад такого дисбалансу за ознаками «впливовість/ продуктивність». Уведено вирази для розрахунку впливовості та продуктивності на основі базових показників користувача CCI. Для кожної з зон розроблено рекомендації щодо ресурсної підтримки або протидії (ворожим лідерам думок). Запропоновано схему балансів «популярність/активність» та «популярність / значущість» для спільнот і методи використання дисбалансів, які дають змогу визначити необхідні для підтримки або протидії ресурси.

<u>У четвертому розділі</u> розглянуто архітектуру та принципи реалізації комплексної системи управління заходами з протидії пропаганді в ССІ, модель її бази даних та функціональні особливості окремих компонент. Побудовано архітектуру системи, яку наведено на рис. 4.

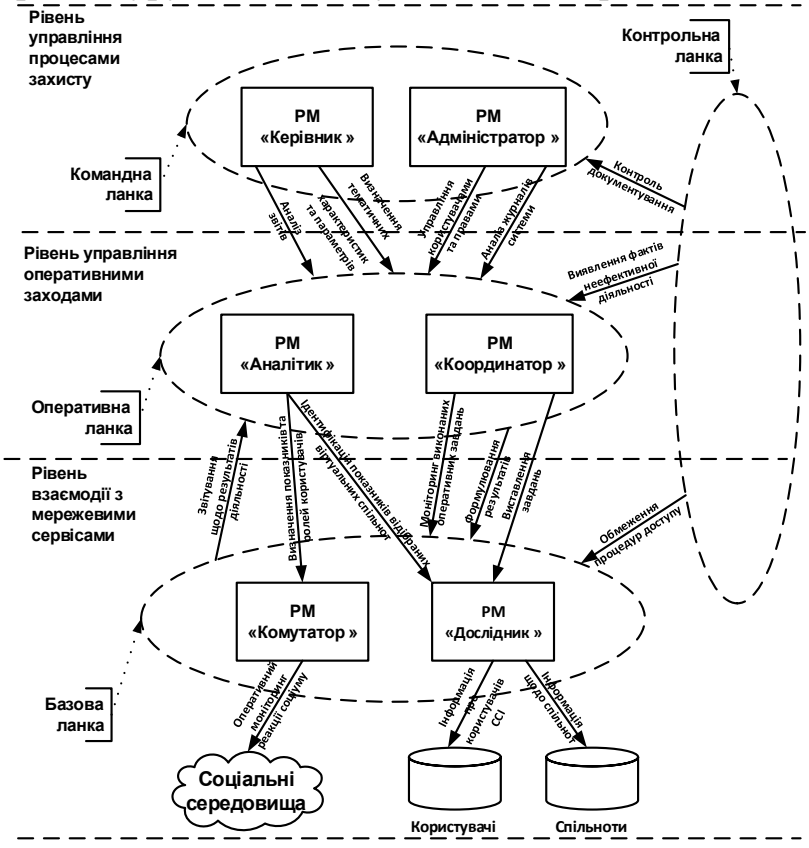

Рис. 4. Загальна архітектура програмного комплексу

Користувачі системи організовані за певними функціональними групами:

- командна ланка – відповідальні за безпеку інформаційного простору за напрямами особи з високою кваліфікацією та компетенціями;
- оперативна ланка – оперативні працівники середньої ланки, відповідальні за безпеку за окремими проєктами або об’єктами;
- базова ланка – виконавці з-поміж оперативних працівників базової ланки або волонтерів;
- контрольна ланка – виконавці серед фахівців кібербезпеки та безпеки прикладних інформаційних систем, адміністратори.

Модель бази даних системи ґрунтується на формальній моделі предметної області, наведеній у другому розділі роботи.

Виділено такі основні складові комплексної БД системи:

- База даних «Користувачі» – охоплює базові масиви даних про користувачів соціальних мереж, що обліковуються.
- База даних «Активність користувачів» – документує дії користувачів соціальних мереж, зокрема зі створення нового контенту.
- База даних «Соціальний портрет користувача» – документує стосунки користувачів з іншими користувачами та спільнотами.
- База даних «Спільноти» – містить базові масиви даних про спільноти соціальних мереж, що обліковуються.

Далі у роботі описано функціональність окремих компонент системи, що є основою для розроблення відповідних АРМів. На закінчення розділу проаналізовано результати впровадження системи та запропонованих у роботі методів і алгоритмів. У межах впровадження підходів, громадські активісти здійснюють системні заходи у соцмережах «Фейсбук» та «Вконтакті» тощо.

Висвітлено результати дворічної діяльності мережевих активістів, що діяли за означеною схемою із захисту інформаційного простору України в окремих, критично важливих для національної безпеки, спільнотах. Визначали такі спільноти з використанням запропонованих у роботі підходів.

Рис. 5. Кількість знешкоджених акаунтів

Рис. 6. Динаміка зміни частки шкідливих лідерів думок

На графіку (рис. 5) наведено дані про знешкоджені акаунти тролів та трансляторів, що ідентифіковано як шкідливі в спільнотах, які підлягають моніторингу. Знешкодженими вважають транслятори, які у середньому проявляють мережеву активність не частіше ніж раз на тиждень або у випадку блокування, ліквідації чи самоліквідації акаунту. На графіку (рис. 6) наведено динаміку зміни частки лідерів думок, діяльність яких шкідлива для України, у загальній кількості лідерів думок. У цьому випадку моніторингу підлягали користувачі, що активно діяли в низці визначених заздалегідь важливих для національної безпеки спільнот. В абсолютних величинах кількість лідерів думок у спільнотах, охоплених моніторингом, збільшилася з 20 до 44, переважно за рахунок патріотично налаштованих користувачів. Зіставлення даних, які надходять про нових лідерів думок та зміну кількості активних лідерів думок, що займались деструктивною діяльністю, дає підстави стверджувати, що більшість шкідливих впливів нейтралізовано та ідентифіковано як шкідливі користувачі припиняли активні дії, втративши можливість ефективно реалізувати агресивні наміри. Указані результати підтверджують працездатність та ефективність запропонованих у роботі методів та засобів протидії ворожій пропаганді.

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 ССІ та їхнього практичного втілення. Зокрема, отримано такі результати:

- проаналізовано розвиток та функціонування ССІ, що підтвердило актуальність наукового завдання із розроблення методів та засобів протидії інформаційній пропаганді;

- набули подальшого розвитку формальні моделі користувачів ССІ 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 ССІ;
- 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 ССІ, 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 інформаційного простору;
- 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 ССІ;
- 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 засоби протидії інформаційній пропаганді у ССІ з використанням їх в окремих, важливих для національної безпеки, спільнотах.

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.

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.

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

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.

5. Пелещишин А., Вус В. Фактори соціальних середовищ інтернету в системі національної безпеки. Вісник інженерної академії України. 2018. № 2. С. 78–82.

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.

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.

8. Вус А. 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, комунікація, суспільство (ICS-2016) : матеріали 5 Міжнар. наук. конф., 19–21 трав. 2016 р. Львів : Вид-во Львів. політехніки, 2016. С. 38–39.

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.

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.

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.

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.

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.

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.

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

АНОТАЦІЯ

Вус В. А. Математичне та програмне забезпечення протидії інформаційній пропаганді в соціальних середовищах Інтернету. – На правах рукопису.

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

У дисертаційній роботі вирішено важливе наукове завдання – розроблення математичного та програмного забезпечення протидії інформаційній пропаганді в соціальних середовищах Інтернету. Це дало змогу формалізувати та вирішити важливі завдання організації ефективної взаємодії з користувачами соціальних середовищ Інтернету.

У роботі обґрунтовано методи планування заходів із протидії інформаційній пропаганді у соціальних середовищах Інтернету, що основані на запропонованих формальних моделях та зведених показниках і забезпечують можливість організації неперервної системної протидії комплексним загрозам для безпеки національного інформаційного простору. Розроблено комплексну систему управління заходами з протидії пропаганді, яка ґрунтується 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

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

АННОТАЦИЯ

Вус В. А. Математическое и программное обеспечение противодействия информационной пропаганде в социальных средах Интернета. – На правах рукописи.

Диссертация на соискание ученой степени кандидата технических наук по специальности 01.05.03 – математическое и программное обеспечение вычислительных машин и систем. – Национальный университет «Львивська политэхника» МОН Украины, Львов, 2019.

В диссертационной работе решена важная научная задача – разработка математического и программного обеспечения противодействия информационной пропаганде в социальных средах Интернета, что позволило формализовать и решить важные задачи организации эффективного взаимодействия с пользователями социальных сред Интернета.

В работе предложены методы планирования мероприятий по противодействию информационной пропаганде в социальных средах Интернета, которые основаны на предложенных формальных моделях и сводных показателях и обеспечивают возможность организации непрерывного системного противодействия комплексным угрозам безопасности национального информационного пространства. Разработана комплексная система управления мероприятиями по противодействию пропаганде, которая базируется на предложенных в работе формальных моделях, методах и алгоритмах и обеспечивает автоматизацию и эффективное выполнение основных задач организации и координации действий ответственных лиц и волонтеров по защите информационного пространства государства.

Ключевые слова: социальная среда Интернета, защита информации, модель безопасности пользователя, социальный портрет пользователя, сетевая активность, характеристика государственной безопасности.

ANNOTATION

Vus V. A. Mathematical and software counter to informational propaganda in social Internet environments. – 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, Lviv, 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. 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.

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. 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.

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 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. Individual results of practical testing of dissertation research in the information space of Ukraine are presented.

In the thesis, it is justified 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; 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; system of aggregated indicators of virtual communities focused on the task of protecting the information space of the state; methods of planning measures to counter informational propaganda in the social media on the Internet; methods and algorithms for detecting and responding to individual users' groups, that carry out destructive activity in the state information space; developed a comprehensive system for managing anti-propaganda measures, based on the formal models, methods and algorithms proposed in the work; 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.

Підписано до друку 06.11.2019 р.
Формат 60×90 1/16. Папір офсетний.
Друк на різографі. Умовн. друк. арк. 1,5. Обл.-видав. арк. 0,89.
Тираж 100 прим. Зам. 191786.

Поліграфічний центр
Видавництва Національного університету "Львівська політехніка"
вул. Ф.Колесси, 4, 79013, Львів
Реєстраційне свідоцтво серії ДК № 4459 від 27.12.2012 р.