Міністерство освіти і науки України
Національний авіаційний університет

Гумінський Руслан Вікторович

УДК 004.738.5+004.773.2

Методи і засоби виявлення інформаційних загроз віртуальних спільнот в інтернет середовищі соціальних мереж

Спеціальність 21.05.01 – інформаційна безпека держави

АВТОРЕФЕРАТ
дисертації на здобуття наукового ступеня
кандидата технічних наук

Київ – 2016

Дисертацією є рукопис.

Робота виконана в Національній академії сухопутних військ імені гетьмана Петра Сагайдачного Міністерства оборони 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,
Смірнов Олексій Анатолійович,
Кіровоградський національний технічний університет,
завідувач кафедри програмного забезпечення;

кандидат технічних наук, доцент,
Дзюба Тарас Михайлович,
Національний університет оборони України імені Івана Черняховського,
професор кафедри застосування інформаційних технологій та інформаційної безпеки.

Захист відбудеться “___” _____ 2016 р. о ____ годині на засіданні спеціалізованої вченої ради Д 26.062.17 у Національному авіаційному університеті за адресою: 03680, м. Київ, пр. Космонавта Комарова, 1.

З дисертацією можна ознайомитися у науково-технічній бібліотеці Національного авіаційного університету.

Автореферат розісланий “___” _____ 2016 р.

Учений секретар
Спеціалізованої вченої ради Д 26.062.17 Гнатюк С. О.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність роботи. У сучасному інформаційному суспільстві відбувається зародження і становлення соціальних формацій – віртуальних спільнот (далі – ВС) з принципово іншими (порівняно з традиційними формами впливу на соціальні структури в індустріальному суспільстві) можливостями впливу на традиційні громадські та державні структури, поява яких пов’язана з програмами створення оперативного доступу через канали відкритих телекомунікаційних мереж до розподілених інтелектуальних і матеріальних ресурсів у будь-якій точці земної кулі. Багато в чому поява таких ВС пов’язана з проведенням телекомунікаційної глобалізації.

Віртуальні спільноти (англ. virtual communities, e-communities) – новий тип спільнот, які виникають і функціонують в електронному просторі (передусім за допомогою мережі Інтернет) з метою сприяння вирішенню своїх професійних, політичних завдань, задоволення своїх потреб у мистецтві, дозвіллі тощо.

Поряд з конструктивними ВС, які прагнуть активно взаємодіяти з суспільством, маючи на меті поліпшення життя як суспільства загалом, так і окремих соціальних груп та індивідів, соціальні мережі все частіше використовують для створення деструктивних ВС. Проте деструктивні ВС, на відміну від конструктивних, намагаються з цим співтовариством боротися усілякими, не завжди законними, методами. Об'єктом агресії деструктивних ВС є усе суспільство або прихильники тих чи інших соціальних груп, як правило, вороже налаштованих до цієї деструктивної ВС.

Крім того, ВС все активніше і масштабніше використовують в інтересах інформаційно-психологічного впливу (далі – ІПсВ). Вони надають широкі можливості в плані впливу на формування громадської думки, прийняття політичних, економічних і військових рішень, впливу на інформаційні ресурси противника і поширення спеціально підготовленої інформації (дезінформації).

Процеси в соціальних мережах викликають підвищений інтерес в науці, однак темпи наукових досліджень істотно відстають від розвитку соціальних мереж.

У наукових дослідженнях, пов’язаних з протидією деструктивному інформаційному впливу (далі – ІВ) виокремлюють такі напрями:

– дослідження проблем створення систем контент-моніторингу соціальних ресурсів мережі Інтернет з метою розвідки та інформаційного протиборства;

– розроблення методів і алгоритмів проведення інформаційних операцій у відкритих (закритих) ресурсах Інтернету.

Перший напрям об’єднує розроблення та розвиток методів і засобів пошуку, збору та аналізу інформації з різних джерел мережі Інтернет, що дає змогу розглядати її у визначений момент часу (роботи Д. В. Ланде, О. Г. Додонов).

Другий напрям об’єднує декілька піднапрямів – розроблення алгоритмів, моделей інформаційних операцій (роботи В. П. Горбулін, О. Г. Додонов, В. М. Фурашев) та моделей ІВ в соціальних мережах (Д. А. Губанов, А. Г. Чхаршвілі, E. R. Smith) з метою вироблення управлінських рішень щодо інформаційного протиборства в соціальних мережах.

Сьогодні саме об’єднання цих напрямів досліджень з метою створення технічних та програмних засобів для виявлення та протидії деструктивному впливу інформаційного наповнення (далі – ІН) ВС у соціальних мережах є найактуальнішим.

Це зумовлено тим, що деструктивні ВС в соціальних мережах створюють нові інформаційні загрози (далі – ІЗ), оскільки держава вже не здатна контролювати їх у повному обсязі через особливості їх функціонування у соціальних мережах, що ускладнюється відсутністю типових методик і рішень, неповнотою відповідних технологічних підходів. Дослідження з цих проблем поки що найчастіше є вузькоспеціалізованими.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційну роботу виконано у межах зареєстрованої тематики Академії сухопутних військ імені гетьмана Петра Сагайдачного «Основні напрямки роботи засобів масової інформації щодо протидії негативному інформаційному впливу противника», шифр «ЗМІ» (№ державної реєстрації 0101u001889).

Мета і завдання дослідження. Мета дисертаційної роботи – забезпечення інформаційної безпеки держави в соціальних мережах шляхом розроблення методів і засобів виявлення та оцінки ІЗ ВС в інтернет середовищі соціальних мереж.

Мета дисертаційної роботи визначає необхідність розв'язання таких задач:

– аналіз ВС у соціальних мережах як суб'єктів інформаційної безпеки держави;

– побудова математичних моделей інформаційного середовища (далі – ІС) ВС та визначення характеристик ВС у соціальних мережах;

– формування показника ІЗ ВС на підставі визначених характеристик;

– розроблення методів і алгоритмів виявлення та оцінки ІЗ ВС у соціальних мережах;

– розроблення архітектури програмно-алгоритмічного комплексу моніторингу та аналізу ІЗ ВС у соціальних мережах, який вирішуватиме завдання виявлення та оцінки ІЗ ВС у соціальних мережах.

Об'єктом дослідження є процеси функціонування ВС в інтернет середовищі соціальних мереж.

Предметом дослідження є методи і засоби виявлення та оцінки ІЗ ВС в інтернет середовищі соціальних мереж.

Методи дослідження. Для вирішення завдань моделювання ІС ВС використано теоретико-множинні підходи, теорію відношень, апарат теорії реляційної алгебри, баз даних та контент-аналізу. Для пошуку ВС у соціальних мережах застосовано сучасні засади пошуку інформації в Інтернеті, а також апарат формальних мов для формування параметризованих запитів до глобальних пошукових систем (далі – ГПС). Для формування ІС використано методи автоматичної кластеризації текстів. Для визначення рекомендацій щодо протидії ІЗ ВС у соціальних мережах застосовано алгоритми теорії графів. Під час проектування програмного комплексу використано апарат розподілених інформаційних систем класу "клієнт – сервер" та технології обміну інформацією у відкритих системах.

Наукова новизна одержаних результатів полягає в обґрунтуванні та виконанні наукового завдання розроблення методів і засобів для організації виявлення та оцінки ІЗ ВС у соціальних мережах. Отримано такі наукові результати:

– *удосконалено* модель ВС за допомогою розширення її до моделі ІС ВС в соціальних мережах, що включає моделі зовнішнього та внутрішнього ІС, яка стала

основою для розроблення структури бази даних щодо обліку та аналізу ІЗ ВС у соціальних мережах;

– *уперше* уведено показник ІЗ ВС в соціальних мережах шляхом визначення цінності ВС, що враховує структуру, кількість учасників та якість ІН сторінок дискусій ВС, та став основою для методів щодо прийняття рішення з протидії ІЗ ВС у соціальних мережах та визначення рекомендацій щодо ІВ на структуру ВС в соціальних мережах;

– *уперше* розроблено метод щодо прийняття рішення з протидії ІЗ ВС у соціальних мережах шляхом об'єднання показників ІЗ, для яких визначення критичних цінностей ВС ґрунтується на встановленні експертами кількості учасників ВС, при якій реалізовується ІЗ, та загальної кількості учасників деструктивної та конкурентної ВС, що дало змогу надати рекомендації щодо прийняття рішення з протидії ІЗ ВС в соціальних мережах;

– *отримали подальший розвиток* графові моделі соціальних мереж на основі матричного представлення графів, які, завдяки врахуванню характеристик моделі ІС ВС та запропонованого показника ІЗ, стали основою для розробки методу прийняття обґрунтованих рішень щодо вибору дискусій ВС для ІВ;

– *уперше* розроблено архітектуру програмно-алгоритмічного комплексу моніторингу та аналізу ІЗ ВС у соціальних мережах, функціональність якого базується на запропонованих у роботі методах та алгоритмах, що дає змогу організувати виявлення та оцінку ІЗ ВС у соціальних мережах.

Практичне значення одержаних результатів. Практичне значення одержаних результатів дисертаційної роботи зумовлено тим, що вони дають змогу організувати виявлення та оцінку ІЗ ВС у соціальних мережах. Зокрема, практично цінними є результати:

– розроблено стратегії протидії ІЗ ВС у соціальних мережах відповідно до правил протидії держави ІЗ ВС у соціальних мережах, що дало змогу вибору підходів щодо протидії ІЗ ВС у соціальних мережах;

– розроблено алгоритми пошуку сторінок дискусій у соціальних мережах з використанням розширених можливостей ГПС та запитів API-методів соціальних мереж, які дають змогу виявити сторінки дискусій у соціальних мережах відповідно їх ІН;

– розроблено алгоритм формування ІС ВС в соціальних мережах шляхом застосування кластеризації сторінок дискусій у соціальних мережах відповідно до їхнього ІН та розподілу сторінок дискусій залежно від напряму ІН для розподілу сторінок дискусій на деструктивну та конкурентну ВС.

Практичне значення отриманих результатів підтверджено відповідними реалізаціями (акт управління інформаційних технологій Міністерства оборони України від 15.05.2015 року та акт управління Служби безпеки України у Львівській області від 20.05.2015 року).

Особистий внесок здобувача. Усі наукові результати дисертаційної роботи автор отримав самостійно. У друкованих працях, опублікованих у співавторстві, здобувачеві належать: [4] – аналіз ВС у соціальних мережах як суб'єктів інформаційної безпеки держави, визначення основних ІЗ, які можуть виникати під час функціонування ВС у

соціальних мережах; [5] – алгоритм пошуку ВС за допомогою ГПС та їх особливостей; [6] – модель ІС ВС та методи розрахунку основних характеристик; [12] – визначення складових показника ІЗ ВС у соціальних мережах; [1] – введено поняття показника ІЗ ВС та метод його розрахунку; [2, 7] – метод визначення рекомендацій щодо ІВ на структуру ВС; [9] – запропоновано структуру системи моніторингу та аналізу ІЗ ВС у соціальних мережах; [10] – алгоритм моніторингу та аналізу ВС у соціальних мережах; [14] – аналіз стратегій ІВ на ІС ВС; [16] – алгоритм формування ІС ВС у соціальних мережах; [18] – архітектура програмного комплексу моніторингу та аналізу ІЗ ВС у соціальних мережах.

Апробація результатів дисертації. Основні результати наукових досліджень неодноразово доповідалися на міжнародних та всеукраїнських наукових конференціях, зокрема: міжвідомча науково-технічна конференція «Проблемні питання розвитку озброєння і військової техніки» (Київ, 2012); науково-практичний форум «IV Січневі Гіси»: «Інтелектуальна оборона» (Львів, 2013); дев'ята наукова конференція Харківського університету Повітряних Сил імені Івана Кожедуба «Новітні технології – для захисту повітряного простору» (Харків, 2013); IV науково-технічна конференція «Проблемні питання розвитку озброєння і військової техніки» (Київ, 2013); II, III та IV міжнародні наукові конференції «Інформація, комунікація, суспільство» (Львів, 2013 – 2015); IV міжнародна науково-технічна конференція «ITSEC-2014»: «Безпека інформаційних технологій» (Київ, 2014); міжвідомча науково-практична конференція «Інформаційна безпека у воєнній сфері. Сучасний стан та перспективи розвитку» (Київ, 2015); міжнародна науково-практична конференція «Перспективи розвитку озброєння та військової техніки Сухопутних військ» (Львів, 2015).

Результати дисертаційних досліджень регулярно доповідалися на науково-технічній раді Наукового центру Сухопутних військ Академії сухопутних військ.

Публікації. За результатами виконаних досліджень опубліковано 18 наукових праць, серед яких 6 статей у фахових наукових виданнях (технічні науки), 2 публікації у закордонних періодичних виданнях та 10 публікацій – у працях наукових конференцій.

Структура та обсяг дисертації. Дисертаційна робота складається зі вступу, чотирьох розділів, висновків, списку літератури з 154 найменувань та двох додатків. Загальний обсяг дисертації становить 158 сторінок, з них 108 сторінок основного тексту, який містить 35 рисунків та 7 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. Розглянуто практичну цінність, реалізацію і впровадження результатів роботи. Наведено дані про особистий внесок здобувача, апробацію роботи та публікації.

У першому розділі здійснено аналіз ВС в інтернет середовищі та особливостей їх організації в соціальних мережах. Розглянуто ВС в соціальних мережах та їхні властивості як суб’єктів інформаційної безпеки держави, суспільства. Визначено, що

основним інструментом, що використовується у ВС деструктивного характеру, є ІПсВ, який передбачає цілеспрямоване розроблення та поширення спеціальної актуальної інформації, здатної справляти безпосередній або непрямий вплив на суспільну свідомість, психологію і поведінку населення. Проаналізовано основні реальні та потенційні загрози інформаційній безпеці, які можуть виникати в ІН ВС. Дослідження сучасної теоретичної та практичної бази, систем та методів протидії деструктивному впливу в соціальних мережах показали неможливість виявлення та оцінки ІЗ ВС у соціальних мережах.

У другому розділі здійснено загальний опис ІС ВС у соціальних мережах. Розроблено та деталізовано модель внутрішнього ІС до моделі дискусії ВС. На основі формальної моделі ІС ВС, з врахуванням якості ІН, визначений показник ІЗ.

У роботі формальна модель соціальної мережі подана так:

$$SocialNetworks = \langle Members, Content, Link \rangle, \quad (1)$$

де $Members$ – зареєстровані користувачі соціальної мережі; $Content$ – ІН (контент); $Link$ – зв'язки між зареєстрованими користувачами соціальної мережі.

Формальна модель ВС визначена, як і формальна модель соціальної мережі (1), ІН та учасниками:

$$VirtualCommunity = \langle Content, Member \rangle, \quad (2)$$

де $Content$ – ІН; $Member$ – множина учасників.

Розглянуте середовище, в якому функціонують ВС в соціальних мережах, відповідає властивостям та функціям ІС та складається із зовнішнього ІС та внутрішнього ІС.

Враховуючи (1), (2) зовнішнє ІС ВС подано у вигляді:

$$InfSpace = \langle VirtualCommunity, AgentInfl, Shadow(VirtualCommunity), LinkExternal(VirtualCommunity), LinkExternal(AgentInfl) \rangle, \quad (3)$$

де $VirtualCommunity$ – сукупність ВС в ІС; $AgentInfl$ – сукупність агентів зовнішнього впливу; $LinkExternal(VirtualCommunity)$ – матриця зв'язків між ВС в ІС; $LinkExternal(AgentInfl)$ – матриця зв'язків між ВС та агентами зовнішнього впливу в ІС; $Shadow(VirtualCommunity)$ – множина зареєстрованих користувачів соціальної мережі, які є тінню ВС. Модель внутрішнього ІС подано у вигляд:

$$InfSpace(VirtualCommunity_i) = \langle Thread(VirtualCommunity_i), LinkInternal(Tread), Member(VirtualCommunity_i), Shadow(VirtualCommunity_i) \rangle, \quad (4)$$

де $Thread(VirtualCommunity_i)$ – сукупність дискусій i-ї ВС; $LinkInternal(Thread)$ – матриця зв'язків між дискусіями i-ї ВС; $Member(VirtualCommunity_i)$ – множина учасників дискусій i-ї ВС, зареєстровані користувачі соціальних мереж;

$$Member(VirtualCommunity_i) = \bigcup_{j=1}^{N_i} Member(Thread_j),$$

де $Member(Thread_j)$ – множина учасників j-ї дискусії, зареєстрованих користувачів соціальних мереж; N_i – кількість дискусій в i-й ВС; $Shadow(VirtualCommunity_i)$ –

множина зареєстрованих користувачів соціальних мереж, які зацікавлені ідеологією (тематикою) *i*-ї ВС;

$$Shadow(VirtualCommunity_i) = \bigcup_{j=1}^{N_i} Shadow(Thread_j),$$

де $Shadow(Thr\ ead_j)$ – множина зареєстрованих користувачів соціальних мереж, які зацікавлені тематикою *j*-ї дискусії та не є учасниками дискусії; N_i – кількість дискусій в *i*-й ВС. При цьому $Member(Vir\ tualCommun\ ity_i) \neq Shadow(Vir\ tualCommun\ ity_i)$.

Модель (4) деталізовано до моделі дискусії, з урахуванням зв'язків між елементами ВС та особливостями побудови сторінок дискусій у соціальних мережах:

$$Thread_i = \langle ThreadTitle_i, ThreadDescription_i, ThreadMembers_i, Post(Thread_i), Link(Thread_i) \rangle, \quad (5)$$

де $ThreadTitl\,e_i$ – назва *i*-ї дискусії; $ThreadDescription_i$ – опис *i*-ї дискусії; $ThreadMembers_i$ – множина учасників *i*-ї дискусії; $Post(Thread_i) = \{Post_{ij}\}_{j=1}^{N^{(PT_i)}}$ – множина повідомлень, що належить до *i*-ї дискусії; $N^{(PT_i)}$ – кількість повідомлень у дискусії $Thread_i$; $Link(Thread_i)$ – множина зв'язків у структурі та в ІН *i*-ї дискусії.

Повідомлення визначено як:

$$Post_i = \langle PostAuthor_i, PostDate_i, PostText_i, PostReply(Post_i) \rangle, \quad (6)$$

де $PostAuthor_i$ – автор *i*-го повідомлення; $PostDate_i$ – дата *i*-го повідомлення; $PostText_i$ – текст *i*-го повідомлення; $PostReply(Post_i) = \{PostReply_{ij}\}_{j=1}^{N^{(PR_i)}}$ – множина дописів до *i*-го повідомлення; $N^{(PR_i)}$ – кількість дописів до *i*-го повідомлення.

Допис подано у вигляді:

$$PostReply_i = \langle PostReplyAuthor_i, PostReplyDate_i, PostReplyText_i \rangle, \quad (7)$$

де $PostReplyAuthor_i$ – автор *i*-го допису; $PostReplyDate_i$ – дата *i*-го допису; $PostReplyText_i$ – текст *i*-го допису.

Для аналізу ІН ВС, використовуючи (5), (6), (7), розроблено векторно-просторову модель ВС:

$$\overline{VirtualCommunity}^{(Term)} = \langle Term, W \rangle, \quad (8)$$

де $Term = \{term_i\}_{i=1}^{N}$ – множина термів ВС; $W = \{w_i\}_{i=1}^{N}$ – множина вагових коефіцієнтів термів ВС; N – кількість термів у ВС.

Та векторно-просторову модель дискусії:

$$\overline{Thread}^{(Term)} = \langle Term, W \rangle, \quad (9)$$

де $Term = \{term_i\}_{i=1}^{N}$ – множина термів дискусії; $W = \{w_i\}_{i=1}^{N}$ – множина вагових коефіцієнтів термів дискусії; N – кількість термів у дискусії.

Для визначення вагових коефіцієнтів термів автором застосовано *tf*idf* міра оцінки термів як найефективніша для кластеризації інформаційних потоків у мережі Інтернет.

Використавши векторно-просторову модель дискусії (9) та ВС (8) побудовано центроїд ВС: $Centroid(VirtualCommunity) = \langle Keyword, W^* \rangle$,

де $Keyword = \{keyword_i\}_{i=1}^{N}$ – множина ключових термів, що характеризує ІН ВС; $W_i^* = \{w_i^*\}_{i=1}^{N}$ – множина вагових коефіцієнтів ключових термів з нормованого вектора вагових коефіцієнтів ВС; N – кількість ключових термів.

Та дискусії: $Centroid\,(Thread) = \langle Keyword, W^* \rangle$,

де $Keyword = \{keyword_i\}_{i=1}^{N}$ – множина ключових термів дискусії; $W_i^* = \{w_i^*\}_{i=1}^{N}$ – множина вагових коефіцієнтів ключових термів з нормованого вектора вагових коефіцієнтів дискусії; N – кількість ключових термів.

Зважаючи на особливості використаної в ІН дискусій ВС мови, введено міру відповідності тематичного напряму повідомлень у дискусії, яку визначено в роботі як ознаку, що залежить від позитивного чи негативного напряму повідомлень у дискусії, відповідно до тематичного напряму ВС:

$$Sim(Thread_i) = \max\{Sim(Thread_i)^{Positive}, Sim(Thread_i)^{Negative}\}, \quad (10)$$

де $Sim(Thread_i)^{Positive}$ – міра відповідності позитивних повідомлень в *i*-й дискусії, згідно з тематикою ІН; $Sim(Thread_i)^{Negative}$ – міра відповідності негативних повідомлень в *i*-й дискусії, згідно з тематикою ІН, що спричиняє ІЗ. Міра відповідності позитивних (негативних) повідомлень визначається за двома підходами: перший як відношення кількості позитивних (негативних) повідомлень до загальної кількості повідомлень; другий підхід як відношення суми ваги ключових слів, які є в тексті позитивних (негативних) повідомлень до загальної суми ключових слів, які є в тексті повідомлень.

Матрицю наявності зв'язків між дискусіями у ВС подано у вигляді:

$$LinkIntern\,al(Thread) = \|link_{ij}\|_{n*n}, \quad (11)$$

де $link_{ij}$ – ознака наявності зв'язків між *i*-ю та *j*-ю дискусією у ВС; *n* – кількість дискусій у ВС.

Для визначення ознаки наявності зв'язків між дискусіями ВС автор визначив умови, а саме:

– наявність гіперпосилань у структурі дискусії та наявність гіперпосилань в ІН повідомлень дискусії на сторінки інших дискусій ВС:

$$link_{ij} = \begin{cases} 1, \textit{якщо є гіперпосилання до } j\text{ - ї дискусії}; \\ 0, \textit{відсутнє гіперпосилання до } j\text{ - ї дискусії}; \end{cases}$$

– наявність спільних зареєстрованих учасників у дискусіях ВС:

$$link_{ij} = \begin{cases} 1, \textit{якщо} ThreadMembers_i \cap ThreadMembers_j; \\ 0. \end{cases}$$

де $ThreadMembers_i$ – множина учасників *i*-ї дискусії.

Далі введено показник ІЗВС – як кількісну оцінку реалізації ІЗ, яку становить ІН дискусій ВС.

Для визначення показника ІЗ процесу функціонування ВС використано цінність ВС, яка враховує кількість учасників, якість ІН сторінок дискусій та зв'язки між ними.

Цінність віртуальної спільноти – це потенційна доступність учасників спільноти, з якими будь-який учасник спільноти може «сконтактуватися» в разі необхідності.

Отже, показник ІЗ ВС в загальному вигляді подано у вигляді:

$$InfThreat(VirtualCommunity) = \begin{cases} \dfrac{Value(VirtualCommunity)}{Value(VirtualCommunity)^*}, \\ 1, якщо \dfrac{Value(VirtualCommunity)}{Value(VirtualCommunity)^*} > 1 \end{cases}, \quad (12)$$

де $Value(VirtualCommunity)$ – цінність ВС; $Value(VirtualCommunity)^*$ – критична цінність ВС, за якої реалізується ІЗ.

Використовуючи підхід, що ґрунтується на законі більш помірнішого зростання цінності мережі порівняно із законом Ципфа для визначення цінності ВС з урахуванням кількості її учасників, якості ІН, структури між її елементами та можливим мобілізаційним ресурсом ВС, використано вираз:

$$Value(VirtualCommunity)^{(Mob)} = \sum_{i=1}^{N}\left(M^{(Group_i)} \sum_{j=1} \left(Sim(Thread_j) \cdot card(ThreadMembers_j)\right) \right) \cdot$$

$$\cdot \ln\left(M^{(Group_j)} \sum_{j=1} \left(Sim(Thread_j) \cdot card(ThreadMembers_j)\right) \right) - \quad , \quad (13)$$

$$- M^{(Group_j)} \sum_{j=1} \left(Sim(Thread_j) \cdot card(ThreadMembers_j)\right) \Bigg) + card\left(Shadow(VirtualCommunity)\right)$$

де $ThreadMembers_i$ – множина учасників i-ї дискусії; $Sim(Thread_i)$ – міра відповідності тематичного напряму дописів i-ї дискусії; $M^{(Group_i)}$ – кількість дискусій в i-ій групі; N – кількість груп у ВС; $Shadow(VirtualCommunity)$ – множина зареєстрованих користувачів соціальних мереж, які зацікавлені ідеологією (тематикою) ВС та не є учасниками дискусії.

Для утворення груп визначені правила їх формування: група не може бути пустою, тобто повинна містити хоча б одну дискусію; у ВС може бути від 1 до n груп (n – кількість дискусій у віртуальній спільноті), тобто в групі може бути від 1 до n дискусій; всі дискусії в групі взаємозв'язані внутрішніми та зовнішніми гіперпосиланнями або спільними зареєстрованими учасниками; всі дискусії групи не можуть мати внутрішніх та зовнішніх гіперпосилань або спільних зареєстрованих учасників з дискусіями інших груп.

Для визначення критичної цінності ВС, при якій реалізується ІЗ запропоновано два підходи. Перший підхід для визначення критичної цінності ВС ґрунтується на тому, що експерти визначають кількість учасників ВС, при якій реалізується i-та ІЗ, без урахування якості ІН ВС, структури зв'язків дискусій у ній. Отже, згідно з (13), критична цінність ВС подано у вигляді:

$$Value(VirtualCommunity)^* = Members(InfThreat_i) \cdot \ln\left(Members(InfThreat_i)\right) - \quad , \quad (14)$$
$$- Members(InfThreat_i)$$

де $Members(InfThreat_i)$ – критична кількість учасників ВС, що визначили експерти, при якій реалізується *i*-та ІЗ без урахування якості ІН ВС, структури зв'язків дискусій у ній.

Другий підхід ґрунтується на урахуванні визначення критичної цінності ВС щодо загальної кількості учасників деструктивної та конкурентної ВС, які зацікавлені цією тематикою, з урахуванням якості ІН та структури зв'язків дискусій в цих ВС. Отже, критична цінність ВС має вигляд:

$$Value(VirtualCommunity)^* = \sum_{i=1}^{N} Value(VirtualCommunity_i) \ , \qquad (15)$$

де $Value(VirtualCom\ munity_i)$ – цінність *i*-ї ВС; N – кількість ВС, зацікавлених цією тематикою (як правило, деструктивна та конкурентна).

Цінності для деструктивної та конкурентної ВС розраховуємо, використовуючи формулу (13).

Відповідно до розрахунку показника ІЗ (12), його значення лежатиме в межах [0,1], що спрощує подальше прийняття рішення з протидії ІЗ ВС у соціальних мережах.

У третьому розділі розроблено алгоритми пошуку сторінок дискусій у соціальних мережах з використанням запитів ГПС.

Рис. 1. Формалізований запит для виявлення сторінок у соціальній мережі «Facebook»

Крок 3. Визначаємо частини URL-адреси дискусій, аналізуючи Html-код сторінки переліку тематично зв'язаних дискусій (рис. 3).

Крок 4. За результатами виявлених частин URL-адреси формуємо URL-адресу тематично зв'язаних груп. Приклад формування URL-адреси тематично зв'язаних груп наведено в табл. 1.

Алгоритм пошуку сторінок дискусій для соціальної мережі «Facebook» ґрунтується на виконанні наступних кроків:

Крок 1. Формування пошукового запиту з використання ГПС (рис. 1) та збереження результатів пошуку.

Крок 2. Для кожної сторінки проводиться аналіз Html-коду для виявлення URL-адреси сторінки переліку тематично зв'язаних груп (рис. 2).

Рис. 2. Аналіз Html-коду сторінки для виявлення URL-адреси сторінки переліку тематично зв'язаних груп

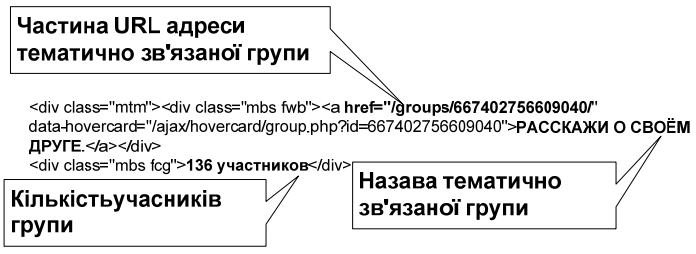

Рис. 3. Аналіз Html-коду сторінки переліку тематично зв'язаних дискусій для виявлення частини URL-адреси дискусій

Таблиця 1

Формування URL-адреси тематично зв'язаних груп

Адреса сторінки	Частина адреси тематично зв'язаної групи	Адреса тематично зв'язаної групи
www.facebook.com/valerij.klock	/groups/667402756609/	www.facebook.com/groups/667402756609/
www.facebook.com/valerij.klock	/groups/Ivan.SOS/	www.facebook.com/groups/Ivan.SOS/
www.facebook.com/valerij.klock	/groups/180978166552/	www.facebook.com/groups/180978166552/

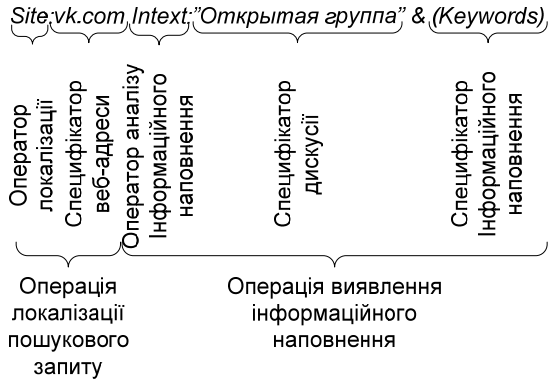

Рис. 4. Формалізований запит для виявлення дискусій у соціальній мережі «Вконтакті»

Результатами роботи алгоритмів є адреси сторінок дискусій у «Вконтакті» та «Facebook», знайдених за допомогою формалізованих запитів ГПС та аналізу Html-коду сторінок дискусій у соціальних мережах.

В зв'язку з особливостями функціонування ВС у соціальних мережах було розроблено структурну схему пошукового робота для проведення глибинного пошуку з використанням запитів API-методів соціальних мереж, вхідними даними для якого є результати пошуку з використанням ГПС. Результатами роботи глибинного пошуку є уточнення переліку дискусій, які пов'язані з відповідною тематикою, та формування переліку агентів зовнішнього впливу (3).

Алгоритм пошуку сторінок дискусій для соціальної мережі «Вконтакті» грунтується на виконанні наступних кроків:

Крок 1. Формування пошукового запиту з використання ГПС (рис. 4) та збереження результатів пошуку.

Крок 2. Для кожної знайденої дискусії проводиться аналіз Html-коду сторінки на наявність ідентифікатора внутрішніх дискусій (рис. 2). При наявності ідентифікатора внутрішніх дискусій їх адреси додаються до результатів пошуку.

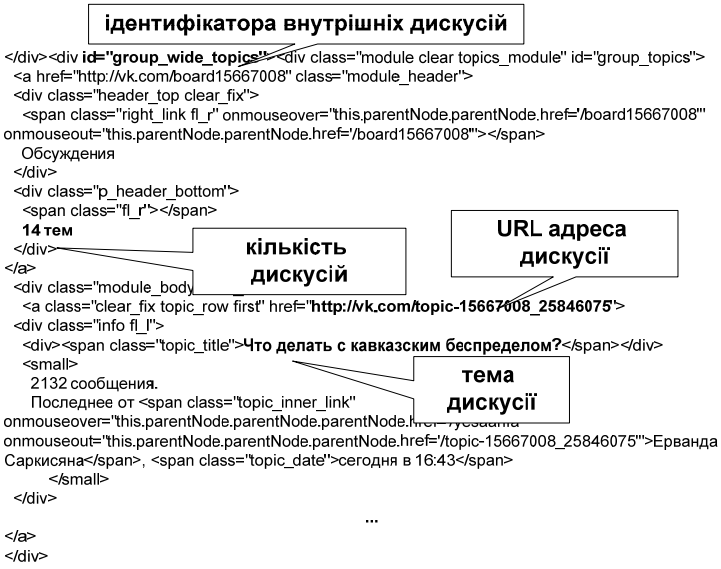

Рис. 5. Аналіз Html-коду сторінки дискусії для виявлення Url-адрес внутрішніх дискусій

Для формування ІС ВС запропоновано алгоритм, що складається з наступних кроків:

Крок 1. Для кластеризації результатів пошуку використаємо векторно-просторову модель дискусії та віртуальної спільноти (8), (9). Дискусії обробляються послідовно

згідно з підходом Солтона. В результаті роботи алгоритму кожен кластер містить дискусії, які об'єднуються за ознакою мети та ідеології існування.

Крок 2. Далі для кожного кластера дискусії розподіляються на деструктивну та конкурентну ВС. Розподіл проводиться, використовуючи значення позитивних та негативних напрямів дописів в дискусіях (10). Дискусія, для якої: $Sim(Thread_i)^{Negative} \geq Sim(Thread_i)^{Positive}$ належатиме до деструктивної ВС, в іншому випадку дискусія входить у конкурентну ВС.

Для прийняття рішення щодо протидії ІЗ ВС у соціальних мережах розроблено метод, який включає наступні кроки:

Крок 1. Формується модель загроз, яка складається з: об'єкта загрози; сфери застосування загрози; переліку загроз; оцінки ризиків загрози. Об'єкт, сферу застосування та перелік загроз визначають відповідно до нормативно-правових документів з інформаційної безпеки держави. Оцінка ризиків визначається як критична кількість учасників ВС, при якій реалізується ця загроза.

Крок 2. Розраховуємо $InfThreat_{InfConfr}(VirtualCommunity)$ – показник ІЗ, для якого визначення критичної цінності ВС ґрунтується, на загальній кількості учасників деструктивної та конкурентної ВС, які зацікавлені цією тематикою з урахуванням якості ІН та структури зв'язків дискусій у цих ВС (15).

Крок 3. Розраховуємо $InfThreat_{CritMembers}(VirtualCommunity)$ – показник ІЗ, для якого визначення критичної цінності ВС ґрунтується на встановленні експертами кількості учасників ВС, при якій реалізовується ІЗ з моделі загроз (14).

Крок 4. Розраховуємо ступінь ІЗ $InfThreat$ використовуючи метод адитивного згортання критеріїв:

$$InfThreat = 1 - \left(InfThreat_{InfConfr}(VirtualCommunity) + InfThreat_{CritMembers}(VirtualCommunity)\right).$$

При значенні $InfThreat \leq 0$ приймається рішення щодо протидії ІЗ ВС.

Схематичне зображення методу прийняття рішення щодо протидії ІЗ ВС відображено на рис. 6.

Рис. 6. Схематичне зображення методу прийняття рішення щодо протидії інформаційним загрозам віртуальних спільнот

Далі було розроблено стратегії ІВ на структуру внутрішнього ІС ВС, а саме: **Стратегія 1** – блокування дискусій або ІПсВ на них з метою зміни тематичної спрямованості дискусій та їх переміщення до конкурентної ВС, що пов'язано зі зменшенням кількості дискусій та учасників у ВС; **Стратегія 2** – руйнування зв'язків окремої дискусії, щоб зробити її ізольованою дискусією без зменшення загальної кількості дискусій та учасників у ВС; **Стратегія 3** – руйнування зв'язків окремої дискусії задля формування окремих груп дискусій без зменшення загальної кількості дискусій та учасників у ВС. Проведено дослідження з метою аналізу використання стратегій ІВ на внутрішнє ІС. Визначено, що ефективними стратегіями впливу є змішані стратегії 1&2 та 1&3, у разі використання яких можливі такі варіанти впливу: руйнування зв'язків між дискусіями групи за допомогою блокування дискусій (силовий метод); ІПсВ на дискусії з метою зменшення ступеня відповідності тематичного напряму дописів у дискусії та переходу дискусії до конкурентної ВС (моніторинг ВС та протидія методами ІПсВ).

Щоб сформувати рекомендації щодо ІВ на структуру ВС, використовуючи модель внутрішнього ІС (4), ВС подано у вигляді незв'язного, неорієнтованого графа матричним способом: $G = (V, A)$, де V – множина вершин, яка складається із сукупностей дискусій i-ї ВС $Thread(VirtualCommunity_i)$; A – матриця суміжності графа G. Елементи матриці суміжності A визначаються з матриці зв'язків між дискусіями ВС (11): $a_{ij} = link_{ij}$.

На основі характеристик дискусій $Sim(Thread_i)$ (10) та моделі дискусії (5) визначено вагові показники вершин графа:

$$V = \left\| Sim(Thread_i), card(ThreadMembers_i) \right\|_{i=\overline{1,n}},$$

де $Sim(Thread_i)$ – міра відповідності тематичного напряму дописів i-ї дискусії; $card(ThreadMembers_i)$ – кількість учасників дискусії.

Використовуючи алгоритми теорії графів, розв'язано задачу щодо визначення мінімального переліку дискусій $Thread$ ВС $VirtualCommunity$, після видалення яких показник ІЗ отриманої ВС зменшився до порогового значення $InfThreat(VirtualCommunity) \le \varepsilon$. Крім того, виконані такі часткові завдання: сформовано групи дискусій; під час повторного використання алгоритму враховано зворотний зв'язок за результатами ІВ на ВС. Схематичне зображення запропонованого методу відображено на рис. 7.

Блок 1. Формуються групи дискусій ВС відповідно до розроблених правил. Для цього використовуємо матрицю суміжності A та розраховуємо матрицю досяжності R, використовуючи паралельний алгоритм знаходження матриці досяжності у графі. Елементи, що мають однакові рядки і стовпці в матриці R, групуємо, переставляючи рядки і стовпці, отримуємо блочно-діагональну матрицю R_B, кожна група елементів якої є групою дискусій ВС. Для створених груп визначаємо їхні цінності згідно з формулою (13). Вибираємо групу, для якої цінність максимальна та кількість елементів більша за два.

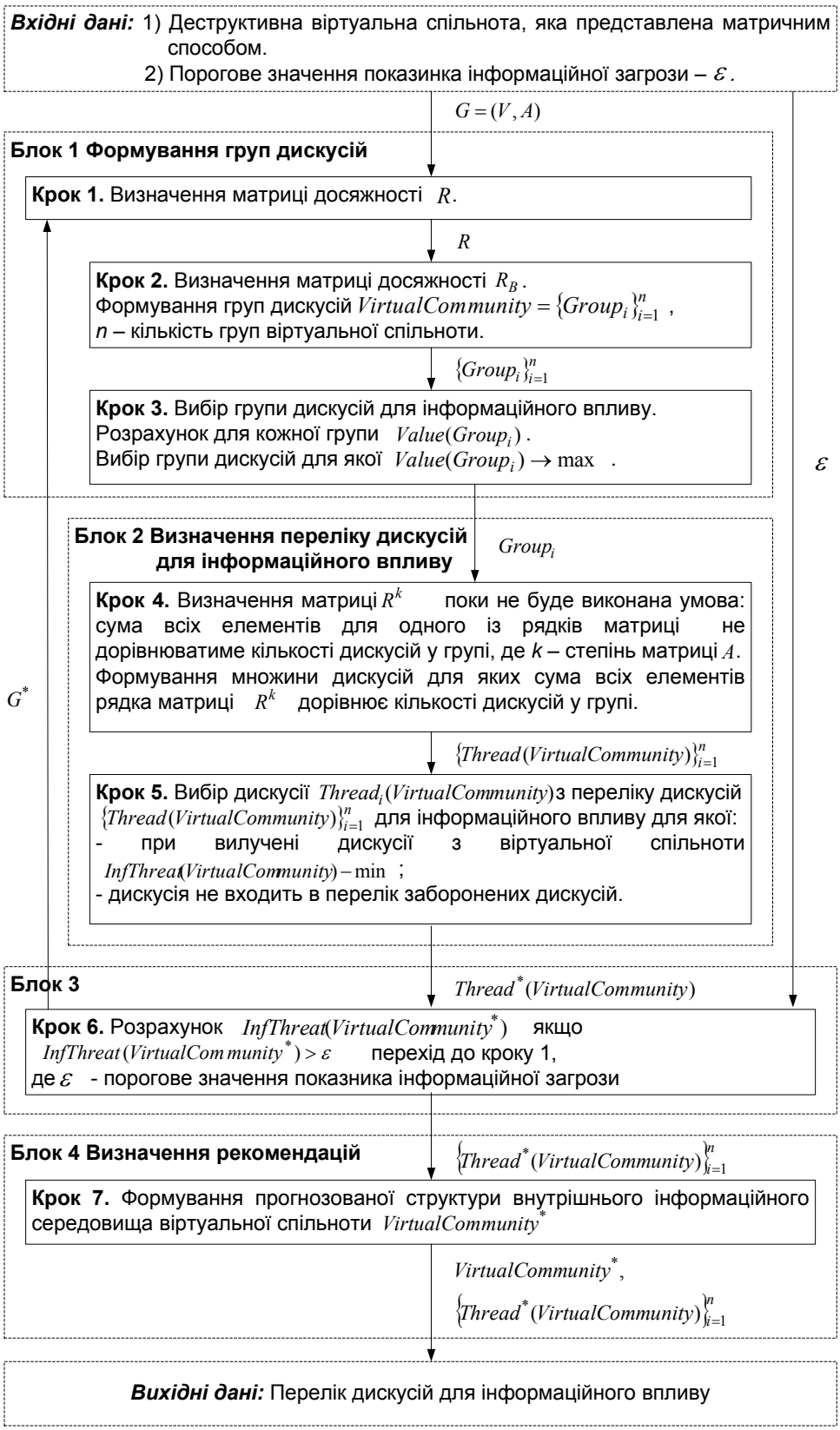

Рис. 7. Схематичне зображення методу визначення рекомендацій щодо інформаційного впливу на структуру віртуальної спільноти

Блок 2. Для вибраної групи визначаємо дискусію або перелік дискусій для ІВ. Для визначення дискусії використовуємо властивості матриці суміжності, піднесеної до степеня, алгоритмічні дії між її елементами замінюємо на логічні (суму замінюємо на диз'юнкцію, а добуток на кон'юнкцію). За результатами роботи алгоритму отримуємо

від однієї до декількох дискусій, з найкоротшим шляхом до всіх дискусій групи ВС. За наявності декількох дискусій вибираємо ту дискусію, у разі видалення якої показник ІЗ зменшується найбільше. Вибираючи дискусії враховується, що під час повторного моніторингу та визначення стратегії впливу на внутрішнє ІС створюється перелік заборонених дискусій, на які неможливий подальший ІВ. Визначена дискусія включається в перелік дискусій для ІВ.

Блок 3. Для отриманої ВС розраховуємо показник ІЗ відповідно до виразу (12). Якщо показник ІЗ більший від порогового значення, переходимо до блока 1.

Блок 4. Надання рекомендацій щодо переліку дискусій для ІВ на внутрішнє ІС. Вони формулюють після того, як сформовано повний перелік дискусій, видалення яких з ВС забезпечує зменшення показника ІЗ до порогового значення. Крім переліку дискусій, формується прогнозована структура внутрішнього та зовнішнього ІС ВС після ІВ.

Для подальшого моніторингу ВС визначається вікно спостереження, яке забезпечить очікування результатів після виконання дій щодо ІВ. Під час повторного моніторингу соціальної мережі здійснюють всі заходи для виявлення та формування ВС за визначеною тематикою ІН. Перед повторним моніторингом соціальної мережі формується перелік заборонених дискусій на які неможливий подальший ІВ, оскільки: дискусія сильно модерована, адміністратори та модератори дискусії постійно видаляють небажане ІН; ІВ призвів до негативного результату для учасників дискусії.

Був проведений експеримент (рис. 8) для змодельованої ВС за варіантами:

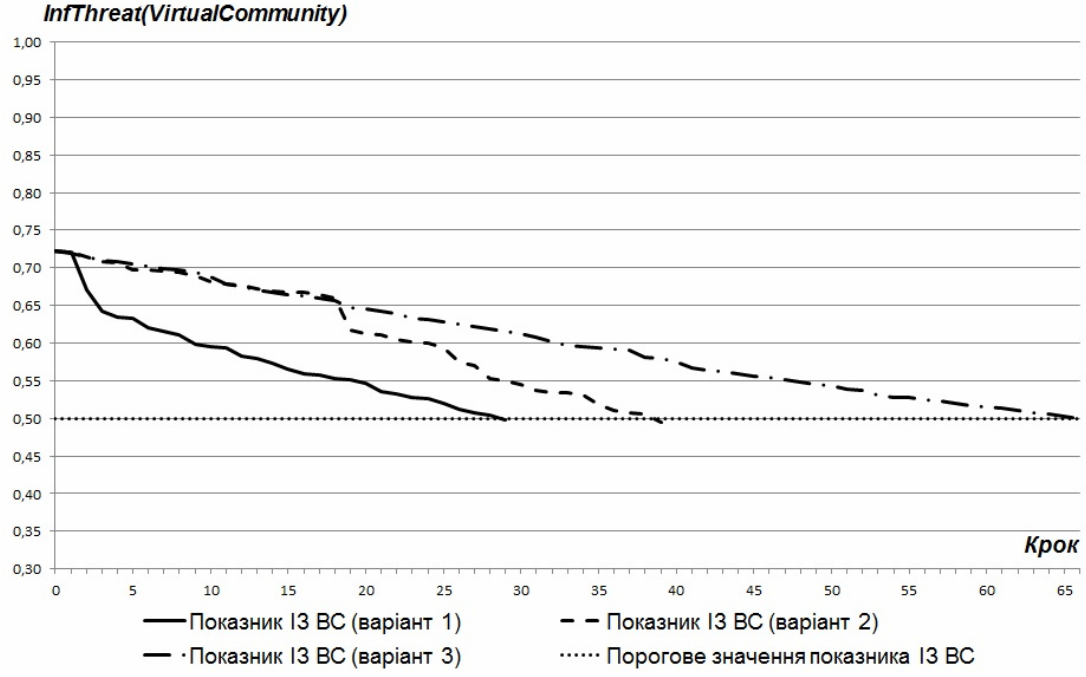

Рис. 8. Графіки змін показника інформаційної загрози для 1, 2 та 3 варіантів

Варіант 1: для ВС, в якій не визначено перелік заборонених дискусій, на які неможливий подальший ІВ з використанням методу визначення рекомендацій щодо ІВ на структуру ВС.

Варіант 2: для ВС, у якій визначено перелік заборонених дискусій, на які неможливий подальший ІВ за результатами розрахунків за варіантом 1 з використанням методу визначення рекомендацій щодо ІВ на структуру ВС.

Варіант 3: відповідно до стратегії 1, що пов’язано зі зменшенням кількості дискусій, учасників у ВС та випадковим руйнуванням структури ВС без використання методу визначення рекомендацій щодо ІВ на структуру ВС.

Відповідно до результатів експериментів встановлено, що при використанні методу визначення рекомендацій щодо ІВ на структуру внутрішнього ІС ВС для зменшення показника ІЗ до порогового значення, необхідно проводити ІВ на меншу кількість дискусій ВС, ніж при впливі на дискусії з максимальною кількістю учасників.

У четвертому розділі розроблено архітектуру програмного комплексу моніторингу та аналізу ІЗ ВС у соціальних мережах (рис. 9), описано основні складові системи, їхні функції та технічні аспекти реалізації.

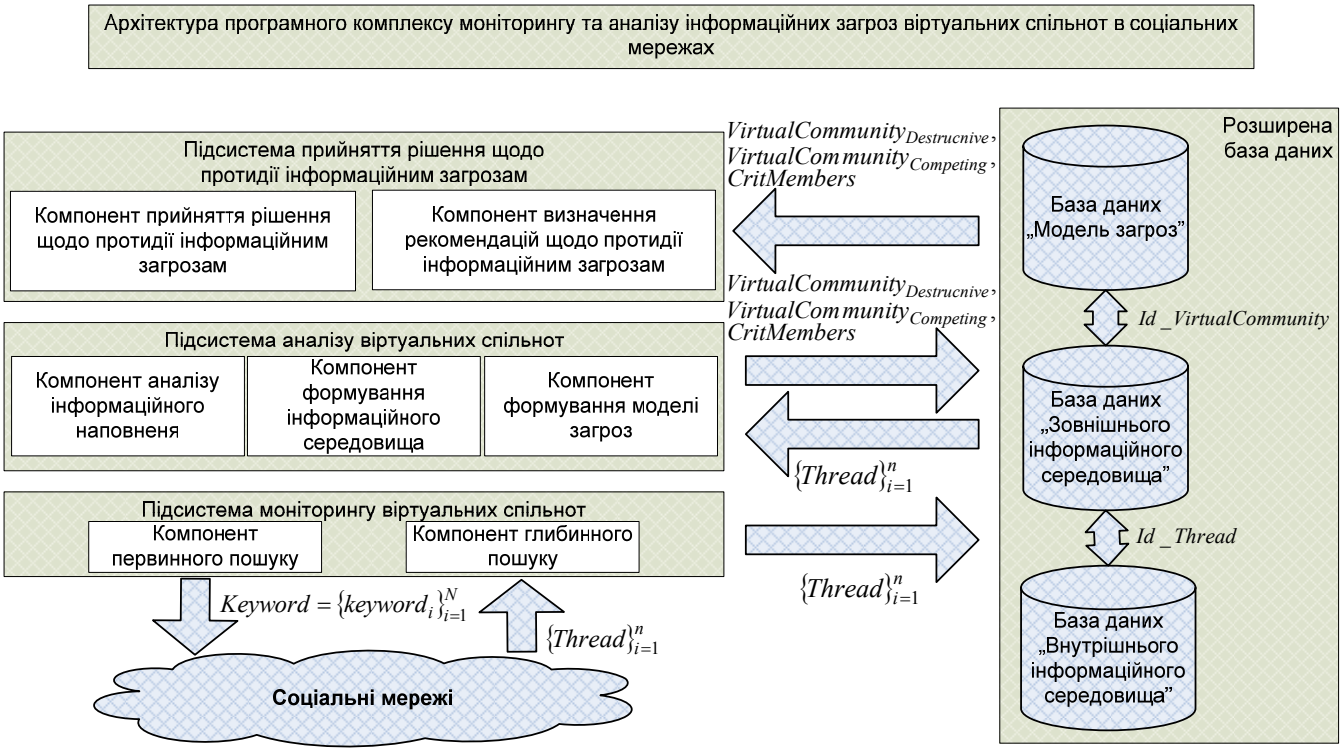

Рис. 9. Архітектура програмного комплексу моніторингу та аналізу інформаційних загроз віртуальних спільнот у соціальних мережах

Програмний комплекс відповідно до завдань, які виникають у процесі виявлення та протидії ІЗ ВС у соціальних мережах, складається з трьох підсистем: підсистема моніторингу ВС, призначена для пошуку дискусій у соціальних мережах відповідно до їх ІН; підсистема аналізу ВС, що слугує для аналізу ІН з метою формування ІС ВС; підсистема прийняття рішення щодо протидії ІЗ ВС у соціальних мережах, призначена для оцінювання ІЗ та визначення рекомендацій щодо ІВ на структуру ВС в соціальних мережах.

Основою програмно-алгоритмічного комплексу автоматизації моніторингу та аналізу ІЗ ВС у соціальних мережах стали запропоновані у попередніх розділах методи та алгоритми виявлення та оцінки ІЗ ВС у соціальних мережах.

Для обліку даних у комплексі використовується розширена база даних, структура якої ґрунтується на побудованій у другому розділі формальній моделі ІС ВС.

У розділі описано використання окремих результатів дисертаційних досліджень під час реалізації державної інформаційної політики.

ОСНОВНІ РЕЗУЛЬТАТИ ТА ВИСНОВКИ

У дисертаційній роботі розв’язано актуальну наукову задачу розроблення методів і засобів виявлення та оцінки ІЗ ВС у соціальних мережах. У роботі отримано такі основні наукові та практичні результати.

1. У результаті аналізу ВС в інтернет середовищі встановлено, що вони створюють нові загрози інформаційній безпеці держави. Дослідження сучасної теоретичної та практичної бази, систем та методів протидії деструктивному впливу в соціальних мережах показали неможливість виявлення та оцінки ІЗ ВС у соціальних мережах. Таким чином виникла необхідність щодо розробки методів і засобів виявлення та оцінки ІЗ ВС в інтернет середовищі соціальних мереж.

2. Удосконалено модель ВС за допомогою розширення її до моделі ІС ВС в соціальних мережах, що включає моделі зовнішнього та внутрішнього ІС, яка стала основою для розроблення структури бази даних щодо обліку та аналізу ІЗ ВС у соціальних мережах;

3. Уведено показник ІЗ ВС в соціальних мережах, шляхом визначення цінності ВС, що враховує структуру, кількість учасників та якість ІН сторінок дискусій ВС, та став основою для методів щодо прийняття рішення з протидії ІЗ ВС у соціальних мережах та визначення рекомендацій щодо ІВ на структуру ВС в соціальних мережах;

4. Розроблено метод щодо прийняття рішення з протидії ІЗ ВС у соціальних мережах шляхом об’єднання показників ІЗ, для яких визначення критичних цінностей ВС ґрунтується на встановленні експертами кількості учасників ВС, при якій реалізовується ІЗ, та загальній кількості учасників деструктивної та конкурентної ВС, що дало змогу надати рекомендації щодо прийняття рішення з протидії ІЗ ВС у соціальних мережах;

5. Отримали подальший розвиток графові моделі соціальних мереж на основі матричного представлення графів, які завдяки врахуванню характеристик моделі ІС ВС та запропонованого показника ІЗ, стали основою для розробки методу прийняття обґрунтованих рішень щодо вибору дискусій ВС для ІВ.

6. Розроблено архітектуру програмно-алгоритмічного комплексу моніторингу та аналізу ІЗ ВС у соціальних мережах, функціональність якого базується на запропонованих у роботі методах та алгоритмах, що дає змогу організувати виявлення та оцінку ІЗ ВС у соціальних мережах.

7. Розроблено стратегії протидії ІЗ ВС у соціальних мережах відповідно до правил протидії держави ІЗ ВС у соціальних мережах, що дало змогу вибору підходів щодо протидії ІЗ ВС у соціальних мережах.

8. Розроблено алгоритми пошуку сторінок дискусій у соціальних мережах з використанням розширених можливостей ГПС та запитів API-методів соціальних мереж, які дають змогу виявити сторінки дискусій у соціальних мережах відповідно їх ІН.

9. Розроблено алгоритм формування ІС ВС в соціальних мережах, шляхом застосування кластеризації сторінок дискусій у соціальних мережах відповідно до їх ІН та розподілу сторінок дискусій в залежності від напряму ІН для розподілу сторінок дискусій на деструктивну та конкурентну ВС.

10. Проведені експериментальні дослідження запропонованих методів і засобів, які підтвердили достовірність теоретичних і практичних результатів дисертаційної роботи щодо можливості виявляти та оцінювати ІЗ ВС в інтернет середовищі соціальних мереж. Зазначені результати впроваджені у діяльність управління інформаційних технологій Міністерства оборони України та управління Служби безпеки України у Львівський області, що підтверджено відповідними актами впровадження.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Гумінський Р. В. Віртуальні спільноти, як суб'єкт інформаційної безпеки держави / Р. В. Гумінський // Захист інформації. – 2012. – № 3 (56). – С. 18 – 25.

2. Пелещишин А. М. Загрози інформаційної безпеки держави в соціальних мережах / А. М. Пелещишин, Р. В. Гумінський // Наука і техніка Повітряних Сил Збройних Сил України. – 2013. – 2(11). – С.192 – 199.

3. Пелещишин А. М. Пошук сторінок дискусій в соціальних мережах глобальними пошуковими системами / А. М. Пелещишин, Р. В. Гумінський, О. Ю. Тимовчак-Максимець // Безпека інформації. – 2013. – № 3 (19). – С. 181 – 187.

4. Пелещишин А. М. Модель інформаційного середовища віртуальної спільноти / А. М. Пелещишин, Р. В. Гумінський // Східно-Європейський журнал передових технологій. – 2014. – № 2/2 (68). – С. 10 – 16.

5. Huminskyi R., Peleshchyshyn A. An assessment of informational threat in the functioning process of virtual community [Electronic resourse] // Cybernetic Letters, 2014. – Mode of access: http://www.cybletter.com. Last access: 2014. – Title from the screen.

6. Пелещишин А. М. Визначення рекомендацій щодо інформаційного впливу на структуру віртуальної спільноти / А. М. Пелещишин, Р. О. Корж, Р. В. Гумінський // Безпека інформації. – 2014. – № 3 (20). – С. 264 – 273.

7. Huminskyi R.V., Peleshchyshyn A.M. and Holub Z. Suggestions for Informational Influence on a Virtual Community // International Journal of Computer Science and Business Informatics, 2015. – Vol. 15. – No. 1, pp. 47 – 65.

8. Гумінський Р. В. Методика прийняття рішення щодо протидії інформаційним загрозам віртуальних спільнот / Р. В. Гумінський // Східно-Європейський журнал передових технологій. – 2015. – № 2/2 (74). – С. 4 – 8.

9. Гумінський Р. В. Система розвідки та моніторингу інтернет середовища / Гумінський Р. В. / Проблемні питання розвитку озброєння і військової техніки: матеріали міжвідомчої наук.-техн. конференції, Київ, 17-20 груд. 2012 р. / ЦНДІ ОВТ. – Київ, 2012. – С. 217 – 218.

10. Пелещишин А. М. Системи моніторингу та протидії інформаційним загрозам у віртуальних спільнотах / А. М. Пелещишин, Р. В. Гумінський // «IV Січневі Гіси»: інтелектуальна оборона: зб. праць наук.-практ. форуму, Львів, 22-24 січ. 2013 р. / АСВ. – Львів, 2013. – С. 45 – 47.

11. Пелещишин А. М. Визначення інформаційної загрози процесу функціонування віртуальних спільнот / А. М. Пелещишин, Р. В. Гумінський // Новітні технології – для захисту повітряного простору: тези доповідей Дев'ятої наукової конференції Харківського університету Повітряних Сил імені Івана Кожедуба, Харків, 17-18 квіт. 2013 р. / ХУПС. – Харків, 2013. – С.176.

12. Пелещишин А. Вибір складових показника інформаційної загрози процесу функціонування віртуальних спільнот / А. Пелещишин, Р. Гумінський // Інформація, комунікація, суспільство 2013 : матеріали 2-ї Міжнародної наукової конференції ІКС-2013, Львів, Славське, 16-19 трав. 2013 р. / Національний університет «Львівська політехніка». – Львів, 2013. – С. 100 – 101.

13. Пелещишин А. М. Алгоритми пошуку сторінок дискусій в соціальних мережах глобальними пошуковими системами / А. М. Пелещишин, О. Ю. Тимовчак-Максимець, Р. В. Гумінський // Проблемні питання розвитку озброєння і військової техніки: матеріали IV наук.-техн. конференції, Київ, 16-20 груд. 2013 р. / ЦНДІ ОВТ. – Київ, 2013. – С. 184 – 185.

14. Пелещишин А. М. Вибір стратегії інформаційного впливу на інформаційне середовище віртуальної спільноти / А. М. Пелещишин, Р. В. Гумінський // 3rd International academic conference «Information, Communication, Society» ICS-2014, Львів, Славське, 19-21 трав. 2014 р. / Національний університет «Львівська політехніка». – Львів, 2014. – С. 30 – 31.

15. Пелещишин А. М. Оцінка інформаційних загроз процесу функціонування віртуальних спільнот / А. М. Пелещишин, Р. В. Гумінський // Безпека інформаційних технологій «ITSEC-2014»: матеріали IV міжнар. наук.-техн. конференції, Київ, 21-24 трав. 2014 р. / НАУ. – Київ, 2014. – С. 26 – 27.

16. Huminskyi R.V. Algorithm of search results clusterization / R. V. Huminskyi, O. M. Sovhar // Перспективи розвитку озброєння та військової техніки Сухопутних військ: матеріали міжнар. наук.-техн. конференції, Львів, 14-15 трав. 2015 р. / АСВ. – Львів, 2015. – С. 175 – 176.

17. Гумінський Р. В. Підходи щодо визначення критичної цінності віртуальної спільноти в соціальних мережах / Р. В. Гумінський // Інформаційна безпека у воєнній сфері. Сучасний стан та перспективи розвитку: матеріали міжвідомчої наук.-практ. конференції, Київ, 31 берез. 2015 р. / НУОУ. – Київ, 2015. – С. 104 – 107.

18. Пелещишин А. М. Архітектура програмного комплексу моніторингу та аналізу інформаційних загроз у віртуальних спільнотах / А. М. Пелещишин, Р. В. Гумінський // 4th International academic conference «Information, Communication, Society» ICS-2015, Львів, Славське, 20-23 трав. 2015 р. / Національний університет «Львівська політехніка». – Львів, 2015. – С. 20 – 21.

АНОТАЦІЯ

Гумінський Р.В. Методи і засоби виявлення інформаційних загроз віртуальних спільнот в інтернет середовищі соціальних мереж. – Рукопис.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю *21.05.01 – інформаційна безпека держави*. – Національний авіаційний університет Міністерства освіти і науки України, Київ, 2016.

Дисертацію присвячено розробленню методів і засобів виявлення та оцінки інформаційних загроз віртуальних спільнот. У роботі побудована формальна модель інформаційного середовища віртуальної спільноти, яка включає моделі внутрішнього та зовнішнього інформаційного середовища. Запропоновано показник інформаційної загрози шляхом визначення цінності віртуальної спільноти, з урахуванням кількості учасників віртуальної спільноти, структуру зв'язків між дискусіями у віртуальній спільноті та якість інформаційного наповнення сторінок дискусій. Розроблено метод

щодо прийняття рішення з протидії інформаційним загрозам віртуальних спільнот та метод прийняття обґрунтованих рішень щодо вибору дискусій віртуальної спільноти для інформаційного впливу. Розроблено алгоритми пошуку сторінок дискусій віртуальної спільноти з використанням формалізованих запитів глобальних пошукових систем та запитів API-методів соціальних мереж, відповідно до їх інформаційного наповнення та алгоритми формування інформаційного середовища віртуальної спільноти. Розроблено архітектуру програмно-алгоритмічного комплексу моніторингу та аналізу інформаційних загроз віртуальних спільнот у соціальних мережах.

Ключові слова: Інтернет, соціальна мережа, віртуальна спільнота, інформаційні загрози.

АННОТАЦИЯ

Гуминский Р.В. Методы и средства обнаружения информационных угроз виртуальных сообществ в интернет среде социальных сетей. – Рукопись.

Диссертация на соискание учёной степени кандидата технических наук по специальности *21.05.01 – информационная безопасность государства*. – Национальный авиационный университет Министерства образования и науки Украины, Киев, 2016.

Диссертация посвящена разработке методов и средств выявлению, и оценке информационных угроз виртуальных сообществ. В работе построена формальная модель информационной среды виртуального сообщества, которая включает модели внутренней и внешней информационной среды. Предложен показатель информационной угрозы путем определения ценности виртуального сообщества с учетом количества участников виртуального сообщества, структуры связей между дискуссиями в виртуальном сообществе и качества информационного наполнения страниц дискуссий. Разработаны метод для принятия решения по противодействию информационным угрозам виртуальных сообществ и метод принятия обоснованных решений по выбору дискуссий виртуального сообщества для информационного воздействия. Разработаны алгоритмы поиска страниц дискуссий виртуального сообщества, с использованием формализованных запросов глобальных поисковых систем и запросов API-методов социальных сетей, в соответствии с их информационным наполнением и алгоритмы формирования информационной среды виртуального сообщества. Разработана архитектура программно-алгоритмического комплекса мониторинга и анализа информационных угроз виртуальных сообществ в социальных сетях.

Ключевые слова: Интернет, социальная сеть, виртуальное сообщество, информационные угрозы.

ABSTRACT

Huminskyi R.V. Methods and means of detection to information threats to virtual communities in the social networks internet environment. – Manuscript.

Thesis for a Ph.D. degree in speciality *21.05.01 – information security of the state*. – National Aviation university of the Ministry of Education and Science of Ukraine, Kyiv, 2016.

The dissertation is dedicated to the solution of an essential scientific task of development of methods and techniques for detection and assessment of information threats of virtual communities in the social networks internet environment.

The first chapter provides analysis of virtual communities as objects of informational security. Threats to informational security that may occur in the informational content of virtual communities have been considered. Regulations of state counteraction against information threats in virtual communities have been considered.

In the second chapter the formal model of the virtual community information environment which consists of internal and external information spaces has been designed. Main characteristics of the virtual community have been defined. Employing the model of the virtual community information environment indicator of the information threat has been offered on the basis of this information which is based on the virtual community value determination, which considers number of virtual community participants, structure of connections between the discussions in virtual community and the quality of information content. Approaches for determining critical value of virtual community have been developed.

Methods and means of acquisition and assessment of information communities' virtual threats have been developed in the third chapter. Algorithms of search of pages of virtual community discussion depending on their information content using formalized requests for global search engine Google have been proposed. The structure of search robot for the in-depth search, functioning of which is based on the usage of requests be API-methods of social networks has been developed. The algorithm of forming information environment according to information content of discussion pages and degree of correspondence thematic line has been developed. Using the indicator of the information threat a method of decision making on virtual communities information threats counteraction has been developed by means of merging information threat indicators, for which the definition of critical values of virtual community is based on establishing the number of virtual community participants at which the realization of the virtual threat occurs, as well as the general number of participants of destructive and competitive virtual threats. Using graph models of social networks based on matrix graph presentation and proposed indicator of informational threat, a method of grounded decisions making on the selection of discussions of virtual community for information influence has been developed.

The fourth chapter provides description of the architecture of program-algorithm complex of monitoring and analysis of information threats of virtual communities in social networks, functioning of which is based on the developed methods and means of acquisition and assessment of information threats in social networks internet environment, namely their integral components, functions and technical aspects of realization. Distributed database, which structure is based on the formal model of information environment virtual community model, designed in the second chapter, has been created.

Experimental research of proposed methods and means, which prove the validity of theoretical and practical results of the thesis concerning the capability to detect and assess information threats of virtual communities in social networks internet environment has been done.

Key words: Internet, social network, virtual community, information threats.

Підписано до друку 02.02.16. Зам. №02-02(1)/16.
Формат 60х84/16. Обл. вид. арк. 1,20. Наклад 100 прим.
Друк «НВФ «Славутич-Дельфін».
пр-т Космонавта Комарова, 1.
Тел./факс: 406-74-41