# ТЕХНОЛОГІЯ ВИЯВЛЕННЯ ОРГАНІЗАЦІЙНИХ ОЗНАК ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ У СОЦІАЛЬНИХ ІНТЕРНЕТ-СЕРВІСАХ

**УДК004.738.5:004.056.5**

**МОЛОДЕЦЬКА Катерина Валеріївна**
к.т.н., доцент кафедри комп'ютерних технологій і моделювання систем,
Житомирський національний агроекологічний університет
**Наукові інтереси:** математичне моделювання, системний аналіз, інформаційна безпека.

## ВСТУП

Сьогодні соціальні інтернет-сервіси (СІС) увійшли практично у всі сфери суспільного життя і є ефективними засобами комунікації між учасниками віртуальних спільнот, яких в [1] прийнято називати акторами. Перевагами СІС є високі темпи поширення контенту між акторами, транскордонні можливості організації акторів у групи за спільними інтересами тощо. Однак, завдяки високій популярності СІС останнім часом стали засобом проведення інформаційних операцій проти людини, суспільства, держави [2, 3]. У [4] показано, що залежно від поставленої мети інформаційні операції у СІС розрізняються за способом реалізації: інформаційні операції через окремих авторитетних акторів або провідні віртуальні спільноти; несанкціонований доступ до акантів і кібератаки на них; розголошення від імені акторів інформації з обмеженим доступом; розповсюдження акторами шкідливого програмного забезпечення тощо.У свою чергу, досвід «гібридної війни» з Російською Федерацією показав також, що увесь спектр інформаційних операцій у СІС має ряд характерних ознак, встановлення особливостей і дослідження яких може бути використано для організації ефективної протидії [2].З метою поширення у СІС контентудеструктивного змісту суб'єкти інформаційних операцій використовують різноманітні методи, засоби і технології інформаційного впливу, що істотно ускладнює процедури їх виявлення,оцінювання та протидію.Тому своєчасне виявленняознак інформаційних операційє актуальним теоретико-прикладним завданням, яке потребує свого розв'язання на шляху вирішення проблеми забезпечення інформаційної безпеки держави.

**Аналіз останніх досліджень і публікацій** показав, що сьогодні не існує однозначного переліку ознак, які характеризують інформаційнуопераціюв СІС.Поряд з тим, проблемі виявлення інформаційних операцій, наприклад,у засобах масової інформації (ЗМІ)присвячено публікаціїпрофесора Д. Ланде та його наукової школи. Так, з цією метою ними застосовуєтьсятеоріяфракталів і вейвлет-аналіз [3, 5]. Однак, запропонований підхід доцільно застосовувати для аналізу апостеріорної інформації.Його використання ускладнюється у випадку інтенсивних швид-

коплинних інформаційних акцій, які описуються часовими рядами малої довжини.Питання виявлення інформаційних загроз віртуальним спільнотам в соціальних мережах розглянуто в працях професора А. Пелещишина і Р. Гумінського [6, 7]. Авторами запропоновано модель протиборства двох антагоністичних віртуальних спільнот на основі показника їх цінності і теоретико-множинного підходу. Недоліками запропонованих колективом авторів методів є істотне обмеження врахованого числа загроз акторам віртуальних спільнот і ознак інформаційних впливів у СІС. У публікаціях[8, 9] висвітленоособливості виявлення інформаційного впливу в СІС і3МІ з метою детектування ознак маніпулювання суспільною свідомістю. Але автори не розкриваютьметодику детектування таких загроз для їх подальшої нейтралізації на практиці.

Загальним недоліком існуючих досліджень щодо виявлення і оцінювання загроз інформаційній безпеці держави у СІС є відсутність комплексного підходу, який узагальнює різні ознаки інформаційних операцій. Аналіз особливостей проведених інформаційних операцій у СІС [7, 9-12] показує, що вони пов'язані з сукупністю окремих ознак, повне врахування яких в процесі функціонуванні системи інформаційної безпеки держави набуває вигляду задачі експоненціальної складності.Тому перспективним напрямком досліджень є групування ознак інформаційних операцій за спільними ознаками з подальшим їх дослідженням.

**Метою** статті є розробленнятехнології виявлення організаційних ознак інформаційних операцій у СІСдля підвищення ефективності функціонування системи забезпечення інформаційної безпеки людини, суспільства, держави.

Для досягнення поставленої мети необхідно розв'язати частинні задачі:

1) проаналізуватиі узагальнити існуючі ознакиінформаційних операцій в СІС;

2) дослідити сучасні програмні засоби моніторингу і управління взаємодією акторів СІС, які використовуються для реалізації інформаційних операцій;

3) встановити організаційні ознакипоширення інформаційних операцій в СІС на основі оцінювання контенту, який містить деструктивний інформаційний посил;

4) розробити технологію виявлення організаційних ознак інформаційних операцій в СІС.

## ОСНОВНА ЧАСТИНА

В СІС джерелом позитивного і деструктивного контенту найчастіше виступають безпосередньо актори віртуальних спільнот, які можуть генерувати контент самостійно, поширювати матеріали ЗМІ або інших акторів, додаючи до них власні коментарі із суб'єктивною оцінкою публікації тощо. Такі дії акторів ускладнюють правові процедури регулювання відносин в інформаційному просторі держави і закладають передумови проявам загроз інформаційній безпеці держави у СІС.

*Інформаційна операціяв СІС*у самому загальному вигляді являє собою взаємопов'язаний комплекс інформаційних акцій з маніпулювання контентом, якийцілеспрямовано здійснюється для досягнення поставленої метишляхом прихованого впливу на акторів віртуальних спільнот і управління індивідуальною чи суспільною свідомістю [8, 10]. Серед особливостей інформаційних операційв СІС виділяють [13]:прихований характер

проведення; транскордонність і масштабність; застосування значних інформаційних ресурсів; цілеспрямованість та вибірковість інформаційного впливу тощо.

Узагальнюючи відомі підходи [7-10, 13] до виявлення деструктивних інформаційних операцій у СІС встановлено, що їх ознаки доцільно об'єднати у групи за такими характеристиками.

1. *Організаційні* ознаки, які вказують на цільове використання інформаційних ресурсів і спеціального програмного забезпеченняу СІС для досягнення поставленої мети. Суб'єкти інформаційних операцій об'єднуються у групи з горизонтальним поділом функцій між собою і використовують диференційований підхід залежно від особливостей об'єктів маніпуляцій.Такі групи координуються і управляються на вищому ієрархічному рівні та використовують методи й засоби впливу залежно від поточної обстановки інформаційного середовища.

2. *Змістовні* ознаки інформаційних операцій характеризують наявність у контенті, що поширюється у СІС, деструктивного інформаційного посилу, який застосовується для впливу на акторіввіртуальних спільнот. Часто деструктивний інформаційний посил формується на основі актуальної і критичної для акторів тематики. Виявлення таких ознак загроз пов'язане з аналізом природомовних текстів у СІС.

3. *Маніпулятивні* ознаки інформаційних операцію контентіє індикатором застосування технологій прихованого управління акторами СІС чи сугестії для проявув них бажаних психічних станів, реакції на поширюваний контент, впливу на свободу вибору тощо. Маніпулятивні ознаки проявляються емоційним перенасиченням контенту віртуальних спільнот, наявністю риторичних запитань, оцінювальних суджень тощо.Приховування такого впливу на акторів є умовою успіхупроведення інформаційної операції, якщо об'єкт впливу не підозрює про маніпулювання і вважає, що події розвиваються природно та невідворотно.

4. Оцінка *актора чи віртуальної спільноти-джерела контенту* вказує на можливих авторів чи поширювачів деструктивного інформаційного посилу і зв'язки між ними.Така оцінка полягає у встановленні першоджерела досліджуваного контенту, аналізі достовірності та виявленні випадків його залучення до інформаційних операцій чи акційв минулому.

Дослідження оперативної робочої групи зі стратегічних комунікацій *EastStratComTaskForce*[14], яка відстежує російську пропаганду в медіапросторі європейських країн, свідчать, що Україна залишається головною ціллюїх інформаційних операцій. При цьому одним із найбільш ефективних інструментівпоширення суб'єктами інформаційних операційдеструктивного контенту є СІС, для чого використовуються спеціальні інформаційні ресурси.Так,ще в2012 р. компанією «*Iтеранет*»на замовлення Служби зовнішньої розвідки Російської Федераціїрозпочато реалізацію проекту з «вироблення нових методик моніторингу блогосфери» [15,16].

Спеціалізований програмний комплекс складається з трьох модулів – «*Диспут*», «*Монитор-3*» і «*Шторм-12*». Модуль «*Диспут*» використовується для моніторингу блогосфери, «дослідження процесів формування співтовариств інтернет-центрів поширення інформації в соціальних мережах» і «визначення факторів, що впливають на популярність і поширюваність інформації»

[15, 16]. Отримані на попередньому етапі дані обробляє «*Монитор-3*», завданням якого є «розробка методів організації та управління в інтернеті віртуальною спільнотою залучених експертів, які передбачають постановку завдань, контроль роботи в соціальних медіа та регулярне отримання від експертів інформації в заданих предметних областях» [15, 16].Отримані від експертів дані поширюються модулем «*Шторм-12*», перед яким ставляться завдання «автоматизованого поширення інформації в великих соціальних мережах та організації інформаційної підтримки заходів по підготовленим сценаріями впливу на задану масову аудиторію соціальних мереж» [15, 16].Крім Російської Федерації, Міністерством оборони і спецслужбамиСША також активно розробляються спеціалізовані програмні та апаратні засоби для управління взаємодією акторів у СІС [16]. В 2011 р. розроблено програмний комплекс *SMISC* (Соціальні медіа в стратегічній комунікації) для відслідковування ворожої до США пропаганди і допомоги ведення контрпропаганди в *Facebook*, *Twitter*, *YouTube* та інших популярних СІС.В процесі функціонуванні *SMISC* використовуються наступні технології: лінгвістичний аналіз; аналіз трендів, настроїв, громадської думки і «культурних наративів»; автоматичне створення контенту; боти і краудсорсінг [17].Також у 2010 р. в США впроваджено програмний комплекс *PersonaManagementSoftware* з метою створення і поширення через мережу ботів заданого контенту для формування громадської думки з актуальних питань [16]. Система функціонує за участі астротерферів, кожен з яких формує групу соціальних ботів здесяти віртуальних акаунтів.Програмний комплекс призначений для підміни IP-адреси бота та його соціалізації.

Отже, як показав аналіз можливостей проведення держав світу,для проведення інформаційних операцій у СІС використовується спеціалізоване програмне забезпечення, яке використовує соціальних ботів для поширення заданого контенту.

*Ботами в СІС*будемо називати спеціалізовані програмні комплекси, які призначені для автоматичного виконання функцій актора засобами інтерфейсу СІС відповідно до поставленого завдання. До таких функційактора відносять публікаціїзаданого контенту, ґенерацію зв'язків з іншими акторами, додавання коментарів, гештегіві відміток тощо. Залежно від задач, які ставляться перед ботами у СІС, виділяють наступніїх види [18-20] (рис. 1).

*Технічні боти* – використовуються для виконання одноманітних дій у СІС, наприклад, збільшення кількості схвальних відгуків («накручення лайків») для її просування у новинній стрічці, додавання простих односкладних коментарів або повторної публікації дописів («репостів»). Такі дії справляють на акторів враження високого рівня обговорення окремої теми та її актуальності й критичності для суспільства. Також технічні боти виконують функцію соціалізації інших акторів або ботів СІС шляхом додавання їх в список «друзів» чи «послідовників» для підвищення рівня довіри до них віртуальної спільноти.

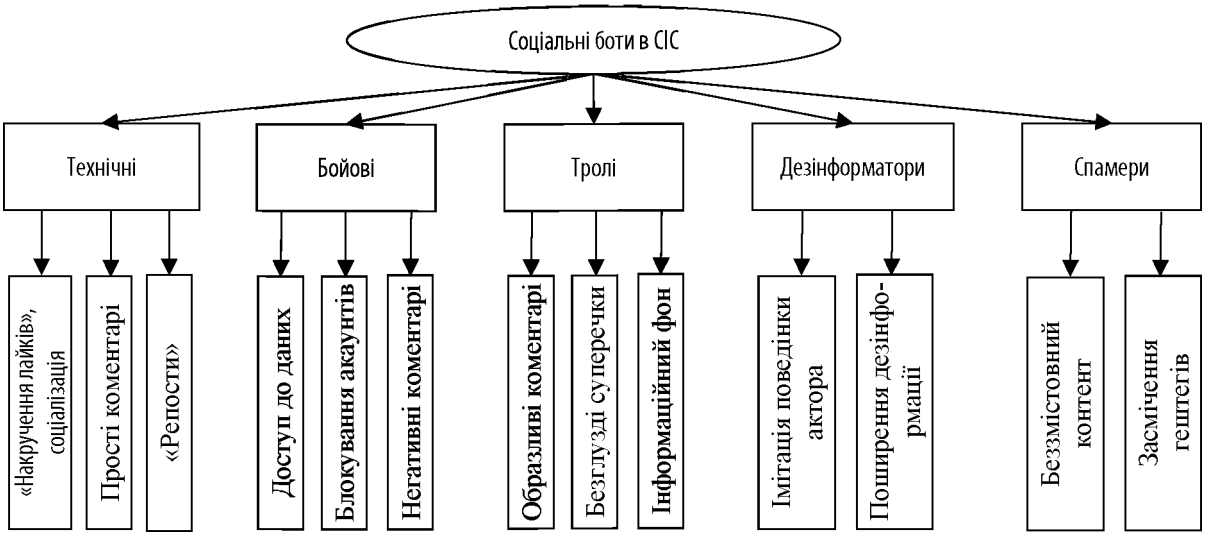


***Рис. 1. Види соціальних ботів у СІС***

*Бойові боти* призначені для ведення відкладених активних дій з обліковими записами акторів СІС. Такі боти тривалий час не проявляють своїх справжніх намірів. Бойові боти отримують доступ до персональних даних актора внаслідок утворення зв'язку («друзі», «послідовники») і в момент початку інформаційної операції залучаються для його блокування, поширення заданого контенту, негативних коментарів тощо.

*Тролі*представляють собою найбільш агресивний тип ботів у СІС. Такий тип ботів ґрунтується на застосуванні семантичних ядер, які містять текстові набори ключових слів на задану тематику. За семантичним ядром боти знаходять необхідні публікації у СІС, публікують образливі і ворожі коментарі, провокують безглузді суперечки серед віртуальної спільноти, створюють інформаційний фон для поширення деструктивного інформаційного посилу.

*Дезінформатори* представляють собою тролів, які імітують діяльність реальних акторів СІС, а в деякий момент часу публікують заданий контент для інформаційного впливу на віртуальну спільноту. Часто цей контент міститьсимулякр–опис реальності, якої не існує, або дезінформацію. У випадках успішної інформаційної операції публікації ботів-дезінформаторів поширюються у СІС, висвітлюються у ЗМІ тощо до їх спростування.

*Боти-спамери* застосовуються у СІС для поширення беззмістовного контенту: публікація старихпублікацій абоїх уривків тощо. Метою даного виду ботів є ускладнення сприйняття акторами контенту, засмічення гештегів через публікацію під ним невідповідного змісту.

Слід зазначити, що соціальні боти можуть відноситися й до інших видів, окрім розглянутих (див. рис. 1), а алгоритми їх функціонування змінюються відповідно від поставлених завдань. У ролі тролямо-жуть виступати реальні люди, які реагують на заданий ланцюг логічних конструкцій. Така поведінка пояснюється впливом маніпулятивних технологій на свідомість акторів, а нездатність до критичного сприйняття ними контенту в СІС компенсується агресивною поведінкою і нападами на співрозмовників.

Результати досліджень Латвійського Центру НАТО з покращення стратегічних комунікацій [14] показали, що ознаками гібридних тролів у СІС є: коментарі публікацій інших акторів або віртуальних спільнот великої довжини; зміст таких коментарів не відповідає тематиці діалогу; прояви ворожості і агресивності; містять велику кількість граматичних помилок тощо. Однак, наявність усіх перерахованих ознак у актора СІС не доводить, що він є гібридним тролем.

Внаслідок аналізу і узагальнення ознак застосування спеціалізованих інформаційних ресурсів у СІС і ботів зокрема [14, 21-25]розроблено технологіювиявлення організаційних ознак інформаційних операційв СІС. Її сутність зводиться до такого.

***Етап 1.*** *Виявлення дублікатів публікацій контенту або коментарів акторів у СІС.*Для реалізації даного етапу необхідно скористатися алгоритмом, який задовольняє умову швидкодії для оперативного моніторингу СІС в інформаційномупросторі. Тому серед відомих підходів до виявлення неповних дублікатів [20-21] обрано алгоритм шинглів («лусочок»).Сутність алгоритму полягає у виявленні повторів ланцюгів сліву досліджуваному контентіта наведена нижче [26, 27].

*Крок 1*полягає в канонізації досліджуваноготекстового контенту $T_j$, $j=1...k$ шляхом його приведення до заданого нормального виду $T_j \to T_{jnorm}$. З цією метою видаляються смайли, хештеги, HTML теги, гіперпосилання, знаки пунктуації, прийменники, сполучники й інші компоненти, які не несуть змістовного навантаження контенту. В окремих випадках слід здійснювати нормалізацію іменників до однини називного відмінка.

*Крок 2* призначений для розбиття нормалізованого тексту $T_{jnorm}$ на шингли $Sh_{ij}$, де $i=L-N+1$ – кількість шинглів; $L$ – довжина тексту, який досліджується; $N$ – довжина шингла. Вибір значення довжини шингла $N$ залежить від довжини самого тексту $L$ і лежить в інтервалі $N=\overline{5,10}$. Зростання довжини вихідного тексту вимагає збільшення показника $N$.

На *кроці 3*обчислюється гешшинглів $HSh_{ij}^{m}$ текстового контенту, який порівнюється,з використанням $m=84$ функцій (SHA1, HAVAL, MD5, CRC32 тощо) і записується в двовимірний масив даних. Після цього випадково обирають зі збережених гешівшинглів $HSh_{ij}^{m}$ значення для порівняння між собою.

Заключний *крок 4*зводиться дорозрахунку показника відповідності $P$ порівнюваного текстового контенту $T_j$ як співвідношення кількості $S$гешівшинглів $HSh_{ij}^{m}$ з однаковими значеннями до їх загальної кількості $m$, тобто

$$P=\frac{S}{m}100\%.$$

Таким чином, виявлення дублікатів контенту у віртуальних спільнотах свідчить про використання спеціалізованого програмного забезпечення і ботів зокрема для поширення публікацій на задану тематику і реалізації загроз інформаційній безпеці держави у СІС.

***Етап 2.*** *Розрахунок показників читабельностіпублікацій акторів СІС.* Відомо [28],що індекс читабельності текстів визначає складністьтакого контенту для сприйняття актором віртуальної спільноти. Ефективність використання такого показника для детектування деструктивних інформаційних посилів у СІС пояснюється наявністю мовного бар'єру між українськими користувачами і зарубіжними суб'єктами інформаційних

операцій. Зокрема, для публікації повідомлень українською мовою застосовуються онлайн-сервіси перекладу контенту, які не забезпечують високої якості, погіршують його читабельність, а в окремих випадках, у тому числі й цілеспрямовано, спотворюють зміст.

Серед найбільш поширених показників оцінки читабельності текстового контенту виділяють індекс туманності Ґаннінга, індекс Колеман-Ліу, автоматизований індекс читабельності ARI [28, 29]. В інтересах підвищення ефективності системи інформаційної безпеки держави для широкого класу задач контенту СІС доцільно скористатися показником ARI, який на відміну від інших показників, забезпечує спрощення процедури дослідження складності тексту. Перевагами даного методу є відсутність потреби аналізу виключно значних об'ємів текстових даних і необхідності залученнядо обробки текстових процесорів. Автоматизований індекс читабельності ARI $I_{ARI}$ контенту $T_j$ СІС може бути розрахованийяк [28] із врахуванням особливостей українського алфавіту

$$I_{ARI} = 5,98\frac{C}{W} + 0,63\frac{W}{S} - 27,2,$$

де $C$ – кількість друкованих знаків у текстовому контенті $T_j$, що містяться в СІС, який аналізується;

$W$ – кількість слів у текстовому котенті $T_j$;

$S$ – кількість речень у текстовому котенті $T_j$.

Зростання значення автоматизованого індексу читабельності ARI $I_{ARI}$ показує ускладнення текстового контенту СІС для сприйняття акторів. Однією з причин високого індексу читабельності є публікація контенту актором, який не є носієм мови поширеного матеріалу, тому дозволяє опосередковано детектувати додавання в інформаційне середовище СІС контенту з деструктивним інформаційним посилом.

**Етап 3.** *Ведення діалогу з актором, який аналізується.* Для перевірки актора, чи є він реальною особистістю, а не ботом, доцільно задати йому запитання $Question = \bigcup_k Q_k$ на деяку тематику $k = 1,2,\ldots.$ В більшості випадків поява відповіді на задане запитання неможлива $Answer = \bigcup_k A_k$, $Answer = \varnothing$, що пояснюється вищезгаданим мовним бар'єром ботів і акторів СІС. Іноді сформульована відповідь і її ключові слова можуть не відповідати тематиці запитання, тобто $Q_k \neq A_k^*$.

*Обмеження.* Аналізу підлягає контент СІС текстового типу, а дослідження зображень та відео не проводиться. Вибір контенту для досягнення мети дослідження проводиться експертами або спеціальними підрозділами відповідно до вимог критичності і значущості його тематики для громадянського суспільства.

Технологія виявлення організаційних ознак інформаційних операцій в СІС на основі алгоритму виявлення дублікатів текстового контенту може бути подана у вигляді структурної схеми (рис. 2).

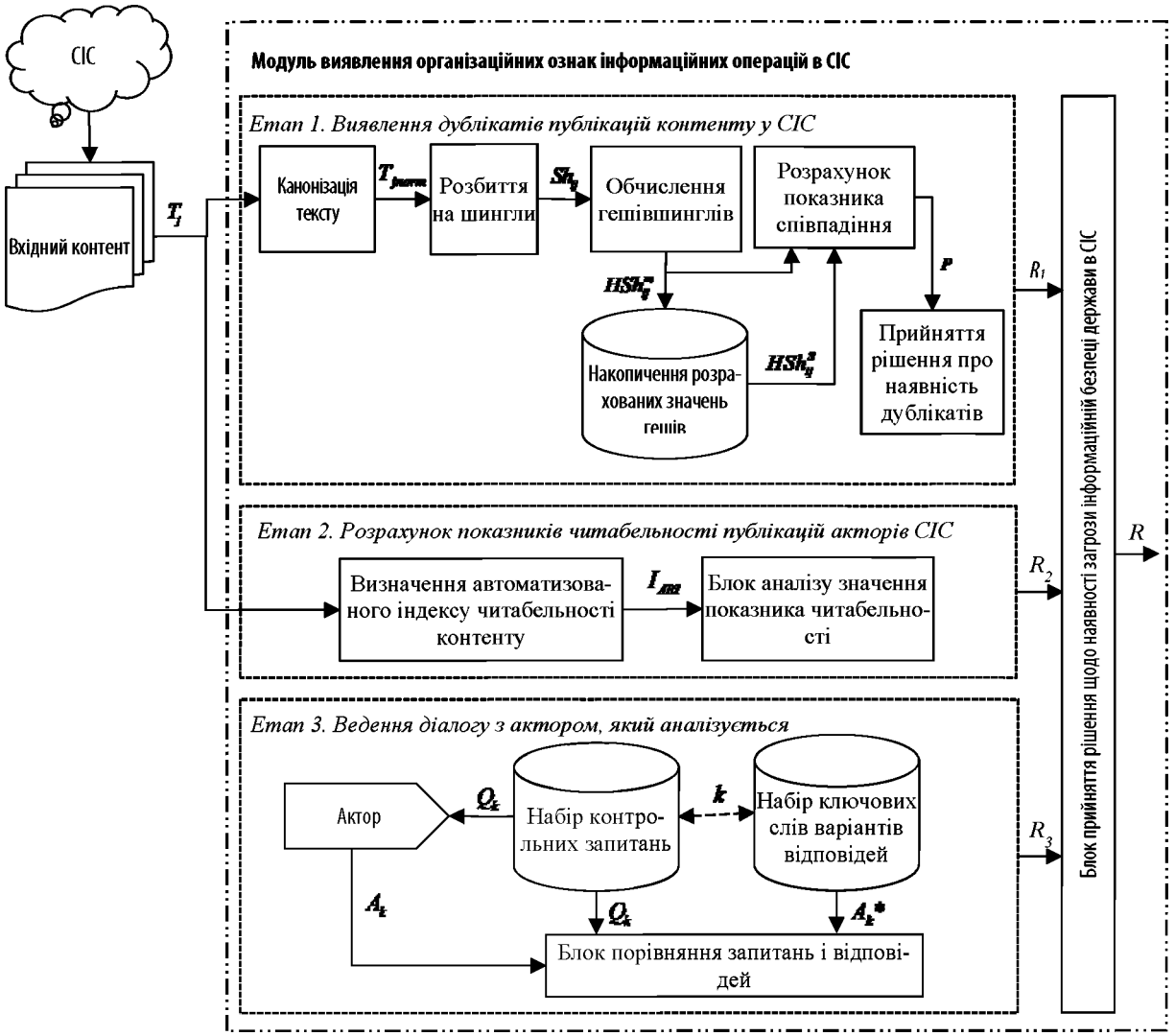


*Рис. 2. Структурна схема технології виявлення організаційних ознак інформаційних операцій в СІС*

Отже, відповідність контентув СІС, який аналізується, усім перерахованимвище ознакам дозволяє зробити висновок про цілеспрямовану інформаційну операцію у віртуальних спільнотах, направлену проти інформаційної безпеки людини, суспільства, держави з використанням суб'єктами інформаційної операції інструментальних засобів спеціального програмного забезпечення. Розроблена технологія в СІС забезпечує формалізацію процесів виявлення інформаційних операцій у розрізі їх організаційних ознак і використання для автоматизації моніторингу національного інформаційного простору. Формування остаточних висновків про проведення інформаційних операцій в СІС досягається в результаті дослідження наявності в контенті змістовних і маніпулятивних ознак, а також оцінки актора або віртуальної спільноти, які його поширюють.

## ВИСНОВОК

Вперше розроблено технологію виявлення організаційних ознак інформаційних операцій в СІС, яка дозволяє автоматизувати процедури раннього виявлення загроз інформаційній безпеці держави у віртуальних спільнотах. Запропонована

технологія відрізняється від існуючих підходів до виявлення інформаційних операцій врахуванням функціонування спеціалізованого програмного забезпечення у СІС для впливу на інформаційний простір і акторів. Розроблена технологія нині реалізується в компонентах системи забезпечення інформаційної безпеки держави й сприяє підвищенню її ефективності, швидкодії та достовірності. Напрямок подальших досліджень полягає у автоматизації процесів змістовного аналізу контенту в СІС для детектування загроз інформаційній безпеці держави.

**ЛІТЕРАТУРА**


1. Hanneman R. A., Riddle M. Introduction to social network methods. – Riverside, CA: University of California, Riverside, 2005. – 322 p.
2. Lipkan V. A. Sutnist hibrydnoi viiny proty Ukrainy //Imperatyvy rozvytku tsyvilizatsii. – 2015. – № 2. – S. 13–16.
3. Horbulin V. P., Dodonov O. H., Lande D. V. Informatsiini operatsii ta bezpeka suspilstva: zahrozy, protydiia, modeliuvannia : monohrafiia. – K. : Intertekhnolohiia, 2009. – 164 s.
4. Molodetska K. V. Uzahalnena klasyfikatsiia zahroz informatsiinii bezpetsi derzhavy v sotsialnykh internet-servisakh // Zakhyst informatsii : zb. nauk. prats. – 2016. – Vyp. 23. – S. 75–87.
5. Dodonov A. G., Lande D. V. Modelirovanie i analiz tematicheskih informatsionnyih potokov // Informatsionnoe protivodeystvie ugrozam terrorizma. – 2013. – № 20. – S. 52–59.
6. Huminskyi R. V. Metody i zasoby vyiavlennia informatsiinykh zahroz virtualnykh spilnot v internet seredovyshchi sotsialnykh merezh : dys. … kand. tekhn. nauk : 21.05.01. – Kyiv, 2016. – 157 s.
7. Peleshchyshyn A. M., Kravets R. B., Sierov Yu. O., Fedushko S. S. Metody vidstezhennia poiavy nebazhanoho informatsiinoho napovnennia Veb-forumu // Visn. Nats. un-tu "Lvivska politekhnika". – 2010. – № 689 : Informatsiini systemy ta merezhi. – S. 303–312.
8. Panchenko V. M., Polevyi V. I. Metodyka vyiavlennia oznak informatsiinoho vplyvu v zasobakh masovoi informatsii // Informatsiina bezpeka liudyny, suspilstva, derzhavy. – 2011. – №3 (7). – S. 70–77.
9. Panchenko V. M. Linhvostatystychni oznaky manipuliuvannia suspilnoiu svidomistiu v zasobakh masovoi komunikatsii // Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony. – 2009. – №1 (4). – S. 81–85.
10. Veprintsev V. B., Manoylo A. V., Petrenko A. I., Frolov D. B. Operatsii informatsionno-psihologicheskoy voynyi: kratkiy entsiklopedicheskiy slovar-spravochnik. – M., 2005. – 496 s.
11. Lipkan V. A., Sopilko I. M., Kirian V. O. Pravovi zasady rozvytku informatsiinoho suspilstva v Ukraini : [monohr.]. – K. : FOP O. S. Lipkan, 2015. – 664 s.
12. Hryshchuk R. V., Danyk Yu. H. Synerhiia informatsiinykh ta kibernetychnykh dii // Trudy universytetu. – K. : NUOU, 2014. – № 6 (127). – S. 132–143.
13. Kushnir O. V. Informatsiini operatsii yak kharakterna osoblyvist suchasnosti – Sait Hlobalnoi orhanizatsii soiuznytskoho liderstva GOAL. – Rezhym dostupu: http://goal-int.org/informacijni-operacii-yak-xarakterna-osoblivist-suchasnosti/ (data zvernennia: 2.07.2016). – Nazva z ekranu.
14. «Gibridnyie trolli» Kremlya: propaganda v deystvii. – Rezhim dostupa: http://trip-trial.blogspot.com/2016/05/Gibridnye-trolli-Kremlja-propaganda-v-dejstvii.html (data obrascheniya: 2.07.2016). – Nazvanie s ekrana.
15. Barabanov I., Safronov I. , Chernenko E. Razvedka botom // Gazeta Komersantъ. – Rezhim dostupa: http://kommersant.ru/doc/2009256 (data obrascheniya: 2.07.2016). – Nazvanie s ekrana.
16. Hryshchuk R. V., Kankin I. O., Okhrimchuk V. V. Tekhnolohichni aspekty informatsiinoho protyborstva na suchasnomu etapi // Zakhyst informatsii. – 2015. – T. 17. – № 1. – S. 80–86.
17. Chernenko E. Agentstvo natsionalnoy dezinformatsii SShA // Gazeta Komersantъ. – Rezhim dostupa: http://kommersant.ru/doc/2009289 (data obrascheniya: 2.07.2016). – Nazvanie s ekrana.
18. Mordiuk A. O. Yak pratsiuvaty z internet-kontentom, shchob ne staty zhertvoiu manipuliatsii: porady zhurnalistam vid vitchyznianykh ta yevropeiskykh ekspertiv // Naukovi zapysky Instytutu zhurnalistyky. – 2014. – T. 56. – S. 240–246.
19. Chistyakov Z. Botyi. S chem ih edyat, ili rukovodstvo k deystviyu // Gazeta dlya biznesa. – Rezhim dostupa: http://maub.com.ua/n/v/2753 (data obrascheniya: 2.07.2016). – Nazvanie s ekrana.
20. Informatsiina viina: 50-tsentova armiia atakuie Tvitter / Sait Teksty.org.ua. – Rezhym dostupu: http://texty.org.ua/pg/blog/lizard/read/52605/Informacijna_vijna_50centova_armija_atakuje_Tvitter (data zvernennia: 2.07.2016 r.). – Nazva z ekranu.
21. Ferrara E., Davis C., Varol O. [and other]. The Rise of Social Bots // Communications of the ACM. – 2016. – № 59(7). – P. 96–104.
22. Wagner C., Mitter S., Körner C., Strohmaier M. When social bots attack: Modeling susceptibility of users in online social networks // Making Sense of Microposts (# MSM-2012). – 2012. – P. 41–48.

23. Zhao D., Traore I., Sayed B., Lu W., Saad S., Ghorbani A., Garant D. Botnet detection based on traffic behavior analysis and flow intervals // Computers & Security. – 2013. – № 39. – P. 2–16.
24. Haustein S., Bowman T. D., Holmberg K., Tsou A., Sugimoto C. R., Larivière V. Tweets as impact indicators: Examining the implications of automated "bot" accounts on Twitter // Journal of the Association for Information Science and Technology. – 2016. – № 67(1). – P. 232–238.
25. Kartaltepe E. J., Morales J. A., Xu S., Sandhu R. Social network-based botnet command-and-control: emerging threats and countermeasures // International Conference on Applied Cryptography and Network Security. – Springer : Berlin Heidelberg, 2010. – P. 511–528.
26. Rodnenko V. Algoritm shinglov dlya veb-dokumentov // Code is Art. – Rezhim dostupa: http://www.codeisart.ru/blog/part-1-shingles-algorithm-for-web-documents/ (data obrascheniya: 2.07.2016 r.). – Nazvanie s ekrana.
27. Lande D. V., Darmohval A. T., Morozov A. Yu. Podhod k vyiyavleniyu dublirovaniya soobscheniy v novostnyih informatsionnyih potokah // Elektronnyie biblioteki: perspektivnyie metodyi i tehnologii, elektronnyie kollektsii (RCDL'2006) : trudyi 8 Vseros. nauch. konf. – Rossiya : Suzdal, 2006. – S. 1–5.
28. Krychkovska A. M., Parashchyn Zh. P., Shved O. V. [ta in.]. Zastosuvannia informatsiinykh tekhnolohii dlia standartyzatsii metodolohii stvorennia navchalnoi literatury // Visn. Nats. un-tu "Lvivska politekhnika". Informatyzatsiia vyshchoho navchalnoho zakladu. – 2014. – № 803. – S. 81–85.
29. William H. DuBay. The Principles of Readability Impact Information. – Costa Mesa, California, 2004. – 73 p.

**Рецензент:** д.т.н., старший науковий співробітник Грищук Р. В.,
начальник науково-дослідного відділу інформаційної та
кібернетичної безпеки наукового центру
Житомирського військового інституту імені С.П. Корольова