

УДК 004.056:004.738.5

Р.В. Гришук¹, К.В. Молодецька²¹ Житомирський військовий інститут імені С.П. Корольова, Житомир² Житомирський національний агроекологічний університет, Житомир

МЕТОД ПРОГНОЗУВАННЯ ДИНАМІКИ ПОШИРЕННЯ КОНТЕНТУ Й ЗАПИТІВ НА НЬОГО ЗА ДАНИМИ КОНТЕНТ-АНАЛІЗУ ПОВІДОМЛЕНЬ У СОЦІАЛЬНИХ ІНТЕРНЕТ-СЕРВІСАХ

Запропоновано методологічний інструментарій для прогнозування динаміки поширення контенту й запитів на нього за даними контент-аналізу повідомлень у соціальних інтернет-сервісах. Застосування метрики самоподібності дозволило виявити постійну складову контент-функції і встановити її природу. В результаті система забезпечення інформаційної безпеки держави набуває нових властивостей для вироблення необхідних механізмів інформаційної протидії.

Ключові слова: соціальний інтернет-сервіс, актори, контент-функція, деструктивний інформаційний посыл, показник Херста, інформаційна безпека, прогнозування, синергетичне управління.

Вступ

У сучасному високотехнологічному суспільстві постійно зростає роль соціальних інтернет-сервісів (СІС) як інструмента масової електронної комунікації між його суб'єктами – громадянами [1–6]. Можливості СІС також використовуються учасниками віртуальних спільнот – акторами [4] й для реалізації особистісних і групових інтересів як окремо взятих громадян та їх соціальних утворень, так і провідних держав світу. Вивчення досвіду подій, які відбулися під час “Арабської весни” [7–9] та під час “Кольорових революцій” [7, 10] дозволяє зробити висновок про те, що СІС відіграють не останню роль і в державоутворюючих процесах.

У період збройної агресії Російської Федерації проти України [11] СІС стали одними з найдієвіших інструментів “гібридної війни” [12, 13]. Так поширення в СІС недостовірного та упередженого контенту призводило й надалі призводить до суттєвого збільшення кількості загроз інформаційній безпеці держави [10, 12, 13]. Аналогічна ситуація характерна і формуванню акторами запитів на відповідний контент. Тому організація ефективної інформаційної протидії неминуче пов'язана зі знаходженням в СІС контенту або запитів на такий контент, що містять такі деструктивні інформаційні посили, його оцінюванням та прогнозуванням динаміки поширення, тобто вирішенням завдань контент-аналізу [14]. Таким чином, прогнозування динаміки поширення контенту або запитів на нього за даними контент-аналізу повідомлень у СІС є актуальним теоретико-прикладним завданням, яке на шляху вирішення проблеми забезпечення інформаційної безпеки держави, потребує свого розв'язання.

Аналіз останніх досліджень і публікацій [1–6, 15] показав, що СІС належать до класу складних

нелінійних динамічних систем, а тому їх можна віднести до високоорганізованих систем з багатьма ієрархічними рівнями управління. Як наслідок, суттєво обмежуються можливості застосування відомих математичних методів і моделей для прогнозування динаміки поширення контенту або запитів на нього в СІС. Також у результаті аналізу встановлено, що для розв'язання поставленого вище завдання найбільш адаптованими є основні положення теорії динамічних систем [16–19], оскільки спостережуваний показник взаємодії акторів в СІС є деякою функцією, яку надалі будемо називати контент-функцією. Тобто, *контент-функція* – це функція, яка в часі описує зміну динаміки поширення контенту або запитів на нього за даними контент-аналізу повідомлень у СІС.

Основною проблемою на шляху визначення контент-функції є те, що закономірності, які описують динаміку процесів, що досліджуються мають прихований характер. У [20, 21] показано, що найбільш перспективним для розкриття прихованих залежностей і виокремлення у них закономірностей процесів є застосування можливостей інтелектуального аналізу і вилучення даних *Data Mining*. З [21] відомо, що в структурі *Data Mining* виділяють дві групи методів – кібернетичні і статистичні, останні з яких забезпечують реалізацію можливостей з дослідження природи взаємодії акторів СІС на основі аналізу часових рядів. Таким чином, контент-аналіз повідомлень в СІС становить значний інтерес з точки зору подальшого прогнозування динаміки поширення контенту в інтересах забезпечення інформаційної безпеки людини, суспільства та держави.

Метою статті є розроблення нового методологічного інструментарію для оперативного і ефективного вивчення й дослідження динаміки поширення контенту або запитів на нього за даними контент-аналізу повідомлень в СІС.

Виклад основного матеріалу

Припущення. Аналіз динаміки зміни показників взаємодії акторів у віртуальних спільнотах у СІС на основі часових рядів в роботі використано для аналітичного дослідження й подальшої екстраполяції показників взаємодії. Передбачається, що реакція акторів на контент у СІС відбувається із деяким запізненням відносно часу його публікації. Тому динаміка взаємодії акторів у СІС описується часовим рядом із запізненням [19, 20]. Виходячи з описаних вище припущень можливо також припустити, що специфіка поширення контенту в СІС або запитів на нього має деякі стійкі тенденції, які тривають значно довше ніж сам процес, який їх утворює. Даний висновок дозволяє висунути гіпотезу дослідження – прогнозування динаміки поширення контенту й запитів на нього за даними контент-аналізу повідомлень у СІС може бути здійснено на основі однієї з відомих метрик самоподібності [22 – 24]. У даній статті в основу такої метрики запропоновано покласти показник Херста [22, 23]. На відміну від

інших метрик самоподібності показник Херста дозволяє встановлювати не тільки трендовість ряду, а й що головне – його природу.

Обмеження. Контент, або запити на нього прогнозування динаміки яких має бути здійснено, містить деструктивні інформаційні посили [10]. Решта контенту в СІС – не розглядається.

Сутність розробленого методу розкрито на рис. 1 у вигляді узагальненої структурної схеми.

Опис узагальненої структурної схеми методу (рис. 1). На акторів віртуальних спільнот у СІС постійно здійснюються цілеспрямовані деструктивні інформаційні впливи, інформаційні посили від джерел загроз інформаційній безпеці, в яких описуються вектором загроз вигляду $D = \{D_1, D_2, \dots, D_\alpha\}$, [10].

Для виявлення відповідного контенту або фіксації кількості запитів на такий контент системою забезпечення інформаційної безпеки використовуються можливості сервісів контент-аналізу повідомлень в СІС.

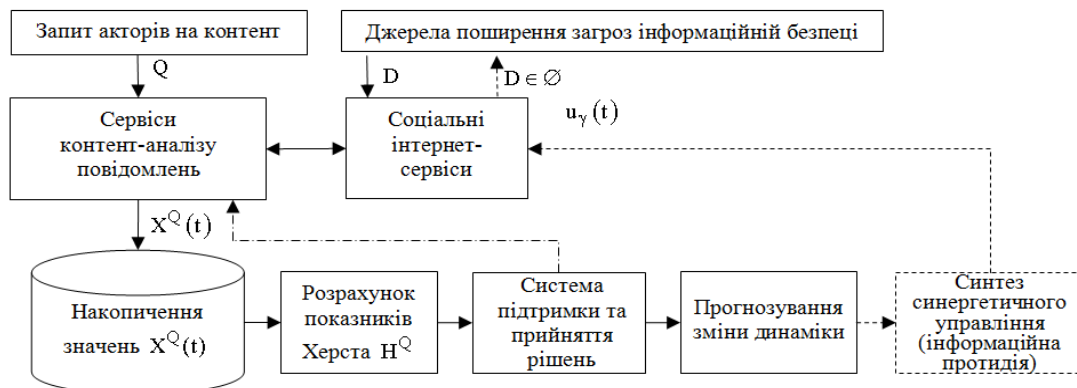


Рис. 1. Узагальнена структурна схема методу

На практиці такими сервісами можуть бути *Socialmention*, *Стрічка.Ком*, *InfoStream*, *Яндекс.Блоги*, *IQBuzz*, *YouScan*, *TweetDeck*, *Wobot*, *SemanticForce* [25] тощо або спеціалізовані інформаційно-аналітичні системи такі як *Призма* [26]. Запити акторів в СІС на контент описуються кортежем Q . Як результат генерування запитів на контент й надходження його від відповідних джерел відбувається зміна динаміки процесів взаємодії акторів $X^Q(t)$. За накопиченими даними надалі розраховуються значення обраної метрики самоподібності – показника Херста H_Q . Після аналізу отриманих значень системою підтримки та прийняття рішень на основі визначених правил приймається рішення про доцільність або недоцільність прогнозування динаміки показників взаємодії акторів в СІС з метою вироблення заходів інформаційної протидії – формування синергетичного управління $u_Y(t)$, спрямованого на керування параметрами взаємодії акторів в СІС й нейтралізацію джерел загроз інформаційній безпеці $D \in \emptyset$.

У випадку персистентності часового ряду $X^Q(t)$ здійснюється екстраполяція одержаних даних на основі одного з обраних методів. У протилежному випадку екстраполяція не проводиться, а продовжується процедура контент-аналізу згідно зі схемою методу (див. рис. 1).

Зміст методу. *Етап 1. Формування контент-функції* полягає у визначенні множини СІС $A = \bigcup_k A_k$, $k = 1, 2, \dots$, для яких проводиться дослідження поширення контенту акторами віртуальних спільнот або запитів та такий контент, що містить деструктивні інформаційні посили. Встановлюється аспект процесів взаємодії акторів СІС із множини параметрів $K = \bigcup_\beta K_\beta$, $\beta = 1, 2, \dots$ для подальшого вивчення. Такими параметрами взаємодії акторів у СІС є: попит на визначений контент; поширення контенту у віртуальних спільнотах СІС тощо.

Задається семантичне ядро $I = \bigcup_n I_n$, $n = 1, 2, \dots$ деструктивного інформаційного посилу

D_α , яке складається з ключових слів для пошуку контенту в СІС. Контент-функцію визначають на заданому часовому інтервалі T_m , $m = 1, 2, \dots$. Тому в формалізованому вигляді запит до сервісу контент-аналізу публікацій акторів у СІС приймає вигляд кортежу Q :

$$Q = \langle A, K, I, T_m \rangle. \quad (1)$$

У результаті виконання запиту одержується контент-функція $X^Q(t)$, $t = 1, \dots, l$, яка визначається на основі кількості тематичних публікацій акторами обраного контенту з деструктивним інформаційним посилом I_n або запитів на нього.

Етап 2. Розрахунок показника Херста. Полягає у встановленні стабільності контент-функції $X^Q(t)$ залежно від кількості публікацій в СІС й ґрунтується на методі Г. Херста (методі R/S-аналізу). Для цього розраховується показник за виразом [24]

$$H^Q = \log(R/S) / \log(l/2), \quad (2)$$

де H^Q – показник Херста для контент-функції $X^Q(t)$; S – середньоквадратичне відхилення контент-функції $X^Q(t)$; R – розкид накопиченого відхилення

контент-функції $X^Q(t)$; l – кількість спостережень. Середньоквадратичне відхилення S контент-функції $X^Q(t)$ розраховується за виразом

$$S = \sqrt{\ell^{-1} \cdot \sum_{t=1}^{\ell} (X^Q(t) - \bar{X}^Q)^2}, \quad (3)$$

$$\text{де } \bar{X}^Q = \ell^{-1} \cdot \sum_{t=1}^{\ell} X^Q(t).$$

Розкид накопиченого відхилення R розраховують як

$$R = \max_{1 \leq t \leq l} \tilde{X}^Q - \min_{1 \leq t \leq l} \tilde{X}^Q, \quad (4)$$

$$\text{де } \tilde{X}^Q = \sum_{t=1}^{\ell} (X^Q(t) - \bar{X}^Q).$$

Етап 3. Прогнозування зміни динаміки контент-функції. Для прийняття рішення про доцільність екстраполяції динаміки поширення контенту в СІС або запитів на нього встановлюється природа досліджуваних процесів. Залежно від характеру інформаційних акцій, ступеня деструктивності поширюваного контенту або запитів на нього, інтенсивності функціонування джерела загроз інформаційній безпеці тощо контент-функції можуть бути віднесені до одного з трьох типів (табл. 1) [19].

Таблиця 1

Природа контент-функції

Тип кореляційної динаміки ряду $X^Q(t)$	Природа процесів поширення контенту або запитів на нього в СІС
випадковий	процеси незалежні і некорельовані, інформаційні акції можуть носити разовий випадковий характер
антиперсистентний (ергодичний)	контент-функція є волатильною і складається із реверсів типу «спад-підйом». Якщо динаміка поширення контенту зростає за поточний період контент-аналізу, то найбільш ймовірним є його спад за наступний період
персистентний	якщо динаміка публікацій контенту або формування запитів на нього зростає (або відповідно зменшується) за період контент-аналізу, то його динаміка поведінки не зміниться й в наступному періоді. Динаміка поширення контенту має стійкий тренд, а інформаційна акція – цільовий характер

Персистентність ряду збільшується зі зростанням показника Херста й наближенням його до своєї верхньої межі, тобто $H^Q \rightarrow 1$. У протилежному випадку прогнозування динаміки не проводиться.

Правила прийняття рішень щодо прогнозування контент-функції ґрунтуються на значенні розрахованого показника Херста H^Q на етапі 2 методу. У формалізованому вигляді правила прийняття рішень з урахуванням [5] наведено в табл. 2.

Таблиця 2

Правила прийняття рішень

№	Значення показника Херста, H^Q	Рішення щодо прогнозу, W
1	$H^Q = 0,5$	недоцільний
2	$0 \leq H^Q < 0,5$	недоцільний
3	$0,5 \leq H^Q \leq 1$	доцільний

Етап 4. Прогнозування зміни показника взаємодії. Встановлюється функціональна залежність між контент-функцією $X^Q(t)$ і часом t . Для найбільшого узгодження експериментальних даних $X^Q(t)$ і їх найкращого згладжування доцільно використати метод найменших квадратів (МНК). Сутність МНК

полягає в пошуку апроксимуючого багаточлена $P^Q(t)$ за відомою методикою [27], для якого

$$F = \sum_{t=1}^l (P^Q(t) - X^Q(t))^2 \rightarrow \min. \quad (5)$$

На основі побудованого апроксимуючого багаточлена $P^Q(t)$ контент-функції реалізують прогноз динаміки поширення контенту або запитів на нього в СІС. Це дозволяє підвищити оперативність і ефективність управління взаємодією акторів віртуальних спільнот у розрізі попиту на деструктивний контент шляхом завчасного корегування управляючих дій і запобігання реалізації загроз інформаційній безпеці.

Експерименти. Розглянемо реальні інформаційні акції, які мали місце в інформаційному просторі України у 2015 році.

Експериментальні дані: приклад 1. Дослідимо зміну кількості публікацій акторів віртуальних спільнот СІС деякого контенту. З цією метою визначимо динаміку поширення контенту, який містить деструктивні інформаційні посили на тему «Яценюк воював у Чечні», спрямованого на дискредитацію вищого політичного керівництва держави. Запит до контент-

сервісу *IQBuzz* набуває таких параметрів пошуку: мова документів – документи на будь-якій мові; тип документів – пост, коментар, форум, відео, мікро-блог, соціальні мережі; дата створення – за весь час.

Результати роботи запиту до контент-сервісу *IQBuzz* подано в табл. 3. Розрахунок метрики самоподібності H_Q за даними табл. 3 проведено за виразами (2)–(4) [5] й встановлено, що показник Херста дорівнює $H^{Q_1} = 0,816$. Спираючись на дані табл. 2 можна зробити висновок, що поширення в СІС контенту «Яценюк воював у Чечні» має персистентну (невипадкову) природу, а ряд володіє ознаками тренду.

Таблиця 3
Вихідні дані поширення контенту
«Яценюк воював у Чечні»

День	Дата	К-сть повідомлень акторів СІС
1	26.12.2015	76
2	27.12.2015	64
3	28.12.2015	27
4	29.12.2015	27
5	30.12.2015	16
6	31.12.2015	13
7	01.01.2016	9
8	02.01.2016	12
9	03.01.2016	4
10	04.01.2016	4

Засобами табличного процесора MS Excel за МНК побудовано апроксимуючу криву досліджуваної контент-функції $P^{Q_1}(t) = 96,502e^{-0,324t}$. Коефіцієнт достовірності апроксимації дорівнює $R^2 = 0,942$ (рис. 2). На основі отриманої апроксимуючої кривої $P^Q(t)$ виконано екстраполяцію кількості публікацій на наступні 4 дні (табл. 4). Аналіз табл. 4 показує, що результати прогнозування апроксимуючою кривою $P^Q(t)$ узгоджуються з експериментальними даними, а кількість публікацій контент в яких вміщує деструктивні інформації посилює зменшується з експоненціальною швидкістю. Отже, для даного прикладу недоцільно витрачати ресурси системи забезпечення інформаційної безпеки держави для організації інформаційної протидії.

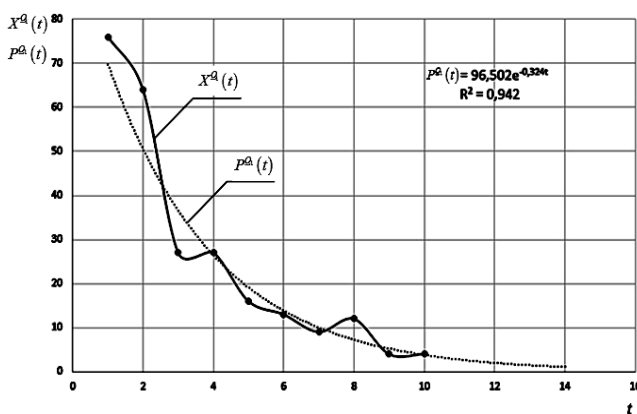


Рис. 2. Динаміка поширення контенту «Яценюк воював у Чечні» в СІС: результати екстраполяції

Таблиця 4
Прогноз динаміки публікацій
контенту «Яценюк воював у Чечні»

День	Дата	Прогноз кількості публікацій акторів СІС	Експериментальні значення кількості публікацій акторів СІС
11	05.01.2016	3	2
12	06.01.2016	2	1
13	07.01.2016	2	4
14	08.01.2016	1	2

Експериментальні дані: приклад 2. Проаналізуємо динаміку запитів в СІС на контент «візитка Яроша». Засобами сервісу контекстного пошуку *Google AdWords* було визначено середню кількість запитів акторів СІС на словосполучення «візитка Яроша» в період з жовтня 2014 р. по вересень 2015 р. із таргетингом території України і використанням пошукового сервісу *Google* (табл. 5). Показник Херста для даних табл. 5 набуває значення $H^{Q_2} = 0,891$, що свідчить про персистентність ряду і наявність постійної складової. У такому разі вважається за потрібне здійснення процедури прогнозування. У результаті екстраполяції засобами табличного процесора MS Excel за МНК побудовано апроксимуючу криву $P^{Q_2}(t) = 1605,3e^{-0,139t}$ для часового ряду $X^{Q_2}(t)$ зміни попиту акторів СІС (табл. 5) з коефіцієнтом детермінації рівним $R^2 = 0,91$.

Таблиця 5
Вихідні дані попиту акторів
на контент «візитка Яроша»

Період	Дата	Кількість запитів акторів СІС, тис.
1	31.10.2014	1,30
2	30.11.2014	1,30
3	31.12.2014	1,00
4	31.01.2015	1,00
5	28.02.2015	0,72
6	31.03.2015	0,88
7	30.04.2015	0,72
8	31.05.2015	0,48
9	30.06.2015	0,32
10	31.07.2015	0,39
11	31.08.2015	0,36
12	30.09.2015	0,35

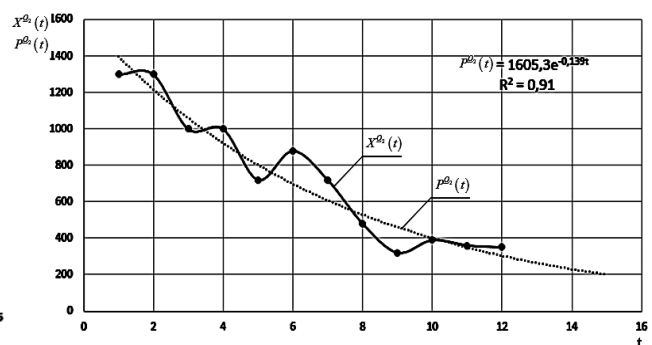


Рис. 3. Динаміка поширення запитів на контент «візитка Яроша» в СІС: результати екстраполяції

З рис. 3 видно, що рівень зацікавленості акторів СІС до шуканого контенту повільно спадає за експоненціальним законом. Для прискорення перехідних процесів й найбільш інтенсивного зменшення попиту на контент «візитка Яроша» відповідно до викладеної в [16] концепції застосовуються принципи синергетичного управління. Так взаємодія акторів у СІС у формалізованому вигляді описується системою нелінійних диференціальних рівнянь вигляду

$$\begin{cases} \frac{dx(t)}{dt} = ax - xy - bx^2; \\ \frac{dy(t)}{dt} = -cy + xy, \end{cases} \quad (6)$$

де $x(t)$ – процес, що описує попит акторів СІС на контент, що становить інтерес для досліджуваної віртуальної спільноти; $y(t)$ – процес, що описує пропозицію з надання контенту, що становить інтерес джерелом загроз інформаційній безпеці; a – показник зміни швидкості попиту акторів СІС на контент, що становить інтерес; b – показник зміну стану процесу конкуренції акторів у СІС на публікацію контенту аналогічного за сутністю та змістом; c – показник зміни швидкості пропозиції з надання акторам взаємодії в СІС контенту, що становить інтерес.

Встановлено, що робочі параметри системи нелінійних диференціальних рівнянь (6) приймають значення: зміни швидкості попиту на контент $a = 0,7$; зміна процесу конкуренції $b = 0,45$ і швидкість пропозиції з надання контенту $c = 0,3$. Для регуляризації попиту акторів на контент СІС, пов'язаний зі словосполученням «візитка Яроша» використано модель притягуючого атратора

$$\psi_v(x, y) = \varphi_1 x + \varphi_2 (1 - y/N), \quad (7)$$

де φ_1, φ_2 – коефіцієнти регуляризації попиту та пропозиції на контент, що становить інтерес в акторів взаємодії в СІС; N – рівень пропозиції з надання контенту, що становить інтерес з урахуванням його цінності. Відповідно до концепції [16] на основі параметра порядку (7) синтезовано синергетичне управління вигляду

$$u_\gamma(x, y) = \frac{\varphi_1}{\varphi_2} N(ax - xy - bx^2) + \frac{1}{\varphi_2 T_0} N\psi_v(x, y) + cy - xy.$$

Параметрами синергетичного управління $u_\gamma(x, y)$ є: рівень пропозиції з надання контенту $N = 0,35$; параметри регуляризації $\varphi_1 = 0,6$ і $\varphi_2 = 0,3$; тривалість перехідних процесів у системі $T_0 = 1$ міс.

Внаслідок організації інформаційної протидії синергетично керований попит на контент, що містить деструктивні інформаційні посилювачі буде змінюватися як показано на рис. 4.

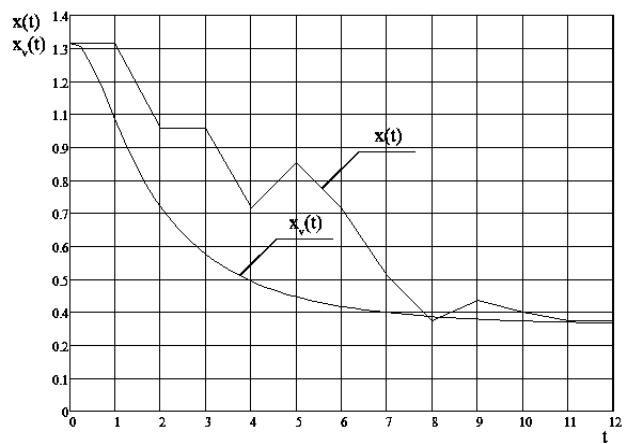


Рис. 4. Зміна динаміки попиту акторів на контент «візитка Яроша»: $x(t)$ – попит на контент, тис. запитів (за даними Google AdWords); $x_v(t)$ – синергетично керований попит, тис. запитів (унаслідок інформаційної протидії)

Таким чином, синергетичне управління попитом акторів на контент сприяє виробленню своєчасних та дієвих механізмів інформаційної протидії з нейтралізації джерел загроз інформаційній безпеці людини, суспільства та держави в СІС.

Верифікація розробленого методу на реальних експериментальних даних контент-аналізу повідомлень в СІС дозволило встановити його переваги. Основними з них є: метод забезпечує виявлення постійної складової в досліджуваних процесах; у разі виявлення ознак персистентності метод дозволяє встановити ознаки тренду ряду; метод створює передумови для організації системою забезпечення інформаційної безпеки держави ефективної інформаційної протидії; впровадження методу сприяє ефективному розподілу витрат ресурсів на функціонування системи забезпечення інформаційної безпеки держави.

Висновки

Вперше розроблено метод прогнозування динаміки поширення контенту й запитів на нього за даними контент-аналізу повідомлень у СІС, який ґрунтується на значеннях метрики самоподібності й забезпечує встановлення природи контент-функції та, у разі потреби, на основі концепції синергетичного управління сприяє виробленню ефективних заходів інформаційної протидії системою забезпечення інформаційної безпеки держави, або в протилежному випадку – сприяє економії витрат ресурсів системи на її функціонування.

Список літератури

1. Hanneman R.A. *Introduction to social network methods* / R.A. Hanneman, M. Riddle. – Riverside, CA: University of California, Riverside, 2005. – 322 p.
2. Scott John. *Social Network Analysis [3-rd edition]* / John Scott. – Sage Publication Ltd, 2016. – 216 p.
3. Пелешишин А. М. *Процеси управління інтерактивними соціальними комунікаціями в умовах розвитку*

інформаційного суспільства : моногр. / А.М. Пелецишин, Ю.О. Серов, О.Л. Березко [та ін.] ; за ред. А. М. Пелецишина. – Л. : Вид-во Львівської політехніки, 2012. – 368 с.

4. Carrington P. J. *Models and Methods in Social Network Analysis* / P. J. Carrington, J. Scott, S. Wasserman. – Cambridge : Cambridge University Press, 2005. – 344 p.

5. Горбулін В. П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання : монографія / В. П. Горбулін, О. Г. Додонов, Д. В. Ланде. – К. : Інтертехнологія, 2009. – 164 с.

6. Earl J. *Digitally Enabled Social Change: Activism in the Internet Age* / J. Earl, K. Kimport. – Cambridge: MIT, 2011. – 170 p.

7. Morozov E. *The Net Delusion: The Dark Side of Internet Freedom* / E. Morozov. – NY : Public Affairs, 2012. – 448 p.

8. Tufekci Z. *Social media and the decision to participate in political protest: observations from Tahrir Square* / Z. Tufekci, C. Wilson. // *J. Commun.* – 2012. – № 62(2). – P. 363–379.

9. Онищук М. І. Роль соціальних мереж в політичних процесах на близькому сході та в північній Африці / М. І. Онищук // *Вісн. Київ. нац. ун-ту ім. Т. Шевченка*. – 2012. – № 28. – С. 15–17.

10. Гіда О. Ф. Соціальні мережі як засіб деструктивних впливів через інформаційний простір / О. Ф. Гіда // *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. – 2013. – № 3(31). – С. 268–278.

11. Українська революція гідності, агресія РФ і міжнародне право : моногр. – К. : К.І.С., 2014. – 1016 с.

12. Курбан О. В. Теорія інформаційної війни: базові основи, методологія та понятійний апарат / О. В. Курбан // *ScienceRise*. – 2015. – № 11/1(16). – С. 95–100.

13. Гришук Р. В. Технологічні аспекти інформаційного протистояння на сучасному етапі / Р. В. Гришук, І. О. Канкін, В. В. Охрімчук // *Захист інформації*. – 2015. – Т. 17, №1. – С. 80–86.

14. Іванов О. В. Класичний контент-аналіз та аналіз тексту: термінологічні та методологічні відмінності / О. В. Іванов // *Вісн. Харк. нац. ун-ту ім. В. Н. Каразіна*. – 2013. – № 1045. – С. 69–74.

15. Даник Ю. Г. Мобільні соціальні інтернет-сервіси як один із різновидів масової комунікації на сучасному етапі / Ю. Г. Даник, Р. В. Гришук, О. В. Самчишин // *Безпека інформації*. – 2015. – Т. 21, ч. I. – С. 16–20.

16. Гришук Р. В. Концепція синергетичного управління процесами взаємодії агентів у соціальних інтернет-сервісах / Р. В. Гришук, К. В. Молодецька // *Безпека інформації*. – 2015. – Т. 21, ч. II. – С. 123–130.

17. Молодецька К. В. Спосіб підтримання заданого рівня попиту акторів соціальних інтернет-сервісів на контент / К. В. Молодецька // *Радіоелектроніка, інформатика, управління*. – 2015. – № 4(35). – С. 113–117.

18. Молодецька К. В. Синтез синергетичного управління попитом агентів на контент у соціальних інтернет-сервісах / К. В. Молодецька // *Інформатика та математичні методи в моделюванні*. – 2015. – Т. 5, № 4. – С. 330–338.

19. Рогоза М.Є. Нелінійні моделі та аналіз складних систем : навч. посіб. / М.Є. Рогоза, С.К. Рамазанов, Е.К. Мусаєва. – Полтава : ПВВ ПУЕТ, 2011. – Ч. 1. – 300 с.

20. Колодчак О. М. Інтелектуальний аналіз даних / О. М. Колодчак // *Вісн. нац. ун-ту "Львівська політехніка". Комп'ютерні системи та мережі*. – 2013. – № 773. – С. 49–58.

21. Методы и модели анализа данных OLAP и DataMining / Ф. Барсегян, М. Куприянов, В. Степаненко, И. Холод. – СПб. : БХВ-Петербург, 2008. – 354 с.

22. Голубев С. Н. R/S-анализ стабильности запаздывающего временного ряда [Электронный ресурс] / Лаборатория фрактального анализа, экологии, программирования. – Режим доступа: <http://labfranep.com/r-s-analiz-stabilnosti-zapazdyvayushchego-vremennogo-ryada> (дата звернення: 25.12.2015). – Назва з екрану.

23. Кронвер Р. М. Фракталы и хаос в динамических системах. Основы теории / Р. М. Кронвер. – М. : Постмаркет, 2000. – 352 с.

24. Гришук Р. В. Стартап віртуальних спільнот у соціальних мережах за принципом критичної маси / Р. В. Гришук // *Захист інформації*. – 2015. – Спеціальний випуск. – С. 19–25.

25. Халилов Д. Маркетинг в социальных сетях / Дамир Халилов. – М. : Манн, Иванов и Фербер, 2014. – 240 с.

26. Алексейчук П. Система слежки PRISM собирала персональные данные через лидеров IT-индустрии [Электронный ресурс] / Проект WebScience.ru. – Режим доступа: <http://webscience.ru> (дата обращения: 25.12.2015). – Название с экрана.

27. Бродський Ю. Б. Інформатика і системологія : [навч. посіб.] / Ю. Б. Бродський, К. В. Молодецька. – Житомир : ЖНАЕУ, 2014. – 244 с.

Надійшла до редколегії 29.10.2015

Рецензент: д-р техн. наук, проф. Г.А. Кучук, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.

МЕТОД ПРОГНОЗИРОВАНИЯ ДИНАМИКИ РАСПРОСТРАНЕНИЯ КОНТЕНТА И ЗАПРОСОВ НА НЕГО ПО ДАННЫМ КОНТЕНТ-АНАЛИЗА СООБЩЕНИЙ В СОЦИАЛЬНЫХ ИНТЕРНЕТ-СЕРВИСАХ

Р.В. Гришук, К.В. Молодецкая

Предложено методологический инструментарий для прогнозирования динамики распространения контента и запросов на него по данным контент-анализа сообщений в социальных интернет-сервисах. Применение метрики самоподобия позволило выявить постоянную составляющую контент-функции и установить ее природу. В результате система обеспечения информационной безопасности государства приобретает новые свойства для выработки необходимых механизмов информационного противодействия.

Ключевые слова: социальный интернет-сервис, акторы, контент-функция, деструктивный информационный посыл, показатель Херста, информационная безопасность, прогнозирование, синергетическое управление.

THE METHOD TO PREDICT THE DYNAMICS OF THE WEB CONTENT DISSEMINATION AND OF THAT CONTENT ASSOCIATIVE ONLINE SEARCH BEHAVIOR USING CONTENT ANALYSIS OF THE POSTS ON SOCIAL NETWORKING SERVICES

R.V. Hryshchuk, K.V. Molodetska

A methodological tools for predicting the dynamics of content distribution and requests it according to content analysis messages of social Internet services. The use of self-similarity metrics revealed constant component content features and set its nature. As a result, information security system of the state acquires new properties to generate the information mechanisms to counter.

Keywords: social networking services, actors, content-function, destructive outreaches, Hurst exponent, information security, prediction, synergetic control.