© Molodetska-Hrynchuk K. The model of decision making support system for detection and assessment of the state information security threat of social networking services // Ukrainian Scientific Journal of Information Security, 2017, vol. 23, issue 2, p. 136-144.

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ / INFORMATION SECURITY MANAGEMENT

DOI: 10.18372/2225-5036.23.11803

МОДЕЛЬ СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ДЛЯ ВИЯВЛЕННЯ ОЗНАК ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ДЕРЖАВИ У СОЦІАЛЬНИХ ІНТЕРНЕТ-СЕРВІСАХ ТА ОЦІНЮВАННЯ ЇХ РІВНЯ

Катерина Молодецька-Гринчук

Житомирський національний агроекологічний університет, Україна

МОЛОДЕЦЬКА-ГРИНЧУК Катерина Валеріївна, к.т.н.

Рік та місце народження: 1985 рік, м. Житомир, Україна.
Освіта: Житомирський військовий інститут радіоелектроніки ім. С.П. Корольова, 2007 рік.
Посада: доцент кафедри комп'ютерних технологій і моделювання систем з 2013 року.
Наукові інтереси: інформаційна безпека, математичне моделювання.
Публікації: більше 90 наукових публікацій, серед яких монографія, підручник, навчальні посібники, наукові статті.
E-mail: kmolodetska@hotmail.com

Анотація. *Соціальні інтернет-сервіси представляють собою прогресивний засіб комунікації учасників віртуальних спільнот – акторів. У випадку поширення у віртуальних спільнотах недостовірного, неповного або викривленого контенту соціальні інтернет-сервіси перетворюються на дієвий інструмент проведення інформаційних акцій, спрямованих на маніпуляцію суспільною думкою, вплив на свободу вибору, поширення закликів до сепаратизму тощо. Тому виникає потреба у розробленні адекватної моделі системи підтримки прийняття рішень для виявлення ознак загроз інформаційній безпеці держави у соціальних інтернет-сервісах та оцінювання їх рівня. В основу запропонованої моделі покладено методи виявлення частинних ознак інформаційних акцій у соціальних інтернет-сервісах, нелінійну схему компромісів для їх оцінювання та синергетичне управління для забезпечення керованого переходу віртуальної спільноти до заданого стану інформаційної безпеки. У результаті функціонування системою підтримки прийняття рішень виробляються рекомендовані рішення для протидії виявленим загрозам. Залежно від сфери суспільної діяльності, на яку впливає загроза, відповідними державними виконавчими органами здійснюються заходи з її нейтралізації. Таким чином досягається оперативність, ефективність та швидкодія системи забезпечення інформаційної безпеки держави у соціальних інтернет-сервісах.*

Ключові слова: *соціальний інтернет-сервіс, система підтримки прийняття рішень, загрози, процесний підхід, контент, інформаційна безпека держави.*

Вступ

Сьогодні постійно зростає роль соціальних інтернет-сервісів (СІС) у процесах масової комунікації завдяки їх оперативності, доступності, інтерактивності та постійному збільшенню кількості учасників віртуальних спільнот, яких називають акторами [1, 2]. Такий феномен пояснюється участю широкої аудиторії акторів у обговоренні актуальних проблем, об'єднанням у групи за спільними інтересами, використанням СІС для самоорганізації акторів з метою впливу на суспільне і політичне життя олайн тощо [3-6]. Проте, завдяки комунікаційним перевагам СІС одночасно перетворилися на ефективний інструмент проведення інформаційних операцій проти особистості, суспільства, держави.

Наслідками поширення у СІС контенту з деструктивним інформаційним посилом є маніпуляції суспільною думкою, вплив на свободу вибору акторів, розпалювання ворожнечі на національному або етнічному підґрунті, заклики до сепаратизму тощо [7-9]. Досвід «гібридної війни» з Російською Федерацією показав, що в Україні відсутня цілісна методологія побудови системи забезпечення інформаційної безпеки (СЗІБ) держави у СІС. Встановлено, що існуючі засоби і підсистеми інформаційної

безпеки держави у СІС не відповідають рівню сучасних загроз, тому розроблення дієвого наукового інструментарію для автоматизації процесів виявлення і протидії загрозам у СІС є актуальним теоретико-прикладним завданням.

Аналіз існуючих досліджень

Аналіз останніх досліджень і публікацій за напрямком дослідження [4, 6-12] показав недостатній рівень теоретичного опрацювання і відсутність практичних рекомендацій щодо розроблення СЗІБ держави у СІС. У цілому, СЗІБ є компонентом системи забезпечення національної безпеки і може складатися з підсистем для розв'язку окремих завдань [9]. У наукових працях професора Ліпкана А. В. [10, 11] сформульовано мету і завдання СЗІБ держави, визначено, що вона розробляється відповідно до Конституції України та нормативно-правового забезпечення у галузі інформаційної безпеки. Вказано, що в основу СЗІБ покладено комплекс засобів забезпечення інформаційної безпеки, які застосовують адміністративно-правові, інформаційно-аналітичні, організаційно-управлінські та інші дії для сталого розвитку інформаційного середовища держави.

У свою чергу, в дослідженні [12] запропоновано архітектуру програмного комплексу моніторингу та аналізу інформаційних загроз віртуальних спільнот у соціальних мережах. Введено поняття цінності віртуальної спільноти для узагальнення структури, кількість акторів та якості контенту. Однак, розроблена модель оцінювання загроз не враховує активність профілів і публікацій акторів та прихований характер загроз у СІС. Тому перспективним є застосування запропонованих на попередніх етапах досліджень методик, методів і технологій [13-22] вивлення ознак загроз та оцінювання їх рівня, що відрізняються від відомих [4, 12] узагальненням на СІС, врахуванням різних проявів ознак загроз, зокрема залучення соціальних ботів, наявності деструктивного інформаційного посилу й маніпуляційних технологій у текстовому контенті, оцінюванням профілів інформаційної безпеки акторів.

Комплексний і системний аналіз особливостей функціонування СІС [2-5, 8] показав, що вони належать до класу нелінійних динамічних систем. При цьому процеси соціальної комунікації характеризуються непрогнозованістю взаємодії акторів у випадку зовнішніх інформаційних впливів. Наслідком реалізації загроз інформаційній безпеці держави у СІС є перехід віртуальних спільнот до некерованої хаотичної динаміки. Тому для реалізації протидії виявленим загрозам доцільно використати процеси самоорганізації акторів, які покладено в основу синергетики. Застосування розробленої концепції синергетичного управління взаємодією акторів у СІС [20] забезпечує керований перехід віртуальної спільноти до заданого стійкого стану інформаційної безпеки, уникаючи хаотичної динаміки системи.

Також встановлено, що одна з ключових ролей у забезпеченні інформаційної безпеки відводиться Міністерству інформаційної політики України (МІПУ) і, відповідно до Доктрини інформаційної безпеки України [23], затвердженої 25 лютого 2017 року, полягає у виконанні таких функцій [24]: моніторинг інформаційного середовища держави, зокрема вітчизняного сегменту СІС; моніторинг загроз інформаційній безпеці держави; розроблення та імплементація стратегічного наративу тощо. У Доктрині вказано, що актуальні загрози національній безпеці в інформаційній сфері носять комплексний характер, тому виникає нагальна потреба розроблення інноваційних підходів до формування системи захисту і розвитку інформаційного простору в умовах глобалізації та вільного обігу інформації. Для реалізації визначених у Доктрині механізмів протидії таким загрозам і автоматизації процедур їх раннього виявлення та оцінювання необхідно розробити відомчі підсистеми інформаційної безпеки. Для функціонування таких систем доцільно використати запропоновані у публікаціях [13-18, 20] концепції, методи і підходи.

Отже, з метою забезпечення заданого стану інформаційної безпеки держави у СІС необхідно розробити систему підтримки прийняття рішень (СППР) як компоненту відомчої підсистеми забезпечення інформаційної безпеки держави на основі розроблених методів виявлення, оцінювання і протидії загрозам. Така СППР дозволить підвищити загальну ефективність СЗІБ держави у СІС, що додатково актуалізує обраний напрямок наукових досліджень.

Мета даної роботи полягає у створенні адекватної моделі СППР для виявлення ознак загроз інформаційній безпеці держави у СІС і оцінювання їх рівня, що забезпечить автоматизацію процедур раннього виявлення, оцінювання та підвищить ефективність протидії загрозам.

Для досягнення поставленої мети необхідно розв'язати частинні задачі:

– виконати процесне моделювання СППР, яка розробляється, для структуризації опису і аналізу процесів предметної області дослідження;

– розробити модель прийняття рішень для інформаційної протидії загрозам у СІС;

– розробити алгоритм функціонування і структурну схему СППР для виявлення ознак загроз інформаційній безпеці держави у СІС та оцінювання їх рівня.

Основна частина дослідження

У загальному вигляді вимоги до СППР для виявлення ознак загроз інформаційній безпеці держави у СІС та оцінювання їх рівня сформульовані у міжнародних стандартах ISO серій 27000, 20000, 14000, 9000 [25–29]. У свою чергу, стандарт ISO 27001 формулює вимоги у галузі інформаційної безпеки для створення, розвитку та підтримки систем менеджменту інформаційної безпеки. Розглянуті стандарти узгоджені між собою і грунтуються на процесному підході до побудови систем управління. Суть процесного підходу зводиться до опису функціонування системи як набору взаємозалежних неперервних дій. В основу перерахованих

міжнародних стандартів покладено модель PDCA (цикл Шухарта-Демінга) – структуру життєвого циклу усіх процесів системи [29]. Суть моделі зводиться до неперервного покращення процесів, що забезпечує ефективне керування функціо-нуванням на системній основі. Тому до СППР для виявлення ознак загроз інформаційній безпеці держави у СІС та оцінювання їх рівня висуваються вимоги відповідності серії міжнародних стандартів ISO, моделі PDCA і процесного підходу.

Процесний аналіз предметної області досліджень виконано засобами інтегрованого середовища *ARIS Express*, призначеного для комплексної формалізації функціонування об'єкта у вигляді графічних моделей [31]. Узагальнена карта процесів СППР для виявлення ознак загроз інформаційній безпеці держави у СІС та оцінювання їх рівня подано на рис. 1.

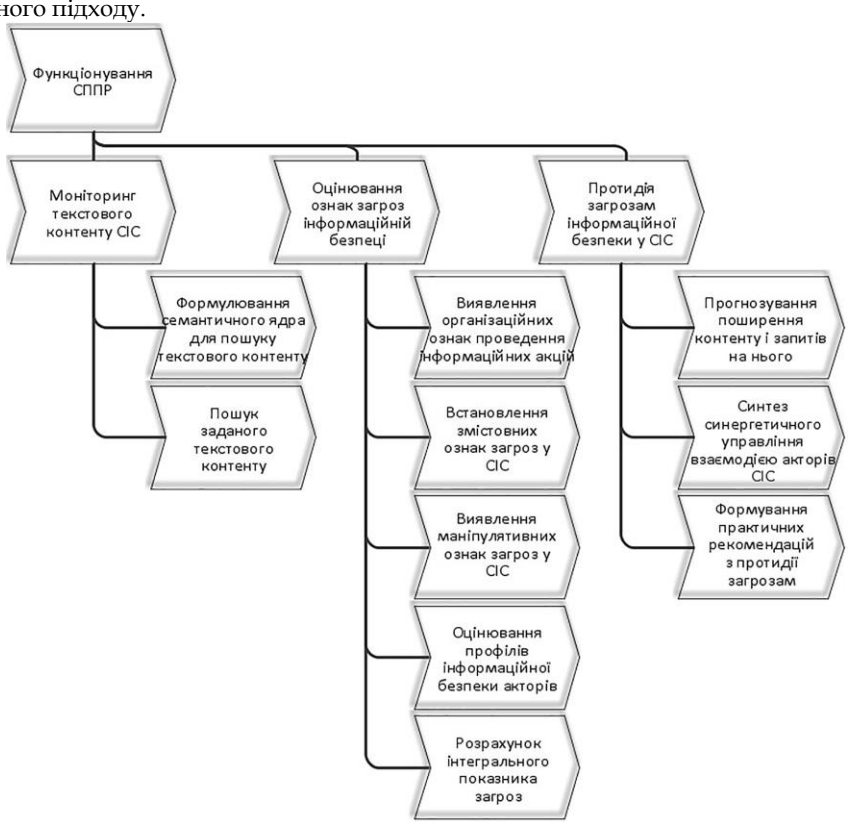

Рис. 1. Карта процесів СППР для виявлення ознак загроз інформаційній безпеці держави у СІС та оцінювання їх рівня

Головним процесом на рис. 1 є функціонування СППР для виявлення ознак загроз інформаційній безпеці держави у СІС та оцінювання їх рівня, який складається з таких складових: моніторинг текстового контенту СІС; оцінювання ознак загроз інформаційній безпеці держави; протидія загрозам інформаційної безпеки у СІС. Кожен з визначених етапів деталізується на складові компоненти. Так, моніторинг текстового контенту складається із формулювання співробітниками спеціалізованих підрозділів семантичного ядра зі слів, які визначають критичні та актуальні теми для суспільства і подальшої індексації текстового контенту на основі визначених слів.

На наступному етапі проводиться оцінювання ознак загроз інформаційній безпеці держави у СІС, що зводиться до розрахунку частинних показників ознак загроз – організаційних, змістовних, маніпулятивних і профілів інформаційної безпеки акторів СІС. Суть організаційних ознак загроз зводиться до використання інформаційних ресурсів та спеціалізованого програмного забезпечення у СІС, зокрема соціальних ботів, для поширення контенту і його соціалізації. Змістовні ознаки загроз інформаційної безпеки у СІС характеризуються наявністю деструктивного інформаційного посилу у текстовому контенті СІС. Маніпулятивні ознаки загроз полягають у застосуванні прихованого впливу на акторів для управління їх поведінкою або психологічними характеристиками в інтересах суб'єкта впливу. Профіль інформаційної безпеки акторів СІС представляє собою набір агрегованих характеристик профіля актора у СІС, які дозволяють визначити рівень його загрози як можливого учасника інформаційних акцій, направлених проти інформаційної безпеки людини, суспільства, держави. Далі проводять обчислення інтегрального показника загроз для формування висновку про рівень виявлених загроз у СІС.

Завершальний етап функціонування СППР полягає у протидії виявленим загрозам інформаційної безпеки держави у СІС. Кокретні рекомендіції з протидії визначаються залежно від рівня виявленої загрози на попередньому етапі функціонування СППР. Так, якщо рівень загрози є низьким, то доцільно виконати прогнозування поширення контенту й запитів на нього для оперативного коригування управляючих впливів на віртуальні спільноти акторів. У випадку середнього або існуючого рівня загрози інформаційній безпеці держави у

СІС необхідно виконати синтез синергетичного управління взаємодією акторів. Такі дії забезпечать штучно керований перехід віртуальної спільноти до бажаного стійкого стану інформаційної безпеки завдяки підтриманню заданих показників взаємодії акторів СІС і запуску процесів самоорганізації. Завершальним компонентом етапу протидії загрозам є формування практичних рекомендацій відповідним державним виконавчним органам з протидії на основі Доктрини інформаційної безпеки України залежно від рівня загрози та сфери суспільної дільності, на яку вона впливає.

Для побудови СППР для виявлення ознак загроз інформаційній безпеці держави у СІС та оцінювання їх рівня на основі досліджень [5, 7, 13-22, 31-35] запропоновано такий алгоритм функціонування.

Етап І. Моніторинг текстового контенту СІС. На початковому етапі проводиться моніторинг інформаційного середовища СІС з метою виявлення контенту на задану тематику. Аналізу підлягає текстовий вид контенту СІС, який складає найбільшу частку інформації, опублікованої акторами віртуальних спільнот. Перший етап складається з кроків, наведених нижче.

Крок 1.1. Визначення множини загроз інформаційній безпеці держави у СІС. Експерт з інформаційної безпеки на основі аналізу значущої і критичної тематики контенту у суспільстві визначає множину актуальних загроз у СІС. Визначені загрози формалізуються у вигляді кортежу [7, 34]:

$$D = \langle R, S, C, T, Sph, M, F, Sr, P, I \rangle, \quad (1)$$

де R – відношення загрози до акторів СІС; S – вид суб'єкта загроз; C – характер загрози по відношенню до СІС; T – мета загрози; Sph – сфера суспільної діяльності, на яку впливає загроза; M – спосіб дії загрози; F – частота повторюваності; Sr – прихованість прояву; P – можливість реалізації загрози у СІС; I – рівень впливу на акторів і віртуальні спільноти.

Крок 1.2. Пошук текстового контенту СІС. Для пошуку у віртуальних спільнотах текстового контенту, що ставить загрозу інформаційній безпеці держави, задають ключові слова w_i для її опису у вигляді семантичного ядра:

$$W = \langle w_i \rangle, \; i = \overline{1,n}. \quad (2)$$

На основі семантичного ядра W виконується індексація текстового контенту СІС з використанням методів інформаційного пошуку контенту з урахуванням його змісту. Це дозволить знайти релевантний семантичному ядру текстовий контент TC^* і дані акторів A^*, які його поширили. Для вказаних завдань доцільно скористатися методом латентно-семантичної індексації (*LSI*) [32].

Етап ІІ. Розрахунок частинних ознак загроз у відібраному текстовому контенті СІС. Відібраний на попередньому кроці текстовий контент TC^* і дані акторів A^* досліджуються на наявність ознак застосування для проведення інформаційних акцій у СІС [13]. З цією метою проводиться аналіз присутності організаційних, змістовних, маніпулятивних ознак у контенті та оцінюється профіль інформаційної безпеки акторів A^*.

Крок 2.1. Виявлення організаційних ознак проведення інформаційних акцій I_1. Встановлено, що проявом організаційних ознак інформаційних акцій у СІС є застосування спеціалізованого програмного забезпечення для поширення заданого контенту і використання соціальних ботів. Для цього визначаються наступні показники [13]:

– наявність текстового контенту, який є дублікатами P публікацій інших акторів;

– автоматизований індекс читабельності I_{ARI} як рівень складності сприйняття текстового контенту;

– результат ведення діалогу з актором Q.

На основі встановлених значень показників приймається рішення щодо наявності організаційних ознак інформаційних акцій на основі відповідних правил [13]. Таким чином, показник присутності організаційних ознак загроз у текстовому контенті СІС приймає значення:

$$I_1 = I_1^n \to B, \text{ де } B = \{0;1\}, \; n = 1. \quad (3)$$

Крок 2.2. Встановлення змістовних ознак загроз. Проводиться аналіз відібраного текстового контенту TC^* з використанням семантичного аналізу на базі онтологій [14]. Для цього створюються онтологія *Ont* з описом предметної області, яка аналізується, та семантичний опис Sem_t відібраного текстового контенту TC^*. Детектування змістовних ознак загроз виконується з використанням сигнатурного методу і методу виявлення аномалій. З цією метою виявляють [14]:

– зв'язок між об'єктом публікації з його характеристиками у контенті та негативними ознаками для цього об'єкта внаслідок реалізації загрози;

– суперечності шляхом співставлення семантичного опису Sem_t текстового контенту і семантичного шаблону загрози.

У випадках високої релевантності текстового контенту семантичному ядру W і відсутності у ньому виявлених змістовних ознак загроз він підлягає додатковому аналізу експертом з інформаційної безпеки для виявлення небезпечних семантичних конструкцій. Виявлені об'єкти додаються до шаблонів загроз і використовуються для подальшого функціонування системи.

У результаті оцінка змістовних ознак загроз у СІС I_2 набуває значень:

$$I_2 = I_2^n \to B, \text{ де } B = \{0;1\}, \; n = 1. \quad (4)$$

Крок 2.3. Виявлення маніпулятивних ознак загроз виконується відповідно до методики оцінювання маніпуляцій суспільною думкою у СІС, запропонованої у публікації [15]. Для текстового контенту TC^* встановлюються показники: сумнівності викладених фактів; емоційного забарвлення; тональності; сенсаційності; прихованої теми. На основі розрахованих показників визначається величина інформаційної ентропії H_n маніпуляції

суспільною думкою, який характеризує рівень невизначеності відносно застосування технологій прихованого впливу на акторів. Результуючий показник маніпулятивних ознак загроз I_3 приймає значення:

$$I_3 = 1 - H_n, \;\; H_n \in [0;1]. \qquad (5)$$

Крок 2.4. Оцінювання профілів інформаційної безпеки акторів СІС. На даному кроці проводиться дослідження профілів акторів A^* на основі методу, запропонованого у публікації [16]. Його суть зводиться до аналізу таких характеристик: атрибути профіля актора; показники активності публікації контенту; ознаки, властиві контенту профіля актора; аналіз зв'язків актора у СІС. Обчислені показники використовуються для подальшого визначення його класу загрози завдяки класифікації. Результуюча оцінка профіля інформаційної безпеки актора I_4 визначається на діапазоні:

$$I_4 \in [0;1]. \qquad (6)$$

Крок 2.5. Розрахунок інтегральної оцінки ознак загроз інформаційній безпеці держави у СІС. Крок зводиться до багатокритерійної задачі оцінювання ознак загроз із різними ваговими коефіцієнтами [17]. Виконується згортка виявлених на кроках 3.1–3.4 ознак загроз I_j, $j = \overline{1,4}$ по нелінійній схемі компромісів професора Вороніна А.М. [33]. Векторна оптимізація проводиться на основі виразу:

$$I^* = \arg\min_{I \in M} \sum_{j=1}^{4} \alpha_j \left(1 - I_j\right)^{-1}. \qquad (7)$$

Якісна оцінка рівня загрози визначається у результаті нормування скалярної згортки (7) до мінімуму:

$$I = 1 - \frac{1}{I^*} \qquad (8)$$

з подальшим переходом до якісної шкали оцінки [17].

Етап ІІІ. Протидія загрозам інформаційної безпеки держави у СІС. Залежно від отриманого на попередньому етапі значення інтегральної оцінки ознак загроз I приймається відповідне рішення для протидії. Прийняття рішень виконується на основі табл. 1.

Моніторинг загрози інформаційній безпеці держави у СІС проводиться відповідно до першого етапу алгоритму функціонування СППР, а інші рекомендації із протидії представлені нижче.

Крок 3.1. Прогнозування поширення текстового контенту й запитів на нього у СІС. За допомогою інструментів контент-аналізу визначається контент-функція $X^Q(t)$, яка описує зміну динаміки поширення контенту або запитів на нього у СІС [18]. Розраховується показник Херста, який є метрикою самоподібності досліджуваного часового ряду:

$$H^Q = \frac{\lg(R/S)}{\lg(l/2)}, \qquad (9)$$

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.

Правила прийняття рішень Таблиця 1

Інтервальні значення шкали оцінок	*Рівень загрози*	*Рекомендації*
0,00–0,30	відсутня	відсутні;
0,31–0,50	нижча середнього	моніторинг загрози у інформаційному середовищі СІС
0,51–0,70	вища середнього	моніторинг загрози у інформаційному середовищі СІС; прогнозування поширення текстового контенту й запитів на нього
0,71–1,00	існує	моніторинг загрози у інформаційному середовищі СІС; синергетичне управління взаємодією акторів у СІС

На основі розрахованого значення показника Херста H^Q визначається тип динаміки контент-функції – випадкова, антиперсистентна чи персистентна [18]. Якщо контент-функція персистентна, то виконується її прогнозування з використанням методу найменших квадратів. В інших випадках екстраполяція контент-функції не проводиться, а продовжується моніторинг інформаційного середовища СІС.

Крок 3.2. Синтез синергетичного управління взаємодією акторів у СІС. Концепція синергетичного управління взаємодією акторів у СІС представлена у публікаціях [19-22]. Спочатку виконується формалізація взаємодії акторів у СІС як системи нелінійних диференціальних рівнянь. Після цього обирають параметр порядку $\psi_v(t)$, що визначатиме динаміку процесів взаємодії акторів віртуальних спільнот відповідно до поставленого завдання перед СППР для виявлення ознак загроз інформаційній безпеці держави у СІС та оцінювання їх рівня.

Параметр порядку $\psi_v(t)$ складається із двох компонент: керованого аспекту взаємодії акторів і атрактора, який визначає бажаний вигляд системи. За рахунок введення у систему нелінійних диференціальних рівнянь складової $\psi_v(t)$ досягається запуск процесів самоорганізації у системі. Синергетичне управління $u_\gamma(t)$ синтезується із модифікованої системи нелінійних диференціальних рівнянь з урахуванням керованої самоорганізації для досягнення попередньо заданих точок сплеску синергетичного ефекту.

Зауваження. Результати експериментального дослідження методик, методів і технологій, покладених в основу функціонування запропонованої моделі СППР представлені у відповідних публікаціях [14, 15, 17-22].

Крок 3.3. Вироблення практичних рекомендацій з протидії загрозам інформаційної безпеки держави у СІС. У випадку виявлення загрози *D* інформаційній безпеці держави у СІС СППР формує рекомендації для їх протидії та нейтралізації. Залучення окремих виконавчих державних органів проводиться залежно від сфери суспільної діяльності, на яку націлена виявлена загроза *D* [7]. Рекомендації з протидії загрозам інформа-ційної безпеки держави у СІС сформульовані на основі Доктрини інформаційної безпеки України [23] і проведеного аналізу впливу загроз на сфери суспільної діяльності [8] та подані у вигляді схеми на рис. 2.

Рис. 2. Напрямки протидії загрозам інформаційній безпеці держави у СІС

Координацію діяльності державних виконавчих органів, яких залучають до протидії загрозам інформаційній безпеці держави у СІС, виконують Рада національної безпеки і оборони України (РНБОУ) і Кабінет Міністрів України (КМУ). Ефективність організації протидії загрозам, гнучкість процесів управління, координація суб'єктів інформаційної безпеки держави досягається залученням до цих процесів громадських організацій та волонтерських проектів. Перевагою такого підходу є забезпечення громадськими організаціями ефективної взаємодії влади і ЗМІ, участь у розробленні й вдосконаленні законодавчої бази у галузі інформаційної безпеки держави, розвиток громадянського суспільства тощо.

На основі карти процесів (див. рис. 1) і узагальнення розглянутого вище алгоритму функціонування СППР для виявлення ознак загроз інформаційній безпеці держави у СІС та оцінювання їх рівня спроектовано її структурну схему (рис. 3). До складу СППР для виявлення ознак загроз інформаційній безпеці держави у СІС та оцінювання їх рівня входять п'ять основних блоків: моніторингу інформаційного середовища СІС; оцінювання частинних ознак загроз інформаційній безпеці держави у СІС; прогнозування поширення акторами контенту і запитів на нього; інтегрального оцінювання ознак загроз; протидії загрозам у СІС.

Користувачем розробленої СППР є експерт з інформаційної безпеки держави, який формує вхідний масив даних для роботи системи на основі аналізу актуальної тематики контенту у СІС. Результати функціонування блоку моніторингу інформаційного середовища віртуальних спільнот зберігаються у аналітичній базі даних і використовуються у подальшій роботі інших компонентів системи, зокрема блоку оцінювання частинних ознак загроз інформаційній безпеці. Визначені блоком частинні оцінки ознак загроз інформаційній безпеці держави у СІС передаються для обробки модулем і прийняття рішення про рівень загрози. Залежно від результуючого значення оцінки ознак загроз функціонування переходить до блоку прогнозування поширення контенту і запитів на нього чи блоку протидії загрозам.

Прогнозування проводиться на основі накопичених у базі даних значень контент-функції. Блок протидії загрозам у СІС містить базу даних моделей стабілізуючих атракторів і синергетичного управління. Вибір конкретної моделі синергетичного управління проводиться на основі величини прогнозованого показника поширення контету і запитів на нього акторів СІС та безпесередньо рівня загрози. Залежно від особливостей виявленої загрози формуються практичні рекомендації державним виконавчим органам для інформаційної протидії.

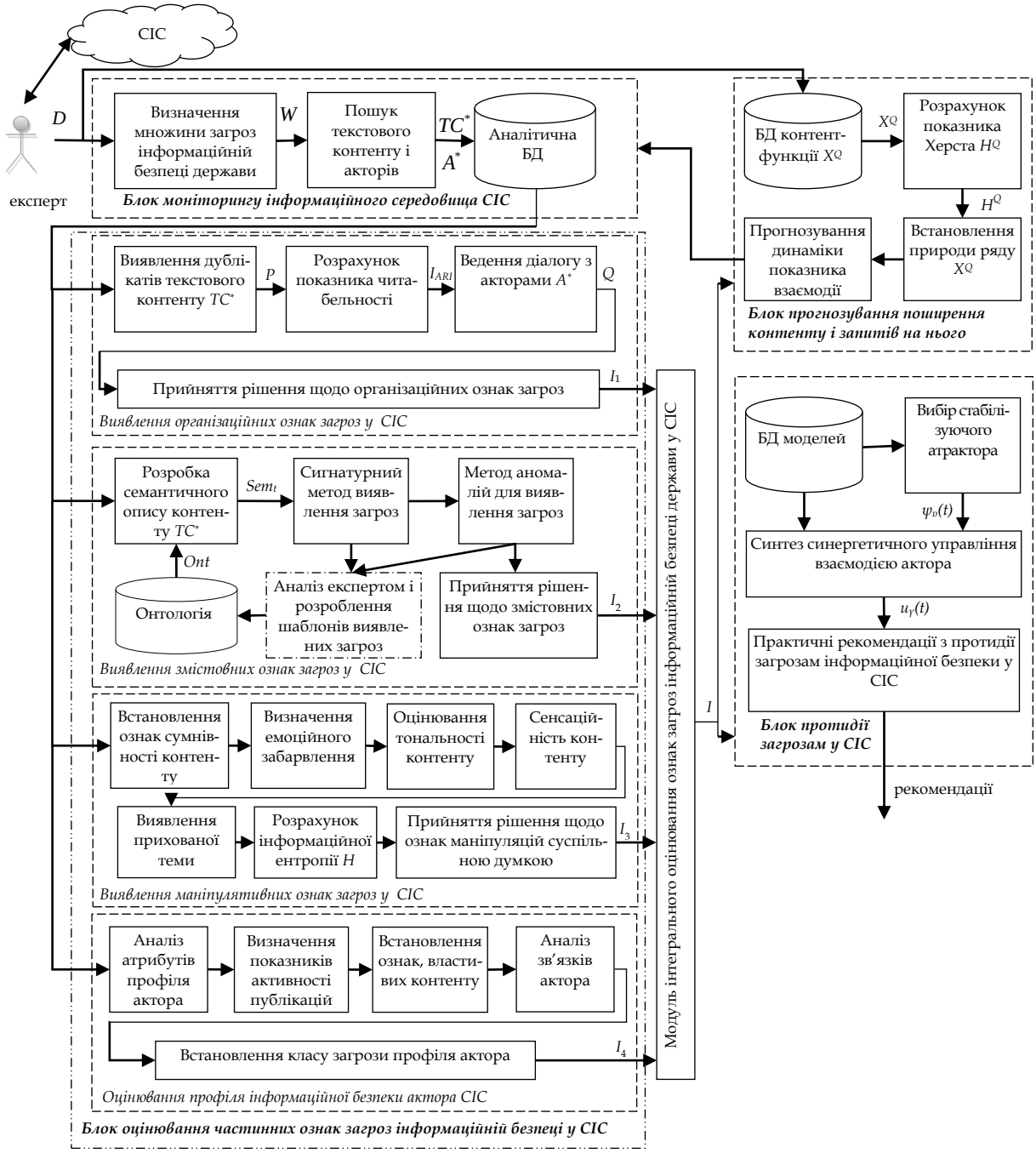

Рис. 3. Структурна схема СППР для виявлення ознак загроз інформаційній безпеці держави у СІС та оцінювання їх рівня

Висновки

Вперше запропоновано модель СППР для виявлення ознак загроз інформаційній безпеці держави у СІС та оцінювання їх рівня, яка є компонентом системи забезпечення інформаційної безпеки держави і забезпечує автоматизацію процедур раннього виявлення та оцінювання загроз. Структурно СППР складаєть з таких модулів: моніторингу інформаційного середовища СІС; оцінювання частинних ознак загроз інформаційній безпеці держави у СІС; прогнозування поширення акторами контенту і запитів на нього; інтегрального оцінювання ознак загроз; протидії загрозам у СІС. Перевагами розробленої моделі СППР є: врахування частинних ознак загроз інформаційній безпеці держави у СІС для детектування різних варіантів прояву інформаційних акцій; визначення рівня загрози на основі інтегрального показника за нелінійною схемою компромісів, що забезпечує досягнення компромісу між частинними критеріями та оптимальність рішення за Парето; прогнозування динаміки поширення контенту й запитів на нього за даними контент-аналізу повідомлень у СІС на основі метрики самоподібності для завчасного корегування вироблених управляючих дій СППР; застосування синергетичного управління взаємодією акторів СІС, що забезпечує запуск у віртуальних спільнотах процесів керованої самоорганізації акторів для переходу віртуальної спільноти до заданого стійкого стану інформаційної безпеки держави.

Таким чином досягається ефективність, оперативність і швидкодія функціонування системи забезпечення інформаційної безпеки держави у СІС,

що є сьогодні вкрай актуальним завданням для України.

Література

[1] С. Гнатюк, ««Нові ідентичності» в Україні та світі: підстави формування, концепції, прогнози. Аналітична записка». [Електронний ресурс]. Режим доступу: http://www.niss.gov.ua/articles/534/.

[2] S. Papadopoulos, Y. Kompatsiaris, A. Vakali, P. Spyridonos, «Community detection in social media», *Data Mining and Knowledge Discovery*, 24(3), pp. 515–554, 2012.

[3] M. Castells, G. Cardoso, «The Network Society: From Knowledge to Policy», *DC: Johns Hopkins Center for Transatlantic Relations*, Washington, 434 p, 2005.

[4] В.П. Горбулін, О.Г. Додонов, Д.В. Ланде, «Інформаційні операції та безпека суспільства: загрози, протидія, моделювання» монографія, К., *Інтертехнологія*, 164 с., 2009.

[5] К.В. Молодецька, «Соціальні інтернет-сервіси як суб'єкт інформаційної безпеки держави», *Information Technology and Security*, vol. 4, Iss. 1(6), с. 13-20, 2016.

[6] А.М. Пелещишин, Р.В. Гумінський, «Загрози інформаційної безпеки держави в соціальних мережах», *Наука і техніка Повітряних Сил Збройних Сил України*, № 2(11), с. 192–199, 2013.

[7] К.В. Молодецька, «Узагальнена класифікація загроз інформаційній безпеці держави в соціальних інтернет-сервісах», *Защита информации*, – вып. 23, с. 75–87, 2016.

[8] Р.В. Грищук, Ю.Г. Даник, «Основи кібернетичної безпеки», монографія, Житомир, 636 с., 2016.

[9] О.К. Юдін, В.М. Богуш, «Інформаційна безпека держави», навч. посіб., Харків, 508 с., 2004.

[10] В.А. Ліпкан, Ю.Є. Максименко, В.М. Желіховський, «Інформаційна безпека Украї-ни в умовах євроінтеграції», навч. посіб., К., КНТ, 280 с., 2006.

[11] В.А. Ліпкан, І.М. Сопілко, В.О. Кір'ян, «Правові засади розвитку інформаційного суспільства в Україні», монографія, К., ФОП О. С. Ліпкан, 664 с., 2015.

[12] Р.В. Гумінський, «Методи і засоби виявлення інформаційних загроз віртуальних спільнот в інтернет середовищі соціальних мереж», дис. канд. техн. наук: 21.05.01, Гумінський Руслан Вікторович, К., 157 с., 2016.

[13] К.В. Молодецька, «Технологія виявлення організаційних ознак інформаційних операцій у соціальних інтернет-сервісах», *Проблеми інформаційних технологій*, № 20. – с. 84–93, – 2016.

[14] К.В. Молодецька-Гринчук, «Метод виявлення ознак інформаційних впливів у соціальних інтернет-сервісах за змістовними ознаками», *Радіоелектроніка, інформатика, управління*, № 2(41), с. 117–126, 2017.

[15] К.В. Молодецька-Гринчук, «Методика виявлення маніпуляцій суспільною думкою у соціальних інтернет-сервісах», *Інформаційна безпека*, № 4 (24), с. 80–92, 2016.

[16] К.В. Молодецька-Гринчук, «Метод побудови профілів інформаційної безпеки акторів соціальних інтернет-сервісів», *Інформаційна безпека*, № 2(26), с. 104–110, 2017.

[17] К.В Молодецька-Гринчук, «Метод оцінювання ознак загроз інформаційній безпеці держави у соціальних інтернет-сервісах», *Автоматизація технологічних і бізнес-процесів*, Vol. 9, Iss. 2/2017, с. 36–42, 2017.

[18] Р.В. Грищук, К.В. Молодецька, «Метод прогнозування динаміки поширення контенту й запитів на нього за даними контент-аналізу повідомлень у соціальних інтернет-сервісах», *Системи управління, навігації та зв'язку*, № 4(36), с. 60–65, 2015.

[19] R. Hryshchuk, K. Molodetska, «Synergetic control of social networking services actors interactions», *Recent Advances in Systems, Control and Information Technology*, Vol. 543, Springer International Publishing, pp. 34 –42, 2017.

[20] Р.В. Грищук, К.В. Молодецька, «Концепція синергетичного управління процесами взаємодії агентів у соціальних інтернет-сервісах», *Безпека інформації*, т. 21, ч. II, с. 123–130, 015.

[21] К.В. Молодецька, «Синтез синергетичного управління попитом агентів на контент у соціальних інтернет-сервісах», *Інформатика та математичні методи в моделюванні*, т. 5, № 4, с. 330–338, 2015.

[22] К.В. Молодецька, «Спосіб підтримання заданого рівня попиту акторів соціальних інтернет-сервісів на контент», *Радіоелектроніка, інформатика, управління*, № 4(35), с. 113–117, 2015.

[23] Доктрина інформаційної безпеки України (затверджена указом Президента України №47 /2017 від 25 лютого 2017 року). [Електронний ресурс]. Режим доступу : http://www.president.gov.ua /documents/472017-21374.

[24] Офіційний сайт Міністерства інформаційної політики України.). [Електронний ресурс]. – Режим доступу: http:/-/mip.gov.ua.

[25] ISO/IEC 27001:2013. Information technology. Security techniques. Information security management systems. Requirements. [Online]. Available at: https://www.iso.org-/standar-d/54534.html.

[26] ISO/IEC 20000-1:2011. Information technology. Service management. Part 1: Service management system requirements. [Online]. Available at: https:// www . iso.org/standard-/51986.htm.

[27] Environmental management. The ISO 14000 family of International Standards. [Online]. Available at: https://www.iso.org/publication/PUB10023-8.html.

[28] ISO 9000:2015. Quality management systems. Fundamentals and vocabulary. [Online]. Available at: https://www.iso.org/standard/45481.html.

[29] M. Sokovic, D. Pavletic, K. Pipan, «Quality improvement metho-dologies–PDCA cycle, RADAR matrix, DMAIC and DFSS», *Journal of Achievements in Materials and Manufacturing Engineering*, 43(1), pp. 476-483, 2010.

[30] А.-В. Шеер, «ARIS – моделирование бизнес-процессов», монография, М., 209 с., 2009.

[31] С.В. Гладиш, «Підтримка прийняття рішень щодо керування інцидентами інформаційної безпеки в організаційно-технічних системах», *Реєстрація, зберігання і обробка даних*, т. 10, № 1, с. 116–124, 2008.

[32] Chr. Manning, P. Raghavan, H. Schütze, «Introduction to Information Retrieval», *Cambridge University Press*, 544 p., 2008.

[33] А.Н. Воронин, «Нелинейная схема компромиссов в многокритериальных задачах оценивания и оптимизации», *Кибернетика и системный анализ*, № 4, с. 106–114, 2009.

[34] Р.В. Грищук, «Диференціально-ігрові моделі та методи моделювання процесів кібернападу», дис. д-ра техн. наук: 21.05.01, Грищук Руслан Валентинович, Нац. авіац. ун-т., Київ, 411 с., 2013.

[35] В.В. Литвин, «Бази знань інтелектуальних систем підтримки прийняття рішень», Львів, *Вид-во Львівської політехніки*, 240 с., 2011.

УДК 004.738.5:004.056.5 (045)

Молодецкая-Гринчук К. В. Модель системы поддержки принятия решений для выявления признаков угроз информационной безопасности страны в социальных интернет-сервисах и оценки их уровня

Аннотация. *Социальные интернет-сервисы представляют собой прогрессивное средство коммуникации участников виртуальных сообществ – акторов. В случае распространения в виртуальных сообществах недостоверного, неполного или искаженного контента социальные интернет-сервисы превращаются в действенный инструмент проведения информационных акций, направленных на манипуляцию общественным мнением, влияние на свободу выбора, распространение призывов к сепаратизму. Поэтому возникает потребность в разработке адекватной модели системы поддержки принятия решений для выявления признаков угроз информационной безопасности государства в социальных интернет-сервисах и оценки их уровня. В основу предложенной модели положены методы выявления частных признаков информационных акций в социальных интернет-сервисах, нелинейную схему компромиссов для их оценки и синергетическое управление для обеспечения управляемого перехода виртуального сообщества к заданному состоянию информационной безопасности. В результате функционирования системы поддержки принятия решений генерируются рекомендуемые решения для противодействия выявленным угрозам. В зависимости от сферы общественной деятельности, на которую влияет угроза, соответствующими государственными исполнительными органами осуществляются мероприятия по ее нейтрализации. Таким образом достигается оперативность, эффективность и быстродействие системы обеспечения информационной безопасности государства в социальных интернет-сервисах.*

Ключевые слова: *социальный интернет-сервис, система поддержки принятия решений, угрозы, процессный подход, контент, информационная безопасность государства.*

Molodetska-Hrynchuk K. The model of decision making support system for detection and assessment of the state information security threat of social networking services

Annotation. *Social networking services represent progressive the communication medium of participants of the virtual communities named actors. In case of distribution in the virtual communities doubtful, incomplete or the distorted content social networking services turn into the effective instrument of holding the information actions directed to manipulation with public opinion, influence on freedom of choice, distribution of appeals to separatism and etc. Therefore there is a need for development the model of decision making support system for detection of the country's information security threat of social networking services and assessment of their level. Controls for support of controlled transition of the virtual community to the given status of information security are the basis for the offered model methods of the of detecting partial signs of information actions in social networking services, the non-linear diagram of compromises for an assessment of signs of threats and synergy. As a result of functioning of decision making support system the recommended decisions are made for counteraction to the revealed threats. Depending on the sphere of public work which the threat influences appropriate public executive bodies carry out actions for its neutralization. Thus efficiency is reached, also high-speed performance of system of support of information security of the state in social networking services is effective.*

Key words: *social networking service, decision support system, threats, process approach, content, state information security.*

Отримано *8 червня 2017 року*, затверджено редколегією *11 липня 2017 року*