DOI: 10.18372/2410-7840.19.12204
УДК 004.056:004.738.5(045)

МЕТОДОЛОГІЯ ПОБУДОВИ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ У СОЦІАЛЬНИХ ІНТЕРНЕТ-СЕРВІСАХ

Руслан Грищук, Катерина Молодецька-Гринчук

Внаслідок впровадження прогресивних інформаційних технологій у всі сфери суспільної діяльності соціальні інтернет-сервіси (СІС) перетворилися на один з найбільш популярних засобів масової комунікацій. Використання СІС для проведення інформаційних операцій може мати наслідками прояви національної ворожнечі, зростання протестних настроїв і перехід віртуальної спільноти до хаотичної динаміки взаємодії. Неконтрольоване поширення таких явищ у реальне життя суспільства становить загрозу інформаційній безпеці держави (ІБД). Тому розроблення ефективної і дієвої методології побудови системи забезпечення ІБД у СІС для протидії зовнішнім і внутрішнім загрозам є актуальним теоретико-прикладним завданням. Запропонована методологія зводиться до трьох етапів – моніторинг текстового контенту в СІС, виявлення і оцінювання ознак загроз, прийняття рішення щодо заходів з протидії виявленим загрозам ІБД у СІС. Виявлення ознак загроз ІБД реалізовано на основі встановлення частинних ознак їх прояву – організаційних, змістовних, маніпулятивних і побудови профілів інформаційної безпеки акторів. З метою протидії виявленим загрозам синтезується синергетичне управління для забезпечення керованого переходу віртуальної спільноти до заданого стану ІБД. Ефективність розробленої методології досягається виробленням своєчасних заходів з виявлення і оцінювання загроз ІБД, використанням природних особливостей взаємодії акторів для синтезу управляючого впливу і штучно-керованого переходу до визначеного стійкого стану ІБД у СІС, що є особливо актуальним для України.

Ключові слова: *соціальний інтернет-сервіс, актор, інформаційна безпека держави, загрози, синергетичне управління, методологія.*

Вступ. Стрімкий розвиток інформаційних технологій в світі й Україні у поєднанні з глобалізаційними процесами призвели до суттєвого зростання ролі соціальних інтернет-сервісів (СІС) у системі соціальних комунікацій [1-4]. СІС надають користувачами, яких називають акторами, інструменти для обміну мультимедійним контентом, утворення зв'язків різного типу з іншими акторами, об'єднання у віртуальні спільноти за відповідними інтересами, фахового розвитку тощо [5]. У сучасних умовах використання СІС забезпечує акумуляцію і розподіл ресурсів з метою максимально повного задоволення суспільних потреб та активізації інноваційної складової розвитку національної економіки. Разом з тим, СІС представляють собою дієвий інструмент для розвитку громадянського суспільства. Завдяки охопленню широкої аудиторії акторів, розвинутим можливостям створення власного контенту та реалізації інформаційної взаємодії СІС стали невід'ємною складовою національного інформаційного простору [1, 4].

Досвід останніх подій показав, що СІС представляють собою джерело загроз інформаційній безпеці держави (ІБД) [3]. Здійснення інформаційно-психологічного впливу на індивідуальну, колективну чи масову свідомість акторів з використанням контенту СІС може призвести до проявів у суспільстві соціальної напруженості, міжнаціональної ворожнечі, протестних настроїв, незадоволення існуючою системою управління в державі тощо [5, 6]. Такі явища можуть неконтрольовано поширитися на реальні суспільні й політичні процеси офлайн. Спираючись на результати вивчення подій «арабської весни», кольорових революцій у країнах СНД, збройної агресії Російської Федерації проти України і анексії Криму можна стверджувати, що СІС відігравали одну з ключових ролей для проведення інформаційних операцій [5]. Зважаючи комплексний характер загроз ІБД у СІС виникає нагальна потреба в розробленні науково обґрунтованої методології забезпечення ІБД у СІС, що є актуальним теоретико-прикладним завданням.

Аналіз останніх досліджень і публікацій [5–9] дозволив визначити пріоритетний напрямок забезпечення ІБД у СІС. Його сутність зводиться до розроблення нових ефективних підходів до виявлення, оцінювання і протидії комплексним загрозам ІБД у СІС. Вагомий внесок у вирішення проблеми забезпечення ІБД, зокрема у СІС, отримано у наукових працях [2, 3, 6–11]. Однак, ці дослідження присвячені розкриттю окремих компонентів існуючої проблеми забезпечення ІБД, застосування яких не дозволяє захистити інформаційний простір СІС від зовнішніх і внутрішніх загроз. Тому вона досі залишається невирішеною у всьому світі й в Україні, де у зв'язку з веденням но-

вої форми протистояння з Російською Федерацією – гібридної війни з використанням СІС зокрема, постала особливо гостро.

Внаслідок складності управління соціотехнічними системами, до яких належать СІС, постійного зростання числа загроз, швидкого розвитку технологій інформаційно-психологічного впливу тощо виникає нагальна потреба у розробленні ефективної та дієвої методології побудови системи забезпечення ІБД у СІС. Встановлено існування об'єктивного протиріччя між проблемою практики, яка пов'язана з необхідністю підвищенні рівня власної ІБД при використанні її громадянами СІС, та проблемою науки, яка зводиться до недосконалості системи ІБД вцілому та відсутності цілісної науково обґрунтованої методології побудови відповідної системи її забезпечення у СІС зокрема, що гарантує системність та комплексність у прийнятті рішень [5]. Тому актуальна науково-прикладна проблема підвищення рівня ІБД у СІС суттєво стримує побудову й розвиток ефективної системи забезпечення інформаційної безпеки людини, суспільства, держави.

Мета статті полягає у розробленні ефективної і дієвої методології побудови системи забезпечення ІБД у СІС для протидії зовнішнім і внутрішнім загрозам.

Основна частина. Дослідження [12-14] функціонування СІС продемонстрували їх належність до класу складних динамічних систем, особливостями яких є ієрархічно організована і цілеспрямована сукупність великої кількості взаємопов'язаних акторів. СІС володіють властивістю самоорганізації акторів у віртуальні спільноти за спільними інтересами і зводиться до спонтанного їх утворення та розпаду, зміни структури чи параметрів взаємодії під впливом зовнішнього інформаційного середовища, внаслідок чого відбувається еволюція системи загалом. Перехід СІС від одного стану ІБД в інший відбувається через хаос внаслідок послаблення зв'язків між акторами віртуальних спільнот. Під час виникнення хаотичної динаміки процесів взаємодії віртуальні спільноти акторів у СІС стають надчутливими до проведення інформаційних операцій, які можуть проводитися в інтересах окремих держав чи груп осіб [2, 5]. У результаті таких дій змінюється шлях розвитку СІС і відбувається перехід на заданий суб'єктом інформаційної операції атрактор. Тому застосування теорії динамічного хаосу для дослідження взаємодії акторів забезпечить адекватність моделей реальним процесам у СІС.

Забезпечення ІБД у СІС може бути досягнутим завдяки управлінню хаотичними процесами взаємодії акторів віртуальних спільнот [15–17]. Для управління хаотичною динамікою віртуальних спільнот доцільно використати процеси самоорганізації акторів, які представляють собою теоретичну основу синергетики. Вивчення результатів захищених дисертацій, науково-дослідних, дослідно-конструкторських робіт, патентів з побудови системи забезпечення ІБД у СІС продемонструвало відсутність використання теорії динамічного хаосу в галузі ІБД у СІС, що визначає пріоритетність даного напрямку наукових досліджень.

Ефективність застосування теорії динамічного хаосу у поєднанні з концепцією синергетичного управління взаємодією акторів у СІС досягається завдяки виконанню наступних вимог [2, 17]:

– взаємодія акторів у СІС має переважно нелінійний характер, що пояснюється не випадковістю таких процесів, а особливостями самого явища соціальних комунікацій. Протікання таких комунікаційних процесів у просторі й часі є корельованим, у результаті чого відбувається підсилення чи послаблення прояву ефектів впливу контенту на індивідуальну, групову чи масову свідомість акторів;

– СІС представляють собою відкриту систему для залучення нових акторів і взаємодії із зовнішнім інформаційним середовищем функціонування, яке формується не тільки вітчизняними засобами масової інформації (ЗМІ), але й глобальним інформаційним простором. Тому СІС перебувають у нерівноважному стані, завдяки чому притік контенту дозволяє не тільки сповільнити зростання ентропії у системі, але й зменшити її величину;

– існування декількох шляхів еволюції СІС на завершальних етапах переходу кількісних змін параметрів взаємодії акторів у якісні зміни стану ІБД. Такі переходи СІС з одного стану ІБД в інший описуються типовими рівняннями відносно параметрів порядку.

Застосування теорії динамічного хаосу для моделювання процесів взаємодії акторів у СІС зводиться до дотримання таких вимог, що обумовлені сутністю даної теорії [17]: існування системи нелінійних диференціальних рівнянь, яка описує досліджуваний аспект взаємодії акторів; вибір атрактора, який визначатиме заданий стан ІБД; вибір параметра порядку, що є показником взаємодії акторів і управління яким забезпечить перехід до заданого атрактора.

Спираючись на сформульовану мету досліджень, загальновживана термінологія теорії динамічного хаосу [16] в статті використовується наступним чином: елемент системи називається актором СІС, фазовий простір представляє собою множину допустимих дій актора у СІС. Зображуюча точка системи визначає конкретні дії актора з множини можливих. Параметр порядку – це змінна, яка визначає динаміку взаємодії акторів при станах, близьких до фазового переходу. Атрактор характеризує деякий стан ІБД, досягнення якої можливе завдяки обраній траєкторії еволюції взаємодії акторів у СІС. Точка біфуркації – це критичний стан віртуальної спільноти акторів, в якому виникає невизначеність щодо вибору деякої траєкторії еволюції для переходу в один з можливих станів ІБД.

Проблема забезпечення ІБД у СІС не обмежується розробленням дієвих підходів до протидії загрозам. Попередній аналіз показав, що наслідками проведення інформаційних операцій у СІС може бути перехід віртуальної спільноти на задану траєкторію еволюції. При цьому в області точок біфуркації виникають суттєві коливання перед вибором конкретного шляху еволюції СІС – флуктуації, перехід до нового напрямку розвитку призводить до появи незворотних змін функціонування, а такі явища називають катастрофами [2]. Швидкість появи катастрофи необмежено зростає, коли прояви її ознак у системі стають очевидними. Тому завчасне попередження виникнення таких станів ІБД у СІС завдяки завчасному виявленню і оцінюванню ознак загроз для прийняття обґрунтованих рішень щодо протидії є важливим завданням на шляху розроблення методології побудови системи забезпечення ІБД у СІС.

Сучасні загрози ІБД у СІС мають комплексний характер, відрізняються між собою за масштабністю, способом впливу на акторів, частотою повторюваності тощо [3]. Процедури детектування таких загроз ІБД у СІС додатково ускладнюються відсутністю узагальнених ознак прояву і постійним розвитком інформаційних технологій прихованого впливу на акторів. Узагальнення досвіду проведення інформаційних операцій проти України в умовах ведення гібридної війни з Російською Федерацією продемонструвало, що з метою формування суспільної думки, поширення заданого контенту, блокування окремих аккаунтів акторів у СІС використовують соціальних ботів [5]. Встановлено, що поширюваний контент містив дезінформацію, технології маніпуляції суспільною думкою для нав'язування та спонукання до певних дій не тільки у СІС, але й реальному житті. Також прихований інформаційний вплив здійснювався завдяки відхиленням від загальноприйнятого вживання лексем відповідної предметної області текстового контенту. Ключовим джерелом контенту в СІС виступають актори, які створюють його самостійно або поширюють від інших акторів, віртуальних спільнот чи ЗМІ. Агрегація і узагальнення інформації профілів акторів, їх зв'язків, віртуальними спільнотами, особливостей поведінки у СІС дозволяє зробити висновок про їх залучення до інформаційних операцій проти ІБД. Тому виявлення і оцінювання ознак загроз доцільно реалізувати за ознаками їх прояву – організаційними, змістовними, маніпулятивними та на основі оцінювання профілів інформаційної безпеки акторів у СІС.

Спираючись на відомий підхід до розроблення методологій [18] на основі результатів проведених досліджень [5, 19-25] у статті запропоновано методологію побудови систем забезпечення ІБД у СІС. Вона складається з таких етапів (рис. 1): моніторинг текстового контенту в СІС; виявлення і оцінювання ознак загроз ІБД у СІС; прийняття рішення щодо заходів з протидії виявленим загрозам ІБД у СІС.

1. Моніторинг текстового контенту в СІС. На першому етапі експертом з ІБД реалізовується аналіз значущої для суспільства тематики публікацій у СІС. Для цього проводиться дослідження текстового контенту TC, який складає найбільшу частку інформаційного простору віртуальних спільнот СІС.

При цьому експерт виконує формалізацію множини можливих загроз ІБД у СІС як кортежу відповідно до моделі

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

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

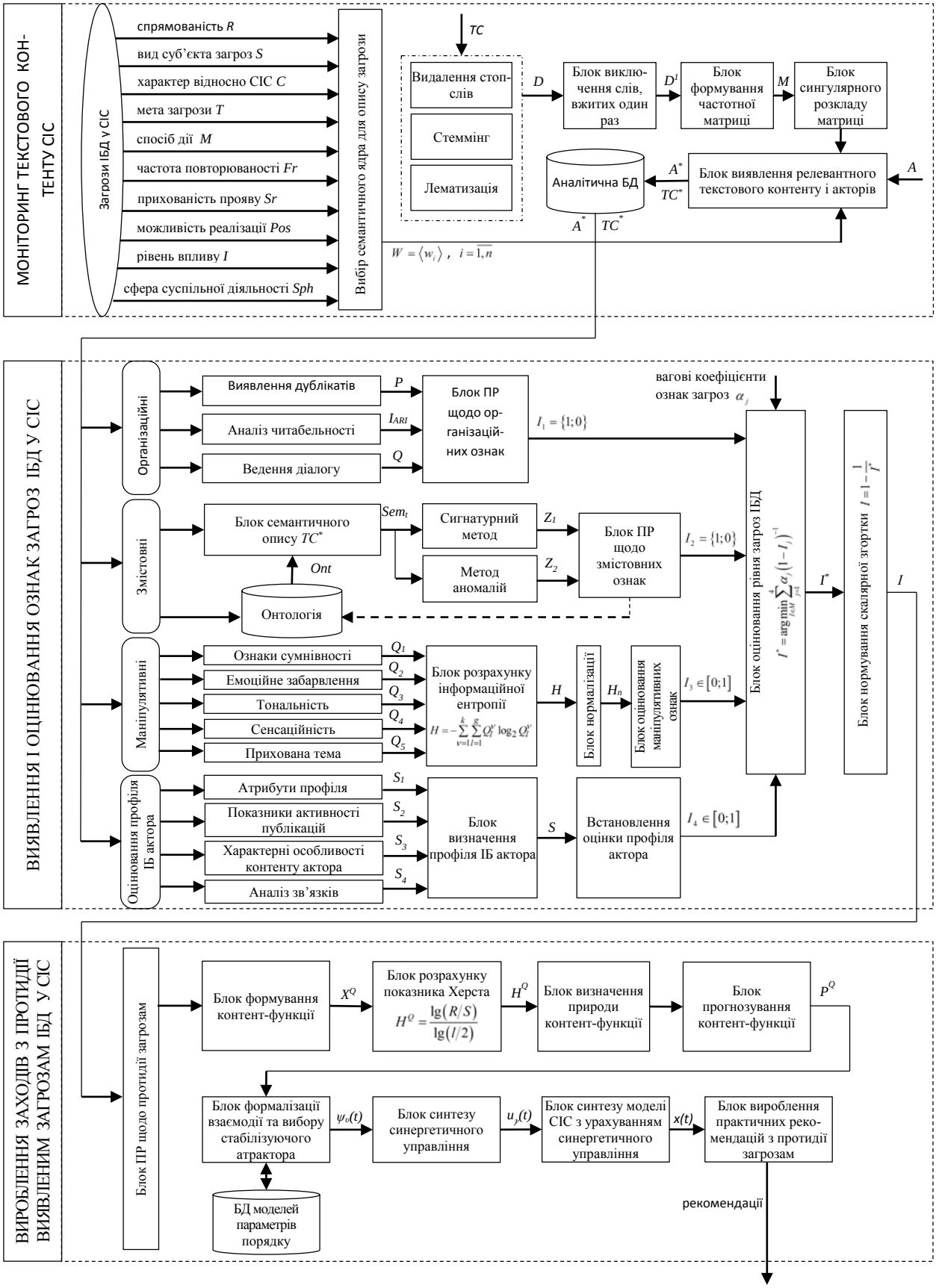

Рис. 1. Схема методології побудови системи забезпечення ІБД у СІС

Моніторинг текстового контенту у СІС здійснюється на основі семантичного ядра $W = \langle w_i \rangle$, $i = \overline{1,n}$. Для інформаційного пошуку застосовується метод латентно-семантичної індексації (*LSI*) з метою індексації контенту з урахуванням його змісту і прихованих семантичних залежностей, суть якого подана у публікації [20]. Спочатку виконується попередня обробка текстового контенту: видалення стоп-слів, стеммінг і лематизація.

Далі виключаються слова, які вживаються тільки один раз і реалізується побудова частотної матриці M. Після цього виконується сингулярний розклад частотної матриці M для знаходження у СІС релевантного семантичному ядру текстового контенту TC^* і акторів, які його поширювали A^*. Відібрані дані накопичуються у відповідній аналітичній базі даних (БД).

2. Виявлення і оцінювання ознак загроз ІБД у СІС. На цьому етапі виконується аналіз попередньо відібраного текстового контенту TC^* і даних акторів A^*. Для цього встановлюється наявність таких ознак ІБД у СІС: організаційних, змістовних, маніпулятивних і виконується оцінювання профілів інформаційної безпеки акторів.

Виявлення організаційних ознак загроз спирається на відповідну запропоновану технологію [19], яка зводиться до пошуку дублікатів P текстового контенту TC^* на основі методу шинглів; розрахунку показника читабельності I_{ARI}, що характеризує складність розуміння текстового контенту; ведення діалогу Q з досліджуваним актором. Після цього приймається рішення (ПР) про наявність організаційних ознак загроз на базі відповідних правил. У результаті відповідний показник I_1 набуває значень $\{0;1\}$.

Знаходження ознак загроз ІБД у змісті текстового контенту TC^* ґрунтується на використанні відповідного методу, представленого у статті [20], і полягає в семантичному аналізі на базі онтологій *Ont*. Спочатку виконується семантичний опис Sem_t досліджуваного текстового контенту TC^*. Виявлення зводиться до застосування сигнатурного методу і методу аномалій. Для цього проводиться детектування випадків вживання у TC^* об'єкта публікації з його характеристиками сумісно з негативними ознаками у випадку реалізації загроз і наявності відповідності між семантичними шаблонами загроз і конструкціями у Sem_t. В окремих випадках текстовий контент TC^* може характеризуватися високою релевантністю до семантичного ядра W з відсутністю змістовних ознак загроз ІБД. Тоді текстовий контент TC^* підлягає додатковій обробці експертом з ІБД для остаточної перевірки і додавання нових семантичних шаблонів загроз та їх використання системою забезпечення ІБД. Результуюча оцінка наявності змістовних ознак загроз I_2 приймає значення $\{0;1\}$.

На основі методики детектування маніпуляцій суспільною думкою у СІС [21] проводиться встановлення рівня прояву даної ознаки загроз ІБД. При цьому на основі методів контент-аналізу, тематичного моделювання і методів машинного навчання виявляються такі ознаки маніпуляцій у текстовому контенті TC^*: сумнівності викладених фактів Q_1; емоційного забарвлення контенту Q_2; тональності Q_3; сенсаційності Q_4; наявності прихованої теми Q_5. Далі проводиться розрахунок інформаційної ентропії H, яка характеризує рівень невизначеності щодо наявності прихованого інформаційно-психологічного впливу на акторів. Перехід до якісної шкали оцінки загроз маніпуляцій суспільною думкою у СІС виконується у результаті нормалізації отриманих розрахункових величин інформаційної ентропії H_n, а показник I_3 визначається на діапазоні $[0;1]$.

Виявлення акторів, які залучені до проведення інформаційних операцій у СІС, спирається на методику оцінювання профілів інформаційної безпеки акторів [22]. Спочатку виконується аналіз атрибутів профіля актора у СІС S_1, визначаються показники активності публікації контенту S_2, встановлюються характерні особливості текстового контенту профіля актора S_3 і аналізуються його зв'язки з іншими акторами та віртуальними спільнотами у СІС S_4. Дані атрибути агрегуються для розподілу досліджуваних акторів у задані класи загроз ІБД як можливих учасників інформаційних операцій. Узагальнена оцінка профілів інформаційної безпеки акторів у СІС I_4 набуває значень на інтервалі $[0;1]$.

Визначення інтегральної оцінки I^* ознак загроз у СІС I_j, $j=\overline{1;4}$ [26] полягає у розв'язку багатокритерійної задачі оцінювання із різними ваговими коефіцієнтами α_j на основі нелінійної схеми компромісів професора Вороніна А. М. $I^* = \arg\min_{I\in M} \sum_{j=1}^{4} \alpha_j \left(1-I_j\right)^{-1}$. Для переходу до якісної шкали оцінювання, отриманий показник I^* нормується до мінімуму $I = 1-\frac{1}{I^*}$. У результаті узагальнена оцінка ознак загроз ІБД у СІС $I \in [0;1]$.

3. Прийняття рішення щодо заходів з протидії виявленим загрозам ІБД у СІС є завершальним етапом розробленої методології. На основі значення інтегральної оцінки ознак загроз ІБД у СІС виконується ПР про заходи з протидії. Якщо $I \in [0;0,3]$, то рівень загрози «відсутня» і не потребує використання ресурсів системи забезпечення ІБД. У випадку оцінки загрози $I \in [0,31;0,50]$ її рівень визначається як «нижча середнього», тоді продовжуються дії з моніторингу інформаційного середовища СІС відповідно до першого етапу. При значеннях оцінки загрози $I \in [0,51;0,70]$ вона приймає значення «вища середнього» і окрім моніторингу інформаційного середовища СІС виконується прогнозування поширення деструктивного текстового контенту та запитів на нього відповідно до методу, описаного у публікації [23].

Для цього проводиться дослідження контент-функції $X^Q(t)$, яка характеризує динаміку публікації контенту і запитів акторів на нього. Виконується розрахунок показника Херста $H^Q = \frac{\lg(R/S)}{\lg(l/2)}$ самоподібності контент-функції, 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. На основі аналізу обчисленого значення встановлюється природа контент-функції $X^Q(t)$ – випадкова, антиперсистентна (ергодична), персистентна. Прогнозування зміни контент-функції $X^Q(t)$ здійснюється для персистентного ряду при $H^Q > 0,5$ з використанням методу найменших квадратів.

Якщо оцінка ознак загроз ІБД у СІС визначена на інтервалі $I \in [0,7;1]$, то загроза набуває значення «існує». Окрім моніторингу інформаційного середовища СІС для реалізації керованого переходу віртуальної спільноти до заданого стану ІБД використовується концепція синергетичного управління взаємодією акторів [24]. Спочатку експерт з ІБД формалізує процеси взаємодії акторів у формі системи нелінійних диференціальних рівнянь і обирає стабілізуючий атрактор $\psi_v(t)$, який описує динаміку взаємодії акторів до досягнення заданого стану ІБД у СІС. Синергетичне управління $u_\gamma(t)$, синтезується у результаті введення у систему показника $\frac{d\psi_v(t)}{dt}$, який забезпечує запуск процесів самоорганізації акторів у віртуальних спільнотах. У точці $\psi_v(t)=0$ досягається заданий стійкий стан ІБД у СІС.

На заключному кроці формуються практичні рекомендації з протидії виявленим загрозам ІБД у СІС, залежно від моделі загрози і сфери суспільної діяльності, на яку вона націлена. Проводиться залучення державних виконавчих органів відповідно до чинної Доктрини інформаційної безпеки України [27].

Експериментальне дослідження розробленого методологічного інструментарію, який покладений в основу запропонованої методології побудови системи забезпечення ІБД у СІС, відображені у відповідних публікаціях [20, 21, 23-25].

Висновки. Запропонована методологія побудови системи забезпечення ІБД у СІС дозволяє розробити дієві програмні комплекси для завчасного виявлення, оцінювання і протидії загрозам, які можуть бути інтегровані з новітніми інформаційними технологіями забезпечення ІБД у СІС в реальному часі. Застосування методології дозволить врахувати частинні прояви ознак загроз ІБД у СІС для завчасного детектування інформаційних операцій у віртуальних спільнотах і забезпечить оптимальність рішення про узагальнений рівень виявлених загроз. Завдяки виконанню прогнозування контент-функції на базі метрики самоподібності забезпечується

корегування вироблених рішень в умовах зміни обстановки у інформаційному просторі СІС та обмеженості ресурсів системи забезпечення ІБД у СІС. Ефективність протидії загрозам ІБД у СІС досягається використанням природних особливостей взаємодії акторів для синтезу управляючого впливу і штучно-керованого переходу до заданого стану ІБД у СІС, що є особливо актуальним для України.

ЛІТЕРАТУРА

[1]. О. Онищенко, В. Горовий, В. Попик, *Соціальні мережі як інструмент взаємовпливу влади та громадянського суспільства. Монографія.* Київ, 2014, 260 с.

[2]. В. Горбулін, О. Додонов, Д. Ланде, *Інформаційні операції та безпека суспільства : загрози, протидія, моделювання. Монографія.* Київ: Інтертехнологія, 2009, 164 с.

[3]. Р. Грищук, Ю. Даник, *Основи кібернетичної безпеки. Монографія.* Житомир: ЖНАЕУ, 2016, 636 с.

[4]. В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа, *Інформаційна та кібербезпека: соціотехнічний аспект.* В. Б. Толубко, Ред. Київ: ДУТ, 2015, 288 с.

[5]. Р. Грищук, К. Молодецька-Гринчук, "Постановка проблеми забезпечення інформаційної безпеки держави у соціальних інтернет-сервісах", *Сучасний захист інформації*, №3(31), С. 86–96, 2017.

[6]. В. Б. Толубко, *Інформаційна боротьба (концептуальні, теоретичні, технологічні аспекти): Монографія.* Київ: НАОУ, 2003, 320 с.

[7]. О. Юдін, В. Богуш, *Інформаційна безпека держави.* Харків: Консум, 2004, 508 с.

[8]. В. Ліпкан, І. Сопілко, В. Кір'ян, *Правові засади розвитку інформаційного суспільства в Україні. Монографія.* К.: ФОП О. С. Ліпкан, 2015, 664 с.

[9]. Р. Гумінський, "Методи і засоби виявлення інформаційних загроз віртуальних спільнот в інтернет середовищі соціальних мереж", дис. канд. техн. наук, Національний авіаційний університет, 2016.

[10]. Д. Губанов, Д. Новиков, А. Чхартишвили, *Социальные сети : модели информационного влияния, управления и противоборства. Монография.* М.: Изд. физ.-мат. лит., 2010, 228 с.

[11]. Г. Остапенко, Д. Новиков, *I Информационные риски в социальных сетях.* Воронеж: Научная книга, 2013, 161 с.

[12]. J. Epstein, *Generative Social Science: Studies in Agent-Based Computational Modeling.* Princeton: Princeton University Press, 2012, 384 p.

[13]. C. Barrett, S. Eubank, M. Marathe, "Modeling and simulation of large biological, information and socio-technical systems: an interaction based approach", in *Interactive Computation*, Berlin: Springer Berlin Heidelberg, 2006, pp. 353–392.

[14]. S. Wasserman, K. Faust, *Social network analysis.* Cambridge: Cambridge university press, 1994, 825 p.

[15]. J. Nicolis, *Dynamics of hierarchical systems.* Berlin: Springer Berlin Heidelberg, 1986, 488 p.

[16]. M. Tabor, *Chaos and integrability in nonlinear dynamics.* New York: Wiley, 1989, p. 318.

[17]. А. Колесников, *Синергетические методы управления сложными системами: теория системного синтеза.* М.: Едиторал УРСС, 2005, 228 с.

[18]. Р. Грищук, О. Корченко, "Методологія синтезу та аналізу диференціально-ігрових моделей та методів моделювання процесів кібернападу на державні інформаційні ресурси", *Захист інформації*, №3, С. 115-122., 2012.

[19]. К. Молодецька, "Технологія виявлення організаційних ознак інформаційних операцій у соціальних інтернет-сервісах", *Проблеми інформаційних технологій*, № 20, С. 84-93, 2016.

[20]. К. Молодецька-Гринчук, "Метод виявлення ознак інформаційних впливів у соціальних інтернет-сервісах за змістовними ознаками", *Радіоелектроніка, інформатика, управління*, №2(41), С. 117-126, 2017.

[21]. К. Молодецька-Гринчук, "Методика виявлення маніпуляцій суспільною думкою у соціальних інтернет-сервісах", *Інформаційна безпека*, №2(24), С. 80-92, 2016.

[22]. К. Молодецька-Гринчук, "Метод побудови профілів інформаційної безпеки акторів соціальних інтернет-сервісів", *Інформаційна безпека*, №2(26), С. 104-110, 2017.

[23]. Р. Грищук, К. 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. 85-92, 2015.

[24]. Р. Грищук, К. Молодецька, "Концепція синергетичного управління процесами взаємодії агентів у соціальних інтернет-сервісах", *Безпека інформації*, Т. 21, №2, С. 123-130, 2015.

[25]. К. Молодецкая, "Валидация синергетического управления взаимодействием акторов в социальных интернет-сервисах", *Computer Science and Telecommunications: electronic journal*, № 2, pp. 18-26, 2016. [Електронний ресурс]. Режим доступа: http:// gesj. networking-academy. org. ge / download. php? id= 2735. pdf. Дата обращения: Ноябрь. 1, 2017.

[26]. А. Н. Воронин, "Нелинейная схема компромиссов в многокритериальных задачах оценивания и оптимизации", *Кибернетика и системный анализ*, № 4, С. 106-114, 2009.

[27]. Офіційне представництво Президента України. (2017, Лют. 25). Указ Президента України №47/2017, Доктрина інформаційної безпеки України. [Електронний ресурс]. Режим доступа: http://www.president.gov.ua/documents/472017-21374.

REFERENCES

[1]. O. Onyshchenko, V. Horovyi, V. Popyk, *Social networks as an instrument of mutual influence of power and civil society. Monohrafiia.* Kyiv, 2014, 260 p.

[2]. V. Horbulin, O. Dodonov, D. Lande, *Information operations and public safety: threats, counteraction, modeling. Monohrafiia.* Kyiv: Intertekhnolohiia, 2009, 164 p.

[3]. R. Hryshchuk, Yu. Danyk, *Fundamentals of cyber security. Monohrafiia.* Zhytomyr: ZhNAEU, 2016, 636 p.

[4]. V. Buriachok, V. Tolubko, V. Khoroshko, S. Toliupa, *Information and cybersecurity: sociotechnical aspect.* V. B. Tolubko, Red. Kyiv: DUT, 2015, 288 p.

[5]. R. Hryshchuk, K. Molodetska-Hrynchuk, "Setting the problem of ensuring state information security in social networking services", *Suchasnyi zakhyst informatsii*, no. 3(31), pp. 86-96, 2017.

[6]. V. Tolubko, *Information struggle (conceptual, theoretical, technological aspects): Monograph.* Kyiv: NAOU, 2003, 320 p.

[7]. O. Yudin and V. Bohush, *Information security of the state.* Kharkiv: Konsum, 2004, 508 p.

[8]. V. Lipkan, I. Sopilko, V. Kirian, *Legal principles of the development of the information society in Ukraine v Ukraini. Monohrafiia.* K.: FOP O. Lipkan, 2015, 664 p.

[9]. R. Huminskyi, "Methods and means of detecting information threats of virtual communities in the Internet environment of social networks", dys. kand. tekhn. nauk, Natsionalnyi aviatsiinyi universytet, 2016.

[10]. D. Hubanov, D. Novykov, A. Chkhartyshvyly, *Social networks: models of information influence, management and confrontation. Monohrafyia.* M.: Yzd. fyz.-mat. lyt., 2010, 228 p.

[11]. H. Ostapenko, D. Novykov, *Information risks in social networks.* Voronezh: Nauchnaia knyha, 2013, 161 p.

[12]. J. Epstein, *Generative Social Science : Studies in Agent-Based Computational Modeling.* Princeton: Princeton University Press, 2012, 384 p.

[13]. C. Barrett, S. Eubank, M. Marathe, "Modeling and simulation of large biological, information and socio-technical systems: an interaction based approach", in *Interactive Computation*, Berlin: Springer Berlin Heidelberg, 2006, pp. 353-392.

[14]. S. Wasserman, K. Faust, *Social network analysis.* Cambridge: Cambridge university press, 1994, 825 p.

[15]. J. Nicolis, *Dynamics of hierarchical systems.* Berlin: Springer Berlin Heidelberg, 1986, 488 p.

[16]. M. Tabor, *Chaos and integrability in nonlinear dynamics.* New York: Wiley, 1989, 318 p.

[17]. A. Kolesnykov, *Synergetic methods for controling complex systems: the theory of system synthesis.* Moskov: Edytoral URSS, 2005, 228 p.

[18]. R. Hryshchuk, O. Korchenko, "Methodology of synthesis and analysis of differential game models and methods for modeling cyber attack processes on state information resources", *Zakhyst informatsii*, no. 3, pp. 115-122, 2012.

[19]. K. Molodetska, "Technology of identifying organizational features of information operations in social networking services", *Problemy informatsiinykh tekhnolohii*, no. 20, pp. 84-93, 2016.

[20]. K. Molodetska-Hrynchuk, "Method of revealing signs of information influences in social Internet services on the basis of content", *Radioelektronika, informatyka, upravlinnia*, no. 2(41), pp. 117-126, 2017.

[21]. K. Molodetska-Hrynchuk, "A method of detecting manipulation of public opinion in social networking services", *Informatsiina bezpeka*, no. 2(24), pp. 80-92, 2016.

[22]. K. Molodetska-Hrynchuk, "Method of constructing profiles of information security actors of social networking services", *Informatsiina bezpeka*, no. 2(26), pp. 104-110, 2017.

[23]. R. Hryshchuk, K. Molodetska, "Method of forecasting the distribution dynamics of content and requests for it according to the content analysis of messages in social networking services", *Systemy upravlinnia, navihatsii ta zviazku*, no. 4(36), pp. 85-92, 2015.

[24]. R. Hryshchuk, K. Molodetska, "The concept of synergistic management of agents interaction in social networking services", *Bezpeka informatsii*, vol. 21, no. 2, pp. 123-130, 2015.

[25]. K. Molodetskaia, " Validating the social networking services actors' interaction synergetic control", Computer Science and Telecommunications: electronic journal. [Online]. Available: http://gesj. networking-academy.org.ge/download.php? id=2735.pdf. Accessed: Nov. 1, 2017.

[26]. A. Voronin, "Nonlinear Compromise Scheme in Multi-Criteria Evaluation and Optimization Problems", *Cybernetics and System Analysis*, no. 4, pp. 106-114, 2009.

[27]. President of Ukraine official Web-site. (2017, Feb. 25). Decree of the President of Ukraine No. 47/2017, Doctrine of Information Security of Ukraine. [Online]. Available: http://www.president.gov.ua/documents/472017-21374.

МЕТОДОЛОГИЯ ПОСТРОЕНИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА В СОЦИАЛЬНЫХ ИНТЕРНЕТ-СЕРВИСАХ

В результате внедрения прогрессивных информационных технологий во все сферы общественной деятельности социальные интернет-сервисы (СИС) превратились в одно из самых популярных средств массовой коммуникаций. Результатами проведения информационных операций в СИС могут быть проявления национальной розни, рост протестных на-

строений и переход виртуального сообщества к хаотической динамике взаимодействия. Неконтролируемое распространение таких явлений в реальную жизнь общества представляет угрозу информационной безопасности государства (ИБД). Поэтому разработка эффективной и действенной методологии построения системы обеспечения ИБД в СИС для противодействия внешним и внутренним угрозам является актуальной теоретико-прикладной задачей. Предложенная методология сводится к трем этапам – мониторинг текстового контента в СИС, выявление и оценка признаков угроз, принятие решения о мерах по противодействию выявленным угрозам ИБД в СИС. Выявление признаков угроз ИБД реализовано на основе установления частных признаков их проявления - организационных, содержательных, манипулятивных и построения профилей информационной безопасности акторов. С целью противодействия выявленным угрозам синтезируется синергетическое управления для обеспечения управляемого перехода виртуального сообщества к заданному состоянию ИБД. Эффективность разработанной методологии достигается выработкой своевременных мер по выявлению и оценке угроз ИБД, использованием природных особенностей взаимодействия акторов для синтеза управляющего воздействия и искусственно управляемого перехода к определенному состоянию ИБД в СИС, что особенно актуально для Украины.

Ключевые слова: социальный интернет-сервис, актер, информационная безопасность государства, угрозы, синергетическое управления, методология.

METHODOLOGY FOR THE CONSTRUCTION THE SYSTEM OF STATE INFORMATION SECURITY PROVIDING IN SOCIAL NETWORKING SERVICES

Social networking services (SNS) have become one of the most popular media outlets in a result of the introduction advanced information technologies in all spheres of social activity. Consequences of conducting information operations in the SNS can be manifestations of national enmity, the growth of protest sentiment and the transition of the virtual community to the chaotic interaction dynamics. The uncontrolled spread of such phenomena in the real life of a society poses is a threat to the state information security (SIS). Therefore, the development of an effective and efficient methodology for the constructing a system for SIS providing in SNS to counter the external and internal threats is an actual theoretical and applied task. The proposed methodology is divided into three stages - monitoring text content in the SIS, identifying and evaluating the signs of threats, making decisions on measures to counter identified threats to the SIS in the SNS. Detection the signs of SIS threats is realized on the basis of the establishment of partial features of their manifestation - organizational, informative, manipulative and building profiles of actors' information security. In order to counteract the identified threats, synergistic control is synthesized to provide a managed transition of the virtual community to a given state of the SIS. The effectiveness of the developed methodology is achieved by developing timely measures to identify and assess the threats of the SIS, using the natural peculiarities of the actors' interaction for the synthesis of controlling influence and the artificially-controlled transition to a definite state of the SIS in the SNS, which is especially relevant for Ukraine.

Keywords: social networking service, actor, state information security, threats, synergetic control, methodology.

Грищук Руслан Валентинович, доктор технічних наук, старший науковий співробітник, начальник відділу інформаційної та кібернетичної безпеки наукового центру Житомирського військового інституту імені С. П. Корольова.
E-mail: Dr.Hry@i.ua

Грищук Руслан Валентинович, доктор технических наук, старший научный сотрудник, начальник отдела информационной и кибернетической безопасности научного центра Житомирского военного института имени С. П. Королева.

Hryshchuk Ruslan, Dr. Eng. (Information security), Senior Scientific Advisor, Senior Research Officer, Cybersecurity Department of the Research Center of Sergey Korolyov Military Institute.

Молодецька-Гринчук Катерина Валеріївна, кандидат технічних наук, доцент, доцент кафедри комп'ютерних технологій і моделювання систем Житомирського національного агроекологічного університету.
E-mail: kmolodetska@gmail.com

Молодецкая-Гринчук Екатерина Валерьевна, кандидат технических наук, доцент, доцент кафедры компьютерных технологий и моделирования систем Житомирского национального агроэкологического университета.

Molodetska-Hrynchuk Kateryna, PhD in Eng., associate professor of IT and systems modeling department, Zhytomyr National Agroecological University.