UDC 004.738.5:004.056.5(045)

МЕТОД ОЦІНЮВАННЯ ОЗНАК ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ДЕРЖАВИ У СОЦІАЛЬНИХ ІНТЕРНЕТ-СЕРВІСАХ

К. Молодецька-Гринчук [1]

[1]Житомирський національний агроекологічний університет, Житомир, Ukraine
ORCID: [1]0000-0001-9864-2463
E-mail: [1]kmolodetska@gmail.com

DOI: 10.15673/atbp.v9i2.560

Анотація: На сучасному етапі соціальні інтернет-сервіси перетворилися на дієвий інструмент комунікації учасників віртуальних спільнот – акторів. Також соціальні інтернет-сервіси використовуються для самоорганізації громадянського суспільства, координації з метою впливу на політичні й суспільні процеси у державі. У випадку поширення в соціальних інтернет-сервісах недостовірного контенту вони перетворюються на джерело загроз інформаційній безпеці особистості, суспільства, держави. Відсутність ефективних методик виявлення ознак загроз у соціальних інтернет-сервісах створює передумови для проведення інформаційних операцій в інтересах провідних держав світу чи зацікавлених осіб. Серед ознак загроз інформаційній безпеці держави виділено організацій, змістовні, маніпулятивні та оцінки профілів інформаційної безпеки акторів. Розроблено метод оцінювання ознак загроз, який ґрунтується на їх скалярній згортці по нелінійній схемі компромісів. Перевагами методу є застосуванням сучасних підходів до виявлення ознак інформаційних акцій у соціальних інтернет-сервісах, компроміс між частинними критеріями і оптимальність отриманого рішення за Парето. Проведено експертне оцінювання фахівців у галузі інформаційної безпеки для встановлення пріоритетності ознак загроз. Виконано експериментальне дослідження запропонованого методу оцінювання ознак загроз на прикладі реальної інформаційної акції. Отримані результати збіжні з висновками міжнародних організацій, що доводить його дієвість та ефективність. Застосування розробленого методу для функціонування системи забезпечення інформаційної безпеки держави у соціальних інтернет-сервісах дозволить автоматизувати процедури раннього виявлення загроз, підвищити її оперативність і швидкодію.

Abstract: At the present stage of social networking services have become an effective tool of communication participants virtual communities named actors. Also social networking services are used for coordination self-civil society to influence political and social processes at the country. If social networking services spread unreliable content, they become a source of threats to information security of the individual, society and state. The absence of effective methods detection of threats at the social networking services creates conditions for conducting information operations in the interests of leading countries or stakeholders. Among the signs of threats to information security are selected organizations comprehensive, manipulative and evaluation of information security profiles of actors. The method of evaluating characteristics of threats based on their scalar convolution in nonlinear circuit compromise. The advantages of this method are using modern approaches to share information signs of social networking services, partial compromise between optimality criteria and the resulting solution Pareto. Experimental study of the proposed evaluation method signs of threats on the example of real information action. The results concordant with the findings of international organizations prove its efficiency and effectiveness. Application of the developed method for the functioning of the information security of the state in social networking services will automate procedures for early detection, increase its efficiency and performance.

Ключові слова: Інформаційна безпека, соціальні інтернет-сервіси, актори, загрози, нелінійна схема компромісів.
Keywords: Information security, social networking services, actor, threats, non-linear scheme of compromises.

Вступ

Сьогодні соціальні інтернет-сервіси (СІС) використовуються учасниками віртуальних спільнот – акторами, для утворення інформаційних зв’язків з іншими акторами, оперативного поширення власного контенту, самоорганізації з метою впливу на суспільні та політичні процеси в державі [1, 2]. Висока популярність СІС у процесах соціальної комунікації пояснюється їх доступністю для пересічних користувачів, наявністю засобів організації у групи зі

спільними інтересами, транскордонністю процесів взаємодії тощо. Однак, практичний досвід використання СІС як засобу масової комунікації показав, що вони перетворилися на дієвий інструмент проведення інформаційних операцій і реалізації загроз інформаційній безпеці особистості, суспільства, держави.

У попередніх дослідженнях [3] встановлено, що метою таких загроз може бути вплив на психічний і емоційний стан, свободу вибору акторів СІС; поширення закликів до сепаратизму, повалення конституційного ладу, порушення територіальної цілісності; дискредитація органів державної влади; підтримка, супроводження чи активізація злочинної або терористичної діяльності тощо. У свою чергу, ведення Російською Федерацією гібридної війни проти України продемонструвало появу якісно нових і дієвих технологій інформаційного впливу на акторів СІС. Це призвело до виникнення протиріччя між рівнем новітніх інформаційних технологій впливу на акторів СІС і науковим базисом оцінки рівня загроз інформаційній безпеці держави. Тому виникає нагальна потреба у розробленні дієвих методів оцінювання рівня таких загроз для організації ефективної протидії, які будуть покладені в основу функціонування системи забезпечення інформаційної безпеки держави у СІС.

Аналіз літературних даних і постановка проблеми

Останні дослідження і публікації [4–7] показали відсутність загальноприйнятої методики оцінювання рівня загроз інформаційній безпеці держави у СІС. Міжнародний досвід європейських країн [7], зокрема Латвії, Естонії, Німеччини, Італії, Польщі та інших показав, що провідна роль у виявленні та протидії загрозам інформаційній безпеці держави належить об'єднаному центру передових технологій з кібероборони НАТО (*NATO Cooperative Cyber Defence Centre of Excellence*) із штаб-квартирою у Талліні (Естонія). Також у рамках проекту Академії електронного управління (*eGA*) Естонії використовується глобальний індекс *National Cyber Security Index (NCSI)* [8], який оцінює готовність країн запобігти реалізації основних загроз та управляти інцидентами, злочинами і великомасштабними кризами. *NCSI* представляє собою інструмент для оцінки потенціалу інформаційної безпеки і заходів захисту інформаційного простору. Індекс *NCSI* формується для окремих країн на основі таких даних [8]: загальний показник інформаційної безпеки; базові показники інформаційної безпеки; показники управління інцидентами і кризами; показники міжнародного впливу. Складність застосування індексу *NCSI* для вирішення проблеми оцінювання загроз інформаційній безпеці держави у СІС полягає у відсутності докладної методології оцінювання у відкритому доступі, неможливості її окремого виділення і використання із сукупності інших інтегральних показників.

У загальному випадку для оцінювання загроз використовують дві групи методів: кількісні та якісні [4]. Суть кількісних методів зводиться до розрахунку показників ймовірності реалізації загроз на основі апріорної або апостеріорної інформації про їх прояви [5]. Апостеріорні методи ґрунтуються на побудові гістограм розподілу проявів ознак загроз і частот їх реалізації, а група апріорних методів полягає в розрахунку статистичних характеристик процесів, які супроводжують реалізацію таких загроз. Недоліком такого підходу є обмеженість застосування для оцінювання загроз інформаційній безпеці держави у СІС, пов'язана зі складністю збору необхідного об'єму статистичних даних і формалізації ознак інформаційних акцій. Якісне оцінювання рівня загроз інформаційній безпеці держави ґрунтується на експертних методах [5, 6] і зводиться до узагальнення і статистичної обробки думок кваліфікованих спеціалістів цієї галузі. Однак, застосування експертного оцінювання в задачах виявлення загроз у СІС суттєво обмежується необхідністю обробки великих масивів вхідних даних, низькою швидкодією процедури оцінювання, потребою підготовки великої кількості висококваліфікованих експертів, суб'єктивністю експертних оцінок тощо.

Дослідження джерел і галузевих звітів [7, 9] свідчать про різке зростання кількості загроз інформаційній безпеці держави у СІС. Поява протиріччя між рівнем сучасних загроз і науковим базисом їх оцінювання, зокрема відсутність ефективних і дієвих методів оцінювання загроз інформаційній безпеці держави у СІС, додатково актуалізує обраний напрямок наукових досліджень.

Мета і задачі дослідження

Метою статті є розроблення методу оцінювання ознак загроз для підвищення оперативності, ефективності та швидкодії системи забезпечення інформаційної безпеки держави у СІС.

Для досягнення поставленої мети необхідно розв'язати частинні задачі:

узагальнити ознаки інформаційних акцій у СІС;

розробити метод оцінювання ознак загроз інформаційній безпеці держави у СІС;

провести експертне оцінювання для встановлення пріоритетності ознак загроз;

виконати експериментальне дослідження запропонованого методу оцінювання ознак загроз.

Основна частина

Систематизація проведених досліджень [10–13], присвячених розробленню методів і технологій раннього виявлення загроз інформаційній безпеці держави у СІС продемонструвала, що їх характерними ознаками є наступні:

- організаційні, які пов'язані з цільовим використанням інформаційних ресурсів і спеціального програмного забезпечення. Проявом організаційних ознак є застосування соціальних ботів для поширення заданого контенту, ґенерації зв'язків з іншими акторами, додавання коментарів, ґештегів і відміток тощо;
- змістовні ознаки, проявом яких є деструктивний інформаційний вплив на акторів засобами текстового контенту СІС. Такі ознаки зводиться до використання у фрагментах текстового контенту СІС небезпечних семантичних конструкцій для створення деструктивного наративу;
- маніпулятивні ознаки, які є показником застосування прихованого впливу на акторів СІС у текстовому контенті з метою зміни їх поведінки, цілей, намірів чи інших психологічних характеристик в інтересах суб'єкта впливу.

Виявлення маніпуляцій суспільною думкою акторів у СІС реалізується внаслідок аналізу текстового контенту, який ґрунтується на сучасних методах обробки даних – контент-аналізі та машинному навчанні;

- оцінка профіля інформаційної безпеки актора, що представляє собою набір агрегованих характеристик профіля актора у СІС, які дозволяють визначити рівень його загрози як можливого учасника інформаційних акцій, направлених проти інформаційної безпеки особистості, суспільства, держави.

Ефективність виявлення загроз у СІС системою забезпечення інформаційної безпеки держави досягається завдяки врахуванню прояву ознак інформаційних акцій. Таким чином, задача оцінювання ознак загроз інформаційній безпеці держави у СІС зводиться до багатокритерійної оптимізації векторного критерію [14–17]. Залежно від принципів багатокритерійної оптимізації виділяють наступні групи методів [17]:

- оптимізації ієрархічної послідовності критеріїв якості;
- визначення множини непокращуваних рішень;
- на основі компромісу.

Серед недоліків перших двох груп методів слід відмітити складність визначення структури ієрархічної послідовності частинних критерії, суттєву обмеженість непокращуваних рішень областю компромісів тощо. У свою чергу, використання принципу справедливого компромісу, покладеного в основу третьої групи методів, забезпечує зниження якості за одними критеріями, яке не перевершує підвищення якості за іншими критеріями. Тому використання методів на основі компромісу для виявлення загроз у СІС є перспективним напрямком досліджень. Встановлено, що серед третьої групи методів нелінійна схема компромісів, запропонована професором А. М. Вороніним, забезпечує компроміс між частинними критеріями, а отримане рішення є оптимальним за Парето [14, 17]. Серед переваг даного методу виділяють обчислювальну простоту; унімодальність скалярної згортки, що забезпечує одноекстремальність задачі; адаптацію до умов прийняття рішення.

Таким чином, запропонований метод оцінювання ознак загроз інформаційній безпеці держави у СІС ґрунтується на нелінійній схемі компромісів [14, 16] і зводиться до такого.

Етап 1. Розрахунок показника I_1 на основі технології виявлення організаційних ознак інформаційних акцій у СІС. Технологія [10] зводиться до пошуку дублікатів публікацій і коментарів у СІС, розрахунку показника читабельності текстового контенту та ведення діалогу з акторами, які є авторами такого контенту. Висновок про цілеспрямовану інформаційну акцію у СІС, направлену проти інформаційної безпеки особистості, суспільства, держави з використанням спеціального програмного забезпечення формується на основі відповідного узагальненого показника I_1, який приймає значення

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

Етап 2. Визначення показника I_2 наявності деструктивного інформаційного впливу у контенті СІС. Виявлення таких прихованих інформаційних впливів ґрунтується на методі, запропонованому у публікації [11] і полягає в інтелектуальному пошуку текстового контенту СІС відповідно до заданого семантичного ядра за критерієм актуальності, критичності та рівня обговорення у суспільстві. Відібраний контент підлягає семантичному аналізу на основі онтологій з використанням сигнатурного методу і методу виявлення аномалій. У результаті формується відповідний показник I_2

$$I_2 = I_2^n \to B, \text{ де } B = \{0;1\},\ n = 1. \quad (2)$$

Етап 3. Оцінка прояву I_3 ознак маніпуляцій суспільною думкою у СІС. Розрахунок показника I_3 проводиться відповідно до розробленої методики виявлення маніпуляцій суспільною думкою [12]. Узагальнення частинних ознак маніпуляцій виконано на основі оцінки інформаційної ентропії H_n контенту СІС, тобто встановлення рівня невизначеності щодо використання технологій прихованого впливу на акторів. Зростання величини інформаційної ентропії H_n характеризує зменшення невизначеності, тому для задачі оцінки прояву ознак маніпуляцій суспільною з показник I_3 набуває значень

$$I_3 = 1 - H_n,\ H_n \in [0;1]. \quad (3)$$

Етап 4. Оцінка профіля інформаційної безпеки актора I_4. Розрахунок показника I_4 реалізований з використанням методу побудови профілів інформаційної безпеки акторів [13]. Запропонований метод ґрунтується на технологіях інтелектуального аналізу даних, зокрема методах машинного навчання з учителем. Оцінка профіля інформаційної безпеки I_4 приймає значення у заданому діапазоні

$$I_4 \in [0;1]. \quad (4)$$

Узагальнення ознак I_j, $j = \overline{1,4}$ загроз інформаційній безпеці особистості, суспільства, держави у СІС та їх нормованих шкал оцінки подано в табл. 1.

Таблиця 1 – Частинні ознаки загроз інформаційній безпеці у СІС

Ознаки	Шкала оцінки	Якісний показник рівня загрози
Організаційні I_1	0	відсутня
	1	існує
Змістовні I_2	0	відсутня
	1	існує
Маніпулятивні I_3	0,91–1,00	дуже висока
	0,75–0,90	висока
	0,50–0,74	значна
	0,21–0,49	низька
	0,00–0,20	дуже низька
Оцінка профіля інформаційної безпеки актора I_4	0,70–1,00	дуже високий
	0,50–0,70	високий
	0,40–0,50	значний
	0,20–0,40	допустимий
	0,00–0,20	низький

З іншої точки зору, параметри α_j представляють собою вагові коефіцієнти змістовної регресійної моделі корисності експерта на основі концепції нелінійної схеми компромісів [15]. Тому вагові коефіцієнти загроз інформаційній безпеці у СІС розраховують відповідно до виразу [16]

$$\alpha_j = \frac{f_j}{\sum_{i=1}^{m} f_i}, \ j \in [1; m],$$

де f_j – оцінка пріоритетності ознаки загрози, яку встановлює експерт.

Для встановлення значень вагових коефіцієнтів проведено експертне опитування співробітників науково-дослідного відділу інформаційної та кібернетичної безпеки наукового центру Житомирського військового інституту імені С. П. Корольова. За результатами обробки даних анкетування вагові коефіцієнти ознак загроз інформаційній безпеці у СІС приймають значення, подані в табл. 2.

Таблиця 2 – Результати експертного опитування

Оцінка f_i	Експертна оцінка у балах	Вагові коефіцієнти частинних ознак загроз
f_1	9	0,31
f_2	8	0,28
f_3	7	0,24
f_4	5	0,17
Сума	29	1

Етап 6. Скалярна згортка ознак загроз I по нелінійній схемі компромісів. Багатокритерійна задача оцінки (1)–(4) зводиться до моделі векторної оптимізації з різними ваговими коефіцієнтами ознак загроз інформаційній безпеці держави у СІС [14–16]

$$I^* = \arg\min_{I \in M} \sum_{j=1}^{m} \alpha_j \left(1 - I_j\right)^{-1}. \quad (5)$$

Для якісної оцінки загроз проводиться нормування скалярної згортки (5) до мінімального значення [16]

$$I = 1 - \frac{1}{I^*}. \quad (6)$$

Отримане значення ставиться у відповідність якісній шкалі загроз (табл. 3), сформованій на основі оберненої нормованої фундаментальної шкали, запропонованої професором А. М. Вороніним [14].

Таблиця 3 – Якісна шкала рівнів загроз

Рівень загрози	Інтервальні значення шкали оцінок
існує	0,71–1,00
вищий середнього	0,51–0,70
нижчий середнього	0,31–0,50
відсутній	0,00–0,30

Зауваження. Ознаки I_1 та I_2 приймають тільки граничні значення 0 або 1, що характеризує високий рівень напруженості ситуації у СІС. Напруженість ситуації у СІС виникає при наближенні значень ознак загроз інформаційній безпеці до граничних [15, 16]

$$\rho_j = 1 - I_{0j},\ \rho_j \in [0;1],\ j \in [1;m].$$

З метою виключення необхідності ділення на нуль у виразі (8) для значень ознак $I_j \geq 0,95$ необхідно використовувати величину $I_{0j} = 0,95$.

Запропонований метод оцінювання ознак загроз у вигляді структурної схеми подано на рис. 1.

У результаті моніторингу інформаційного середовища СІС з метою оцінювання загроз інформаційній безпеці держави відбирається текстовий контент і дані акторів, які його поширюють. Такий текстовий контент досліджується на предмет наявності ознак проведення інформаційної акції, деструктивного інформаційного впливу і маніпуляцій суспільною думкою. На основі відібраних аккаунтів акторів СІС проводиться оцінка їх профілів інформаційної безпеки. Експерт після аналізу предметної області оцінює пріоритетність ознак загроз інформаційній безпеці держави, на основі яких розраховуються значення вагових коефіцієнтів α_j. Сформований вектор ознак загроз I_j використовується для скалярної згортки по нелінійній схемі компромісів. На заключному етапі виконується перехід від числових значень I до якісної шкали оцінок рівня загроз інформаційній безпеці держави у СІС. Отримані оцінки використовуються для вироблення рекомендацій щодо переходу віртуальної спільноти до бажаного стану інформаційної безпеки у СІС.

Експеримент

Дослідження запропонованого методу оцінювання ознак загроз інформаційній безпеці держави у СІС проведено на прикладі реальної інформаційної акції. У січні 2017 року Німеччина розмістила у Литві контингент Батальйону передового базування НАТО у зв'язку з діями Росії в Україні та регіоні Балтійського моря. В лютому 2017 року через литовські ЗМІ поширено інформацію про згвалтування солдатами Бундесверу неповнолітньої дівчини [18, 19].

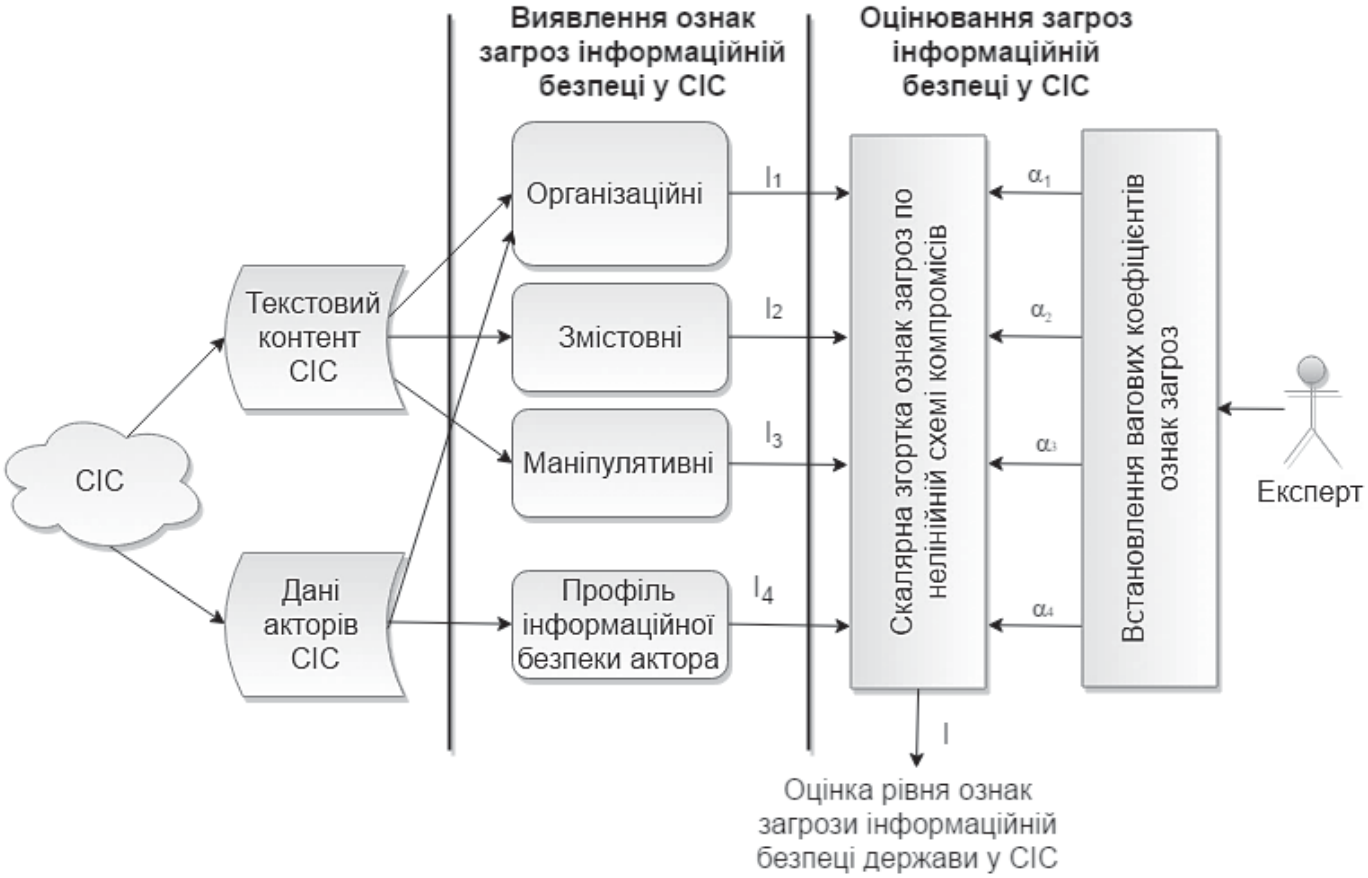

Рис. 1 – Структурна схема методу оцінювання загроз інформаційній безпеці держави у СІС

Проведено аналіз публікацій російськомовного сегменту мікроблогу *Twitter* на задану тематику з використанням розроблених підходів до виявлення загроз інформаційній безпеці держави [10–13]. Результати досліджень показали, що ознаки загрози приймають такі значення: організаційні $I_1 = 0$; змістовні $I_2 = 0,95$; маніпулятивні $I_3 = 0,4$; оцінка

профіля інформаційної безпеки $I_4 = 0,2$. Скалярна згортка частинних ознак I по нелінійній схемі компромісів (5) набуває значення

$$I^* = \frac{0,31}{1-0} + \frac{0,28}{1-0,95} + \frac{0,24}{1-0,4} + \frac{0,17}{1-0,2} = 7,42.$$

Перехід від скалярної згортки до якісної шкали оцінки загроз виконано відповідно до виразу (6) і табл. 3

$$I = 1 - \frac{1}{7,42} = 0,87,$$

тому досліджувану інформаційну акцію визначено як існуючу загрозу інформаційній безпеці держави у СІС.

Аналіз показав, що високий рівень загрози пояснюється наявністю деструктивного інформаційного посилу у контенті, який поширювався у мікроблозі *Twitter*, та застосуванням маніпулятивних технологій для прихованого впливу на суспільну свідомість з метою дискредитації сил НАТО. Оперативна реакція командування, організація розслідування інциденту правоохоронними органами, об'єктивна оцінка рівня загрози і високий рівень системи забезпечення інформаційної безпеки Литви забезпечили швидку нейтралізацію загрози. Так, індекс кібернетичного захисту *NCSI* Литви у 2017 році дорівнює 65,15 і є найвищим показником серед інших країн у рейтингу [8]. Отже, отримані результати збіжні з висновками міжнародних організацій, що доводить дієвість та ефективність запропонованого методу оцінювання ознак загроз інформаційній безпеці держави у СІС.

Висновки

Вперше запропоновано метод оцінювання ознак загроз інформаційній безпеці держави у СІС, який ґрунтується на нелінійній схемі компромісів і відрізняється від відомих підходів застосуванням сучасних методів виявлення ознак інформаційних акцій у віртуальних спільнотах. Розроблений метод покладено в основу функціонування системи забезпечення інформаційної безпеки держави у СІС, що дозволило автоматизувати процедури раннього виявлення загроз. Таким чином досягається оперативність і швидкодія системи забезпечення інформаційної безпеки держави у СІС, що є сьогодні вкрай актуальним завданням для України. Напрямок подальших досліджень полягає у розробленні моделі системи підтримки прийняття рішень щодо протидії загрозам інформаційній безпеці держави у СІС.

Література

[1] Онищенко О. Соціальні мережі як інструмент взаємовпливу влади та громадянського суспільства / О. Онищенко, В. Горовий, В. Попик. – Київ : НАН України, Нац. б-ка України ім. В. І. Вернадського, 2014. – 295 с.
[2] Молодецька К. Соціальні інтернет-сервіси як суб'єкт інформаційної безпеки держави / К. Молодецька. // Information technology and security. – 2016. – № 1. – С. 13–20.
[3] Молодецька К. Узагальнена класифікація загроз інформаційній безпеці держави в соціальних інтернет-сервісах / К. Молодецька // Защита информации. – 2016. – № 23. – С. 75–87.
[4] Черниш В. Методика оцінки інформаційних ризиків з використанням методу аналізу ієрархій / В. Черниш. // Радіоелектронні і комп'ютерні системи. – 2012. – № 1. – С. 46–50.
[5] Пузиренко О. Математична модель загроз інформаційної безпеки в інформаційно-телекомунікаційних системах спеціального призначення / О. Пузиренко // Наука і техніка Повітряних Сил Збройних Сил України. – 2014. – № 3. – С. 129–133.
[6] Хмелевський Р. Дослідження оцінки загроз інформаційній безпеці об'єктів інформаційної діяльності / Р. Хмелевський. // Сучасний захист інформації. – 2016. – № 4. – С. 65–70.
[7] Грищук Р. Основи кібернетичної безпеки / Р. Грищук, Ю. Даник. – Житомир : ЖНАЕУ, 2016. – 636 с.
[8] NCSI – National Cyber Security Index [Electronic resource]. – Access mode: http://ncsi.ega.ee – Title from the screen.
[9] Cybersecurity Engineering | The CERT Division [Electronic resource]. – Access mode: http://www.cert.org/cybersecurity-engineering/ – Title from the screen.
[10] Молодецька К. Технологія виявлення організаційних ознак інформаційних операцій у соціальних інтернет-сервісах / К. Молодецька. // Проблеми інформаційних технологій. – 2016. – № 20. – С. 84–93.
[11] Молодецька-Гринчук К. Виявлення інформаційних впливів у соціальних інтернет-сервісах на основі інтелектуального аналізу текстового контенту / К. Молодецька-Гринчук. // Актуальні питання забезпечення кібербезпеки та захисту інформації. – 2017. – С. 121–122.
[12] Молодецька-Гринчук К. Методика виявлення маніпуляцій суспільною думкою у соціальних інтернет-сервісах / К. Молодецька-Гринчук. // Інформаційна безпека. – 2016. – № 24. – С. 80–92.
[13] Молодецька-Гринчук К. Метод побудови профілів інформаційної безпеки акторів соціальних інтернет-сервісів / К. Молодецька-Гринчук. // Інформаційна безпека. – 2017. – № 26. – С. 104–110.
[14] Воронин, А. Многокритериальный синтез динамических систем, 1st ed / А. Воронин. – Киев : Наукова думка, 1992. – 160 с.
[15] Воронин А. Нелинейная схема компромиссов в многокритериальных задачах оценивания и оптимизации / А. Воронин, Ю. Зиатдинов. // Кибернетика и системный анализ. – 2009. – № 4. – С. 106–114.

[16] Воронин А. Нелинейная схема компромиссов в многокритериальных задачах / А. Воронин. // Artificial Intelligence and Decision Making. International Book Series “Information Science & Computing”. – 2008. – № 7. – С. 7985.
[17] Грищук Р. Теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальних ігор та диференціальних перетворень, 1st ed / Р. Грищук. – Житомир : Рута, 2010. – 280 с.
[18] Einsatz in Litauen: Nato vermutet Russland hinter Fake-News-Kampagne gegen Bundeswehr – SPIEGEL ONLINE – Politik [Electronic resource]. – Access mode: http://www.spiegel.de/politik/ausland/bundeswehr-fake-news-attacke-gegen-deutsche-soldaten-in-litauen-a-1134925.html. – Title from the screen.
[19] Російська гібридна війна: в Литві запустили "фейк" про згвалтування школярки солдатами бундесверу, щоб підірвати довіру до НАТО [Электронный ресурс]. – Режим доступа: http://ua.censor.net.ua/news/428466/rosiyiska_gibrydna_viyina_v_lytvi_zapustyly_feyik_pro_zvaltuvannya_shkolyarky_soldatamy_bundesveru_schob. – Загл. с экрана.

References

[1] O. Onyshchenko, V. Horovyi and V. Popyk, *Sotsialni merezhi yak instrument vzaiemovplyvu vlady ta hromadianskoho suspilstva*, 1st ed. Kyiv: NAN Ukrainy, Nats. b-ka Ukrainy im. V. I. Vernadskoho, 2014.
[2] K. Molodetska, "Sotsialni internet-servisy yak subiekt informatsiinoi bezpeky derzhavy", *Information technology and security*, vol. 4, no. 1, pp. 13–20, 2016.
[3] K. Molodetska, "Uzahalnena klasyfikatsiia zahroz informatsiinii bezpetsi derzhavy v sotsialnykh internet-servisakh", *Zashchyta ynformatsyy*, no. 23, pp. 75–87, 2016.
[4] V. Chernysh, "Metodyka otsinky informatsiinykh ryzykiv z vykorystanniam metodu analizu iierarkhii", *Radioelektronni i kompiuterni systemy*, no. 1, pp. 46–50, 2012.
[5] O. Puzyrenko, "Matematychna model zahroz informatsiinoi bezpeky v informatsiino-telekomunikatsiinykh systemakh spetsialnoho pryznachennia", *Nauka i tekhnika Povitrianykh Syl Zbroinykh Syl Ukrainy*, no. 3, pp. 129–133, 2014.
[6] R. Khmelevskyi, "Doslidzhennia otsinky zahroz informatsiinii bezpetsi obiektiv informatsiinoi diialnosti", *Suchasnyi zakhyst informatsii*, no. 4, pp. 65–70, 2016.
[7] R. Hryshchuk and Yu. Danyk, *Osnovy kibernetychnoi bezpeky*, 1st ed. Zhytomyr: ZhNAEU, 2016.
[8] "NCSI – National Cyber Security Index", *Ncsi.ega.ee*, 2017. [Online]. Available: http://ncsi.ega.ee. [Accessed: 20-May- 2017].
[9] "Cybersecurity Engineering | The CERT Division", *Cert.org*, 2017. [Online]. Available: http://www.cert.org/cybersecurity-engineering/. [Accessed: 20-May-2017].
[10] K. Molodetska, "Tekhnolohiia vyiavlennia orhanizatsiinykh oznak informatsiinykh operatsii u sotsialnykh internet-servisakh", *Problemy informatsiinykh tekhnolohii*, no. 20, pp. 84–93, 2016.
[11] K. Molodetska-Hrynchuk, "Vyiavlennia informatsiinykh vplyviv u sotsialnykh internet-servisakh na osnovi intelektualnoho analizu tekstovoho kontentu", in *Aktualni pytannia zabezpechennia kiberbezpeky ta zakhystu informatsii*, Mizhhirskyi r-n, s. Verkhnie Studene, 2017, pp. 121–122.
[12] K. Molodetska-Hrynchuk, "Metodyka vyiavlennia manipuliatsii suspilnoiu dumkoiu u sotsialnykh internet-servisakh", *Informatsiina bezpeka*, no. 24, pp. 80–92, 2016.
[13] K. Molodetska-Hrynchuk, "Metod pobudovy profiliv informatsiinoi bezpeky aktoriv sotsialnykh internet-servisiv", *Informatsiina bezpeka*, no. 26, pp. 104–110, 2017.
[14] A. Voronyn, *Mnohokryteryalnii syntez dynamycheskykh system*, 1st ed. Kyev: Naukova dumka, 1992.
[15] A. Voronyn and Yu. Zyatdynov, "Nelyneinaia skhema kompromyssov v mnogokryteryalnykh zadachakh otsenyvanyia y optymyzatsyy", *Kybernetyka y systemnii analyz*, no. 4, pp. 106–114, 2009.
[16] A. Voronyn, "Nelyneinaia skhema kompromyssov v mnohokryteryalnыkh zadachakh", *International Book Series «Information Science & Computing». Artificial Intelligence and Decision Making*, pp. 79–85, 2008.
[17] R. Hryshchuk, *Teoretychni osnovy modeliuvannia protsesiv napadu na informatsiiu metodamy teorii dyferentsialnykh ihor ta dyferentsialnykh peretvoren*, 1st ed. Zhytomyr: Ruta, 2010.
[18] M. Gebauer, "Einsatz in Litauen: Nato vermutet Russland hinter Fake-News-Kampagne gegen Bundeswehr - SPIEGEL ONLINE - Politik", *SPIEGEL ONLINE*, 2017. [Online]. Available: http://www.spiegel.de/politik/ausland/bundeswehr-fake-news-attacke-gegen-deutsche-soldaten-in-litauen-a-1134925.html. [Accessed: 20-May-2017].
[19] "Rosiiska hibrydna viina: v Lytvi zapustyly "feik" pro zgvaltuvannia shkoliarky soldatamy bundesveru, shchob pidirvaty doviru do NATO, – Der Spiegel", *Tsenzor.NET*, 2017. [Online]. Available: http://ua.censor.net.ua/news/428466/rosiyiska_gibrydna_viyina_v_lytvi_zapustyly_feyik_pro_zvaltuvannya_shkolyarky_soldatamy_bundesveru_schob. [Accessed: 20-May-2017].