УДК 004.056:004.738.5(045)

К.В. Молодецька-Гринчук

Житомирський національний агроекологічний університет, Житомир

ПРОТОТИП ПРОГРАМНОГО КОМПЛЕКСУ ВИЯВЛЕННЯ ОЗНАК ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ДЕРЖАВИ У СОЦІАЛЬНИХ ІНТЕРНЕТ-СЕРВІСАХ ТА ОЦІНЮВАННЯ ЇХ РІВНЯ

У статті запропоновано прототип програмного комплексу системи підтримки прийняття рішень для виявлення ознак загроз інформаційній безпеці держави у соціальних інтернет-сервісах та оцінювання їх рівня. Розроблений прототип програмного комплексу є складовою системи забезпечення інформаційної безпеки держави і автоматизує процеси раннього виявлення загроз у соціальних інтернет-сервісах. В основу моделі прийняття рішень покладено сучасні підходи до інформаційного пошуку, інтелектуального аналізу контенту та синергетичного управління взаємодією акторів для досягнення бажаного стану інформаційної безпеки віртуальних спільнот. Створений макет програмного комплексу дозволяє перевірити адекватність використаних для побудови системи підтримки прийняття рішень методів, моделей і технологічних рішень.

Ключові слова: *соціальний інтернет-сервіс, система підтримки прийняття рішень, загроза, інформаційна безпека держави, прототип програмного комплексу, актор, контент, синергетичне управління.*

Вступ

Соціальні інтернет-сервіси (СІС) є одним з найбільш популярних видів засобів масової комунікації. Сучасні СІС забезпечують учасників віртуальних спільнот – акторів, дієвим інструментарієм спілкування, організації у групи за спільними інтересами, взаємодії громадянського суспільства із владою тощо [1–4]. Однак, завдяки своїм комунікаційним перевагам СІС перетворилися на ефективний інструмент проведення інформаційних операцій, спрямованих проти людини, суспільства, держави [5–6]. Встановлено, що для поширення контенту з деструктивним інформаційним посилом у СІС використовують не тільки окремих акторів, але і засоби спеціального програмного забезпечення, зокрема соціальних ботів. Наслідками таких дій є маніпуляція суспільною думкою, поширення закликів до сепаратизму, національної та релігійної ворожнечі тощо. Досвід гібридної війни з Російською Федерацією показав відсутність дієвої системи забезпечення інформаційної безпеки (СЗІБ) держави у СІС для виявлення, оцінювання та протидії комплексним загрозам [7–8]. Тому створення ефективної СЗІБ на основі інноваційних підходів є актуальним теоретико-прикладним завданням.

Аналіз останніх досліджень і публікацій [8–11] показав недостатній рівень теоретичного опрацювання і відсутність загальноприйнятих практичних рекомендацій щодо розроблення СЗІБ держави у СІС. Встановлено, що наведені у Доктрині інформаційної безпеки держави [12] механізми протидії сучасним загрозам доцільно реалізувати при розробленні відомчих підсистем інформаційної безпеки. Провідна роль у забезпеченні інформаційної безпеки держави у СІС належить Міністерству інформаційної політики України (МІПУ) [13–14], на яке покладено функції моніторингу інформаційного середовища і виявлених загроз, розроблення та реалізація стратегічного наративу. Тому створення дієвої системи підтримки прийняття рішень (СППР) як складової відомчої системи інформаційної безпеки є актуальним завданням для забезпечення заданого стану інформаційної безпеки у СІС.

У публікаціях [15–18] запропоновано методи і технології виявлення ознак загроз інформаційній безпеці держави у СІС. Підходи до протидії виявленим загрозам подані у працях [19–25]. Перевагами моделі СППР, яка ґрунтується на розроблених підходах, є: відбір релевантного текстового контенту на основі його змісту і без врахування щільності ключових слів для його подальшого дослідження; автоматизація процедур виявлення ознак інформаційних акцій у СІС та оцінювання рівня загроз; застосування концепції синергетичного управління взаємодією акторів для переходу віртуальної спільноти до заданого стану інформаційної безпеки. Таким чином, перспективним є розроблення прототипу програмного комплексу СППР – макету програмного комплексу для доведення адекватності запропонованих методів, моделей і технологічних рішень.

Розроблення прототипу програмного комплексу доцільно виконати на основі еволюційного прототипування [26] для послідовного створення макету, функціональні характеристики якого наближаються до реального програмного продукту. Перевагами такого підходу до розроблення діючого програмного комплексу є зниження витрат на створення системи,

зменшення проектних ризиків та залучення кінцевих користувачів системи – експертів з інформаційної безпеки, для врахування вимог до інтерфейсу.

Метою статті є розроблення прототипу програмного комплексу виявлення ознак загроз інформаційній безпеці держави у СІС і оцінювання їх рівня для реалізації дієвої та ефективної СЗІБ держави. Для досягнення поставленої мети необхідно розв'язати такі частинні задачі:

визначити сценарії роботи прототипу програмного комплексу;

розробити формалізовану модель функціонування СППР;

реалізувати прототип програмного комплексу з урахуванням вимог до даного класу систем і багатокористувацького доступу до даних.

Виклад основного матеріалу

У процесі проектування програмного комплексу для виявлення ознак загроз інформаційній безпеці держави у СІС та оцінювання їх рівня використано сучасні CASE-технології, зокрема мову *UML* [27]. У результаті застосування даного відкритого стандарту забезпечується уніфікований процес створення програмного забезпечення. Встановлено, що користувачами СППР є експерт з інформаційної безпеки і державні виконавчі органи, які реалізують покладені на них функції з моніторингу інформаційного середовища, виявлення ознак загроз й оцінювання їх рівня. Джерелом досліджуваного контенту є безпосередньо СІС. На рис. 1 подано діаграму прецендентів СППР, побудовану засобами середовища *StarUML*, на якій зображено відношення між користувачами системи (акторами) та варіантами використання системи.

Експерт з інформаційної безпеки держави взаємодіє з СІС для визначення загроз та формування семантично ядра, відповідно до якого виконується пошук релевантного контенту у віртуальних спільнотах. Також експерт додає семантичний опис виявлених загроз до відповідної онтології. Основною функцією СППР для експерта є оцінювання ознак загроз інформаційній безпеці держави у СІС. Для цього необхідно встановити вагові коефіцієнти ознак загроз з метою врахування їх пріоритетності в окремих інформаційних акціях. У процесі оцінювання рівня загрози визначається сфера суспільної діяльності, на яку вона вплинула, для коректного вироблення ефективних рекомендацій з протидії. Результати функціонування передаються державним виконавчим органам для вживання заходів з нейтралізації виявлених загроз.

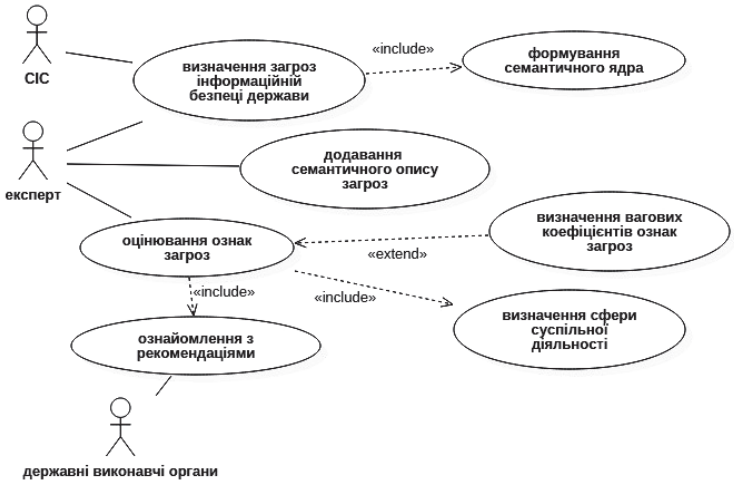

Рис. 1. Діаграма прецендентів прототипу програмного комплексу виявлення ознак загроз інформаційній безпеці держави у СІС та оцінювання їх рівня

Для моделювання потоку подій системи через послідовність виконання операцій спроектовано діаграму діяльності системи (рис. 2).

На рис. 2 представлено три секції для відображення діяльності відповідних акторів діаграми – експерта з інформаційної безпеки, СППР та державних виконавчих органів.

Декомпозицію процесу прийняття рішень для виявлення ознак загроз інформаційній безпеці держави у СІС та оцінювання їх рівня на основі аналізу інформаційних потоків подано у вигляді структурної схеми на рис. 3.

Модуль S_1 призначений для моніторингу інформаційного середовища СІС на основі опису загрози інформаційній безпеці держави D та семантичного ядра W, яке представляє собою набір ключових слів для пошуку. Відбір релевантного текстового контенту TC^* проводиться з використанням методу латентно-семантичної індексації [27], що забезпечує пошук контенту на підставі його змісту без врахування щільності ключових слів. Також вихідним інформаційним потоком модуля S_1 є дані профілів акторів A^*, які публікували відібраний контент TC^*.

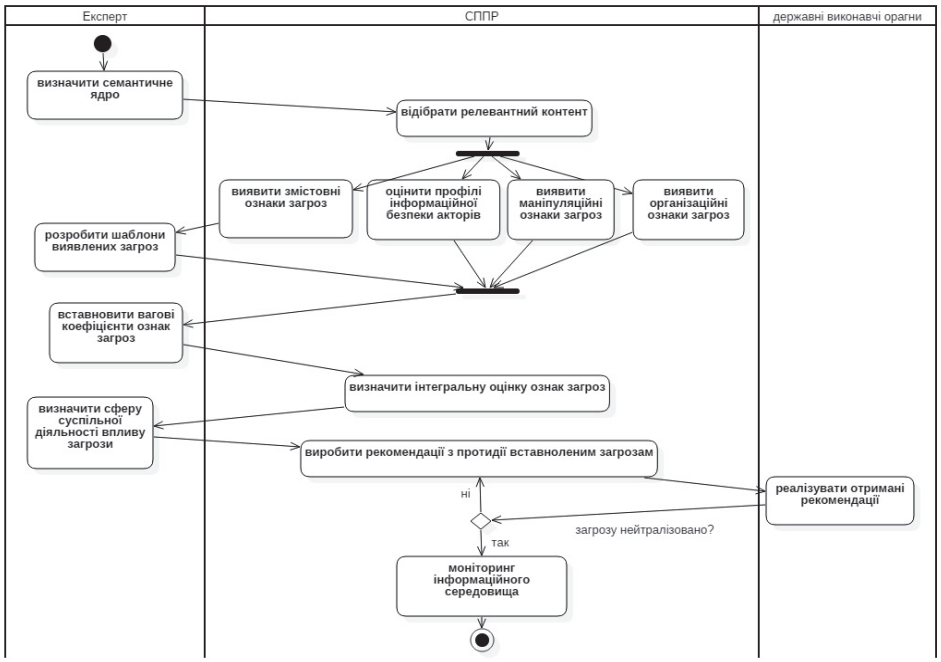

Рис. 2. Діаграма діяльності СППР

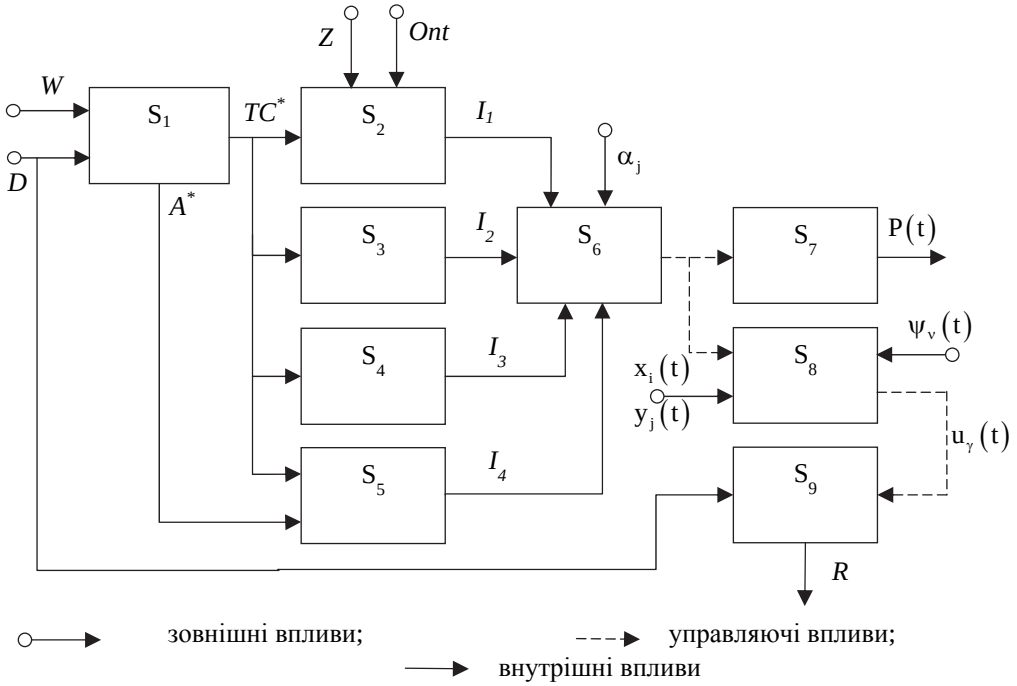

Рис. 3. Структура моделі прийняття рішень для виявлення ознак загроз інформаційній безпеці держави у СІС та оцінювання їх рівня

Вихідні інформаційний потік TC^* передається до модулів $S_2 - S_5$ для виявлення частинних ознак загроз інформаційній безпеці у СІС. Модуль S_2 призначений для виявлення змістовних ознак загроз у текстовому контенті TC^*. Також модулем S_2 використовуються вхідні інформаційні потоки Z семантичних шаблонів загроз і онтологія Ont. Рішення I_1 про наявність у текстовому контенті змістовних ознак загроз приймається на основі методу, запропонованого у публікації [16]. Функцією модуля S_3 є виявлення ознак I_2 використання спеціального програмного забезпечення для публікації контенту у віртуальних спільнотах, зокрема соціальних ботів. Модель прийняття рішення, яка використовується у модулі S_3, запропонована у статті [15]. Вона ґрунтується на аналізі наявності дублікатів текстового контенту, індексу читабельності та діалозі з актором.

Виявлення маніпуляцій суспільною думкою у СІС виконується модулем S_4 після аналізу текстового контенту TC^* з використанням методу, представленого у публікації [17]. При цьому встановлюється

рівень інформаційної ентропії текстового контенту, який характеризує рівень невизначеності щодо наявності у ньому прихованого інформаційного впливу на акторів СІС. Вихідним інформаційним потоком модуля S_4 є показник I_3, що вказує на використання у текстовому контенті прихованих маніпуляцій. Вхідним інформаційним потоком для модуля S_5, окрім відібраного текстового контенту TC^*, є дані профілів акторів СІС A^*. Рішення про віднесення актора до визначеного класу загрози як можливого учасника інформаційних акцій приймається на основі методу [18]. Висновок формується з використанням методів машинного навчання з учителем.

У модулі S_6 виконується розрахунок інтегральної оцінки ознак загроз інформаційній безпеці держави у СІС з використанням частинних показників I_1, I_2, I_3, I_4. Модель оцінювання ознак загроз у СІС ґрунтується на нелінійній схемі компромісів професора А.М. Вороніна [29–30]. Вхідним інформаційним потоком є вагові коефіцієнти ознак загроз α_j, $j = \overline{1,4}$, що встановлюються експертами і відповідають оперативній ситуації у віртуальних спільнотах. Якісна оцінка рівня загроз інформаційній безпеці у СІС визначається у результаті нормування отриманого значення до мінімуму і співвідношення з універсальною якісною шкалою

$$I = \langle \text{відсутня; нижча середнього; вища середнього; існує} \rangle.$$

Вихідний потік I є управляючим для модулів S_7 і S_8. Для значень оцінки загроз у інтервалі $I \in \left[0; I^{n}_{max}\right]$, де I^{n}_{max} – максимальне значення оцінки загрози, яка визначається як «відсутня», система рекомендацій не виробляє. У випадку встановлення оцінки ознак загроз $I \in \left[I^{ns}_{min}; I^{ns}_{max}\right]$, де I^{ns}_{min}, I^{ns}_{max} – мінімальне і максимальне значення оцінки загрози рівня «нижче середнього», продовжується моніторинг загрози у інформаційному середовищі СІС. Якщо рівень загрози приймає значення на інтервалі $I \in \left[I^{vs}_{min}; I^{vs}_{max}\right]$, де I^{vs}_{min}, I^{vs}_{max} – мінімальне і максимальне значення оцінки загрози «вище середнього» рівня, то виконується прогнозування поширення текстового контенту й запитів на нього у СІС $P(t)$. В основу функціонування модуля S_7 покладено метод, розроблений у статті [19], який ґрунтується на контент-аналізі та метриці самоподібності – показнику Херста. Якщо узагальнена оцінка ознак загроз у СІС I набуває значень на інтервалі $I \in \left[I^{i}_{min}; I^{i}_{max}\right]$, де I^{i}_{min}, I^{i}_{max} – мінімальне і максимальне значення загрози рівня «існує», то до обробки інформаційного потоку залучається модуль S_8. Призначення модуля S_8 зводиться до протидії загрозам інформаційній безпеці держави у СІС на основі синергетичного управління процесами взаємодії акторів віртуальних спільнот. Концепція синергетичного управління запропонована у публікації [20]. Вхідними інформаційними потоками для модуля S_8 виступають математична модель взаємодії акторів у СІС $\{x_i(t), y_j(t)\}$ та параметр порядку – атрактор $\psi_v(t)$, який визначає бажану динаміку системи [21–22]. Синтезоване синергетичне управління $u_\gamma(t)$ і модель виявленої загрози інформаційній безпеці D держави використовуються для вироблення практичних рекомендацій державним виконавчим органам R [13].

Прототип програмного комплексу виявлення ознак загроз інформаційній безпеці держави у СІС та оцінювання їх рівня реалізовано засобами гіпертекстового препроцесора *PHP*. Перевагами такого підходу є забезпечення багатокористувацького доступу до даних і кросс-платформенність. На рис. 4 подано інтерфейс модуля S_6 інтегрального оцінювання ознак загроз інформаційній безпеці держави у СІС.

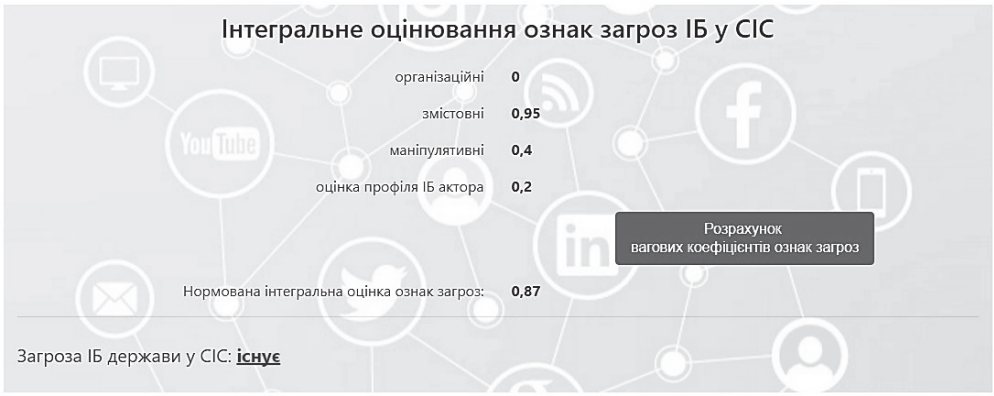

Рис. 4. Інтерфейс модуля інтегрального оцінювання ознак загроз

На сторінці передбачено кнопку для визначення вагових коефіцієнтів ознак загроз інформаційній безпеці у СІС, яка використовується у випадку істотної зміни оперативної ситуації у віртуальних спільнотах. В нижній частині сторінки відображається нормоване значення оцінки та його відповідне значення за якісною шкалою.

Функція вироблення рекомендацій прототипом програмного комплексу СППР з протидії загрозам у СІС реалізована на сторінці, представленій на рис. 5.

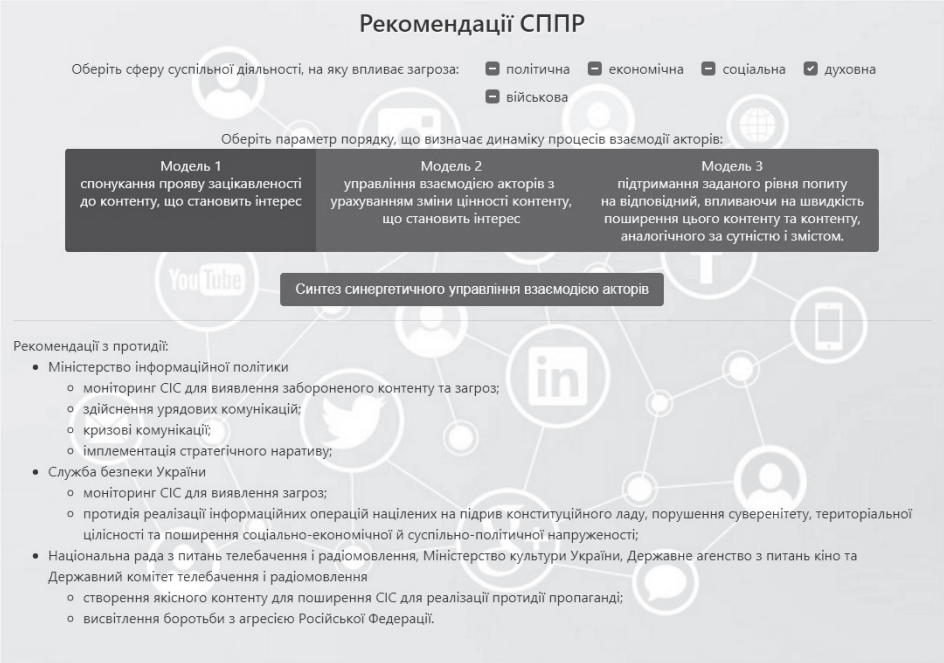

Рис. 5. Інтерфейс модулів протидії загрозам інформаційної безпеки і вироблення рекомендацій

На сторінці, зображеній на рис. 5, експерт з інформаційної безпеки вказує сфери суспільної діяльності, на які впливає виявлена загроза. Після цього обирає параметр порядку для переходу віртуальної спільноти до заданого стану інформаційної безпеки держави.

Модель 1 ґрунтується на спонуканні прояву у акторів зацікавленості до контенту, що становить інтерес [21], модель 2 зводиться до управління взаємодією акторів з урахуванням зміни цінності контенту, що ставить інтерес, та модель 3, яка полягає у підтриманні заданого рівня попиту акторів на відповідний контент, впливаючи на швидкість поширення цього контенту та контенту, аналогічного за сутністю і змістом.

Вибір моделі параметра порядку виконується з урахуванням особливостей виявленої загрози та наявних ресурсів для протидії. У нижній частині сторінки виводяться рекомендації відповідним відомствам для реалізації протидії виявленим загрозам інформаційній безпеці держави у СІС.

Висновки

Вперше запропоновано прототип програмного комплексу виявлення ознак загроз інформаційній безпеці держави у СІС та оцінювання їх рівня, яка забезпечує автоматизацію процесів раннього виявлення загроз і є складовою системи забезпечення інформаційної безпеки держави. Розроблений прототип програмного комплексу покладено в основу створення дієвого програмного продукту і забезпечення врахування вимог кінцевих користувачів – експертів, зниження ризиків при розробці кінцевого програмного продукту. Ефективність прототипу програмного комплексу досягається використанням сучасних підходів до інформаційного пошуку, інтелектуального аналізу контенту та синергетичного управління взаємодією акторів для досягнення бажаного стану інформаційної безпеки віртуальних спільнот.

Список літератури

1. Соціальні мережі як інструмент взаємовпливу влади та громадянського суспільства: [монографія] / [О.С. Онищенко, В.М. Горовий, В.І. Попик та ін.]; НАН України, Нац. б-ка України ім. В.І. Вернадського. – К., 2014. – 260 с.

2. Проблеми суспільної безпеки в процесі розвитку соціальних мереж: [монографія] / [В. Попик (кер. проекту), В. Горовий, О. Онищенко та ін.] ; НАН України, Нац. б-ка України ім. В.І. Вернадського. – Київ, 2015. – 202 с.

3. Информационные риски в социальных сетях / Г.А. Остапенко, Л.В. Паринова, В.И. Белоножкин, И.Л. Батаронов, К.В. Симонов [под ред. член-корр. РАН Д.А. Новикова], 2013. – 161 с.

4. Papacharissi Zizi A. A networked self: identity, community and culture on social network sites / editor Zizi A. Papacharissi. – New York: Routledge, 2011. – 327 p.

5. Молодецька К.В. Соціальні інтернет-сервіси як суб'єкт інформаційної безпеки держави / К.В. Молодецька // Information technology and security. – 2016. – Vol. 4, Iss. 1(6). – P. 13-20.

6. Молодецька К.В. Узагальнена класифікація загроз інформаційній безпеці держави в соціальних інтернет-сервісах / К.В. Молодецька // Защита информации: сб. науч. труд. – 2016. – Вып. 23. – С. 75-87.

7. Грищук Р.В. Основи кібернетичної безпеки: монографія / Р.В. Грищук, ЮГ. Даник; за заг. ред. проф. Ю.Г. Даника. – Житомир: ЖНАЕУ, 2016. – 636 с.

8. Технології розвитку і захисту національного інформаційного простору: [монографія] / [О. Онищенко, В. Горовий, В. Попик та ін.]; НАН України, Нац. б-ка України ім. В. І. Вернадського. – Київ, 2015. – 296 с.

9. Радковець Ю. Погляди на створення системи інформаційної безпеки України та її Збройних Сил / Ю. Радковець, О. Левченко, О. Косогов // Наука і оборона. – 2014. – С. 38-42.

10. Бурячок В. Стратегія оцінювання рівня захищеності держави від ризику стороннього кібернетичного впливу / В. Бурячок, О. Корченко, В. Хорошко, В. Кудінов // Захист інформації. – 2013. – Т. 15. – № 1. – С. 5-14.

11. Грищук Р.В. Методологія синтезу та аналізу диференціально-ігрових моделей та методів моделювання процесів кібернападу на державні інформаційні ресурси / Р.В. Грищук, О.Г. Корченко // Захист інформації: наук.-практ. журнал. – 2012. – № 3. – С. 115-122.

12. Доктрина інформаційної безпеки України (затверджена указом Президента України №47/2017 від 25 лютого 2017 року): [Електронний ресурс] / Офіційне представництво Президента України. – Режим доступу до ресурсу: http://www.president.gov.ua/documents/472017-21374. – Назва з екрану.

13. Молодецька-Гринчук К.В. Аналіз впливу загроз інформаційній безпеці держави у соціальних інтернет-сервісах на сфери суспільної діяльності / К.В. Молодецька-Гринчук // Управління розвитком складних систем. – 2017. – № 30. – С. 121-127.

14. Офіційний сайт Міністерства інформаційної політики України. – Режим доступу до сайту: http://mip.gov.ua. – Назва з екрану.

15. Молодецька К.В. Технологія виявлення організаційних ознак інформаційних операцій у соціальних інтернет-сервісах / К.В. Молодецька // Проблеми інформаційних технологій. – 2016. – № 20. – С. 84-93.

16. Молодецька-Гринчук К.В. Метод виявлення ознак інформаційних впливів у соціальних інтернет-сервісах за змістовними ознаками / К.В. Молодецька-Гринчук // Радіоелектроніка, інформатика, управління. – 2017. – № 2(41). – С. 117-126. – DOI: 10.15588/1607-3274-2017-2-13.

17. Молодецька-Гринчук К.В. Методика виявлення маніпуляцій суспільною думкою у соціальних інтернет-сервісах / К.В. Молодецька-Гринчук // Інформаційна безпека. – 2016. – № 4(24). – С. 80-92.

18. Молодецька-Гринчук К.В. Метод побудови профілів інформаційної безпеки акторів соціальних інтернет-сервісів / К.В. Молодецька-Гринчук // Інформаційна безпека. – 2017. – № 2(26). – С. 104-110.

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

20. Hryshchuk R. Synergetic control of social networking services actors' interactions / R. Hryshchuk, K. Molodetska // Recent Advances in Systems, Control and Information Technology. – Vol. 543. – Springer International Publishing, 2017. – P. 34-42. – DOI:10.1007/978-3-319-48923-0_5.

21. Грищук Р.В. Концепція синергетичного управління процесами взаємодії агентів у соціальних інтернет-сервісах / Р.В. Грищук, К.В. Молодецька // Безпека інформації. – 2015. – Т. 21, ч. ІІ. – С. 123-130. – DOI: 10.18372/2225-5036.21.8730.

22. Молодецька К.В. Методика вибору атрактора для управління динамікою процесів взаємодії акторів у соціальних інтернет-сервісах / К.В. Молодецька // Інформаційна безпека. – 2014. – № 3–4. – С. 146-151.

23. Грищук Р.В. Спосіб синергетичного управління поведінкою акторів у соціальних інтернет-сервісах / Р.В. Грищук, К.В. Молодецька // Системи управління, навігації та зв'язку. – 2016. – № 1(37). – С. 94-99.

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

25. Молодецька К.В. Спосіб підтримання заданого рівня попиту акторів соціальних інтернет-сервісів на контент / К.В. Молодецька // Радіоелектроніка, інформатика, управління. – 2015. – № 4(35). – С. 113-117. – DOI: 10.15588/1607-3274-2015-4-16.

26. Тодд Заки Варфел. Прототипирование. Практическое руководство / Тодд Заки Вар. – Манн, Иванов И Фербер, 2013. – 240 с.

27. Фаулер М. UML. Основы: Пер. с англ. / М. Фаулер, К. Скотт. – СПб.: Символ-Плюс, 2002. –23 с.

28. Manning Chr. Introduction to Information Retrieval / Chr. Manning, P. Raghavan, H. Schütze. – Cambridge University Press, 2008. – 544 p.

29. Воронин А.Н. Нелинейная схема компромиссов в многокритериальных задачах оценивания и оптимизации / А.Н. Воронин // Кибернетика и системный анализ. – 2009. – № 4. – С. 106-114.

30. Воронин А. Нелинейная схема компромиссов в многокритериальных задачах / А. Воронин, Ю. Зиатдинов // International Book Series «Information Science & Computing». Artificial Intelligence and Decision Making. – 2008. – P. 79-85.

References

1. Onyshchenko, O.S., Horovyi, V.M. and Popyk, V.I. (2014), "*Sotsialni merezhi yak instrument vzaiemovplyvu vlady ta hromadianskoho suspilstva: monohrafiia*" [Social networks as an instrument of mutual influence of power and civil society], NAN Ukrainy, Nats. b-ka Ukrainy im. V.I. Vernadskoho, Kyiv, 260 p.

2. Popyk, V.I., Onyshchenko, O.S. and Horovyi, V.M. (2015), "*Problemy suspilnoi bezpeky v protsesi rozvytku sotsialnykh merezh*" [Problems of public safety in the development of social networks], NAN Ukrainy, Nats. b-ka Ukrainy im. V.I. Vernadskoho, Kyiv, 202 p.

3. Ostapenko, G.A., Parinova, L.V., Belonozhkin, V.I., Bataronov, I.L. and Simonov, K.V. (2013), "*Informatsionnyie riski v sotsialnyih setyah*" [Information Risks in Social Networks], Moskow, 161 p.

4. Papacharissi, Z. (2011), *A Networked self: identity, community and culture on social network sites*, Routledge, New York, 327 p.

5. Molodetska, K.V. (2016), "Sotsialni internet-servisy yak subiekt informatsiinoi bezpeky derzhavy" [Social networking services as a subject of information security of the state], *Information technology and security*, Vol. 4, No. 1(6), pp. 13-20.

6. Molodetska, K.V. (2016), "Uzahalnena klasyfikatsiia zahroz informatsiinii bezpetsi derzhavy v sotsialnykh internet-servisakh" [Generalized classification of threats to information security of the state in social networking services], *Information protection*, No. 23, pp. 75-87.

7. Hryshchuk, R.V. and Danyk, Yu.H. (2016), "*Osnovy kibernetychnoi bezpeky: monohrafiia*" [Fundamentals of cybernetic security: monograph], ZhNAEU, Zhytomyr, 636 p.

8. Onyshchenko, O., Horovyi, V. and Popyk, V. (2015), "*Tekhnolohii rozvytku i zakhystu natsionalnoho informatsiinoho prostoru*" [Technologies for the development and protection of the national information space], Kyiv, 296 p.

9. Radkovets, Yu., Levchenko, O. and Kosohov, O. (2014), "Pohliady na stvorennia systemy informatsiinoi bezpeky Ukrainy ta yii Zbroinykh Syl" [Views on the creation of the information security system of Ukraine and its Armed Forces], *Science and Defense*, pp. 38-42.

10. Buriachok, V., Korchenko, O., Khoroshko, V. and Kudinov, V. (2013), "Stratehiia otsiniuvannia rivnia zakhyshchenosti derzhavy vid ryzyku storonnoho kibernetychnoho vplyvu" [Strategy for assessing the level of protection of the state from the risk of extraneous cybernetic influence], *Information protection*, Vol. 15, No. 1, pp. 5-14.

11. Hryshchuk, R.V. and Korchenko, O.H. (2012), "Metodolohiia syntezu ta analizu dyferentsialno-ihrovykh modelei ta metodiv modeliuvannia protsesiv kibernapadu na derzhavni informatsiini resursy" [Methodology of synthesis and analysis of differential game models and methods of modeling of cyber attack processes on state information resources], *Information protection*, No. 3, pp. 115-122.

12. Low of Prezident of Ukraine (2017), "Doktryna informatsiinoi bezpeky Ukrainy" [Doctrine of Information Security of Ukraine], www.president.gov.ua/documents/472017-21374 (accessed 3 August 2017).

13. Molodetska-Hrynchuk, K.V. (2017), "Analiz vplyvu zahroz informatsiinii bezpetsi derzhavy u sotsialnykh-internet servisakh na sfery suspilnoi diialnosti" [Analysis of influence threats of an information security of the state in a social networking service to the spheres of public activities], *Management of the development of complex systems*, No. 30, pp. 121-127.

14. "Ofitsiinyi sait Ministerstva informatsiinoi polityky Ukrainy" [Official site of the Ministry of Information Policy of Ukraine], http://mip.gov.ua (accessed 3 August 2017).

15. Molodetska, K.V. (2016), "Tekhnolohiia vyiavlennia orhanizatsiinykh oznak informatsiinykh operatsii u sotsialnykh internet-servisakh" [Technology of identifying organizational features of information operations in social networking services], *Problems of information technologies*, No. 20, pp. 84-93.

16. Molodetska-Hrynchuk, K.V. (2017), "Metod vyiavlennia oznak informatsiinykh vplyviv u sotsialnykh internet-servisakh za zmistovnymy oznakamy" [Outreaches content tracing technique for social networking services], *Radio Electronics, Computer Science, Control*, No. 4(24), pp. 117-126, DOI: 10.15588/1607-3274-2017-2-13.

17. Molodetska-Hrynchuk, K.V. (2016), "Metodyka vyiavlennia manipuliatsii suspilnoiu dumkoiu u sotsialnykh internet-servisakh" [Method of detection of manipulation of public opinion in social networking services], *Informational security*, No. 4(24), pp. 80-92.

18. Molodetska-Hrynchuk, K.V. (2016), "Metod pobudovy profiliv informatsiinoi bezpeky aktoriv sotsialnykh internet-servisiv" [Method of constructing profiles of information security actors of social networking services], *Informational security*, No. 2(26), pp. 104-110.

19. Hryshchuk, R.V. and Molodetska, K.V. (2015), "Metod prohnozuvannia dynamiky poshyrennia kontentu y zapytiv na noho za danymy kontent-analizu povidomlen u sotsialnykh internet-servisakh" [Method of predicting the dynamics of content distribution and requests for it according to content analysis of messages in social networking services], *Control, navigation and communication systems*, No. 4(36), pp. 60-65.

20. Hryshchuk, R. and Molodetska, K. (2017), Synergetic Control of Social Networking Services Actors' Interactions, *Recent Advances in Systems, Control and Information Technology Advances in Intelligent Systems and Computing*, Vol. 543, pp. 34-42, DOI:10.1007/978-3-319-48923-0_5.

21. Hryshchuk, R. and Molodetska, K. (2015), "Kontseptsiia synerhetychnoho upravlinnia protsesamy vzaiemodii ahentiv u sotsialnykh internet-servisakh" [The concept of synergetic management of agents interaction in social networking services], *Information security*, Vol. 21, Part II, pp. 123-130, DOI: 10.18372/2225-5036.21.8730.

22. Molodetska, K.V. (2014), "Metodyka vyboru atraktora dlia upravlinnia dynamikoiu protsesiv vzaiemodii aktoriv u sotsialnykh internet-servisakh" [Method of selecting attractor to control the dynamics of processes of interaction between actors in social networking services], *Information security*, No. 3–4, pp. 146-151.

23. Hryshchuk, R. and Molodetska, K. (2016), "Sposib synerhetychnoho upravlinnia povedinkoiu aktoriv u sotsialnykh internet-servisakh" [A method of synergetic management of the behavior of actors in social networking services], *Control, navigation and communication systems*, No. 1(37), pp. 94-99.

24. Molodetska, K. (2015), "Syntez synerhetychnoho upravlinnia popytom ahentiv na kontent u sotsialnykh internet-servisakh" [Synthesis of synergetic demand management agents for content in social networking services], *Computer science and mathematical methods in modeling*, Vol. 5, No. 4, pp. 330-338.

25. Molodetska, K. (2015), "Sposib pidtrymannia zadanoho rivnia popytu aktoriv sotsialnykh internet-servisiv na kontent" [A way to maintain a predetermined level of demand for actors of social networking services on content], *Radio Electronics, Computer Science, Control*, No. 4(35), pp. 113-117, DOI: 10.15588/1607-3274-2015-4-16.

26. Warfel, T.Z. (2009), *Prototyping a practitioners guide*, Rosenfeld Media, Brooklyn, NY, 240 p.

27. Fauler, M. and Skott, K. (2002), "*UML. Osnovy*" [UML. Basic], Symvol-Plius, SPb, 23 p.

28. Manning, Chr., Raghavan, P. and Schütze, H. (2008), *Introduction to Information Retrieval*, Cambridge University Press, 544 p.

29. Voronin, A.N. (2009), "Nelineinaia skhema kompromissov v mnogokriterialnykh zadachakh otsenivaniia i optimizatsii" [Nonlinear scheme of compromises in multicriteria estimation and optimization problems], *Cybernetics and Systems Analysis*, No. 4, pp. 106-114.

30. Voronin, A., and Ziatdinov, Yu. (2008), "Nelineynaya shema kompromissov v mnogokriterialnyih zadachah" [Nonlinear scheme of compromises in multicriteria problems], *International Book Series «Information Science & Computing». Artificial Intelligence and Decision Making*, pp. 79-85.

Надійшла до редколегії 12.09.2017
Схвалена до друку 2.11.2017

Відомості про автора:
Молодецька-Гринчук Катерина Валеріївна
кандидат технічних наук доцент
доцент Житомирського національного
агроекологічного університету,
Житомир, Україна
https://orcid.org/0000-0001-9864-2463
e-mail: kmolodetska@gmail.com

Information about the author:
Molodetska-Hrynchuk Kateryna
Candidate of Technical Sciences Associate
Professor Senior Lecturer of Zhytomyr National
Agroecological University,
Zhytomyr, Ukraine
https://orcid.org/0000-0001-9864-2463
e-mail: kmolodetska@gmail.com

ПРОТОТИП ПРОГРАММНОГО КОМПЛЕКСА ОБНАРУЖЕНИЯ ПРИЗНАКОВ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СТРАНЫ В СОЦИАЛЬНЫХ ИНТЕРНЕТ-СЕРВИСАХ И ОЦЕНКИ ИХ УРОВНЯ

К.В. Молодецкая-Гринчук

В статье предложен прототип программного комплекса системы поддержки принятия решений для выявления признаков угроз информационной безопасности государства в социальных интернет-сервисах и оценки их уровня. Разработанный прототип программного комплекса является составной частью системы обеспечения информационной безопасности государства и автоматизирует процессы раннего выявления угроз в социальных интернет-сервисах. В основу модели принятия решений положены современные подходы к информационному поиску, интеллектуальному анализу контента и синергетическое управление взаимодействием акторов для достижения желаемого состояния информационной безопасности виртуальных сообществ. Созданный макет программного комплекса позволяет проверить адекватность использованных для построения системы поддержки принятия решений методов, моделей и технологических решений.

Ключевые слова: *социальный интернет-сервис, система поддержки принятия решений, угроза, информационная безопасность государства, прототип программного комплекса, актор, контент, синергетическое управление.*

MODEL OF THE SOFTWARE FOR DETERMINING THE STATE'S INFORMATION SECURITY THREATS IN THE SOCIAL NETWORKING SERVICES

K. Molodetska-Hrynchuk

Social networking services have become an effective means of mass communication of members of virtual communities named actors. However, the benefits of social networking services are used by intruders to implement threats to the state's information security directed against people, society, and the state. It's important to create an effective system for ensuring information security of the state in social networking services to identify, assess and counteract complex threats. The article proposes a prototype of the program complex of the decision support system for revealing signs of threats to the state's information security in social networking services and assessing their level. The developed prototype of the software complex is an integral part of the state information security system and automates the processes of early detection of threats in social networking services. The basis of the decision-making model is modern approaches to information retrieval, intellectual content analysis and synergistic management of actors interaction to achieve the desired state of information security of virtual communities. The obtained research results prove the adequacy of the proposed methods, models and technological solutions. The software package layout can be used to create an effective software product and to take into account the requirements of users–experts, reducing risks in the development of the final software product.

Keywords*: social networking service, decision support system, threat, information security of the state, software prototype, actor, content, synergetic control.*