*УДК 004.056.5:004.738.5(045)*

Молодецька-Гринчук К. В.

*Канд. техн. наук, доцент, доцент кафедри комп'ютерних технологій і моделювання систем Житомирського національного агроекологічного університету, Житомир, Україна*

# МЕТОД ВИЯВЛЕННЯ ОЗНАК ІНФОРМАЦІЙНИХ ВПЛИВІВ У СОЦІАЛЬНИХ ІНТЕРНЕТ-СЕРВІСАХ ЗА ЗМІСТОВНИМИ ОЗНАКАМИ

**Актуальність.** Сьогодні соціальні інтернет-сервіси перетворилися на ефективний інструмент комунікації між учасниками віртуальних спільнот – акторами. З огляду на високу швидкість поширення контенту, транскордонність процесів взаємодії акторів, наявність засобів для їх організації у групи, соціальні-інтернет сервіси можуть застосовуватися як дієвий засіб проведення інформаційних операцій проти людини, суспільства, держави. В процесах комунікації акторів у віртуальних спільнотах найчастіше використовується текстовий контент. Розроблення ефективних алгоритмів функціонування системи забезпечення інформаційної безпеки держави для вирішення проблеми моніторингу текстового контенту соціальних інтернет-сервісів є актуальним теоретико-прикладним завданням.

**Мета.** Метою досліджень є обгрунтування й розроблення методу виявлення інформаційних впливів у соціальних інтернет-сервісах за змістовними ознаками для підвищення ефективності системи забезпечення інформаційної безпеки держави.

**Метод.** Розроблений метод ґрунтується на сучасних підходах до інтелектуального аналізу текстового контенту – латентно-семантичному індексуванню і семантичному аналізі на базі онтологій.

**Результати.** В результаті латентно-семантичного індексування відбирається релевантний заданій тематиці текстовий контент на основі його змісту і без врахування щільності ключових слів. На етапі семантичного аналізу реалізовано процедури подальшого виявлення небезпечних семантичних конструкцій у відібраному текстовому контенті. У випадку детектування суперечливих фрагментів текстового контенту і онтології та після їх аналізу експертами виконується наповнення онтологічних баз знань шаблонами загроз інформаційній безпеці у соціальних інтернет-сервісах. Таким чином, комбінація методів латентно-семантичного індексування і семантичного аналізу забезпечує взаємну компенсацію їх недоліків та виявлення прихованих залежностей між мовними одиницями.

**Висновки.** Завдяки розробленому методу виявлення ознак інформаційних впливів у соціальних інтернет-сервісах автоматизуються процедури ідентифікації у віртуальних спільнотах інформаційних операцій, направлених проти інформаційної безпеки людини, суспільства, держави. Застосування запропонованого методу виявлення ознак інформаційних впливів дозволяє підвищити ефективність і швидкодію системи забезпечення інформаційної безпеки держави в соціальних інтернет-сервісах як складової національної безпеки України.

**Ключові слова:** соціальний інтернет-сервіс, інформаційна безпека, загроза, текстовий контент, латентно-семантичне індексування, семантичний аналіз, онтологія.

## НОМЕНКЛАТУРА

$i$ – кількість ключових слів;

$j$ – кількість публікацій акторів;

$k$ – кількість сингулярних значень матриці;

$W = \langle w_i \rangle$ – ключові слова;

$M$ – частотна матриця;

$U$ і $V^T$ – ортогональні матриці;

$S$ – діагональна матриця;

$P_n$ – скінченна множина концептів;

$R_n$ – скінченна множина відношень між концептами;

$P_s(p_n) \in P_n$ – підмножина множини концептів $P_n$, суміжних до деякого концепту $p_n$;

$P_{in}(r_n) \in P_n$ – підмножина множини концептів $P_n$, інцидентних до відношення $r_n$;

$R_{in}(p_n) \in R_n$ – підмножина множини відношень $R_n$, інцидентних до деякого концепту $p_n$;

$R_z(p_n) \in R_n$ – підмножина множини відношень $R_n$, яка вказує на небезпеку для концепту $p_n$;

$r_t(p_t)$ – деяке відношення з текстового контенту СІС, що аналізується;

$p_t \in P_n$ – концепт онтології досліджуваної віртуальної спільноти;

$r_t \in R_z(p_n)$ – множина відношень, які вказують на небезпеку для деякого концепту $p_n$;

$D_i$ – колекції публікацій;

LSI – латентно-семантичне індексування;

Ont – онтологія;

СІС – соціальний інтернет-сервіс.

## ВСТУП

На сучасному етапі значну роль в процесах комунікації суспільства відіграють соціальні інтернет-сервіси (СІС), які забезпечують учасників віртуальних спільнот – акторів, новітніми засобами взаємодії [1]. Завдяки комунікаційним перевагам [2] СІС перетворилися на потужний інструмент взаємодії громадянського суспільства і держави, формування суспільної думки з багатьох актуальних питань. Однак, внаслідок широкої популярності СІС стали і дієвим засобом проведення інформаційних операцій проти людини, суспільства, держави. Встановлено, що ознаки інформаційних впливів у СІС доцільно об'єднати в групи за такими характеристиками – організаційні, змістовні та маніпулятивні. Виявлення згаданих ознак, як показано в [1, 3], у першу чергу пов'язане з моніторингом їх контенту.

В свою чергу, контент, який ґенерується акторами віртуальних спільнот, може бути представлений тексто-


DOI 10.15588/1607-3274-2017-2-13

вими, аудіо, відео, графічними та іншими типами даних. Дослідження співвідношення видів контенту в СІС показують, що найбільшу частку інформаційного середовища займає текстовий тип даних [4]. В першу чергу, це пов'язано з високою швидкістю його споживання акторами віртуальних спільнот завдяки універсальності, відсутності залежності якості відображення від типу кінцевого пристрою користувача. Популярність текстового контенту визначається закладеною в його зміст ідеєю, яка приймаючи різні форми покликана донести до актора потрібні картини суспільних чи політичних подій.

Однак, як показано в [1], зміст текстового контенту може містити деструктивний інформаційний вплив у явному або прихованому вигляді. Висока складність процедур аналізу змісту текстового контенту й особливо автоматичного аналізу, призводить до ускладнення процесу виявлення початку та самого факту інформаційного впливу в СІС. Тому розроблення ефективних алгоритмів функціонування системи забезпечення інформаційної безпеки держави для вирішення проблеми моніторингу текстового контенту СІС є актуальним теоретико-прикладним завданням.

Мета статті полягає в обґрунтуванні й розробленні методу виявлення інформаційних впливів в СІС за змістовними ознаками, який дозволить підвищити ефективність функціонування системи забезпечення інформаційної безпеки держави.

Для досягнення поставленої в статті мети необхідно розв'язати такі частинні завдання:

– проаналізувати сучасні підходи до виявлення загроз інформаційній безпеці держави інформаційно-психологічного характеру в розрізі аналізу текстового контенту СІС;

– встановити напрямки підвищення ефективності функціонування системи забезпечення інформаційної безпеки держави для завчасного виявлення ознак інформаційних впливів у СІС;

– розробити метод ідентифікації інформаційних впливів на основі виявлення їх ознак в змісті текстового контенту, який ґенерується або поширюється акторами у віртуальних спільнотах СІС;

– перевірити достовірність запропонованого методу на реальних прикладах.

## 1 ПОСТАНОВКА ЗАДАЧІ

Поставимо задачу розробити метод виявлення інформаційних впливів на акторів віртуальних спільнот СІС, який забезпечить задану достовірність функціонування, виявлення відомих та нових загроз в явному або прихованому вигляді, реалізованість за умови обмеженого забезпечення ресурсами. Вибір текстового контенту для досягнення мети дослідження проводиться відповідно до вимог критичності і значущості його тематики для інформаційної безпеки держави. Для розв'язку задачі необхідно узагальнити і систематизувати змістовні ознаки для виявлення інформаційного впливу на акторів. Використати сучасні підходи до інтелектуального аналізу текстового контенту, а для побудови онтологій обираються предметні області, пов'язані із забезпеченням інформаційної безпеки держави. Розроблений метод повинен забезпечити задану швидкодію для автоматизації процедур виявлення загроз інформаційний безпеці держави і функціонування підсистеми моніторингу інформаційного середовища системи забезпечення інформаційної безпеки держави у СІС.

## 2 ОГЛЯД ЛІТЕРАТУРИ

Аналіз останніх досліджень і публікацій показав, що для обробки і аналізу текстового контенту використовуються методи статистичного й лінгвістичного аналізу [3, 5–9]. Перша група методів ґрунтується на аналізі змісту контенту за частотою слів, які в ньому використовуються. Спільним недоліком групи статистичних методів є неможливість врахування зв'язності текстового контенту і, як наслідок, його представлення у вигляді множини не пов'язаних між собою слів або Bag of Words [3, 5]. Для усунення цього недоліку використовують методи лінгвістичного аналізу, які включають такі рівні: графематичний для виділення абзаців, речень і окремих слів; морфологічний, який має на меті визначення морфологічних характеристик і словоформ вхідного контенту; синтаксичний аналіз для встановлення синтаксичної залежності слів у реченні; семантичний аналіз для змістовного розуміння текстового контенту.

Семантичний аналіз є складною процедурою, яка ґрунтується на використанні баз знань і тезаурусів для відображення зв'язку між окремими словами й словосполученнями [3]. Результатом семантичного аналізу є формалізоване подання текстового контенту, який досліджується, для подальшого інтелектуального аналізу. До недоліків сучасних семантичних аналізаторів можна віднести високу вартість їх підтримки для кожної окремої мови, істотну обчислювальну складність, неоднозначність результатів функціонування [3, 7].

Проблема виявлення ознак інформаційних впливів за змістовними ознаками не обмежується лінгвістичним аналізом текстового контенту СІС. Детектування загроз системою забезпечення інформаційної безпеки держави в СІС належить, зокрема, до задач інформаційного пошуку [7]. Серед класичних методів інформаційного пошуку виділяють теоретико-множинні, алгебричні та ймовірнісні. Однак, їх застосування для пошуку в СІС текстового контенту з деструктивним інформаційним впливом обмежується рядом недоліків [3]: неможливістю ранжування результатів пошуку; розрахунки пов'язані зі значними об'ємами даних; низька обчислювальна масштабованість і необхідність навчання системи. Тому перспективним напрямком є використання моделей семантичного пошуку та аналізу, які враховують зміст текстового контенту.

Встановлено, що в існуючих дослідженнях проблеми виявлення інформаційних впливів у СІС не використовується комплексний підхід, який би систематизував і узагальнив їх частинні ознаки. Протиріччя між рівнем розвитку сучасних інформаційних технологій і науковим базисом автоматизованого виявлення загроз в СІС, відсутність дієвих методик змістовного аналізу текстового контенту СІС на предмет деструктивного інформаційного впливу додатково актуалізують обраний напрямок досліджень.

## 2 ОГЛЯД ЛІТЕРАТУРИ

Аналіз останніх досліджень і публікацій показав, що для обробки і аналізу текстового контенту використовуються методи статистичного й лінгвістичного аналізу [3, 5–9]. Перша група методів ґрунтується на аналізі змісту контенту за частотою слів, які в ньому використовуються. Спільним недоліком групи статистичних методів є неможливість врахування зв'язності текстового контенту і, як наслідок, його представлення у вигляді множини не пов'язаних між собою слів або Bag of Words [3, 5]. Для усунення цього недоліку використовують методи лінгвістичного аналізу, які включають такі рівні: графематичний для виділення абзаців, речень і окремих слів; морфологічний, який має на меті визначення морфологічних характеристик і словоформ вхідного контенту; синтаксичний аналіз для встановлення синтаксичної залежності слів у реченні; семантичний аналіз для змістовного розуміння текстового контенту.

Семантичний аналіз є складною процедурою, яка ґрунтується на використанні баз знань і тезаурусів для відображення зв'язку між окремими словами й словосполученнями [3]. Результатом семантичного аналізу є формалізоване подання текстового контенту, який досліджується, для подальшого інтелектуального аналізу. До недоліків сучасних семантичних аналізаторів можна віднести високу вартість їх підтримки для кожної окремої мови, істотну обчислювальну складність, неоднозначність результатів функціонування [3, 7].

Проблема виявлення ознак інформаційних впливів за змістовними ознаками не обмежується лінгвістичним аналізом текстового контенту СІС. Детектування загроз системою забезпечення інформаційної безпеки держави в СІС належить, зокрема, до задач інформаційного пошуку [7]. Серед класичних методів інформаційного пошуку виділяють теоретико-множинні, алгебричні та ймовірнісні. Однак, їх застосування для пошуку в СІС текстового контенту з деструктивним інформаційним впливом обмежується рядом недоліків [3]: неможливістю ранжування результатів пошуку; розрахунки пов'язані зі значними об'ємами даних; низька обчислювальна масштабованість і необхідність навчання системи. Тому перспективним напрямком є використання моделей семантичного пошуку та аналізу, які враховують зміст текстового контенту.

Встановлено, що в існуючих дослідженнях проблеми виявлення інформаційних впливів у СІС не використовується комплексний підхід, який би систематизував і узагальнив їх частинні ознаки. Протиріччя між рівнем розвитку сучасних інформаційних технологій і науковим базисом автоматизованого виявлення загроз в СІС, відсутність дієвих методик змістовного аналізу текстового контенту СІС на предмет деструктивного інформаційного впливу додатково актуалізують обраний напрямок досліджень.

## 3 МАТЕРІАЛИ І МЕТОДИ

З [5, 6] відомо, що в загальному вигляді сучасні системи виявлення загроз як в текстовому контенті, так і в технічних системах, функціонують на основі таких базових методів:

– сигнатурні, ідея яких полягає в ідентифікації загроз із використанням відомих значень їх параметрів;

– виявлення аномалій на базі відхилень від еталонної моделі функціонування об'єкта досліджень.

Сигнатурні методи відрізняються високою ефективністю, а загроза, в свою чергу, описується у вигляді набору правил чи формальної моделі. Однак, у разі відсутності моделі деякої загрози в системі, її ідентифікація стає неможливою. Детектування системою виявлення загроз аномальної поведінки об'єкта дослідження пов'язане з його навчанням еталонній поведінці, відхилення від якої вказує на появу загрози. В окремих випадках опис загрози може збігатися з еталонною поведінкою об'єкта, що істотно впливає на достовірність функціонування системи виявлення загроз. Тому перспективним напрямком є розробка таких методів виявлення загроз інформаційній безпеці держави в СІС за змістовними ознаками, які забезпечать задану достовірність функціонування, виявлення відомих та нових загроз в явному або прихованому вигляді, реалізованість за умови обмеженого забезпечення ресурсами.

У результаті узагальнення відомих підходів до інформаційного пошуку і лінгвістичного аналізу контенту СІС розроблено метод виявлення інформаційних впливів на основі встановлення їх ознак у змісті текстового контенту, який зводиться до такого.

Етап 1. Пошук текстового контенту в СІС за заданим інформаційним приводом. На цьому етапі визначаються ключові слова $W = \langle w_i \rangle$, $i = \overline{1, n}$ для пошуку текстового контенту в СІС за критерієм актуальності, критичності та рівня обговорення у суспільстві його тематики. В даному випадку поставлена задача зводиться до вибору методу інформаційного пошуку текстового контенту, який задовольняє вимогам релевантного пошуку текстового контенту, ефективній обробці, зокрема, коротких публікацій. Тому пропонується скористатися методом латентно-семантичного індексування (LSI) (латентно-семантичного аналізу (LSA)) [7–9]. Особливостями LSI є пошук контенту в СІС на основі його змісту, а не щільності ключових слів, і пошук прихованих семантичних зв'язків між ключовими словами й безпосередньо контентом. Суть методу LSI, адаптованого під задачі дослідження, наведена нижче [8].

Крок 1.1 методу полягає у попередній підготовці досліджуваного контенту СІС шляхом видалення стоп-слів, стеммінгу або лематизації слів. Стоп-слова зустрічаються у всьому контенті й не мають змістовного навантаження, наприклад, сполучники, частки, прийменники тощо. Стеммінг полягає у виділенні основи слова виключенням закінчень і суфіксів та є необов'язковим на великих наборах публікацій контенту СІС. Для випадку невеликих наборів публікацій доцільно скористатися алгоритмом Портера [10], який не вимагає морфологічних словників, а виділення основи слова реалізоване на основі визначених правил. Лематизація – це приведення слова до словникового виду.

Крок 1.2. Призначений для виключення з досліджуваного текстового контенту СІС слів, які вживаються тільки один раз. Даний крок не є обов'язковим, однак зменшує кількість подальших обчислень і, як наслідок, підвищує швидкодію.

Крок 1.3. Формування частотної матриці $M$ ключових слів $W$, які індексуються. Рядками $i$ цієї матриці є ключові слова $W$ семантичного ядра, за яким виконується моніторинг текстового контенту СІС, а стовпцями $j$-публікації акторів чи віртуальних спільнот. Елементи матриці $m_{ij}$ представляють собою частоту вживання деякого ключового слова $w_i$ в $j$-й публікації.

Крок 1.4 полягає в сингулярному розкладанні початкової матриці $M$ на три компоненти

$$M = U \times S \times V^T, \quad (1)$$

де матриці $U$ і $V^T$ мають розмірність $i \times k$ та $k \times j$ відповідно; $S$ – діагональна матриця розмірністю $k \times k$, причому $k$ – кількість прихованих тематик контенту, а її елементи впорядковані за спаданням.

На кроці 1.5 виділяють ті рядки матриці $U$ і стовпці $V^T$, які відповідають найбільшим сингулярним числам $k$, а їх величина – ступеню прояву ключових слів у колекції публікацій в СІС.

У результаті виконання етапу 1 вдається одержати колекцію публікацій у СІС, які відповідають семантичному ядру пошукового запиту. Такі публікації підлягають подальшому семантичному аналізу на основі онтологій.

Етап 2. Виявлення ознак інформаційних впливів у СІС на основі сигнатурного методу і методу виявлення аномалій. Суть даного етапу полягає у виявленні загроз інформаційній безпеці державі в СІС, які містяться в текстовому контенті, який ґенерується або поширюється віртуальними спільнотами, і мають на меті вплив на акторів, їх свободу вибору, дискредитацію органів влади тощо [11]. Контент віртуальних спільнот, проіндексований і відібраний на попередньому етапі, підлягає семантичному аналізу на базі онтологій [12–17]. В роботі [12] визначено, що онтологія є експліцитною (явною) специфікацією опису множини об'єктів, які називають концептами, і зв'язків між ними – відношеннями. Зміст другого етапу полягає в наступному.

На кроці 2.1 складаються онтологія функціонування віртуальної спільноти в СІС

$$Ont = \langle P_n, R_n \rangle. \quad (2)$$

При цьому в онтології $Ont$ (2) для автоматизації подальшого аналізу текстового контенту віртуальних спільнот виділяються підмножини [5] $P_s(p_n) \in P_n$, $P_{in}(r_n) \in P_n$, $R_{in}(p_n) \in R_n$, $R_z(p_n) \in R_n$.

Крок 2.2 полягає у побудові семантичного опису текстового контенту, виявленого на першому етапі методу

$$Sem_t = \langle P_t, R_t \rangle. \quad (3)$$

Для забезпечення швидкодії функціонування методу доцільно застосовувати автоматичні засоби ґенерації онтологій. До такого класу програмних продуктів відносять Protégé, Ontology Learning Framework, LOGS, ABBYY Compreno тощо [13–16].

Крок 2.3 зводиться до виявлення ознак загрози у попередньо проіндексованому на першому етапі методу текстовому контенті СІС. У формальному вигляді правила виявлення загроз інформаційній безпеці зводяться до такого [5]:

– детектування на основі сигнатурного методу і семантичних ознак

$$\exists r_t(p_t): p_t \in P_n \wedge r_t \in R_z(p_n). \quad (3)$$

Суть правила (3) полягає в наступному: для виявлення загрози інформаційній безпеці у змісті текстового контенту віртуальної спільноти СІС необхідно виявити зв'язок між об'єктом публікації з його характеристиками у контенті та негативними ознаками для цього об'єкта внаслідок реалізації загрози.

Виявлення суперечностей на основі виявлення аномалій шляхом співставлення семантичного опису проіндексованого текстового контенту і семантичного шаблону загрози. При цьому встановлюється невідповідність фактів у контенті СІС, що проявляється як:

– протиріччя понять в змісті контенту віртуальних спільнот – вживання концепту в конкретному відношенні не передбачене онтологією

$$\exists r_t(p_t): p_t \in P_n \wedge r_t \in R_n \wedge p_t \notin P_{in}(r_n). \quad (4)$$

Зміст правила (4) полягає в такому: деякий концепт $p_t$ текстового контенту СІС не може вживатися у конкретному відношенні $r_t(p_t)$.

– протиріччя відношень в контенті – вжите відношення між концептами не визначене онтологією

$$\forall p_n \in P_n \neg \exists r_n \in R_n : r_t = r_n. \quad (5)$$

Правило (5) трактується як: множина відношень $R_n$ онтології функціонування віртуальної спільноти, в які можуть вступати концепти $p_n \in P_n$, які пов'язані між собою відношеннями $r_t$, не містить цих відношень.

Крок 2.4 призначений для розгорнутого аналізу експертами проіндексованого текстового контенту на предмет наявності загроз. Даний крок необхідний, якщо контент СІС є релевантним семантичному ядру пошукового запиту до контенту СІС з етапу 1, однак на етапі 2 не виявлено суперечливих фрагментів такого контенту і онтології. Тоді ідентифіковані експертами небезпечні семантичні конструкції додаються до шаблонів загроз і використовуються в онтології. В результаті таких дій метод LSI забезпечує ефективне виявлення залежностей між лексичними одиницями в контенті СІС для наповнення онтологічних баз знань [18].

Метод виявлення змістовний ознак інформаційних впливів у СІС з використанням латентного семантичного аналізу і семантичного аналізу на базі онтологій поданий у вигляді структурної схеми на рис. 1.

Застосування розробленого методу виявлення ознак інформаційних впливів дозволяє ідентифікувати у віртуальних спільнотах СІС інформаційні операції, направлені проти інформаційної безпеки людини, суспільства, держави. Перспективним є використання запропонованого методу для функціонування системи забезпечення інформаційної безпеки держави в СІС, зокрема автоматизації процесів моніторингу інформаційного середовища віртуальних спільнот. Окреме місце в забезпеченні функціонування методу належить експертам і співробітникам спеціальних підрозділів, перед якими стоїть завдання виявлення деструктивних інформаційних впливів у попередньо проіндексованому й відібраному контенті СІС. На основі таких

ідентифікованих впливів створюються семантичні шаблони загроз і додаються до онтологічних баз знань.

## 4 ЕКСПЕРИМЕНТИ

Відповідно до розробленого методу дослідимо контент СІС Facebook на предмет наявності ознак інформаційного впливу на акторів. Для цього задамо семантичне ядро

W = < майдан; бандити; влада; поліція; корупція; диктатура; війна; злидні; Порошенко; олігархи>

для його пошуку в колекції публікацій $D_i$, $i = \overline{1,10}$ актора Миколи Гайдука в соціальній мережі Facebook. Після виконання першого етапу розробленого методу досліди-мо релевантні до запиту $W$ публікації, використовуючи семантичний аналіз і онтологічні бази знань.

## 5 РЕЗУЛЬТАТИ

Результати першого етапу функціонування методу виявлення інформаційних впливів подано в табл. 1.

Застосуємо до матриці в табл. 1 операцію двовимірного сингулярного розкладу, внаслідок якого отримаємо три матриці (рис. 2).

З метою візуалізації результатів розрахунків зобразимо їх на графіку (рис. 3).

З рис. 3 видно, що проіндексовані документи $D_2$, $D_3$, $D_5$ і $D_{10}$, не зважаючи на наявність слів із заданого семантичного ядра $W$, не релевантні пошуковому запиту.

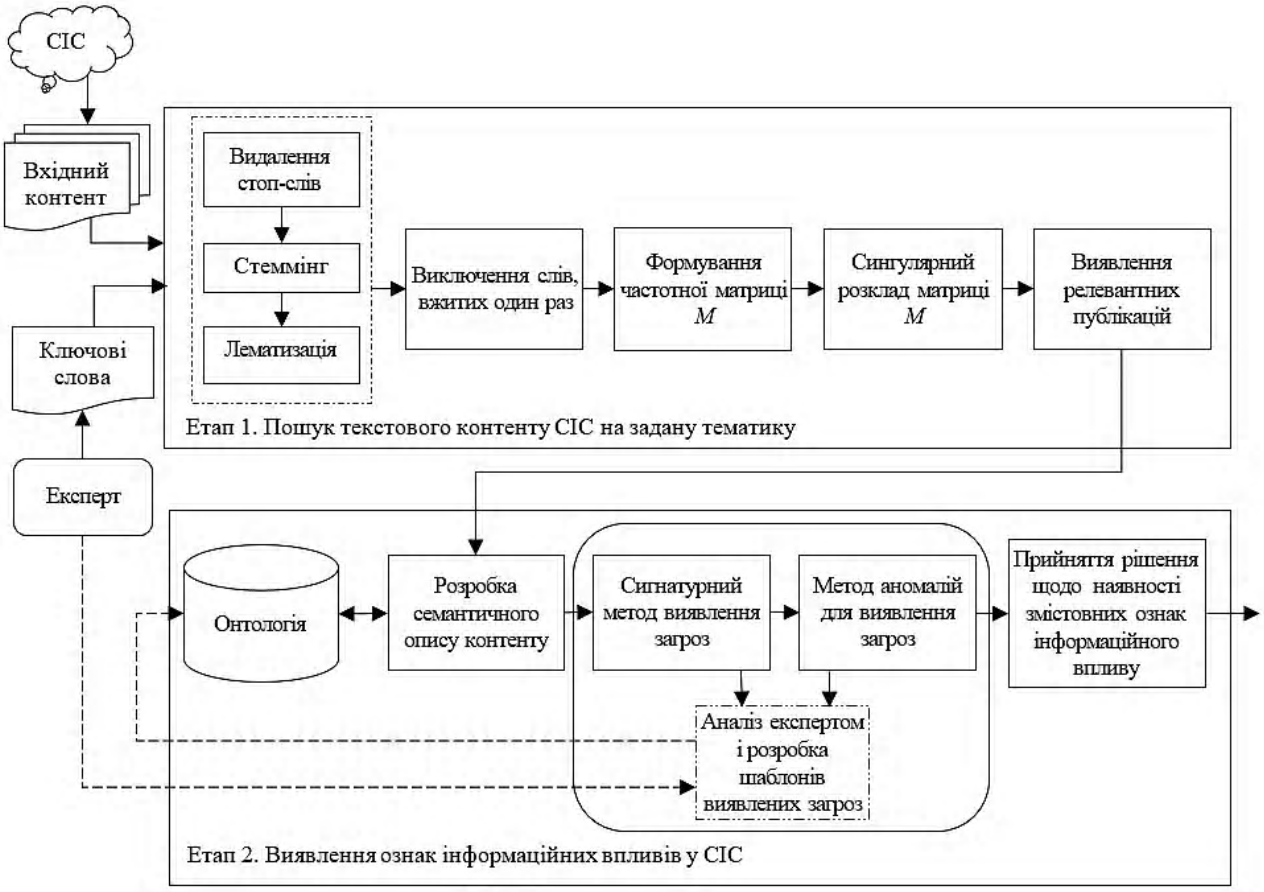


Рисунок 1 – Узагальнена структурна схема методу виявлення інформаційних впливів у СІС за змістовними ознаками

Таблиця 1 – Частотна матриця індексованих слів

| Ключові слова | Публікації | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | $D_1$ | $D_2$ | $D_3$ | $D_4$ | $D_5$ | $D_6$ | $D_7$ | $D_8$ | $D_9$ | $D_{10}$ |
| майдан | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 |
| бандити | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 0 |
| влада | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 |
| поліція | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 |
| корупція | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 |
| диктатура | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 |
| війна | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 |
| злидні | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| Порошенко | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 |
| олігархи | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |

U=

| | |
|---|---|
| -0,316 | -0,140 |
| -0,411 | -0,402 |
| -0,354 | 0,289 |
| -0,427 | 0,430 |
| -0,248 | -0,513 |
| -0,257 | 0,258 |
| -0,299 | -0,395 |
| -0,029 | 0,076 |
| -0,264 | 0,055 |
| -0,368 | 0,235 |

$S^T$=

| | |
|---|---|
| 4,957 | 0 |
| 0 | 2,723 |

$V^T$=

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| -0,367 | 0,297 | 0,253 | -0,336 | 0,035 | -0,302 | -0,440 | -0,398 | 0,004 | 0,395 |
| -0,343 | -0,375 | -0,002 | 0,231 | 0,570 | 0,274 | -0,322 | 0,320 | 0,041 | 0,283 |

Рисунок 2 – Результати розрахунків

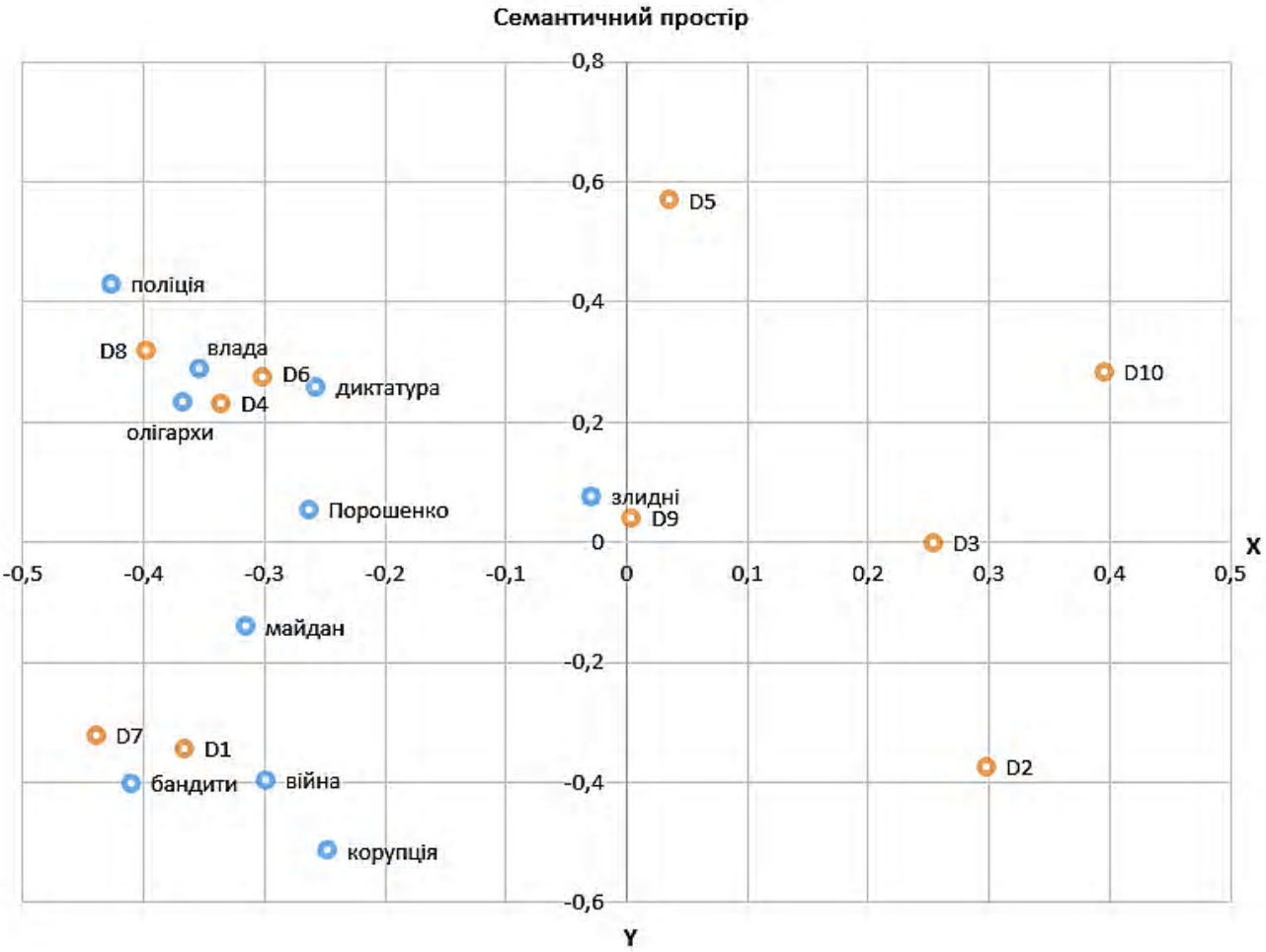


Рисунок 3 – Розподіл колекції публікацій в семантичному просторі

Документи $D_4$, $D_6$, $D_8$ утворюють неочевидний зв'язок з термінами, що пов'язані зі «встановленням диктатури олігархату Порошенка». Близькими для змісту документів $D_1$ і $D_7$ є терміни «бандити», «війна», «корупція» та «майдан», які їх об'єднують в окрему групу. Зміст документу $D_9$ найтісніше пов'язаний з низьким рівнем життя населення і не містить прихованих залежностей від інших слів семантичного ядра.

Отже, подальшому семантичному аналізу підлягають релевантні до семантичного ядра $W$ документи $D_1$, $D_4$, $D_6$, $D_7$, $D_8$. Таким чином зменшується загальна кількість документів для подальшого дослідження модулем моніторингу контенту системи забезпечення інформаційної безпеки в СІС, підвищуються ефективність і швидкодія її функціонування.

Розглянемо окремі етапи семантичного аналізу документу $D_6$, зміст якого наведений на рис. 4.

Фрагмент семантичного опису цього документа наведено на рис. 5.

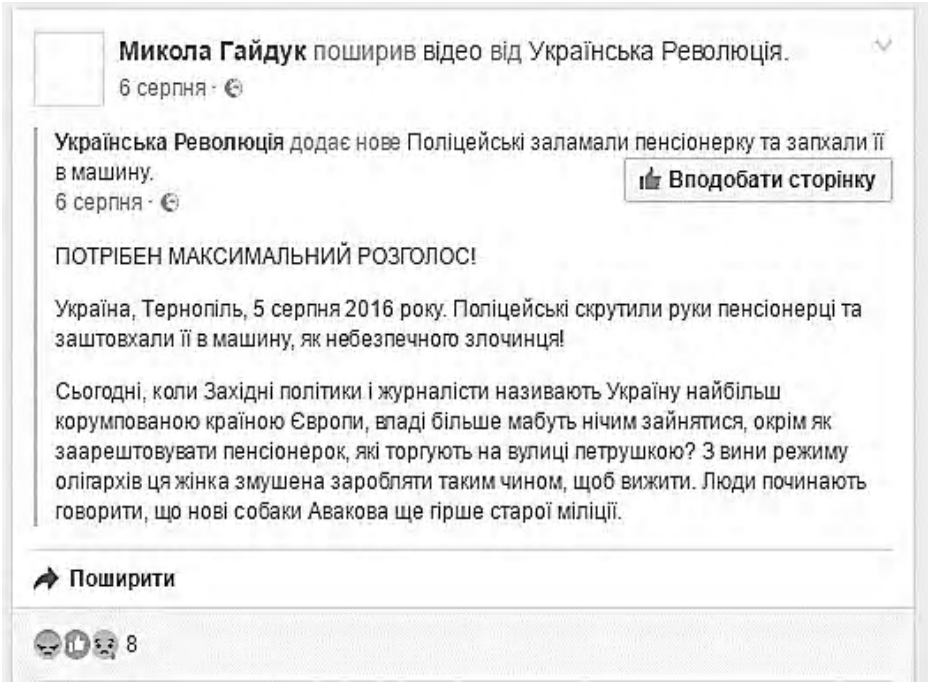


Рисунок 4 – Досліджуваний контент в CIC Facebook

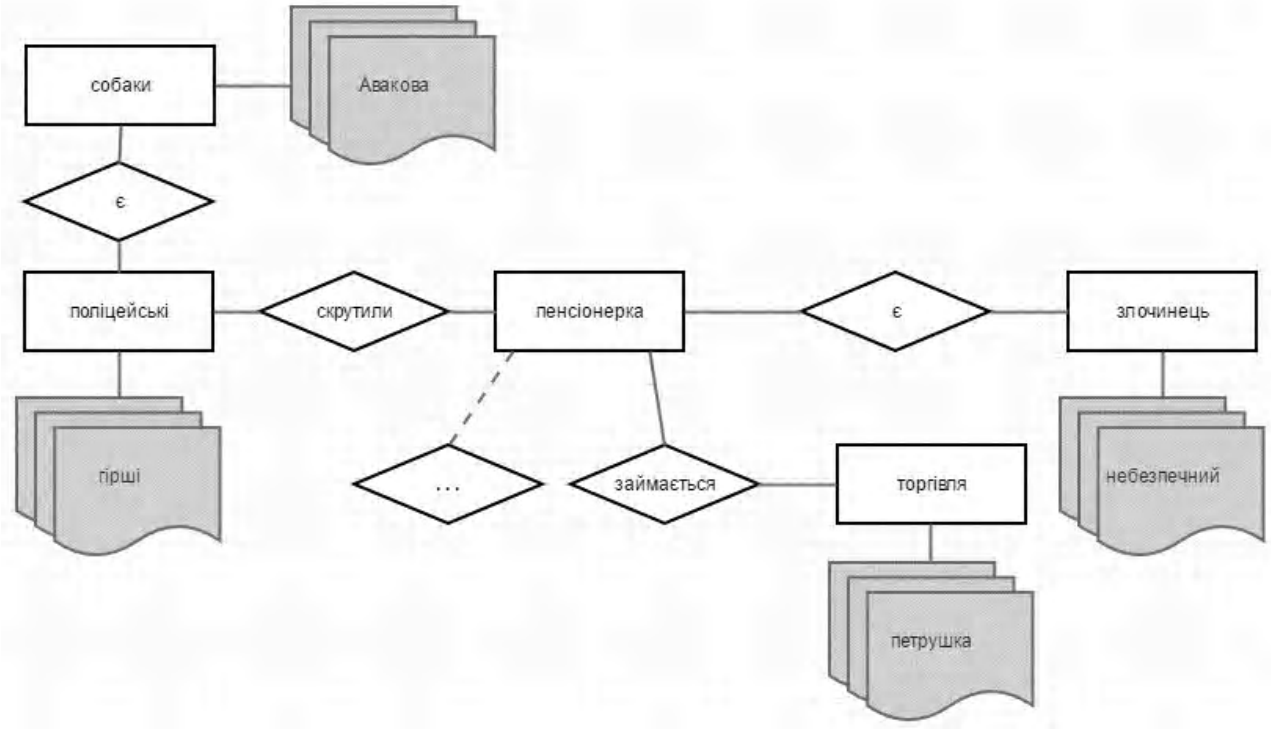


Рисунок 5 – Фрагмент семантичного опису документа $D_6$

Сигнатурне виявлення загроз в текстовому контенті CIC детектувало використання з концептом «пенсіонерка» відношення «скрутили», яке становить фізичну небезпеку для об'єкта. Відповідно до методу аномалій встановлено, що концепт «пенсіонерка» не може вживатися разом з відношенням «є» і концептом «злочинець» з атрибутом «небезпечний». Також в семантичному описі виявлено відношення «скрутили» між концептами «поліцейські» та «пенсіонерка», що не визначено онтологією. В досліджуваному документі вжито порівняння поліцейських з «собаками Авакова», яке необхідно додати до семантичних шаблонів загроз онтологічної бази знань.

## 6 ОБГОВОРЕННЯ

Розглянутий метод поєднує в собі сучасні підходи до обробки текстового контенту – семантичний і латентно-семантичний аналіз. Така комбінація підходів реалізує

взаємну компенсацію їх недоліків [18]: полісемії, омонімії та інших видів лінгвістичних неоднозначностей для LSI; виявлення латентних залежностей між концептами для семантичного аналізу.

Одержані результаті збіжні, наприклад, з дослідженнями аналітичного центру Тексти.org, яким встановлено взаємопов'язані віртуальні спільноти у Вконтакте і Facebook, актори яких закликали до перевороту й протестів в Україні [19]. У результаті розкрито адміністратора таких груп, який зареєстрований у СІС під іменем Микола Гайдук. Отже, дієвість використання запропонованого у статті методу виявлення ознак інформаційного впливу доведено.

## ВИСНОВКИ

Метод виявлення ознак інформаційного впливу у СІС за змістовними ознаками ґрунтується на сучасних підходах інтелектуальної обробки текстового контенту. Перевагою розглянутого методу є застосування LSI для пошуку текстового контенту віртуальних спільнот, який містить деструктивний інформаційний вплив в явному або прихованому вигляді. Завдяки додатковому використанню сигнатурного методу і методу аномалій для детектування відомих та нових загроз інформаційній безпеці досягається взаємна компенсація недоліків таких підходів. Таким чином, досягається підвищення ефективності й швидкодії системи забезпечення інформаційної безпеки держави в СІС, що є сьогодні вкрай актуальним завданням для України.

## ПОДЯКИ

Робота виконана на кафедрі комп'ютерних технологій і моделювання систем Житомирського національного агроекологічного університету в рамках госпдоговірної науково-дослідницької теми «Методологія побудови сучасних інформаційних технологій аналізу і відображення стану інформаційної та екологічної безпеки держави» ДР№ 0115U004181 за сприяння науково-дослідного відділу інформаційної та кібернетичної безпеки наукового центру Житомирського військового інституту ім. С. П. Корольова в особі начальника відділу – д.т.н., с.н.с. Р. В. Грищука. За результати наукових досліджень у напрямку розробки і впровадження новітньої методології побудови систем забезпечення інформаційної безпеки держави в соціальних інтернет-сервісах автора відзначено стипендією Кабінету Міністрів України для молодих учених.

## СПИСОК ЛІТЕРАТУРИ

1. Грищук Р. В. Основи кібернетичної безпеки : моногр. / Р. В. Грищук, Ю. Г. Даник ; за заг. ред. проф. Даника Ю. Г. – Житомир : ЖНАЕУ, 2016. – 636 с.
2. 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. – Київ, 2014. – 260 с.
3. Лапшин С. В. Методы повышения показателей качества фильтрации DLP-систем на основе предметно-ориентированной морфологической модели естественного языка : дисс. … канд. техн. наук : 05.13.19 / Лапшин Сергей Владимирович. – Санкт-Петербург, 2014. – 115 с.
4. Какие бывают типы контента и как с ними работать для реализации успешной стратегии контент-маркетинга / Alphaland.in Интернет Маркетинг [Электронный ресурс]. – Режим доступа: http://alphaland.in/kakie-by-vayut-tipy-kontenta-i-kak-s-nimi/ (дата обращения: 29.10.16). – Название с экрана.
5. Чернишук С. В. Методика виявлення кібернетичних загроз у природномовних текстах / С. В. Чернишук // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем. – 2013. – Вип. 8. – С. 112–121.
6. Грищук Р. В. Теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальних ігор та диференціальних перетворень: монографія / Р. В. Грищук. – Житомир : Рута, 2010. – 280 с.
7. Manning Chr. Introduction to Information Retrieval / Chr. Manning, P. Raghavan, H. Schütze. – Cambridge University Press, 2008. – 544 p.
8. Латентно-семантический анализ / Сайт Хабрхабр [Электронный ресурс]. – Режим доступа : https://habrahabr.ru/post/110078/ (дата обращения : 29.10.16). – Название с экрана.
9. Indexing by latent semantic analysis / [S. Deerwester, S. T. Dumais, G. W. Furnas et al], // Journal of the American Society for Information Science. – 1990. – 41(6). – P. 391–407. DOI: 10.1002/(sici)1097-4571(199009)41:6<391::aid-asi1>3.0.co;2-9.
10. Стеммер Портера для русского языка / О программировании, алгоритмах и не только [Электронный ресурс]. – Режим доступа: http://www.algorithmist.ru/2010/12/porter-stemmer-russian.html/ (дата обращения: 29.10.16). – Название с экрана.
11. Молодецька К. В. Узагальнена класифікація загроз інформаційній безпеці держави в соціальних інтернет-сервісах / К. В. Молодецька // Защита информации. – 2016. – Вып. 23. – С. 75–87.
12. Gruber T. R. A Translation Approach to Portable Ontology Specifications / T. R. Gruber // Knowledge Acquisition. – 1993. – 5(2). – P. 199–220. DOI: 10.1006/knac.1993.1008.
13. Bouiadjra A. B. A framework for evaluating and ranking ontologies / A. B. Bouiadjra, S. M. Benslimane // International Journal of Metadata, Semantics and Ontologies. – 2013. – 8(2). – P. 155. DOI: 10.1504/ijmso.2013.056600.
14. Vargas-Vera M. State of the art on Ontology alignment / M. Vargas-Vera, M. Nagy // International Journal of Knowledge Society Research. – 2015. – 6(1). – P. 17–42. DOI: 10.4018/ijksr.2015010102.
15. Priya M. A survey of state of the art of Ontology construction and merging using formal concept analysis / M. Priya, C. Aswani Kumar // Indian Journal of Science and Technology. – 2015. – 8(24). DOI: 10.17485/ijst/2015/v8i24/82808.
16. Василюк Я. Р. Аналіз моделей, методів, принципів і засобів для побудови онтологій області мікроелектромеханічних систем / Я. Р. Василюк, В. М. Теслюк, А. Я. Зелінський // Наук. вісн. Нац. лісотехн. ун-ту Укр. : зб. наук. -техн. пр. – 2011. – Вип. 21(12). – С. 322–330.
17. Wang W. Probabilistic topic models for learning Terminological Ontologies / W. Wang, P. M. Barnaghi, A. Bargiela // IEEE Transactions on Knowledge and Data Engineering. – 2010. – 22(7). – P. 1028–1040. DOI: 10.1109/tkde.2009.122.
18. Марченко О. О. Порівняння методів онтологічного семантичного аналізу та алгоритмів латентного семантичного аналізу / О. О. Марченко // Вісн. Київського нац. ун-ту ім. Т. Шевченка. Серія фізико-математичні науки. – 2012. – 2. – С. 169–174.
19. Тролесфера / Тексти.org.ua [Електронний ресурс]. – Режим доступу : http://texty.org.ua/d/fb-trolls/ (дата звернення: 29.10.16). – Назва з екрану.

Стаття надійшла до редакції 08.12.2016.
Після доробки 26.12.2016.

Молодецкая-Гринчук К. В.
Канд. техн. наук, доцент, доцент кафедры компьютерных технологий и моделирования систем Житомирского национального агроэкологического университета, Житомир, Украина

**МЕТОД ВЫЯВЛЕНИЯ ПРИЗНАКОВ ИНФОРМАЦИОННОГО ВОЗДЕЙСТВИЯ В СОЦИАЛЬНЫХ ИНТЕРНЕТ-СЕРВИСАХ ПО СОДЕРЖАТЕЛЬНЫМ ПРИЗНАКАМ**

**Актуальность.** Сегодня социальные интернет-сервисы превратились в эффективный инструмент коммуникации между участниками виртуальных сообществ – акторами. Учитывая высокую скорость распространения контента, трансграничность процессов взаимодействия актеров, наличие средств для их организации в группы, социальные-интернет сервисы могут применяться как действенное средство проведения информационных операций против человека, общества, государства. В процессах коммуникации акторов в виртуальных сообществах часто используется текстовый контент. Разработка эффективных алгоритмов функционирования системы обеспечения информационной безопасности государства для решения проблемы мониторинга текстового контента социальных интернет-сервисов является актуальной теоретико-прикладной задачей.

**Цель.** Целью исследований является обоснование и разработка метода выявления информационных воздействий в социальных интернет-сервисах по содержательным признакам для повышения эффективности системы обеспечения информационной безопасности государства.

**Метод.** Разработанный метод основывается на современных подходах к интеллектуальному анализу текстового контента – латентно-семантическом индексировании и семантическом анализе на базе онтологий.

**Результаты.** В результате латентно-семантического индексирования отбирается релевантный заданной тематике текстовый контент на основе его содержания и без учета плотности ключевых слов. На этапе семантического анализа реализовано процедуры последующего обнаружения опасных семантических конструкций в отобранном текстовом контенте. В случае детектирования противоречивых фрагментов текстового контента и онтологии и после их анализа экспертами выполняется наполнение онтологических баз знаний шаблонами угроз информационной безопасности в социальных интернет-сервисах. Таким образом, комбинация методов латентно-семантического индексирования и семантического анализа обеспечивает взаимную компенсацию их недостатков и выявления скрытых зависимостей между языковыми единицами.

**Выводы.** Благодаря разработанному методу выявления признаков информационных воздействий в социальных интернет-сервисах автоматизируются процедуры идентификации в виртуальных сообществах информационных операций, направленных против информационной безопасности человека, общества, государства. Применение предложенного метода выявления признаков информационных воздействий позволяет повысить эффективность и быстродействие системы обеспечения информационной безопасности государства в социальных интернет-сервисах как составляющей национальной безопасности Украины.

**Ключевые слова:** социальный интернет-сервис, информационная безопасность, угроза, текстовый контент, латентно-семантическая индексация, семантический анализ, онтология.

Molodetska-Hrynchuk K.
Candidate of Technical Sciences, Docent, Associate Professor at the Information Technologies and System Modelling sub-Department, Zhitomir National Agroecological University, Ukraine

**OUTREACHES CONTENT TRACING TECHNIQUE FOR SOCIAL NETWORKING SERVICES**

**Context.** Today's social networking services have turned into an efficient communication tool for the members of virtual communities termed actors. The high rate of content dissemination, transboundary interactions between the actors and the drives to group the latter up, could make the services efficient cyberwarfare against the person, society and country. Text content is the most frequently used means of communication between the actors of virtual communities. The actual theoretical and applied research, aimed at designing maintenance procedures for the national cybersecurity system, is to solve the problem of text content monitoring.

**Objective**. The research objective is to suggest and design a method for detecting outreaches by their content in the collection of text to solve the problem of efficient monitoring the social media.

**Method**. The method designed is based on the modern content analysis approaches, i. e. the latent semantic indexing and the semantic analysis based on ontology.

**Results.** The latent semantic indexing selects the concept relevant context by its content ignoring key word density. The semantic analysis will specify the further techniques of detecting harmful semantic structures in the body of text selected. When any conceptual mismatches in the text content and ontology detected and professionally analyzed, the ontology knowledge bases get updates of the social networking service cyberthreat patterns. Thus, the combination of both produces cancelling effect on the defects of and uncovers latent relationships between linguistic units.

**Conclusions.** The outreaches tracing method proactively identifies cyberwarfare in virtual communities waged against individual, social and national cybersecurity. The suggested method increases efficiency and effectiveness of the national cybersecurity system on social networking services.

**Keywords:** social networking services; cybersecurity; threats; text content; latent semantic indexing; semantic analysis; ontology.

## REFERENCES

1. Hryshchuk R. V., Danyk Yu. H. za zah. red. prof. Danyka Yu. H. Osnovy kibernetychnoi bezpeky : monohr. Zhytomyr, ZhNAEU, 2016, 636 p.
2. Onyshchenko O. S., Horovyi V. M., Popyk V. I. ta in. Sotsialni merezhi yak instrument vzaiemovplyvu vlady ta hromadianskoho suspilstva : [monohrafiia] ; NAN Ukrainy, Nats. b-ka Ukrainy im. V. I. Vernadskoho. Kyiv, 2014, 260 p.
3. Lapshin S. V. Metody povysheniya pokazatelej kachestva fil'tracii DLP-sistem na osnove predmetno-orientirovannoj morfologicheskoj modeli estestvennogo yazyka : diss. … kand. texn. nauk : 05.13.19. Sankt-Peterburg, 2014, 115 p.
4. Kakie byvayut tipy kontenta i kak s nimi rabotat' dlya realizacii uspeshnoj strategii kontent-marketinga / Alphaland. in Internet Marketing [E'lektronnyj resurs]. Rezhim dostupa: http://

alphaland.in/kakie-by-vayut-tipy-kontenta-i-kak-s-nimi/ (data obrashheniya: 29.10.16). Nazvanie s e'krana.
5. Chernyshuk S. V. Metodyka vyiavlennia kibernetychnykh zahroz u pryrodnomovnykh tekstakh, *Problemy stvorennia, vyprobuvannia, zastosuvannia ta ekspluatatsii skladnykh informatsiinykh system*, 2013, Vyp. 8, pp. 112–121.
6. Hryshchuk R. V. Teoretychni osnovy modeliuvannia protsesiv napadu na informatsiiu metodamy teorii dyferentsialnykh ihor ta dyferentsialnykh peretvoren: monohrafiia. Zhytomyr, Ruta, 2010, 280 p.
7. Manning Chr., Raghavan P., Schütze H. Introduction to Information Retrieval. Cambridge University Press, 2008, 544 p.
8. Sajt Xabrxabr Latentno-semanticheskij analiz. [E'lektronnyj resurs]. Rezhim dostupa : https://habrahabr.ru/post/110078/ (data obrashheniya : 29.10.16). Nazvanie s e'krana.
9. Deerwester S., Dumais S. T., Furnas G. W., Landauer T. K., Harshman R. Indexing by latent semantic analysis, *Journal of the American Society for Information Science*, 1990, 41(6), pp. 391–407. DOI: 10.1002/(sici)1097-4571(199009)41:6<391::aid-asi1>3.0.co;2-9.
10. Stemmer Portera dlya russkogo yazyka / O programmirovanii, algoritmax i ne tol'ko [E'lektronnyj resurs]. Rezhim dostupa: http://www.algorithmist.ru/2010/12/porter-stemmer-russian.html/ (data obrashheniya: 29.10.16). Nazvanie s e'krana.
11. Molodetska K. V. Uzahalnena klasyfikatsiia zahroz informatsiinii bezpetsi derzhavy v sotsialnykh internet-servisakh, *Zashhita informacii*, 2016, Vyp. 23, pp. 75–87.
12. Gruber T. R. A Translation Approach to Portable Ontology Specifications, *Knowledge Acquisition*, 1993, 5(2), pp. 199–220. DOI: 10.1006/knac.1993.1008.
13. Bouiadjra A. B., Benslimane S. M. A framework for evaluating and ranking ontologies, *International Journal of Metadata, Semantics and Ontologies,* 2013, 8(2), pp. 155. DOI: 10.1504/ijmso.2013.056600.
14. Vargas-Vera M., Nagy M. State of the art on Ontology alignment, *International Journal of Knowledge Society Research,* 2015, 6(1), pp. 17–42. DOI: 10.4018/ijksr.2015010102.
15. Priya M., Aswani Kumar C. A survey of state of the art of Ontology construction and merging using formal concept analysis, *Indian Journal of Science and Technology*, 2015, 8(24). DOI: 10.17485/ijst/2015/v8i24/82808.
16. Vasyliuk Ya. R., Tesliuk V. M., Zelinskyi A. Ya. Analiz modelei, metodiv, pryntsypiv i zasobiv dlia pobudovy ontolohii oblasti mikroelektromekhanichnykh system, Nauk. visn. Nats. lisotekhn. un-tu Ukr. : zb. nauk.-tekhn. pr., 2011, Vyp. 21(12), pp. 322–330.
17. Wang W., Barnaghi P. M., Bargiela A. Probabilistic topic models for learning Terminological Ontologies, *IEEE Transactions on Knowledge and Data Engineering,* 2010, 22(7), pp. 1028–1040. DOI: 10.1109/tkde.2009.122.
18. Marchenko O. O. Porivniannia metodiv ontolohichnoho semantychnoho analizu ta alhorytmiv latentnoho semantychnoho analizu, *Visn. Kyivskoho nats. un-tu im. T. Shevchenka. Seriia fizyko-matematychni nauky*, 2012, 2, pp. 169–174.
19. Trolesfera Teksty.org.ua [Elektronnyi resurs]. Rezhym dostupu : http://texty.org.ua/d/fb-trolls/ (data zvernennia: 29.10.16). Nazva z ekranu.