

DOI 10.31891/2307-5732-2022-313-5-294-300
УДК 004.056:621.397.3:004.942

ДЖУЛІЙ Володимир

Хмельницький національний університет
ORCID <http://orcid.org/0000-0003-1878-4301>
e-mail: dg2303@ukr.net

ПЕТЛЯК Наталія

Хмельницький національний університет
ORCID <http://orcid.org/0000-0001-5971-4428>
e-mail: npetlyak@khmnu.edu.ua

ХМЕЛЬНИЦЬКИЙ Юрій

Хмельницький національний університет
ORCID <http://orcid.org/0000-0002-4005-5669>
e-mail: getman-58@ukr.net,

ПАХАР Олександр

Хмельницький національний університет
e-mail: dg2303@ukr.net

МОДЕЛЬ ПОТОКУ ТЕКСТОВИХ ПОВІДОМЛЕНЬ ТЕМАТИЧНИХ ІНТЕРНЕТ-РЕСУРСІВ СИСТЕМИ ПРОГНОЗУВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Розглянута актуальна задача побудови моделі потоку текстових повідомлень тематичних інтернет-ресурсів системи прогнозування інформаційної безпеки та інформаційної моделі бази даних форуму тематичного інтернет-ресурсу, відрізняється від відомих, універсальністю, дозволяє аналізувати та досліджувати потік даних інтернет-форумів, реалізованих на базі популярних програмних платформ для розробки дискусійних інформаційних тематичних ресурсів. Представлена модель потоку текстових повідомлень тематичних інтернет форумів, відрізняється від відомих, можливістю проводити статистичний аналіз та семантичну фільтрацію повідомлень, враховуючи належність до автора, рейтингу автора, форуму, часу створення, кількості повідомлень, темі форуму, дозволяє здійснювати аналіз та дослідження текстових повідомлень тематичних інтернет-ресурсів.

Ключові слова: моделі, алгоритми, модель потоку повідомлень, тематичні форуми, джерела повідомлень.

DZHULIY Volodymyr, PETLIAK Natalia,
KHMELNYTSKYI Yuri, PAKHAR Oleksandr
Khmelnytsky National University

TEXT MESSAGE FLOW MODEL OF THEMATIC INTERNET RESOURCES INFORMATION SECURITY FORECASTING SYSTEMS

The tasks of analysis and classification of detection of existing mechanisms for the implementation of attacks and threats to information security, which can lead to unauthorized access to confidential information, disruption of the functioning of information systems, are relevant and prioritized at the current stage. The importance of the problems is connected with the following main factors: growth of variety and quantity of means of computer technology and spheres of human activity; a high level of trust in information and search systems for data processing and management; the growth of the number of users of the information space of interaction; accumulation of large volumes of various types of information, intensive exchange of data flow in the network between users, using a wide range of access mechanisms to confidential resources, information processes; industrial espionage and competitive struggle in the sphere of information services of society; insufficient number at the present stage of highly qualified specialists in the field of information security, market relations in the field of software development, maintenance, distribution, production of computing equipment for the implementation of information security.

The presented model of the flow of text messages of thematic Internet resources of the information security forecasting system and the information model of the forum database of the thematic Internet resource, which differs from the known ones in its universality, allows to analyze and study the data flow of Internet forums implemented on the basis of popular software platforms for the development of discussion information thematic resources. The model of the flow of text messages of thematic Internet forums allows statistical analysis and semantic filtering of messages, taking into account authorship, author rating, forum, time of creation, number of messages, forum topic, allows analysis and research of text messages of thematic Internet resources.

Solving the set tasks will allow: to improve the quality of decisions made in the process of identifying and counteracting malicious information; sort information objects of influence for the operator by priority; set the input data settings of the system of detection and countermeasures against the spread of malicious information in networks.

Keywords: models, algorithms, message flow model, thematic forums, message sources.

Постановка проблеми у загальному вигляді

та її зв'язок із важливими науковими чи практичними завданнями

На сучасному етапі, на більшість сфер діяльності суспільства зростає вплив глобальних інформаційних технологій. Відзначаються високі темпи розвитку світових єдиних телекомунікаційного та інформаційного просторів, сформувалися в суспільстві нові соціальні групи, виявляється значний вплив на сформований історично спосіб життя людей. На тлі стрімкого розвитку інформаційних технологій відзначається, зростання активності різноманітності комп'ютерних атак, здійснюваних і запланованих із застосуванням сучасних новітніх технологій [1].

Актуальними та пріоритетними на сучасному етапі є задачі класифікації та аналізу виявлення існуючих механізмів реалізації атак та загроз інформаційної безпеки, які можуть призвести до отримання несанкціонованого доступу до конфіденційної інформації, порушення функціонування інформаційних систем. В результаті, постає задача визначення заходів протидії атакам та загрозам, усунення вразливостей, оцінки заданої шкоди, розробка нормативно-правової бази, механізмів захисту та критеріїв безпеки [2 - 4].

Важливість проблем пов'язана з наступними основними факторами: зростанням різноманітності та кількості засобів комп'ютерної техніки та сфер людської діяльності їх застосування; високим рівнем довіри до інформаційно-пошукових систем обробки та управління даними; зростанням числа користувачів інформаційного простору взаємодії; накопиченням великих об'ємів різнотипної інформації, інтенсивним обміном потоком даних в мережі між користувачами, з використанням широкого спектра механізмів доступу до конфіденційних ресурсів, інформаційних процесів; промисловим шпигунством та конкурентною боротьбою у сфері інформаційних послуг суспільства; недостатньою кількістю, на сучасному етапі, фахівців високої кваліфікації в області інформаційної безпеки, ринковими відношеннями в області розробки програмного забезпечення, обслуговування, розповсюдження, виробництва обчислювальної комп'ютерної техніки для реалізації інформаційної безпеки [5,6].

Постановка задачі

На сучасному етапі, проблеми інформаційної безпеки розвитку суспільства у більшості сфер їх діяльності виходять на передній план. Це пов'язано зі значним зростанням кількості реалізованих проєктів інформатизації. Більшість проєктів інформатизації спрямовані на побудову єдиного телекомунікаційного та інформаційного простору з метою оптимізації процесів обробки різнотипної інформації великих об'ємів, забезпечення оперативного доступу до інформації, надійного зберігання даних для користувачів інформаційного обміну. На даному етапі виникає потреба у проведенні захисту комп'ютерних систем та інформаційних ресурсів від блокування, несанкціонованого доступу до даних, знищення, та інших злочинних, небажаних дій, кількість яких постійно зростає, збитки в інформаційній сфері від злочинів в мережі Інтернет щорічно оцінюються в мільярди доларів [7 - 9].

Темпи розвитку інформаційних та комп'ютерних технологій значно випереджають процес створення програмно-апаратного забезпечення в області інформаційної безпеки. Пріоритетними, в даній ситуації, є задачі проведення аналізу, класифікації, виявлення діючих механізмів та засобів проведення атак і загроз інформаційній безпеці системи, які можуть призвести до отримання несанкціонованого доступу до конфіденційних даних, порушення функціонування інформаційної системи, визначення заходів протидії атакам та загрозам, оцінка заданої шкоди, розробка нормативно-правової бази, механізмів захисту та критеріїв інформаційної безпеки системи протидії.

На сьогодні не існує єдиного підходу до вирішення проблеми захищеності інформаційних систем, стосовно предметних областей, розробниками програмного захисту інформації пропонуються відповідні компоненти на вирішення конкретних задач, забезпечення надійного захисту інформаційних ресурсів потребує реалізації відповідних організаційних та технічних заходів в комплексі, що супроводжуються розробкою відповідної документації [1,2]. Проведене дослідження вказує на необхідність вирішення наступних задач для забезпечення інформаційної безпеки: формування основ для опису процесів виникнення та реалізації загроз інформаційної безпеки системи в умовах невизначеності та непередбачуваності їх прояву; розробка відповідних засобів забезпечення захисту конфіденційної інформації на основі проведеного дослідження та класифікації вразливостей та загроз; визначення загальних підходів до створення інформаційно-аналітичних систем забезпечення захисту конфіденційних даних, механізмів управління захистом на різних рівнях діяльності суспільства [2 - 4].

Вирішення поставлених задач дозволить: підвищити якість прийнятих рішень у процесі виявлення та протидії шкідливій інформації; сортувати інформаційні об'єкти впливу для оператора по пріоритету; задати вхідні дані налаштування системи виявлення та протидії поширенню шкідливої інформації в мережах.

Основна частина

При створенні форумів інтернет-ресурсів найбільшою популярністю користуються наступні програмні платформи: Vanilla, Invision Power Board, vBulletin, PunBB, Simple Machines Forum, XenForo. При реалізації програмних платформ, використовуються бази даних структури, яких значно різняться. Записи даних дозволяють для текстових повідомлень визначати їхню приналежність до конкретного інтернет - форуму, автора, рейтингу автора, часу створення, а також кількості повідомлень відповідної теми форуму. Враховуючи наведену інформацію, запропоновано модель інтернет-форума (рис. 1).

Модель тематичного інтернет-ресурсу відрізняється від існуючих, універсальністю, що надає можливість проводити аналіз та досліджувати повідомлення інтернет-форумів, реалізованих на базі найбільш популярних програмних платформ для створення дискусійних тематичних інформаційних форумів. Застосування на практиці моделі інтернет-форуму, при прогнозуванні вразливостей та загроз інформаційної безпеки, надасть можливість проводити аналіз більшості існуючих тематичних інтернет-форумів, незалежно від задіяної програмної платформи, використовуваної для реалізації форуму [1,2,7].

Текстові повідомлення інтернет мережі є окремою структурою, що складається з пов'язаних між собою елементів (рис. 2). Потік даних в інтернет- мережі є множина текстових повідомлень тематичних інтернет-форумів, створюваних учасниками форуму. Враховуючи те, що моделювання мережевого потоку повідомлень тематичних інтернет-форумів здійснюється з метою наступного прогнозування вразливостей та загроз інформаційної безпеки, при побудові моделі тематичного інтернет- форуму, необхідно передбачити можливість здійснення семантичного та статистичного аналізу текстових повідомлень, враховуючи належність даних до конкретного форуму, кількості повідомлень теми форуму, автора, часу створення, рейтингу автора.

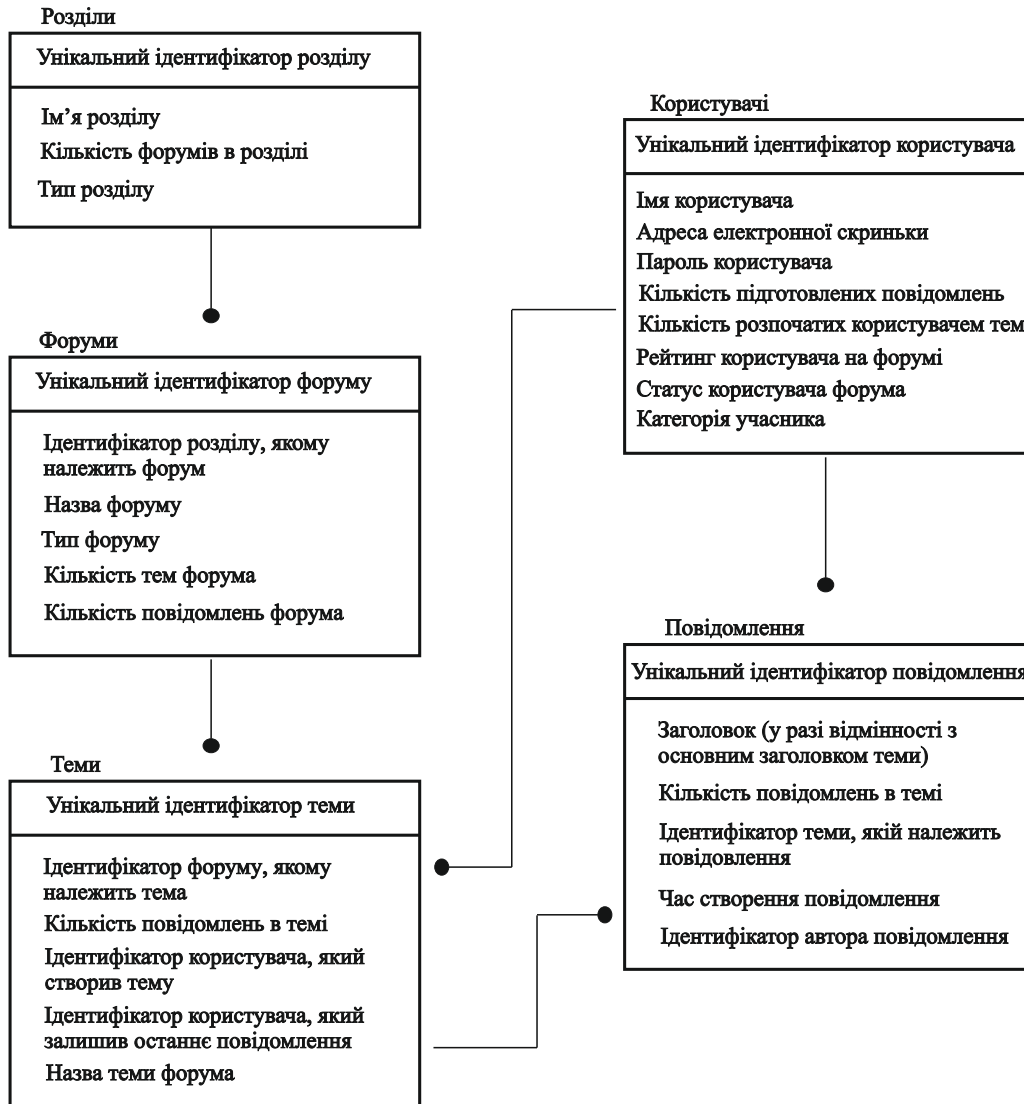


Рис. 1. Логічна модель бази даних тематичних інтернет-ресурсів

Онтологія є найбільш ефективним інструментом для опису конкретної предметної області. Суть онтологічного підходу полягає у представленні предметної області у вигляді організованої множини понять, враховуючи існуючі зв'язки між ними та їх властивості [3, 10]. Модель потоку текстових повідомлень, у загальному вигляді, яка має відношення до предметної області, заданої онтологією, представляється трійкою (1):

$$S_{\tau} = (M, O, T), \tag{1}$$

де S_{τ} – потік текстових повідомлень інтернет мережі у поточний час τ ; M - множина інтернет повідомлень у потоці даних; O - онтологія даної предметної області; $T = \{1, \dots, \tau\}$ - множина часових інтервалів, в які велися спостереження за інтернет потоком повідомлень (годин, днів, місяців).

$$O = (E, R, F), \tag{2}$$

де E - множина термінів заданої предметної області; R - множина взаємозв'язків між термінами даної предметної області; F - множина заданих на відношеннях та термінах онтології функцій

аксіоматизації (інтерпретації). Кожне текстове повідомлення $d \in M$ може бути представлене наступним чином:

$$d \in (s, t, F_d, A), \quad (3)$$

де S - текст інтернет повідомлення, $t = \{1, \dots, \tau\}$ - момент часу створення текстового повідомлення; $F_d = \{w_1, \dots, w_k\}$ - вектор, що представляє текстове повідомлення заданої предметної області, заданою відповідною онтологією O , k - кількість в онтології термінів, координати $w_i (i=1, \dots, k)$ - ваги термінів у текстовому повідомленні, A - рейтинг автора текстового повідомлення.

При розрахунку ваги термінів використовується модель TF-IDF (Term frequency - Inverse document frequency) [10], відповідно до якої вага терміна текстового повідомлення прямо пропорційна частоті входження терміна в інтернет повідомлення і обернено пропорційна кількості текстових повідомлень, у яких зустрічається термін (4):

$$w_i = F_i \cdot \log \left(\frac{D}{DF_i} \right), \quad (4)$$

де w_i - вага i - терміна у текстовому повідомленні; F_i - частота i - терміна у інтернет повідомленні; D - загальна кількість текстових повідомлень; DF_i - кількість текстових повідомлень, у яких зустрічається i - термін.



Рис. 2. Структура повідомлення тематичного інтернет-форуму

Розглянута модель не враховує того, що текстові повідомлення тематичних форумів можуть мати різний розмір, у зв'язку з чим, вага терміна і відповідно частота будуть зменшуватися зі зростанням розміру текстових повідомлень. Враховуючи дану ситуацію необхідно проводити нормування ваг термінів у інтернет повідомленні, діленням їх на довжину вектора-повідомлення (еклідову норму) (5):

$$w_i^* = \frac{w_i}{d} = \frac{w_i}{\sqrt{\sum_{i=1}^k w_i}}, \quad (5)$$

При використанні онтологічних методів для опису та обробки предметної області, необхідно представити її у вигляді організованої структури сукупності термінів (понять), враховуючи існуючі властивості та зв'язки між ними. У задачах, що передбачають подальшу обробку, предметної області, розроблених онтологій, найчастіше застосовується для їх представлення формат OWL (Ontology Web Language) - мова опису онтологій для семантичного павутиння. У термінознавстві та лексикографії застосовуються алгоритми, що ґрунтуються на статистичних та лінгвістичних методах, для видалення термінів [10].

При використанні статистичних методів основним критерієм є ступінь термінологічності, визначається у відповідності до числових закономірностей, характерними для термінів і нетермінів. При використанні лінгвістичних методів терміни відбираються за лінгвістичними ознаками та певними граматичними лексичними шаблонами [6,10].

При використанні онтологічного підходу знання про відповідні предметні області (онтологія) зберігаються у вигляді (6):

$$O = (E, R, F), \quad (6)$$

де E - множина термінів заданої предметної області; R - множина взаємозв'язків між термінами даної предметної області (7):

$$R \subset \{R_{inc}, R_{add}, R_{term}, R_{lem}, R_{NC}\}, \quad (7)$$

де R_{inc} – множина вбудованих відношень між об'єктами («є Підкласом»); R_{add} – множина вбудованих відношень між об'єктами, дозволяють розширювати набір відповідних об'єктів предметної області, для якої проводиться аналіз, шляхом об'єднання лем області, пов'язаних між собою об'єктів («має Відношення», «є Частиною»); R_{term} – відношення «є Терміном», визначається експертним шляхом і носить допоміжний характер, приймає логічний тип значення (в залежності від того, наскільки об'єкт характерний для предметної області). Прикладне застосування R_{term} знаходить при вирішенні задач видалення, з використанням тезаурусного критерію термінологічності термінів; R_{lem} – відношення «має Лемму», дана властивість приймає значення рядкового типу, яке виходить в результаті лемування, приведенні найменування об'єкта до початкової форми; R_{NC} – множина відношень між тематичними об'єктами, описують особливості взаємодії між собою об'єктів даної предметної області (властивості «є Елементом», «є Типом вірусів»); F – множина заданих на термінах та відношеннях онтології предметної області функцій аксіоматизації (інтерпретації).

Задача фільтрації текстових повідомлень, які не належать до предметної області, для якої проводиться аналіз, може бути вирішена із використанням семантичної метрики «термін/не термін». Для використання семантичної метрики необхідно попередньо розробити відповідну онтологію предметної області у форматі OWL. Далі для кожного тематичного повідомлення, що надходять в інтернет мережі, розраховується значення ступеня близькості термінів включених до онтології, в результаті виділяються тематичні повідомлення, що виключно відносяться до даної предметної області [7 – 9].

Значення коефіцієнта ступеня близькості текстового повідомлення до всіх термінів предметної області, який розраховується при використанні семантичної метрики «термін/ не термін», приймає значення в діапазоні від 0 до 1 (текстове повідомлення відноситься до певного терміну, чим ближче значення коефіцієнта k_{Ont} до 1). Для вирішення задач відбору текстових повідомлень, до даної предметної області, заданої у вигляді онтології, використовуються два критерії: вкладених зв'язків та тезаурусний критерій. Застосування тезаурусного підходу до вирішення задачі фільтрації текстових повідомлень полягає в пошуку лем, що містяться в тематичних повідомленнях, надходять в інтернет мережі, серед термінів онтології даної предметної області. Використання тезаурусного підходу для відповідного класу онтології предметної області визначає властивість «має Лемму», шляхом приведення до початкової форми (лемування) найменування об'єкта області, що аналізується.

Для розрахунку коефіцієнта ступеня близькості тематичних повідомлень до термінів даної предметної області відповідно до тезаурусного критерію, необхідно виконати послідовність дій: провести оцінку коефіцієнта ступеня близькості текстового повідомлення до кожного об'єкта онтології, для якої проводиться аналіз; визначити опорний об'єкт заданої онтології, який найбільш близько асоціюється з тематичним повідомленням, що надходить в інтернет мережі.

Розрахунок коефіцієнта ступеня близькості текстового повідомлення термінам заданої предметної області з використанням тезаурусного критерію представлено на рис. 3.

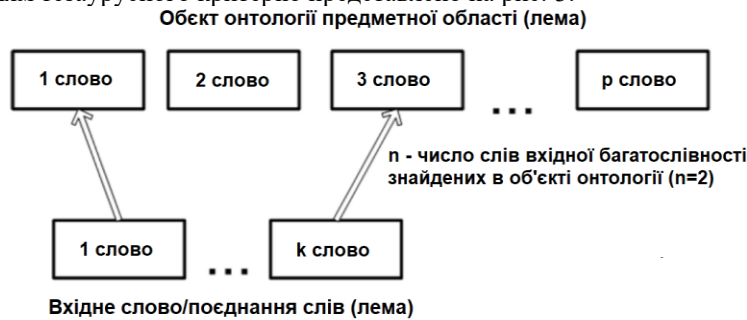


Рис. 3. Визначення опорного об'єкта онтології

Коефіцієнт ступеня близькості опорного об'єкта онтології до тематичного повідомлення, що надходить в інтернет мережі розраховується наступним чином (8):

$$k_t = \max \left(\frac{n_i}{p_i} \right)_{i=1}^m, \quad (8)$$

де m – загальна кількість об'єктів заданої онтології; n_i – кількість слів у лемі тематичного повідомлення, присутніх у лемі i -го об'єкта заданої онтології предметної області; p_i – кількість слів у лемі i -го об'єкта онтології предметної області.

У випадку коли значення коефіцієнта k_t отримано однакове для декількох об'єктів онтології заданої

предметної області, опорним приймається об'єкт онтології, для якого значення n_i набуває максимальної величини. Якщо, при цьому, існує декілька об'єктів онтології, для яких значення n_i і k_t однакові, то в даній ситуації всі об'єкти вважаються опорними і для кожного об'єкта проводиться аналіз по онтологічному критерію.

Відповідно до тезаурусного критерію коефіцієнт ступеня близькості тематичного повідомлення термінам даної предметної області розраховується за наступним чином (9):

$$k_{Ont} = \frac{k_t}{c+1}, \quad (9)$$

де k_t - коефіцієнт ступеня близькості, розрахований на першому етапі проведення аналізу (обчислюється за (8)); c - число відношень між об'єктами, які пов'язують опорний об'єкт онтології предметної області з об'єктами, що мають значення властивості «є Терміном». Якщо опорний об'єкт онтології предметної області є терміном, то $c=0$. Тезаурусний критерій схематично представлений на рис. 4.

Застосування метрики "термін / не термін" для коефіцієнта оцінки ступеня близькості тематичних повідомлень до термінів заданої предметної області передбачається рух графом, при цьому об'єкти класів онтології предметної області є вузлами графа. Якщо у опорного об'єкта онтології предметної області властивість «є Терміном» хибно, і він при цьому не пов'язаний з іншими об'єктами, або у всіх пов'язаних з ним об'єктів онтології значення властивості «є Терміном» хибно, то в даному випадку проводиться пошук інших опорних об'єктів онтології і знову ж таки проводиться оцінка. При цьому тематичне повідомлення не відноситься до предметної області ($k_{Ont} = 0$), коли опорні об'єкти онтології відсутні або для всіх опорних об'єктів предметної області характерна розглянута ситуація.

Критерій вкладених зв'язків онтології ґрунтується на тому, що крім оцінки коефіцієнта ступеня термінологічності кожного текстового повідомлення, метрика «термін/не термін» дозволяє проводити фільтрацію тематичних повідомлень шляхом зіставлення лема повідомлення та поєднаннями лем об'єктів онтології предметної області, пов'язаних відношеннями.



Рис. 4. Схема тезаурусного критерію

Таким чином, тематичне повідомлення вважається таким, що відноситься до заданої предметної області, якщо його лема співпадає з об'єднанням лем об'єктів даної онтології, пов'язаних між собою, при цьому односпрямованими відношеннями.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі

Запропонована інформаційна модель бази даних форуму тематичного інтернет-ресурсу, відрізняється від відомих, універсальністю, дозволяє аналізувати та досліджувати потік даних інтернет-форумів, реалізованих на базі популярних програмних платформ для розробки дискусійних інформаційних тематичних ресурсів.

Запропонована модель потоку текстових повідомлень тематичних інтернет форумів, які відносяться до заданої предметної області, даної онтології, відрізняється від відомих, можливістю проводити статистичний аналіз та семантичну фільтрацію повідомлень, враховуючи належність до автора, рейтингу автора, форуму, часу створення, кількості повідомлень, темі форуму, дозволяє здійснювати аналіз та дослідження текстових повідомлень тематичних інтернет-ресурсів. Особливість запропонованого підходу пов'язана з тим, що об'єкти онтології необхідно представляти переважно однослів'ями, що мають, в даному

випадку максимальну кількість відношень із іншими об'єктами онтології. Для практичного використання методу визначальними є відношення, що дозволяють формувати природним чином словосполучення.

Література

1. Ленков, С.В. Модель безпеки поширення забороненої інформації в інформаційно-телекомунікаційних мережах / С.В. Ленков, В.М. Джулій, В.С. Орленко, О.В. Селюков, А.В. Атаманюк // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2020. – Вип. №68. – С. 53-64.
2. Джулій В.М. Інформаційно-ознакова модель джерела шкідливої інформації в соціальних мережах/ В.М. Джулій І.В. Муляр О.О Зацепіна В. М. Пічуря – Вимірювальна та обчислювальна техніка в технологічних процесах № 3 (2022)- 73 – 78
3. Ленков, С.В. Методы и средства защиты информации. В 2-х томах /С.В. Ленков, Д.А. Перегудов, В.А. Хорошко –К: Арий, 2008.–464с
4. Остапов С. Е. Технології захисту інформації: навчальний посібник / С.Е. Остапов, С.П. Євсєєв, О.Г. Король–Харків : Вид-во ХНЕУ, 2016. – 476 с.
5. Ленков, С.В. Аналіз існуючих методів та алгоритмів виявлення атак в бездротових мережах передачі даних / С.В. Ленков, В.М. Джулій, Н.М. Берназ, С.О. Божук // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2017. – Вип. № 56. – С.124-132
6. Довгий, С.О. Сучасні телекомунікації: мережі, технології, економіка, управління, регулювання / С.О. Довгий, О.Я. Савченко, П.П. Воробієнко – К.: Український Видатничий Центр, 2012. – 520 с.
7. Джулій, В.М. Модель оцінки ймовірно-часових характеристик інформаційної взаємодії в мережі інтернет речей / В.М. Джулій, І.В. Муляр, О.В. Селюков, Б.М. Кізіон // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2019. – Вип. № 63. – С.96-106
8. Джулій, В.М., Кльоц Ю.П., Муляр І.В., Жилевич М.Л., Джулій А.В. Контроль додатків інтернет-трафіка комп'ютерних мереж методами машинного навчання. Вісник Хмельницького національного університету. Технічні науки. 2021. № 5. С. 22-26.
9. Джулій, В.М. Метод класифікації додатків трафіка комп'ютерних мереж на основі машинного навчання в умовах невизначеності / В.М. Джулій, О.В. Мірошніченко, Л.В. Солодєєва // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2022. – Вип. №74. – С. 73-82.
10. Лавров, Є. А. Математичні методи дослідження операцій: підручник / Є. А. Лавров, Л. П. Перхун, В. В. Шендрік – Суми : Сумський державний університет, 2017. – 212 с.

References

1. Lenkov, S.V. (2020), Model bezpeky poshyrennia zaboronenoї informatsii v informatsiino-telekomunikatsiinykh merezhakh / S.V. Lenkov, V.M. Dzhulii, V.S. ORLENKO, O.V. Sieliukov, A.V. Atamaniuk // Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. – K.: VIKNU. – №68. – pp. 53-64.
2. Dzhulii V.M. Informatsiino-oznakova model dzherala shkidlyvoi informatsii v sotsialnykh merezhakh/ V.M. Dzhulii I.V. Muliar O.O Zatssepina V. M. Pichura – Yymi-riuvanna ta obchysliuvanna tekhnika v tekhnolohichnykh protsesakh № 3 (2022)- 73 – 78
3. Lenkov, S.V. (2008), Metodyy sredstva zashchity ynformatsyy. V 2-kh tomakh / S.V. Lenkov, D.A. Perehudov, V.A. Khoroshko – K: Aryi–464s.
4. Ostapov, S. E. (2016) Tekhnolohii zakhystu informatsii: navchalnyi posibnyk / S.E. Ostapov, S.P. Yevseiev, O.H. Korol–Kharkiv : Vyd-vo KhNEU. – 476 s.
5. Lenkov, S.V. (2017), Anallz Isnyuyuchih metodiv ta algoritmiv viyavlennya atak v bezdrotovih merezhah peredachI danih / S.V. Lenkov, V.M. Dzhuliy, N.M. Bernaz, S.O. Bozhuk // Zbirnyk naukovih prats Viiskovoho Institutu Kiyivskogo natsionalnoho universytetu imeni Tarasa Shevchenka. – K.: VIKNU. – Vip. No 56. – p.124-132
6. Dovhyi, S.O. (2012), Suchasni telekomunikatsii: merezhi, tekhnolohii, ekonomika, upravlinnia, rehuliuвання /S.O. Dovhyi, O.I. Savchenko, P.P. Vorobiienko – K.: Ukrainnyi Vydatchnyi Tsentr. – 520p.
7. Dzhulii, V.M. (2019), Model otsinky ymovimisno-chasovykh kharakterystyk informatsiinoї vzaiemodii v merezhi internet rechei / V.M. Dzhulii, I.V. Muliar, O.V. Sieliukov, B.M. Kiziun // Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. – K.: VIKNU. – Vyp. № 63. – p.96-106
8. Dzhulii V.M., Klots Yu.P., Muliar I.V., Zhylevych M.L., Dzhulii A.V. (2021), Kontrol dodatkov internet-trafika kompiuternykh merezh metodamy mashynnoho navchannia. Visnyk Khmelnytskoho natsionalnoho universytetu. Tekhnichni nauky. – Khmelnytskyi. – №5. – pp. 22–26.
9. Dzhulii, V.M. (2022), Metod klasyfikatsii dodatkov trafika kompiuternykh merezh na osnovi mashynnoho navchannia v umovakh nevyznachenosti / V.M. Dzhulii, O.V. Miroshnichenko, L.V. Solodieieva // Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. – K.: VIKNU. – Vyp. №74. – pp. 73-82.
10. Lavrov, Ye. A. (2017.), Matematychni metody doslidzhennia operatsii : pidruchnyk / Ye. A. Lavrov, L. P. Perkhun, V. V. Shendryk – Sumy : Sumskyi derzhavnyi universytet, – 212 p.

Надійшла/Paper received : 13.09.2022 р. Надрукована/Printed :01.11.2022 р.