УДК 355.451 (477)

Прокопенко О., доктор філософії; Федорієнко В., канд. техн. наук; Кульчицький О.
Національний університет оборони України, Україна

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ДАНИХ

Анотація. *Негативний інформаційний вплив, заснований на використанні змісту ворожих пропагандистських наративів активно розповсюджуються у глобальному інформаційному просторі, що негативно впливає на українців, їх соціальну свідомість, нав'язуючи спотворений світогляд, твердження, факти, аргументи, чутки, тощо. На сьогодні, нагально необхідними постають питання розвитку і удосконалення теоретичних і практичних підходів моніторингу інформаційного простору, де найактуальнішим слід виокремити питання аналізу і прогнозування тенденцій розповсюдження інформаційного контенту, виявлення негативного інформаційно-психологічного впливу противника для своєчасного вироблення заходів щодо його протидії.*

Ключові слова: *моніторинг, нейронна мережа, обробка природної мови, семантика тексту, негативний інформаційний вплив.*

Prokopenko O., Ph.D; Fedoriienko V., Ph.D; Kulchytskyi O.
National Defence University of Ukraine, Ukraine

UTILIZATION OF DATA INTELLIGENCE TECHNOLOGIES

Abstract. *The negative informational impact based on the dissemination of hostile propaganda narratives actively spreads in the global information space, adversely affecting Ukrainians, their social consciousness, imposing a distorted worldview, assertions, facts, arguments, rumors, etc. Today, there is an urgent need for the development and improvement of theoretical and practical approaches to monitoring the information space, where the most relevant issue is the analysis and forecasting of trends in the dissemination of information content, identifying the negative informational-psychological impact of the adversary for timely counteraction measures.*

Keywords: *monitoring, neural network, natural language processing, text semantics, negative informational impact.*

Глобалізація існуючих процесів у світі характеризується високим рівнем невизначеності та ризику, що у значній мірі впливає на своєчасне і обґрунтоване прийняття управлінських рішень. Низка подій останніх років посилюють кризові явища практично у всіх сферах діяльності людства, де ступінь прояву найбільш відображається у соціальній, економічній, політичній і воєнній площині [1].

Активізація кризових явищ, як привило супроводжується активізацією інформаційної пропаганди з боку ворожих країн, що у значній мірі підсилює їх прояв. Негативний інформаційний вплив противника вкрай негативно впливає на різні цільові аудиторії, в залежності від мети, яка у собі несе спеціальна інформаційно-психологічна операція ворога проти населення України. Однозначно, можна з впевненістю відзначити і на значний вплив на рівень мотивації особового складу частин і підрозділів Сил оборони України, які ведуть активні бойові дії.

Реалізація антикризових заходів за допомогою комунікативних можливостей держави дозволяє підвищити їх ефективність, за рахунок узгодження дій і формування безпекового формату державної інформаційної політики суб'єктом управління (державними інституціями) і чітким її усвідомленням об'єктом управління (цільовими аудиторіями). Важливою складовою державного антикризового менеджменту є моніторинг глобального інформаційного простору, основною метою якого є виявлення інформаційних загроз, що можуть свідчити про ймовірність вчинення через кіберпростір суттєвої шкоди об'єктам критичної інфраструктури, вплив на

свідомість громадськості (певної цільової аудиторії), дезінформації та відкритої ворожої пропаганди [2].

Аналіз різного роду інформаційного контенту, з урахуванням швидкості його поширення у інформаційному просторі без використання спеціальних методів його обробки, в сучасних реаліях стає практично неможливим. Отже, висока ефективність обробки інформаційного контенту досягається за рахунок ряду можливостей програмно-апаратного забезпечення, а також методів і алгоритмів обробки, які закладені у них.

Текстовий інформаційний контент з великого спектру інтернет джерел для подальшої обробки і аналізу спеціальним програмним забезпеченням отримується за допомоги парсингу [3]. Це є необхідною процедурою для подальшого оброблення тексту, структуруючи його зміст у табличній формі за притаманним набором полів, наприклад: назва повідомлення/статті, автор, дата і час публікації, основний зміст, кількість переглядів, тощо. Наведені показники є кількісними, оскільки їх кількісна складова міститься у структурі джерела даних.

В інтересах виявлення інформаційних загроз більш цінними є якісні показники текстового контенту інформації: класифікація, або відношення текстового контенту до певної теми/рубрики/кейсу, семантика, емоційне навантаження, тональність тексту, тощо.

Останнє десятиліття, для визначення якісних показників текстового контенту, характеризується активним застосуванням новітніх інформаційних технологій, заснованих на основі використання штучного інтелекту. Штучний інтелект (ШІ) є галуззю комп'ютерних наук, яка займається створенням алгоритмів та моделей, здатних виконувати завдання, що традиційно вимагають людського інтелекту. Це включає розуміння мови, визначення зображень, прийняття рішень на основі даних та багато іншого. ШІ знайшов широке застосування у багатьох сферах життя, включаючи обробку природної мови (Natural Language Processing – NLP) [4]. Головною метою NLP є розпізнавання семантики та синтаксису природної мови, що дозволяє генерувати відповіді на запити / запитання, перекладати текст на інші мови, визначати емоційне забарвлення і тональність, перетворювати (транскрибувати) мовлення людини (радіомовлення) у текст і навпаки з тексту – генерувати мовлення людини.

Основними галузями ШІ для обробки текстів природною мовою є машинне навчання (Machine Learning) та глибинне навчання (Deep Learning), які, зокрема, активно використовуються для аналізу текстового контенту. Існують різні підходи до машинного навчання, кожен з яких має свої переваги та обмеження у контексті аналізу тональності і семантики тексту. За архітектурою штучної нейронної мережі, найбільш прийнятними вважаються рекурентні нейронні мережі (РНМ). Їх застосування особливо ефективно для обробки послідовностей даних, таких як текст, оскільки здатні зберігати інформацію про попередні елементи послідовності в своєму внутрішньому стані. Це досягається завдяки використанню петель в архітектурі мережі, що дозволяє інформації передаватися від одного кроку до іншого. Попри свої переваги, РНМ мають декілька важливих обмежень, зокрема проблему зникнення або вибуху градієнтів при її тренуванні. Це ускладнює збереження інформації на довгі періоди. Для вирішення цих проблем були розроблені спеціалізовані варіанти РНМ, такі як LSTM (Long Short Term Memory) та GRU (Gated Recurrent Units). Ці архітектури РНМ впроваджують додаткові механізми більш ефективного управління пам'яттю та збереження інформації на більші часові проміжки.

На сьогодні, для високорівневої мови програмування Python є ряд програмних рішень у вигляді спеціалізованих бібліотек, які реалізують моделі LSTM або GRU для вирішення конкретних специфічних завдань з розпізнавання семантики текстового контенту. Найбільш поширеними є бібліотеки Keras, TensorFlow, PyTorch та інші.

Таким чином, розглянуті вище положення деталізують сучасні технології інтелектуального аналізу даних. За своєю архітектурою рекурентні нейронні мережі є найбільш прийнятними для аналізу і обробки природної мови (NLP). Використання цих технологій під вимоги органів військового управління і підрозділів Збройних Сил України, які здійснюють

цілодобовий моніторинг інформаційного простору з виявлення негативного інформаційного впливу противника, дозволить суттєво підвищити ефективність і якість аналізу текстового контенту, виявляти фази проведення інформаційних кампаній ворога і вживати своєчасні заходи протидії цим загрозам.

Джерела та література

1. Почепцов Г. Сучасні інформаційні війни. Видання третє, доповнене та перероблене. Київ : Видавничий дім "Києво-Могилянська академія", 2016. 504 с.

2. Курбан О. В. Сучасні інформаційні війни у мережевому он-лайн просторі. Навчальний посібник. Київ : ВІКНУ, 2016. 286 с.

3. Парсинг сайтів: що це і навіщо він потрібен? URL : https://web-promo.ua/ua/blog/parsing-sajtov-chto-eto-i-zachem-nuzhen/#:~:text= (дата звернення: 04.04.24).

4. Shervin Minaee Deep Learning Based Text Classification: A Comprehensive Review. URL : chrome-extension: //efaidnbmnnnibpca jpcglclefindmkaj/https://arxiv.org/pdf/2004.03705.pdf (дата звернення: 12.04.24).

УДК 621.39

Химич Г., старший викладач; Дунець В., канд. техн. наук, доц.; Блавіцький М.
Тернопільський національний технічний університет імені Івана Пулюя, Україна

МОБІЛЬНІ МАЛІ АНТИДРОНОВІ СИСТЕМИ. ТЕХНОЛОГІЇ ПРОЄКТУВАННЯ

Анотація. *Антидронові малі системи (рушниці) протидії БПЛА використовуються з метою захисту особового складу, обладнання, техніки від бойових, розвідувальних дронів, які літають на висотах не вище 2000м. Для ефективної роботоздатності таких систем потрібно дотримуватись відповідних наукових та технологічних аспектів при проєктуванні. Крім цього, зважаючи на те, що на лініях розмежування створюється багаточастотний, потужний з великою напруженістю електромагнітного поля спектр, то дані системи повинні бути адаптовані до театру дій, завадостійкі і електромагнітно сумісні з другими системами, щоб мінімізувати завадне середовище для власних систем зв'язку, передачі даних.*

Ключові слова: *безпілотні літаючі апарати (БПЛА), дрон, радіоелектронна боротьба (РЕБ), радіоелектронне подавлення (РЕП), антена, електромагнітний спектр, частотні діапазони, антидронова окопна рушниця (мала РЕБ).*

Khymych G., Senior Lecturer; Dunets V., Ph. D., Assoc. Prof.; Blavitskyi M.
Ternopil Ivan Puluj National Technical University, Ukraine

MOBILE SMALL ANTI-DRONE SYSTEMS. DESIGN TECHNOLOGIES.

Abstract. *Small anti-drone systems (guns) for combating unmanned aerial vehicles are used to protect personnel, equipment, and machinery from combat and reconnaissance drones that fly at altitudes of no more than 2,000 m. For the effective operation of such systems, it is necessary to observe the relevant scientific and technological aspects when designing. In addition, taking into account the fact that a multi-frequency, powerful spectrum with a high intensity of the electromagnetic field is created on the demarcation lines, these systems must be adapted to the theater of operations, resistant to interference and electromagnetically compatible with other systems in order to minimize the harmful environment for their own communication systems , data transmission.*

Keywords: *unmanned aerial vehicles (UAV), drone, electronic warfare (EW), radio electronic suppression (EW), antenna, electromagnetic spectrum, frequency bands, anti-drone trench gun (small EW).*

Військові дії між країнами, угрупуваннями в XXI ст. зводяться в основному до протистояння високих технологій (авіація 4 -6 покоління, ракетні технології, безпілотні літаючі