INFORMATION WARFARE

УДК 004(056.5+738.52)

ВАЛЕНТИН ПЕТРИК
АНДРІЙ ДАВИДЮК

ВИКОРИСТАННЯ СПЕЦІАЛЬНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ АНАЛІЗУ ІНФОРМАЦІЙНОЇ АГРЕСІЇ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ ПРОТИ УКРАЇНИ

У рамках гібридної війни, що точиться на теренах нашої держави, Російська Федерація, з метою приховування правдивої інформації про перебіг бойових дій, введення в оману наших співвітчизників та світової спільноти, широко використовує дезінформування та пропаганду. В свою чергу використання інформаційної зброї створює сприятливі умови для загострення конфлікту на сході нашої держави, дозволяє керівництву Російської Федерації заперечувати присутність своїх збройних сил на території України, забезпечувати дипломатичне прикриття військовим заходам і ведення міжнародної політики Російської Федерації. Це підтверджує існування реальної загрози інформаційному простору України. З метою протидії таким загрозам та, пов'язаним з ними, інформаційними впливами використовуються існуючі методи інтелектуального лінгвістичного аналізу тексту. Застосування цих методів дозволяє провести детальне дослідження інформаційної агресії проти України для більш ефективної протидії та розробки власних засобів захисту в напрямі забезпечення національної безпеки держави. Оскільки основним середовищем поширення інформації є Інтернет, то у статті описується використання розробленого програмного засобу моніторингу глобальної мережі на предмет інформаційної агресії Російської Федерації проти України. Тому аналізування інформаційної агресії Російської Федерації у глобальній мережі Інтернет за допомогою спеціального програмного засобу "Support Ukraine" є метою даної роботи. Для досягнення цієї мети проаналізовано існуючі засоби інтелектуальної обробки даних та інформаційного протистояння. Результатами аналізу підтверджується необхідність створення та використання означеного засобу. Його перевагами є зручність використання і можливість створення власного словника. Завдяки цьому можливе розширення його можливостей.

Ключові слова: інформаційна агресія, пропаганда, дезінформація, спеціальний програмний засіб, інформаційний вплив, інформаційні потоки, контент-моніторинг, агресія Російської Федерації.

Постановка проблеми. Нині інформаційний простір переповнений непотрібною інформацією, яка хаотично розповсюджується. Унаслідок цього пошук глибинних семантичних зв'язків, достовірної інформації та знань ускладнюються. Тому, щоб вирішити цю проблему застосовуються засоби аналізу змісту даних і текстів (Data Mining, Text Mining) [1]. Раніше ці програмні засоби застосовувалися тільки спецслужбами, в особливості Заходу та Радянського Союзу [2]. Проте з розширенням можливостей цивільного сектору, майже кожна компанія, що працює в сфері інформаційних технологій, може собі дозволити обчислювальні ресурси та програмні засоби для реалізації даної задачі. Тим більше, що зі зростаючою інформатизацією, новими відкриттями та знаннями, приватний та державний сектор зіштовхується з проблемою обробки даних [3]. Важливе завдання Text Mining пов'язане з виокремленням із тексту його характерних елементів або властивостей, для технологій, що використовують метадані документа, ключові слова з його анотації. Ці елементи можна використати для віднесення документа до деяких категорій з наперед заданої схеми класифікації. Цим також забезпечується новий рівень семантичного пошуку документів [4].

Аналіз останніх досліджень і публікацій. Одним з найбільш відомих таких програмних рішень є розширений пошук від компанії Google [5]. Також вирішенню задач пов'язаних з інтелектуальним аналізом даних приділено увагу у [6], [7]. Особливості інформаційного протистояння України та Російської Федерації (РФ) описані у [8], [9]. У даних працях чітко та зрозуміло висвітлено головні аспекти аналізу даних у контексті інформаційного протиборства. Однак, вирішенню завдання розроблення програмного забезпечення для інтелектуального аналізу контенту ресурсів глобальної мережі Інтернет стосовно виявлення і, як наслідок, протидії інформаційному впливу не приділено належної уваги. Існуюче рішення від Google є досить практичним і широко використовується [10], та на відміну від «Support Ukraine» не має можливості створення власного словника і відповідно пошуку за словником.

З огляду на аналіз останніх досліджень і публікацій **метою статті** є аналізування інформаційної агресії РФ проти України за допомогою спеціального програмного засобу "Support Ukraine", результати використання якого можуть використовуватися для протидії означеній агресії. Дане програмне забезпечення (ПЗ) має відкритий код, тому користувач може модифікувати його відповідно до своїх потреб.

Виклад основного матеріалу дослідження. Програмний засіб має декілька функцій. Перш за все, його використання дозволяє шукати статті в мережі Інтернет за ключовими словами, власноруч введеними користувачем (див. рис. 1). Наприклад: ДНР, ЛНР, Захарченко.

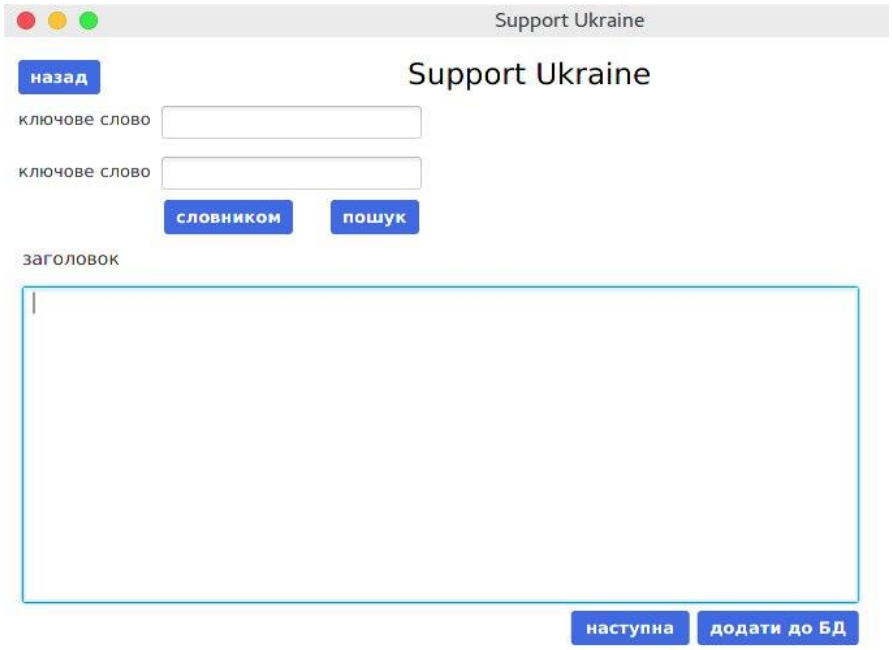

Рисунок 1 – Інтерфейс ПЗ «Support Ukraine»

Функціонал даного ПЗ на перший погляд схожий з розширенним пошуком від Google [11], проте має характерні особливості, зокрема, пошук за словником. Словником в даному випадку вважається особливий набір слів. Даний набір слів задається вручну, мова словника не впливає на працездатність ПЗ. Особливість даного набору полягає в тому, що в переліку слів обирається основне слово, наприклад "ДНР", з яким пов'язані додаткові слова, наприклад "Захарченко, Гиркин". Таким чином, якщо в словнику буде записано: "ДНР + Захарченко Гиркин", то програма буде шукати статті в Інтернет зі згадкою на слово "ДНР" зі словами "Захарченко та/або Гиркин". Ці слова заносяться користувачем до окремого текстового файлу "словник.txt", наступним чином: (Сепар + Донбас, Донецк, Луганск, Новорос, Украина). При цьому словник повинен мати такий вигляд:

Сепар + Донбас, Донецк, Луганск, Новорос, Укра
Повстанцы + Донбас, Донецк, Луганск, Новорос, Укра

Кіборг + аеропорт, Донецк
Киборг + аеропорт, Донецк
Крим + анексія, зелені чоловічки
Крым + возвращение домой, Русская община Крыма, Русское Единство, присоединен, смена власт
Стрелков + Донбас, Донецк, Луганск, Новорос, Украи
Гиркин + Донбас, Донецк, Луганск, Новорос, Украи
Минские договоренности + Донбас, Донецк, Луганск, Новорос, Украи
Мінські домовленості + Донбас, Донецьк, Луганск, Новорос, Украї
Обстрел + Донбас, Донецк, Луганск, Новорос, Украи
Бендеровц + майдан, Донбас, Донецк, Луганск, Новорос
Бандеровц + майдан, Донбас, Донецк, Луганск, Новорос
Правый сектор + Донбас, Донецк, Луганск, Новорос, майдан
Ополчен + Донбас, Донецк, Луганск, Новорос
Освободительная армия + Донбас, Донецк, Луганск, Новорос
Анексия + Чорноморський флот, Крым, АРК
Черноморский флот + Росси, РеспубликКрым, АРК
Гумконвой + Донбас, Донецк, Луганск, Новорос, АРК
Аксьенов + Крым, АРК, Русское Единство
Губарёв + Донбас, Донецк, Луганск, Новорос
Путин + Украин, Донбас, Крым, Донецк, Луганск, Новорос, АРК
Плотницкий + Донбас, Донецк, Луганск, Новорос
Захарченко + Донбас, Донецк, Луганск, Новорос
Кисёльев + Крым, Донбас, Донецк, Луганск, Новорос
Гига + Крым, Донбас, Донецк, Луганск, Новорос
ФСБ + Крым, Донбас, Донецк, Луганск, Новорос, Украи, АРК
Донские козаки + Донбас, Донецк, Луганск, Новорос
Росси + Крым, Донбас, Донецк, Луганск, Новорос, Украи
Референдум + Донбас, Донецк, Луганск, Новорос

Наступною відмінною від пошуку Google важливою функцією даного програмного засобу – є взаємодія з базою даних (БД) (див. рис. 2). Користувач має можливість формування власної БД, до якої може додавати електронні посилання на статті, що зацікавили, та відкриту в мережі інформацію про конкретних осіб.

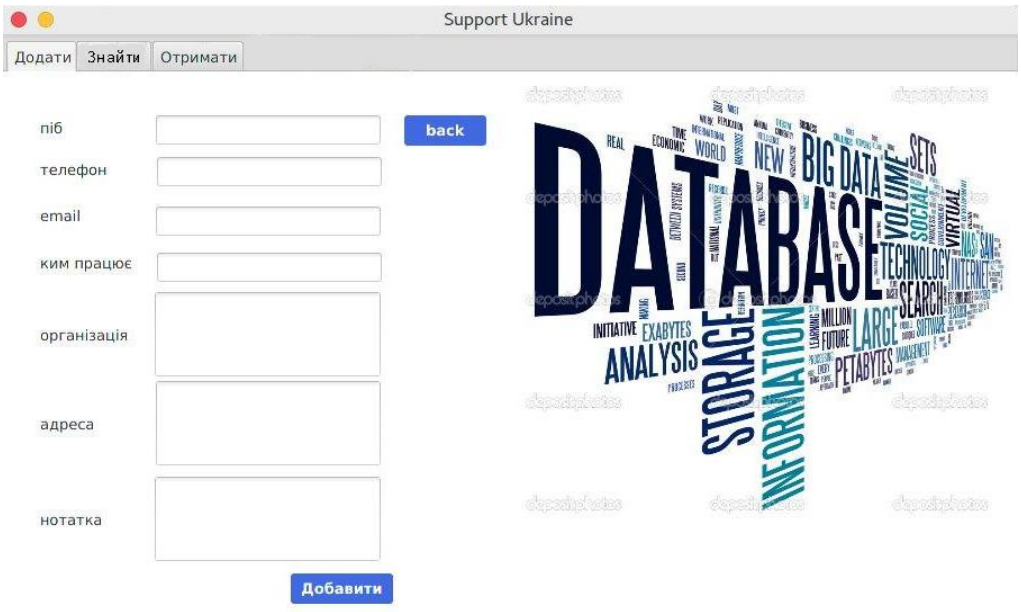

Рисунок 2 – Інтерфейс звернення до БД

В подальшому користувач може здійснювати пошук потрібної йому інформації, використовуючи власну БД. Для формування запису в БД потрібно вказати всю наявну інформацію про особу: ПІБ, телефон, e-mail, ким працює, організація, адреса, тощо та підтвердити збереження натисненням кнопки “Добавити”. Водночас використання даної функції має юридичні обмеження визначені статею 25 Закону України “Про захист персональних даних” від 01.06.2010 [11].

Завдяки цьому можливим є реалізація пошуку даних про особу в БД за трьома критеріями: ПІБ, організація, номер телефону (див. рис. 3). Вибір цих критерії базується на тому, що вони є найбільш вживаними та менш прихованими ідентифікаторами особи та забезпечують отримання точного результату пошуку, кожним наступним критерієм виключаючи можливі співпадання. Кількість критеріїв є оптимальною, за затраченими ресурсами (час, ОЗУ, ЦП) для виконання пошуку.

Останньою операцією з базою даних є пошук, попередньо доданих користувачем до бази даних, статей за їх назвою.

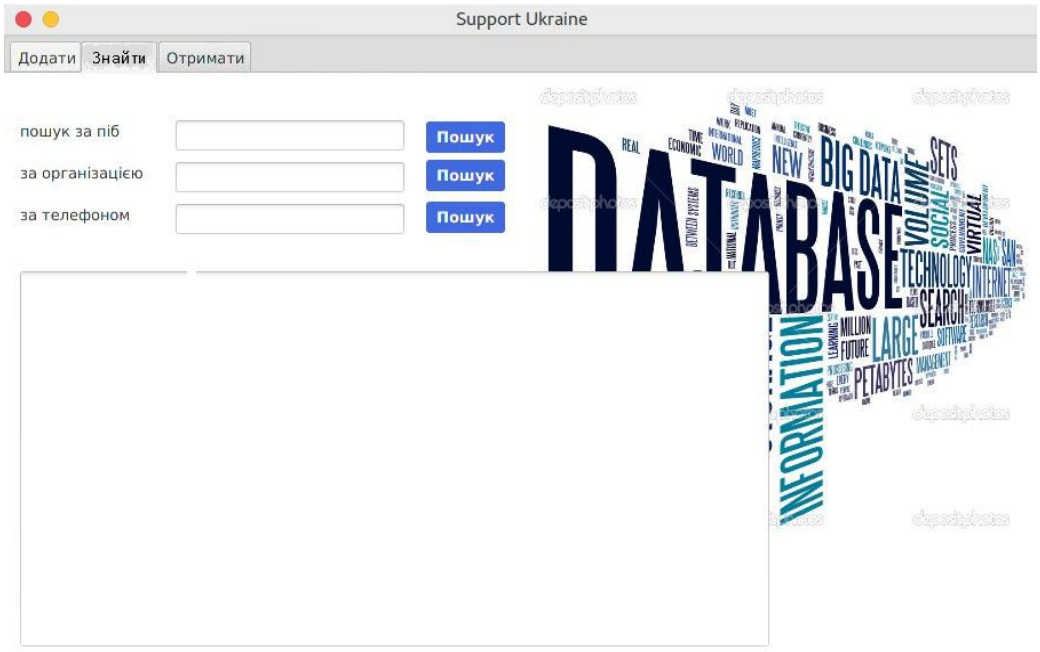

Рисунок 3 – Інтерфейс програми для пошуку особи в БД

Висновки. Розроблений програмний засіб має широку сферу застосування. По-перше, він може застосовуватись силовим сектором, в тому числі спецслужбами і іншими силовими структурами для моніторингу подій та осіб в мережі Інтернет, створення своєї бази даних та для аналізування зв’язків між ними, що є вкрай важливим в умовах сучасної інформаційної війни. Застосування даного ПЗ сприяє вирішенню завдань з забезпечення національної безпеки держави, шляхом своєчасного виявлення засобів інформаційного впливу на суспільство шляхом його дезінформування та пропаганди.

По-друге, програмним засобом можуть користуватися державні та приватні компанії для конкурентної розвідки. Організації мають змогу шукати згадки та потрібну інформацію про конкуруючу організацію одразу по мережі Інтернет. Такий функціонал сприятиме підвищенню конкурентної спроможності наших вітчизняних підприємств задля зменшення імпорту продукції з РФ, тим самим припинити “підживлювати” її економіку, що створить умови для збільшення експорту українського товару.

Перспективи подальших досліджень. У перспективах подальших досліджень планується модернізація програмного засобу за рахунок додання функції “Пошук із виключенням”, що дасть можливість отримувати більш точні результати пошуку. Наприклад, при введені ключового слова “сепар”, потрібно обов’язково виключити з пошуку слово

“сепаратор”, так як “Сепаратор” – апарат, призначений для розділення певного продукту на фракції з різними фізичними або хімічними характеристиками [12]. Або ж при введені ключового слова “Новороссия”, потрібно обов’язково виключити з пошуку фразу “Приморский край”, так як Новоросія – це не тільки терористичний союз угруповань ЛНР та ДНР, але і село у Шкотовському районі Приморського краю РФ.

Ще однією корисною функцією буде автоматичне встановлення зв’язків між даними в БД. Щоб не витрачати час та ресурси на аналізування даних, програма буде сама будувати схему, в якій всі елементи будуть пов’язані певними параметрами. Це дасть можливість встановлювати та візуалізувати зв’язки між людьми та організаціями, які введено в БД.

Не менш важливим для підвищення ефективності застосування даного програмного засобу буде його доопрацювання в напрямку лінгвістичного аналізу статей в мережі Інтернет, на основі використання змістовних ознак маніпулятивності інформаційного впливу через ЗМІ: кількість повторів ключових слів, посилання на інший ЗМІ, використання негативних штампів, кількість прикметників стосовно обсягу тексту, використання метафор, гіпербол, порівнянь, псевдонаукових термінів, неологізмів, ідеальних понять [13].

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Методы и стадии Data Mining. [Электронный ресурс]. Доступно: http://www.intuit.ru. Дата обращения: Март 12, 2017.

[2] “СССР. На страже завоеваний Октября”. [Электронный ресурс]. Доступно: https://www.e-reading.club/chapter.php/1025953/3/Degtyarev-Enciklopediya_specsluzhb.html. Дата обращения: Март 12, 2017.

[3] “Пять ступеней цифровой трансформации”. [Электронный ресурс]. Доступно: http://www.computerworld.ru. Дата обращения: Март 12, 2017.

[4] “DataMining”. [Электронный ресурс]. Доступно: https://www.coursehero.com. Дата обращения: Март 12, 2017.

[5] “Розширений пошук Google”. [Електронний ресурс]. Доступно: https://support.google.com/websearch/answer/35890?hl=uk. Дата звернення: Бер. 13, 2017.

[6] В. Фурашев, та Д. Ланде, ”Інформаційні операції крізь призму системи моніторингу та інтеграції інтернет-ресурсів”, *Правова інформатика*, № 2 (22), с. 49-57, 2009.

[7] Д. Ландэ, В. Фурашев, С. Брайчевский, та А. Григорьев, *Основы моделирования и оценки электронных информационных потоков*. Киев, Украина: Инжиниринг, 2006.

[8] “Інформаційні потоки в організації”. [Електронний ресурс]. Доступно: https://studfiles.net/preview/5043453/page:3/. Дата звернення: Бер. 13, 2017.

[9] В. Панченко, “Інформаційні операції в асиметричній війні Росії проти України: підходи до моделювання”, *Інформація і право*, № 3 (12), с. 13-16, 2014.

[10] “Удобно ли искать в Гугле – фильтры, расширенный поиск и операторы, помогающие быстро гуглить”. [Электронный ресурс]. Доступно: http://ktonanovenkogo.ru/seo/search/iskat-v-gugle-guglit-filtry-rasshirennye-poisk-operatory-google-prikoly.html. Дата обращения: Март 13, 2017.

[11] Верховна Рада України. 6 сесія. (Черв. 01, 2010), *Закон № 2297-VI, “Про захист персональних даних”*. [Електронний ресурс]. Доступно: http://zakon2.rada.gov.ua/laws/show/2297-17. Дата звернення: Бер. 13, 2017.

[12] “Сепаратор”. [Электронный ресурс]. Доступно: https://wikipedia.org. Дата обращения: Бер. 13, 2017.

[13] Я. Жарков, Л. Компанцева, В. Остроухов, В. Петрик, М. Присяжнюк, та Є. Скулиш, *Історія інформаційно-психологічного протиборства*. Київ, Україна: Науково-видавничий. відділ НА СБ України, 2012.

Стаття надійшла до редакції 23 березня 2017 року.

REFERENCE

[1] "Methods and Stages of Data Mining". [Online]. Available: http://www.intuit.ru/. Accessed on: March 12, 2017.

[2] "USSR. On the guard of the victories of October". [Online]. Available: https://www.e-reading.club/chapter.php/1025953/3/Degtyarev-Enciklopediya_specsluzhb.html. Accessed on: March 12, 2017.

[3] "Five stages of digital transformation". [Online]. Available: http://www.computerworld.ru Accessed on: March 12, 2017.

[4] "DataMining". [Online]. Available at: https://www.coursehero.com. Accessed on: March 12, 2017.

[5] "Advanced Search Google". [Online]. Available: https://support.google.com/websearch/ answer/35890?hl=en. Accessed on: March 13, 2017.

[6] V. Furashev, and D. Lande, "Information Operations through the Prism of Monitoring and Integrating Internet Resources", *Legal Informatics*, no. 2 (22), pp. 49-57, 2009.

[7] D. Lande, V. Furashev, S. Braichevskyi, and O. Hryhoriev, *Fundamentals of Modeling and Evaluation of Electronic Information Flows*. Kiev, Ukraine: Engineering, 2006.

[8] "Information flows in the organization". [Online]. Available: https://studfiles.net/preview/ 5043453/page:3/. Accessed on: March 13, 2017.

[9] V. Panchenko, "Information Operations in Russia's Asymmetric War Against Ukraine: Approaches to Modeling", *Information and Law*, no. 3 (12), pp. 13-16, 2014.

[10] "Is it convenient to search in Google". [Online]. Available: http://ktonanovenkogo.ru/seo/ search/iskat-v-gugle-guglit-filtry-rasshirennye-poisk-operatory-google-prikoly.html. Accessed on: March 13, 2017.

[11] The Verkhovna Rada of Ukraine. 6th Session. (June 01, 2010), *Law No. 2297-VI, "On protection of personal data"*. [Online]. Available: http://zakon2.rada.gov.ua/laws/ show/2297-17. Accessed on: March 13, 2017.

[12] "Separator". [Online]. Available: https://wikipedia.org. Accessed: March 13, 2017.

[13] Y. Zharkov, L. Kompantseva, V. Ostroukhov, V. Petryk, M. Prysyazhnyuk, and E. Skulish, *History of information-psychological confrontation*. Kyiv, Ukraine: Science Department at the Security Service of Ukraine, 2012.

ВАЛЕНТИН ПЕТРИК
АНДРЕЙ ДАВИДЮК

ИСПОЛЬЗОВАНИЕ СПЕЦИАЛЬНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ АНАЛИЗА ИНФОРМАЦИОННОЙ АГРЕССИИ РОССИЙСКОЙ ФЕДЕРАЦИИ ПРОТИВ УКРАИНЫ

В рамках гибридной войны, которая идет на территории нашего государства, Российская Федерация, с целью сокрытия правдивой информации о ходе боевых действий, введения в заблуждение наших соотечественников и мирового сообщества, широко использует дезинформацию и пропаганду. В свою очередь использование информационного оружия создает благоприятные условия для обострения конфликта на востоке нашей страны, позволяет руководству Российской Федерации отрицать присутствие своих вооруженных сил на территории Украины, обеспечивать дипломатическое прикрытие военным действиям и ведения международной политики Российской Федерации. Это подтверждает существование реальной угрозы информационному пространству Украины. С целью противодействия таким угрозам и, связанным с ними, информационными воздействиями используются существующие методы интеллектуального лингвистического анализа текста. Применение этих методов позволяет провести детальное исследование информационной агрессии против Украины для более эффективного противодействия и разработки собственных средств защиты в направлении обеспечения национальной безопасности государства. Поскольку основной

средой распространения информации есть Интернет, то в статье описывается использование разработаного программного средства мониторинга глобальной сети на предмет информационной агрессии Российской Федерации против Украины. Поэтому анализ информационной агрессии РФ с помощь специального программного средства "Support Ukraine" является целью данной работы. Для достижения этой цели проанализированы существующие средства интеллектуальной обработки данных и средства информационного противостояния. Результатами анализа подтверждается необходимость создания и использования даного программного средства. Его преимуществами является удобство использования и возможность создания собственного словаря. Благодаря этому возможно расширение его возможностей.

Ключевые слова: информационная агрессия, пропаганда, дезинформация, специальное программное средство, информационное воздействие, информационные потоки, контент-мониторинг, агрессия Российской Федерации.

VALENTYN PETRYK,
ANDRII DAVYDIUK

USE OF SPECIAL SOFTWARE FOR ANALYSIS OF THE INFORMATION AGGRESSION OF THE RUSSIAN FEDERATION AGAINST UKRAINE

In the framework of the hybrid war that is taking place in the territory of our state, the Russian Federation is widely using misinformation and propaganda to conceal the truthful information about the course of hostilities, misleading our compatriots and the international community. In turn, the use of information weapons creates favorable conditions for the intensification of the conflict in the west of our country, allows the leadership of the Russian Federation to deny the presence of its armed forces on the territory of Ukraine, provides a diplomatic coverage of military measures and the conduct of international policy of the Russian Federation. This confirms the existence of a real threat to Ukraine's information space. In order to counter such threats and related information influences, existing methods of intellectual linguistic analysis of the text are used. Usage of these methods allows us to make a detailed research of information aggression against Ukraine for more effective counteraction and development of own means of defense for ensuring the national security of the state. Since the main space for disseminating of information is the Internet, the article describes the use of the developed software for monitoring the global network of the information aggression of the Russian Federation against Ukraine. Consequently, the purpose of this work is to analyze the information aggression of the Russian Federation in the global Internet with the help of a special software "Support Ukraine". Existing tools for intelligent data processing and information confrontation are analyzed in order to achieve this purpose. The results of the analysis confirm the necessity of creating and using the indicated means. Its advantages are the convenience of using and the ability to create your own vocabulary. Due to this possibility, its capabilities are expanding.

Key words: information aggression, propaganda, misinformation, special programmatic tool, information influence, information flows, content monitoring, aggression of the Russian Federation.

Валентин Михайлович Петрик, кандидат наук з державного управління, доцент кафедри управління і тактико-спеціальної підготовки, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

E-mail: ISZZI_open@ukr.net.

Андрій Вікторович Давидюк, курсант, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

E-mail: andrey19941904@gmail.com.

Валентин Михайлович Петрик, кандидат наук по государственному управлению, доцент кафедры управления и тактико-специальной подготовки, Институт специальной связи и защиты информации Национального технического университета Украины “Киевский политехнический институт имени Игоря Сикорского”, Киев, Украина.

Андрей Викторович Давидюк, курсант, Институт специальной связи и защиты информации Национального технического университета Украины “Киевский политехнический институт имени Игоря Сикорского”, Киев, Украина.

Valentyn Petryk, candidate of public administration, associate professor, associate professor at the management and tactical and special training academic department, Institute of special communications and information protection of the National technical university of Ukraine ”Igor Sikorsky Kyiv polytechnic institute”, Kyiv, Ukraine.

Andrii Davydiuk, cadet, Institute of special communication and information protection of the National technical university of Ukraine ”Igor Sikorsky Kyiv polytechnic institute”, Kyiv, Ukraine.