

Київський національний університет імені Тараса Шевченка
Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка
Міністерство освіти і науки України

Кваліфікаційна наукова
праця на правах рукопису

КУБЯВКА МИКОЛА БОГДАНОВИЧ

УДК 004.89:004.912

ДИСЕРТАЦІЯ
МОДЕЛІ ТА МЕТОДИ УПРАВЛІННЯ ІНФОРМАЦІЙНИМ
СУПРОВОДЖЕННЯМ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

Спеціальність 05.13.06 – інформаційні технології

Інформаційні технології

Подається на здобуття наукового ступеня кандидата технічних наук

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ М.Б.Кубявка

Науковий керівник: Тесля Юрій Миколайович, доктор технічних наук, професор

Київ – 2017

АНОТАЦІЯ

Кубявка М.Б. Моделі та методи управління інформаційним супроводженням в умовах гібридної війни. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.06 – «Інформаційні технології». – Київський національний університет імені Тараса Шевченка, Київ, 2017.

Дисертаційна робота присвячена вирішенню актуальної наукової задачі – розробці моделей та методів управління інформаційним супроводженням в умовах гібридної війни та створенню, на їх основі, інформаційної технології адресного (цілеорієнтованого) розподілу інформаційних потоків. В процесі досліджень було розв'язано ряд наукових завдань.

У **вступі** наведено загальну характеристику роботи, яка підкреслює її актуальність, відповідність науковим темам, наукову новизну та практичне значення, визначено предмет та об'єкт дослідження, сформульовано мету та задачі дослідження.

У **першому розділі** «Технології інформаційних війн» проведено аналіз використання інформації в управлінні військовими операціями. Розглянуто процеси, що відбуваються під час ведення гібридної війни та акцентовано увагу на її інформаційній складовій. Виявлено закономірності підвищення результативності несилового впливу на супротивника та ефективності підтримки військ (сил) в процесі супроводження воєнних дій при застосуванні інформаційних технологій. У результаті узагальнення проаналізованих даних виявлено відсутність наукових рішень, щодо автоматично розподілу повідомлень у військовій сфері через оцінку інформаційного впливу цих повідомлень на різні верстви населення та війська. Вважаючи, що інформація про те, кому направити повідомлення, є в самому повідомленні, а адресат повідомлення може бути визначений із самого повідомлення, що є і необхідною, і достатньою умовою,

задачу управління інформаційним супроводженням трансформовано в задачу обробки природномовних текстів. Визначено, що ефективність розпізнавання змісту природномовного повідомлення наявними системами аналізу текстів не дозволяє здійснювати швидке управління інформаційним супроводженням забезпечення прийняття рішення управлінським складом керівництва держави, військ, тощо. У зв'язку з цим висунуто пропозицію в створенні нових інтегрованих підходів до управління впливами та запропоновано реалізувати такі підходи через створення інформаційних систем і технологій, які зможуть оцінити результативність різних способів інформаційного впливу та ефективно вести процес управління реалізацією цих інформаційних впливів за рахунок автоматичного визначення адресатів повідомлень. Сформульовано основні задачі дослідження.

У **другому розділі** «Методологічні основи технології управління інформаційним супроводженням» визначено і обґрунтовано застосування процесів інформаційного впливу для вдосконалення проведення військових операцій. Рекомендовано до застосування науково-методичний базис управління інформаційним супроводженням процесів впливу, в якому виокремлено дві частини: пошук шляхів визначення та зміни інформованості контрагентів взаємодії та розрахунок інформаційного впливу на цих контрагентів. *Основна ідея* цього базису – обґрунтувати та формально представити такі науково-методичні інструменти управління впливами, які забезпечать значне покращення інформаційно-аналітичного забезпечення військ, шляхів підготовки і проведення операцій з інформаційного впливу на контрагента, здійснення контрзаходів та будуть максимально інформативно зрозумілі, прості, результативні і мінімально затратні. Надано основні визначення роботи: методика управління інформацією в системі управління впливами; клас повідомлень; форма впливу; зміст форми впливу; засіб впливу; ідентифікація необхідного відношення до отриманої інформованості; управління інформованістю у впливах; інформаційна технологія управління інформаційним супроводженням; контрагент взаємодії; інформаційне супроводження в умовах гібридної війни. Під *інформаційною технологією*

управління інформаційним супроводженням (ІТ УІС) слід розуміти сукупність методів, процесів і програмно-технічних засобів, інтегрованих з метою збирання, опрацювання, зберігання, розповсюдження, показу і використання інформації в інтересах інформаційної підтримки власних військових підрозділів і сил та впливу на противника. Виходячи з цього, запропоновано математичну модель взаємозалежності впливів та поведінки контрагентів взаємодії, що дозволило формалізувати підхід до оцінки інформації, яку необхідно надати контрагенту з тим, щоб забезпечити його відповідну реакцію. В результаті застосування цієї моделі стало можливим визначити стратегію дій власних сил: застосувати такий набір несилових дій та засобів їх надання, які забезпечать потрібну реакцію противника (відведення військ, перекидання їх на другорядні напрямки, відміна наступу тощо). Запропоновано оцінювати впливи, через різницю в умовних та безумовних ймовірностях реакцій на них контрагентів взаємодії, що забезпечило визначення найбільш інформативних повідомлень для груп населення та військових і стало основою для удосконалення моделі управління інформаційним супроводженням.

Всі ці результати є суттєвим внеском в наукові основи методології управління впливами, оскільки по новому дозволяють підійти до проблеми визначення інформованості контрагентів взаємодії та ефективного управління інформаційними впливами з найкращими результатами.

Третій розділ «Моделі та метод управління інформаційним супроводженням» присвячено управлінню інформаційним супроводженням процесів впливу на контрагентів взаємодії на основі методу адресно-орієнтованого розподілу природномовних текстових повідомлень. Проведено класифікацію контрагентів взаємодії за особливостями сприйняття ними інформації. Розглянуто інформаційне середовище впливу на контрагентів та визначено класи повідомлень у розрізі функціональних ролей впливу. Зазначено, що управління інформованістю контрагентів взаємодії полягає в адресації тієї чи іншої інформації конкретним споживачам, а адресат повідомлення може бути визначений із самого повідомлення. Тому задачу управління інформаційним

супроводженням було трансформовано в задачу обробки природно-мовних текстів з певними особливостями, які полягають в тому, що визначається не зміст (як робить більшість систем обробки і аналізу природно-мовних текстів), а той адресат повідомлення, для якого імовірність потрібної реакції збільшиться. Введено можливість відсіювання повідомлень, в яких не міститься інформація про адресата, на якого ця інформація найбільше вплине. На відміну від рішення задачі по визначенню впливу на противника, було підібрано для кожного повідомлення такі класи контрагентів, на які вплив буде максимальний. На основі попередньої класифікації сформована інтегрована експертна оцінка суб'єктивної імовірності реалізації одного із атрибутів моделі при умові, що буде реалізовано інший. По цим ймовірностям можна судити про суб'єктивне відношення експертів до застосування різноманітних форм інформаційних представлень в різних умовах. З урахуванням отриманих результатів сформульовано нове бачення методу управління інформаційним супроводженням в процесах інформаційного впливу в умовах гібридної війни, який дозволив наблизитися до автоматичного розподілу повідомлень по найбільш сприятливим до цих повідомлень класам контрагентів взаємодії. Застосувавши ймовірнісно-рефлекторний підхід удосконалено модель визначення найбільш інформативних компонентів природномовного тексту, з позиції автоматичної адресації цих повідомлень різним класам контрагентів. Поєднавши модель взаємозалежності між впливами та поведінкою і модель визначення найбільш інформативних компонентів природномовного тексту, але вже не по відношенню до впливу на контрагентів взаємодії, а по відношенню до визначення адресата інформації, розроблено рефлекторний метод автоматичного реагування на зміст повідомлення. Використання запропонованого методу дозволило вирішити завдання автоматичного визначення адресата повідомлення.

У **четвертому розділі** «Реалізація технології управління інформаційним супроводженням» сформульовано основні принципи побудови технології інформаційного супроводження. Наведено функціональні та не функціональні вимоги до аналогічних систем, а також встановлено критерії якості

функціонування технології інформаційного супроводження процесів впливу на контрагентів взаємодії. В результаті чого побудовано узагальнену структуру технології інформаційного супроводження, розроблено структуру інформаційної технології у вигляді схеми даних, а її сутності, атрибути та ідентифікатори елементів представлені в вигляді таблиць. Побудовано логічну та фізичну моделі бази даних та проведено їх опис. Розроблено програмний засіб Adres, який здатний аналізувати повідомлення на природній мові та автоматично адресувати їх визначеним контрагентам взаємодії. Отримані результати експериментальних досліджень практично довели спроможність програмного засобу Adres автоматично ідентифікувати адресатів повідомлень з метою ціленаправленого (вибіркового) інформаційного впливу на контрагентів взаємодії. Результати роботи програмного засобу Adres мають високу збіжність з математичними розрахунками проведеними в дисертації, що свідчить про адекватність запропонованих математичних моделей і достовірність наукових положень та висновків, отриманих в роботі.

Результати дослідження використані у науково-дослідній роботі Військового інституту Київського національного університету імені Тараса Шевченка, впроваджені в інформаційне забезпечення служб Проектного офісу реформ Міністерства оборони України, виробничу діяльність ТОВ «Авіаційна виробнича компанія СГ «Скаетон», в постійну роботу служб Управління інформаційних технологій Міністерства оборони України та в навчальний процес Київського національного університету імені Тараса Шевченка.

Ключові слова: інформаційна технологія, управління впливами, контрагент взаємодії, інформаційне супроводження, рефлексорний підхід.

ANNOTATION

Kubyavka M.B. The models and methods of management of information support in terms of hybrid warfare. - Qualifying scientific work on the manuscript.

The thesis for the degree of candidate of technical sciences, specialty 05.13.06 «Information technologies». - Taras Shevchenko National University of Kyiv, Kyiv, 2017.

The dissertation is aimed at the solution of the relevant scientific tasks such as the development of models and information support management methods in the conditions of hybrid warfare; as well as the creation of information technology of the targeted (target-oriented) distribution of information flows, based on the abovementioned models and methods. A number of scientific tasks were solved in the process of the research.

The introduction provides a general description of the work, which emphasizes its relevance, correspondence with scientific topics, scientific novelty and practical significance. It also contains the determined subject and object of the research, as well as the formulated purpose and objectives.

An analysis of the use of information in the military operations management was carried out in the first section "**Technologies of Information Wars**". The processes taking place during hybrid warfare and the emphasis on its information component were also considered in the section. It was managed to reveal the regularities of the non-military influence on the enemy efficiency increase and the troops (forces) support effectiveness in the process of military actions support, while applying the information technologies. As a result of the analyzed data synthesis, there were no scientific decisions found, regarding the automatic messages distribution in the military sphere through the assessment of the information impact of these messages on different segments of population and troops. Assuming that the information about the message recipient is in the message itself, and the message addresser can also be identified from the message, i.e. a necessary and sufficient condition, the task of information support

management is transformed into the task of processing natural language texts. It was determined that the effectiveness of the natural-language message recognition by the existing text analysis systems does not allow rapid information support management to ensure decision-making by the state, troops, etc. authorities. In this connection, it was suggested to create new integrated approaches to impact management and to implement such approaches through the creation of information systems and technologies that will be able to assess the efficiency of different ways of information influence and to effectively manage the process of these informational impacts' implementation management by automatically identifying messages' addressees. The main tasks of the research are also formulated in the section.

In the second section, "**Methodological bases of technology of information support management**", the use of the informational influence processes has been determined and grounded in order to improve the conduct of military operations. The recommendations concerning the application of the scientific and methodological basis of management of information support of the processes of influence are given. In this basis, two parts are identified: the search for ways to determine and change the awareness of counteragents of interaction and the calculation of information impact on these counterparties. The basic idea of this basis is to substantiate and formally present such scientific and methodological tools of management of influences that will provide significant improvement of information-analytical support of troops, ways of preparation and conducting of operations on informational influence on counteragent, carrying out of countermeasures and will be as informatively clear, simple, productive and will be minimal cost. The basic definitions of work are given: method of information management in the system of influence management; class of messages; form of influence; content of the form of influence; means of influence; identification of the necessary relation to the received information; awareness management in influences; information technology management information support; counteragent interaction; information support in hybrid war conditions. Information technology management information support (IT MIS) should be understood as a set of methods, processes and software, integrated for the purpose of collecting, processing, storing, distributing,

displaying and using information in the interests of information support of their own military units and forces and the impact on the enemy. Proceeding from this, the mathematical model of interdependence of influences and behavior of counteragents of interaction was proposed, which allowed formalizing the approach to the evaluation of the information that must be provided to the counterparty in order to ensure its corresponding reaction. As a result of this model, it became possible to determine the strategy of action of own forces: to apply such a set of non-force actions and means of their provision that would provide the enemy's desired reaction (withdrawal of troops, transferring them to secondary directions, abolishing offensive, etc.). It is proposed to evaluate the effects, due to the difference in the conditional and unconditional probabilities of reaction of counteragents to the interaction. This provided the definition of the most informative messages for groups of the population and the military and became the basis for improving the model of the information support management. All these results are a significant contribution to the scientific foundations of the impact management methodology. They provide a new way of addressing the problem of defining the awareness of counterparties in interaction and effective management of information influences with the best results.

The second section "**Methodological bases of information support management technology**" identifies and justifies the application of information influence processes to improve the conduct of military operations. It was recommended to use the scientific and methodological basis for processes of influence information support management, which consists of two elements: search of ways to identify and change information awareness of interaction counterparties and estimation of the information influence on them. *The main idea* of the basis is to substantiate and formally submit such scientific and methodical influences management tools which will provide significant improvement of information and analytical troops support, ways of preparation and conducting of information operations against the counter-agents, implementation of countermeasures, and will be maximally informatively clear, simple, productive and minimally costly. The basic definitions of the research given in the section are, as follows: methods of information management in the influence

management system; class of messages; form of influence; content of the form of influence; means of influence; identification of the necessary relation to the received information; awareness management in influences; information technology management of the information support; interaction counteragent; information support in hybrid war conditions. *Information technology management of information support* (IT MIS) is a set of methods, processes, software and hardware, integrated for the collection, processing, storage, distribution, display and use the information in the interests of information support of the own troops and forces and the impact on the enemy. Proceeding from this, a mathematical model of the influences interdependence and interaction counteragents behavior was proposed, which allowed to formalize the approach to the assessment of information that must be provided to the counterparty in order to receive the corresponding reaction. The application of this model has made it possible to determine the strategy of action of the own forces, which is, as follows: to use a set of non-coercive actions and means of their application, which will provide the desired reaction of the enemy (withdrawal of troops, their redeployment to secondary directions, cancellation of offensive, etc.) It was suggested to assess the impacts through the differences in conditional and unconditional possible reactions of the interaction counterparties. This allowed to define the most informative messages for groups of people and military men, and became the basis for the improvement of the information support management model.

All these results are a significant contribution to the scientific fundamentals of the influence management methodology. It allows us to approach the problems of defining the awareness of interaction counteragents and effective information influence management with the best results from the new point of view.

The third section, "**Models and method of information support management**", deals with the information support management of the processes of influence on interaction counteragents on the basis of the address-oriented distribution of natural-language text messages method. The interaction counteragents were classified according to the peculiarities of their perception of information. While considering the information environment of influence on counteragents, the classes of messages in terms of

functional influence roles were defined. It is noted that interaction counteragents awareness management includes addressing one or another information to specific consumers, and the addressee can be determined from the message itself. Therefore, the task of information support management was transformed into the task of processing natural-language texts with certain features. They do not determine the content (as most systems for the processing and analysis of natural-language texts do), but the recipient of the message, for which the probability of reaction is likely to increase. It was managed to add an option to scan messages that do not contain information about the recipient to whom this information may be the most influential. Unlike the task of determining the impact on the enemy, it was decided to select the classes of counteragents for each message, which will be influenced the most. On the basis of the previous classification, an integrated expert assessment of the subjective probability of implementing one of the attributes of the model was formed, provided that another will be implemented. On these probabilities one can judge the subjective relation of experts to the application of various forms of information representation in different conditions. Taking into account the obtained results, a new vision of the information support management method in the processes of information influence in the conditions of hybrid warfare was formulated. This allowed to deal with the automatic distribution of messages according to the messages which are the most favorable for interaction counteragents classes. Having applied the probabilistic-reflexive approach, the model for identifying the most informative components of the natural-language text, provided the position of automatic addressing of these messages to different classes of counterparts, was improved. The reflex method of automatic response to the message content was developed by combining the model of interdependence between influences and behavior and the model of determining the most informative components of the natural language text, but not in relation to the impact on interaction counteragents, but in relation to the definition of the information addressee. The proposed method allowed to solve the problem of automatic determination of the addressee.

The fourth section "**Implementation of the information support management technology**" contains the basic principles of information support technology

mechanism. The functional and non-functional requirements for similar systems are presented in the section, as well as the criteria of the quality of the functioning of the information support technology of the processes of influence on the interaction counteragents. It resulted in the establishment of the general information support technology structure and in the development of the information technology structure in the form of a data scheme, its essence, attributes and identifiers of elements were presented in the form of tables. The logical and physical models of the database were constructed and described in the section. The Adres program, capable of analyzing messages of the natural language and automatically addressing them to certain interaction counterparties, has been developed. The obtained results of the experimental research have practically proved the ability of the Adres software to automatically identify the recipients of messages in order to target (selective) information influence on interaction counteragents. The results of the Adres software work are highly convergent with the mathematical calculations performed in the dissertation, which proves the adequacy of the proposed mathematical models and the reliability of the scientific statements and conclusions obtained in the work.

The results of the work were used in the research work at Military Institute of Taras Shevchenko National University of Kyiv, they were introduced into the information support of the services of the Project Office of Reforms of the Ministry of Defense of Ukraine, the production activities of LLC "Aviation Production Company SG "Skaeton ", the permanent work of the Information Technologies Department of the Ministry of Defense of Ukraine And in the educational process at Taras Shevchenko National University of Kyiv.

Keywords: information technology, management effects, contractor interaction, information support, reflex approach.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

Список публікацій здобувача в яких опубліковані основні наукові результати дисертації:

1. Кубявка М. Б. , Кубявка Л. Б. Модель інформаційної дії на контрагентів впливу. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2016. № 3(27). С. 54–58.

2. Кубявка М. Б. Математична модель несилої взаємодії в інформаційній технології інформаційного супроводження. *Information Technology and Security*. 2016. Vol. 4, No. 2 (7). P. 206–212.

3. Кубявка М. Б. Управління інформаційними впливами на противника з врахуванням поточної ситуації. *Збірник наук. праць Військового інституту Київського націон. ун-ту ім. Шевченка*. 2016. №53. С. 99–104.

4. Кубявка М. Б. Інформаційні дії по формуванню необхідної інформованості контрагента впливу. *Телекомунікаційні та інформаційні технології*. 2016. №4. С. 24–28.

5. Кубявка М. Б., Тесля Ю. М., Кубявка Л. Б. Визначення міри впливу на противника в інформаційній технології супроводження процесів підготовки та проведення військових операцій. *Збірник наук. праць Військового інституту Київського націон. ун-ту ім. Шевченка*. 2017. №55. С. 135–144.

6. Кубявка М.Б., Тесля Ю. М., Кубявка Л. Б. Інформаційна технологія управління інформаційним супроводженням. *Науково-технічний збірник “Управління розвитком складних систем” Київського націон. унів-ту будівництва і архітектури*. 2017. №29. С. 95–102.

7. Кубявка М.Б., Тесля Ю. М., Кубявка Л. Б. Рефлекторний метод управління інформаційним супроводженням військ (сил). *Збірник наук. праць Харківського націон. унів-ту Повітряних Сил*. 2017. №1(50). С. 48–53.

Список публікацій здобувача, які засвідчують апробацію матеріалів дисертації:

8. Кубявка Л. Б., Кубявка М. Б. Протидія впливам в програмах інформатизації вищих навчальних закладів. *Сучасні інформаційні технології в економіці та управлінні підприємствами, програмами, проектами*: матеріали XII Міжнарод. наук.-практ. конф. (м. Харків, 08–12 вересня 2014 р.). Харків, 2014. С.56–58.

9. Кубявка М. Б., Тесля Ю. М. Теорія несилової взаємодії як метод забезпечення інформаційної безпеки військ та держави в цілому. *Information Technologies & Interactions*: матеріали II Міжнарод. конф. (м. Київ, 3-5 листопада 2015 р.). Київ, 2015. С. 229–231.

10. Кубявка М. Б., Тесля Ю. М. Інформаційні технології на захисті інформаційного простору нашої держави. *Молодіжна військова наука у Київському націон. унів-ті ім. Тараса Шевченка*: матеріали Всеукр. наук.-практ. конф. молодих вчених, ад'юнктів, слухачів, курсантів і студентів. (м. Київ, 26 квітня 2016 р.). Київ, 2016. С. 64–65.

11. Кубявка М. Б., Кубявка Л. Б. Теорія несилової взаємодії - фундамент для побудови інформаційної технології супроводження процесів впливу на противника. *Інформаційні технології в освіті, науці і техніці*: матеріали III Міжнарод. наук.-практ. конф. (м. Черкаси, 12-14 травня 2016 р.). Черкаси, 2016. С. 63–64.

12. Кубявка М. Б., Тесля Ю. М., Кубявка Л. Б. Information management technology by non-forceful influence on the enemy during the preparation and conduction of military actions. *The 1th IEEE International Conference on Data Stream Mining & Processing*. (м. Львів, 23-27 серпня 2016 р.). Львів, 2016. С. 85–89.

13. Кубявка М. Б., Кубявка Л. Б. Інформаційна технологія формування необхідної інформованості у контрагентів взаємодії. *Спільні дії військових формувань і правоохоронних органів держави: проблеми та перспективи*: матеріали III Всеукр. наук.-практ. конф. (м. Одеса, 22-23 вересня 2016 р.). Одеса, 2016. С. 151–152.

14. Кубявка М. Б. Поточна ситуація в управлінні інформаційними впливами. *Information Technologies & Interactions*: матеріали III Міжнарод. наук.-практ. конф. (м. Київ, 8-10 листопада 2016 р.). Київ, 2016. С. 85–89.

15. Кубявка М. Б., Кубявка Л. Б. Концептуальна модель визначення необхідних інформаційних впливів на противника. *Національна безпека України: актуальні проблеми та шляхи їх вирішення*: матеріали II Всеукр. курсантсько-студентської наук.-практ. конф. (м.Одеса, 24 листопада 2016 р.). Одеса, 2016. С. 148–150.

16. Кубявка М. Б., Тесля Ю. М. Формування необхідної інформованості контрагента впливу. *Військова освіта і наука: сьогодення та майбутнє*: матеріали XII Міжнарод. наук.-практ. конф. (м. Київ, 25 листопада 2016 р.). Київ, 2016. С. 57.

17. Кубявка М. Б., Кубявка Л. Б. Метод автоматичного визначення адресата повідомлення на основі використання ймовірно-рефлекторного підходу. *Прикладні науково-технічні дослідження*: матеріали I Міжнарод. інтернет-конф., АТН України. (м. Івано-Франківськ, 5 квітня 2017 р.). Івано-Франківськ, 2017. С.20–21.

18. Кубявка М. Б., Тесля Ю. М., Кубявка Л. Б. Модель визначення найбільш інформативних компонентів природно-мовного тексту з позиції автоматичної адресації цих повідомлень різним класам контрагентів. *Інформаційна безпека та комп'ютерні технології*: матеріали II Міжнарод. наук.-практ. конф. (м. Кропивницький, 20-22 квітня 2017 р.). Кропивницький, 2017. С.192–193.

19. Кубявка М. Б., Кубявка Л. Б. Рефлекторний метод автоматичного реагування на зміст повідомлення. *Молодіжна військова наука у Київському націон. унів-ті ім. Тараса Шевченка*: Всеукр. наук.-практ. конф. молодих вчених, ад'юнктів, слухачів, курсантів і студентів. (м. Київ, 28 квітня 2017 р.). Київ, 2017. С. 91–92.

Список публікацій здобувача, які додатково відображають наукові результати дисертації:

20. Kubiavka N. B. The control of information support of the processes of influence on the opponent. *Збірник наук. праць Військового інституту Київського націон. ун-ту ім. Шевченка*. 2016. №54. С. 171–178.

21. Кубявка М. Б., Тесля Ю. М., Кубявка Л. Б. Основи інформаційних технологій супроводження процесів впливу на контрагентів взаємодії. *Збірник наук. праць Військового інституту Київського націон. ун-ту ім. Шевченка*. 2016. №52. С. 123–128.

22. Кубявка М. Б., Кубявка Л. Б. Концептуальна модель визначення необхідних інформаційних впливів на противника. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2016. №2(26). С. 44–47.

23. Тесля Ю. М., Кубявка М. Б., Кубявка Л. Б. Можливості застосування теорії несилового впливу в військовій контррозвідці. *Scientific Journal “ScienceRise”*. 2015. №2/1(7). С. 18–22.

24. Кубявка М. Б., Кубявка Л. Б., Миколенко А. О. Інформаційні технології - як засіб несилового впливу під час підготовки та проведення бойових дій. *International Journal “Information Technologies & Knowledge”*. 2014. Vol. 8. No. 4. p. 380–382.

25. Kubiavka L. B., Kolomiets A. S, Kubiavka N. B. Applying the theory of non-forceful cooperation in influence management, on project human resources. *Nauka i Studia*. 2016. No. 20(151). p. 94–99.

26. Тесля Ю. М., Кубявка М. Б., Кубявка Л. Б., Миколенко А. О. Використання технологій інформаційного впливу під час підготовки та проведення бойових дій. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2014. №2 (20). С. 147-152.

1.

ЗМІСТ

ВСТУП	19
РОЗДІЛ 1. ТЕХНОЛОГІЇ ІНФОРМАЦІЙНИХ ВІЙН	27
1.1. Аналіз інструментів впливу в інформаційних війнах	27
1.2. Технології супроводження інформаційних війн	32
1.3. Управління інформаційним супроводженням процесів впливу на противника.....	36
1.4. Аналіз сучасних технологій управління інформаційним супроводженням в процесах обробки природномовних текстів.....	40
1.5. Гібридна війна.....	46
1.6. Постановка задачі досліджень	49
Висновки до розділу 1	51
Список використаних джерел.....	51
РОЗДІЛ 2. МЕТОДОЛОГІЧНІ ОСНОВИ ТЕХНОЛОГІЇ УПРАВЛІННЯ ІНФОРМАЦІЙНИМ СУПРОВОДЖЕННЯМ	62
2.1. Термінологічний базис досліджень. Основні поняття та визначення....	63
2.2. Концептуальна модель визначення необхідних інформаційних впливів на контрагентів взаємодії	66
2.3. Модель впливу на контрагентів взаємодії.....	71
2.4. Математична модель взаємозалежності впливів та поведінки контрагента взаємодії.....	89
Висновки до розділу 2	93
Список використаних джерел.....	95
РОЗДІЛ 3. МОДЕЛІ ТА МЕТОД УПРАВЛІННЯ ІНФОРМАЦІЙНИМ СУПРОВОДЖЕННЯМ	97
3.1. Управління інформаційним супроводженням процесів впливу на контрагента взаємодії.....	97
3.2. Інформаційне середовище впливу на контрагента взаємодії	105
3.3. Метод адресно-орієнтованого управління інформаційним супроводженням	106

3.4. Експертний аналіз зв'язку класів контрагентів інформаційної взаємодії з класами повідомлень.....	117
Висновки до розділу 3	118
Список використаних джерел.....	120
РОЗДІЛ 4. РЕАЛІЗАЦІЯ ТЕХНОЛОГІЇ УПРАВЛІННЯ ІНФОРМАЦІЙНИМ СУПРОВОДЖЕННЯМ.....	121
4.1. Структура технології інформаційного супроводження.....	122
4.2. База даних інформаційної технології управління інформаційним супроводженням	124
4.3. Алгоритм визначення адресності повідомлення у інформаційній технології супроводження процесів впливу.....	130
4.4. Програмне забезпечення інформаційної технології управління інформаційним супроводженням.....	134
4.5. Експериментальне дослідження інформаційної технології управління інформаційним супроводженням.....	142
Висновки до розділу 4	154
Список використаних джерел.....	156
ВИСНОВКИ.....	159
ДОДАТОК А – АКТИ ПРО ВПРОВАДЖЕННЯ РЕЗУЛЬТАТІВ ДИСЕРТАЦІЙНОГО ДОСЛІДЖЕННЯ	163
ДОДАТОК Б – ЕКСПЕРТНА ОЦІНКА КЛАСУ ПОВІДОМЛЕНЬ	170
ДОДАТОК В – СХЕМАТИЧНЕ ПРЕДСТАВЛЕННЯ ФІЗИЧНОЇ МОДЕЛІ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ УПРАВЛІННЯ ІНФОРМАЦІЙНИМ СУПРОВОДЖЕННЯМ	185
ДОДАТОК Д – ГРАФІЧНА ВІЗУАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ПРОВЕДЕНИХ ДОСЛІДЖЕНЬ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ УПРАВЛІННЯ ІНФОРМАЦІЙНИМ СУПРОВОДЖЕННЯМ	190
ДОДАТОК Е – СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ ТА ВІДОМОСТІ ПРО АПРОБАЦІЮ РЕЗУЛЬТАТІВ ДИСЕРТАЦІЇ	195

ВСТУП

Актуальність теми. Розвиток інформаційно-орієнтованого суспільства формує новий контекст протистояння, в тому числі збройного. Такому новому типу конфлікту, як гібридна війна, приділяється значна увага у наукових працях як в Україні, так і за її межами. Відомо, що гібридна війна базується на значному інформаційному впливі країни-агресора на населення, інфраструктуру і економіку країни-цілі агресії. Інформаційна війна на сьогодні є буденною складовою сучасного суспільства. Шляхом заперечення чи викривлення фактів можна легко маніпулювати населенням, переконувати політиків. Тому інформаційний вплив можливо розглядати як одну з передумов для гібридної агресії, її складовою.

У інформаційного впливу є два вектора: наступаючий (вплив на цільову аудиторію контрагента) і оборонний (вплив на власну цільову аудиторію). Управління інформаційними впливами за обома векторами передбачає адресно-орієнтоване управління інформаційними потоками, а саме: керованого автоматичного розподілення повідомлень за їх адресністю, на основі розпізнавання змісту природномовного повідомлення. На сучасному етапі розвитку суспільства існує багато інформаційних систем, які здійснюють аналіз природномовних текстів, проте ефективність розпізнавання змісту природної мови у них невелика. Це в першу чергу зумовлено використанням ресурсномістких функцій логічно-семантичного аналізу, що робить програми обробки текстів занадто складними та повільними, що є недопустимим при динамічному характері інформації, зокрема, в бойовій обстановці, де від якості і швидкості її отримання залежить прийняття оптимальних управлінських рішень. Наявні на сьогоднішній час системи аналізу і обробки природних мов не спроможні, також, реалізувати функцію автоматичного адресно-орієнтованого розподілу природномовних текстових повідомлень, що значно могло б зменшити час доведення інформації до її адресата.

Динамічний характер інформаційних потоків, як у військовій так і в політичній, соціокультурній, техніко-економічній сферах, вимагає створення

предметно-орієнтованих науково-методичних, організаційних та програмно-інформаційних інструментів управління потоками інформації. А для цього необхідна розробка методів і способів адресно-орієнтованого управління інформаційним супроводженням процесів інформаційного впливу, як комплексу заходів, направлених на забезпечення інформацією (інформаційну підтримку) процесів діяльності в організаційно-технічних системах, зокрема, в військових.

Враховуючи вище викладене, для того, щоб мати можливість ефективно управляти інформаційним супроводженням процесів інформаційного впливу необхідно навчитись розподіляти повідомлення за їх адресністю, тобто направляти інформацію тим споживачам, яким вона необхідна і забезпечити їх обмеження від зайвих (не релевантних) повідомлень. А для цього необхідно, в першу чергу, створити науковий базис управління інформаційним супроводженням процесів інформаційного впливу в умовах гібридної війни.

Отже, виникає актуальна наукова задача – управління інформаційним супроводженням процесів інформаційного впливу, які можливо реалізувати в складних умовах, пов'язаних із значною кількістю негативних інформаційних впливів в умовах гібридної війни.

Рішення цієї задачі потребує розвитку теоретичних основ і методів управління інформаційним супроводженням, як в умовах гібридної війни, так і при постійному інформаційному забезпеченні життєдіяльності країни, фундамент яких закладено завдяки значній науковій діяльності багатьох вчених, у першу чергу: Горбуліна В.П., Загорки О.М., Замаруєвої І.В., Ланде К.В., Пермякова О.Ю., Петрика В.М., Поспелової Г.С., Рачинського А.П., Рось А.О., Руснака І.С., Самохвалова Ю.Я., Сбітнева А.І., Снитюка В.Є., Теслі Ю.М., Телелима В.М., Толюпи С.В. та інших авторів.

Актуальність теми дисертаційного дослідження обумовлена відсутністю в методології інформаційного супроводження моделей і методів автоматичного визначення адресатів повідомлень на основі аналізу змісту цих повідомлень.

Все вищезазначене і зумовило вибір теми дисертаційної роботи, її мету, дослідницькі завдання.

Зв'язок роботи з науковими програмами, планами, темами.

Дисертаційна робота виконана у відповідності з планами науково-дослідних робіт Військового інституту Київського національного університету імені Тараса Шевченка за темою «Автоматизована система розповсюдження інформаційних матеріалів на web- ресурси» Шифр: «Вектор-С» (№ держреєстрації 0101U002293, 2017 р.), де автором запропонований підхід до вибору шляхів адресування інформаційних матеріалів на web- ресурси [56].

Тему дисертаційного дослідження затверджено вченою радою Військового інституту Київського національного університету імені Тараса Шевченка (протокол № 7 від 22 січня 2015 р.) та перезатверджено (протокол № 14 від 27 березня 2017 р.)

Робота відповідає пріоритетним напрямкам розвитку науки і техніки в Україні в області інформаційних та комунікаційних технологій.

Мета і завдання дослідження. Метою роботи є підвищення ефективності управління інформаційним супроводженням процесів інформаційного впливу в умовах гібридної війни за рахунок створення та використання моделей, методів і засобів автоматичного визначення адресатів повідомлень за їх змістом.

Для досягнення цієї мети в роботі сформульовані і вирішені наступні **наукові завдання:**

- аналізу моделей, методів та засобів інформаційного супроводження процесів впливу в умовах гібридної війни;
- виявлення причинно-наслідкових зв'язків між інформаційним впливом та інформованістю контрагентів взаємодії;
- обґрунтування застосування процесів інформаційного впливу для вдосконалення проведення військових операцій та розробки концепції несилового впливу на контрагентів взаємодії з метою спонукання їх до задуманих агентами впливу дій;
- розробки моделі взаємозалежності впливів та поведінки контрагентів взаємодії;
- розробки моделі визначення найбільш інформативних компонентів

природномовного тексту, з позиції автоматичної адресації цих повідомлень різним класам контрагентів;

– розробки моделі та методу автоматичного розподілу інформаційних потоків за рахунок реагування на зміст повідомлень під час супроводження процесів інформаційного впливу;

– створення інформаційної технології адресного (цілеорієнтованого) розподілу інформаційних потоків.

Об’єктом дослідження є процеси автоматичного розподілу інформації і управління прийняттям рішень про адресатів повідомлень (контрагентів взаємодії).

Предметом дослідження є моделі та методи розподілу повідомлень за рахунок автоматичного реагування на їх зміст під час супроводження процесів інформаційного впливу.

Методи дослідження. Для вирішення зазначених завдань були використані методи теорії систем, теорії несилової взаємодії, методології управління проектами, теорії ймовірностей, експертних методів, розрахунково-аналітичного та статистичного методів. Теорія систем застосована для створення організаційних та технологічних інструментів управління інформацією. Математичний апарат теорії несилової взаємодії застосований для створення моделей і методів управління інформованістю контрагентів взаємодії, а саме, для розробки інструментів несилового організаційного управління. Інструменти методології управління проектами використані для розробки структури технології супроводження процесів впливу. Крім того, метод декомпозиції застосований для розробки структур та управління інформованістю. Методи теорії ймовірностей застосовані для розрахунку ймовірності наслідків інформаційних впливів та ймовірності отримання потрібного результату при таких впливах. Для аналізу та класифікації різноманітних впливів використано метод експертних оцінок. Розрахунково-аналітичний метод та статистичний метод (статистична оцінка впливу) використані для числової оцінки величини інформаційного впливу.

Наукова новизна одержаних результатів. Основний науковий результат дисертаційної роботи полягає в створенні теоретико-методичної основи технології управління інформаційним супроводженням процесів інформаційного впливу на контрагентів взаємодії в умовах гібридної війни.

У результаті дослідження автором отримано наступні наукові результати:

1. Уперше запропонована модель взаємозалежності впливів та поведінки контрагентів взаємодії, яка базується на розрахунку відхилень умовних та безумовних ймовірностей реакцій контрагентів взаємодії дозволяє формалізувати підхід до оцінки інформації, яку необхідно надати контрагенту з тим, щоб забезпечити його відповідну реакцію;

2. Уперше розроблено рефлекторний метод автоматичного реагування на зміст повідомлення, що забезпечує адресно-орієнтовне управління інформаційним супроводженням процесів інформаційної дії. Науковий результат полягає у поєднанні моделі взаємозалежності впливів та поведінки і моделі визначення найбільш інформативних компонентів природномовного тексту. Розроблений метод дозволив автоматично розподіляти повідомлення за найбільш сприятливими до цих повідомлень класами контрагентів інформаційного впливу;

3. Удосконалено модель управління інформаційним супроводженням, яка базується у визначенні найбільш інформативних повідомлень для груп населення та військових за рахунок оцінки умовних ймовірностей їх реакції. Запропоноване удосконалення моделі управління інформованістю контрагентів взаємодії відрізняється від існуючих оцінюванням впливу, через різницю в умовних та безумовних ймовірностях реакцій контрагентів та забезпечує визначення найбільш інформативних повідомлень для груп населення та військових;

4. Удосконалено модель визначення найбільш інформативних компонентів природномовного тексту, характерних для гібридної війни, з позиції автоматичної адресації цих повідомлень різним класам контрагентів. Модель базується на використанні ймовірнісно-рефлекторного підходу для визначення адресата повідомлень та відрізняється від існуючих ідентифікацією різниці в умовних ймовірностей появи адресатів повідомлень як величини інформаційного впливу

фрагментів природномовного тексту, що дозволило автоматично визначати адресатів повідомлень.

У сукупності отримані результати утворюють теоретико-методичну основу технології управління інформаційним супроводження процесів несилового впливу на контрагентів взаємодії в умовах гібридної війни.

Практичне значення одержаних результатів. На базі розроблених моделей і методів були запропоновані практичні інструменти управління інформаційним супроводженням процесів інформаційного впливу через реалізацію методик, алгоритмів, структур процесів та програмного засобу адресно-орієнтованого розподілу природномовних текстових повідомлень.

Практичне значення дисертаційної роботи полягає у можливості застосування отриманих результатів у роботі підрозділів спеціальних операцій для підготовки у здійсненні цілеорієнтованого інформаційного впливу на визначених контрагентів взаємодії, як складової процесів, що відбуваються в умовах гібридної війни. Розроблені програмні засоби включають в себе, компоненти формування вхідних даних, компоненти адресно-орієнтованого розподілу повідомлень, компоненти аналізу результатів. Крім того розроблені рекомендації щодо впровадження цих засобів у підрозділах спеціальних операцій.

Результати дисертаційної роботи впроваджені:

- в інформаційному забезпеченні процесів управління військами, службами, підрозділами в умовах гібридної війни. Розроблені засоби автоматично розподіляють повідомлення тим адресатам, які їх потребують. Це оптимізувало обсяг інформації, що надходить до адресатів і дозволило скоротити витрати і підвищити точність обробки повідомлень (акт впровадження від 03 квітня 2017 року №71/04-П, акт впровадження від 10 квітня 2017 року та акт впровадження від 12 квітня 2017 року №183/2/387);

- у навчальному процесі. Матеріали дослідження були використані при викладанні дисципліни “Методи інформаційної розвідки та впливів” магістрам вищих навчальних закладів спеціальності “Консолідована інформація” та освітньої програми “Інформаційна аналітика та впливи” (довідка про

впровадження від 10 квітня 2017 р.), у навчальному процесі для студентів III курсу Інституту філології, спеціальності 035.10 “Прикладна лінгвістика” (довідка про впровадження від 25 травня 2017 р.), а також враховані при підготовці навчальної та наукової літератури з цієї тематики.

Особистий внесок здобувача. Наукові положення, розробки та висновки дисертаційної роботи є результатом самостійно проведеного автором дослідження. Основні наукові результати, що представлені в дисертації отримані здобувачем особисто. Автору, в працях, що опубліковані у співавторстві, належить наступне: [7] - модель інформаційного впливу на контрагентів взаємодії, [5] – математичний опис міри інформаційного впливу на контрагента взаємодії, [6] – розробка, створення бази даних, графічний дизайн, опис, тести, [7] – формулювання рефлекторного методу, проведення розрахунків на його основі, [21] – дано основні визначення роботи, [22] – формулювання концептуальної моделі інформаційних впливів, [23] – запропоновано використати теорію несилової взаємодії в роботі військової контрозвідки, [24] – ідея реалізації несилових впливів в інформаційній технології, [25] – міркування щодо застосування теорії несилової взаємодії в управлінні впливами на проектні людські ресурси, [26] – аналіз застосування інформаційного супроводження для інформаційного забезпечення сил військових операцій.

Апробація результатів. Основні результати і дисертаційна робота в цілому апробовані на 12-ти Міжнародних та Всеукраїнських науково-практичних конференціях: XII Міжнародна науково-практична конференція «Сучасні інформаційні технології в економіці та управлінні підприємствами, програмами, проектами» (м. Харків, 08–12 вересня 2014 р.); II Міжнародна конференції: «Information Technologies & Interactions» (м. Київ, 3-5 листопада 2015 р.); Всеукраїнська науково-практичної конференції молодих вчених, ад’юнктів, слухачів, курсантів і студентів «Молодіжна військова наука у Київському національному університеті імені Тараса Шевченка» (м. Київ, 26 квітня 2016 р.); III Міжнародна науково-практична конференція «Інформаційні технології в освіті, науці і техніці» (м. Київ, 12-14 травня 2016 р.); «The 1th IEEE International

Conference on Data Stream Mining & Processing» (м. Львів, 23-27 серпня 2016 р.); III Всеукраїнська науково-практична конференція «Спільні дії військових формувань і правоохоронних органів держави: проблеми та перспективи» (м. Одеса, 22-23 вересня 2016 р.); III Міжнародна науково-практична конференція «Information Technologies & Interactions» (м. Київ, 8-10 листопада 2016 р.); II Всеукраїнська курсантсько-студентська науково-практична конференція «Національна безпека України: актуальні проблеми та шляхи їх вирішення» (м. Одеса, 24 листопада 2016 р.); XII Міжнародна науково-практична конференція «Військова освіта і наука: сьогоднішня та майбутня» (м. Київ, 25 листопада 2016 р.); I міжнародна інтернет-конференція «Прикладні науково-технічні дослідження» (м. Івано-Франківськ, 5 квітня 2017 р.); II Міжнародна науково-практична конференція «Інформаційна безпека та комп'ютерні технології» (м. Кропивницький, 20-22 квітня 2017 р.); Всеукраїнська науково-практична конференція молодих вчених, ад'юнктів, слухачів, курсантів і студентів «Молодіжна військова наука у Київському національному університеті імені Тараса Шевченка» (м. Київ, 28 квітня 2017 р.).

Публікації. Основні результати дисертаційної роботи опубліковані у 26 наукових працях, серед яких 11 статей у фахових виданнях, зарубіжних статей - 2, в інших виданнях - 1, а також 12 робіт – в матеріалах конференцій.

Структура й обсяг роботи. Дисертація складається зі вступу, чотирьох розділів, висновків, містить 14 таблиць і 34 рисунка, список використаних джерел загальною кількістю 152 найменування, що розміщені на 14 сторінках, 5 додатків, що розміщені на 38 сторінках. Загальний обсяг дисертаційної роботи - 199 сторінок друкованого тексту. Основний текст викладений на 140 сторінках.

Робота виконана у науково-дослідному центрі військового інституту Київського національного університету імені Тараса Шевченка.

РОЗДІЛ 1

ТЕХНОЛОГІЇ ІНФОРМАЦІЙНИХ ВІЙН

1.1. Аналіз інструментів впливу в інформаційних війнах

У третьому тисячолітті, на тлі переходу людства від індустріальної до інформаційної цивілізації, інформація стала однією з головних складових історичного прогресу. Вона має ключове значення для успішного функціонування всіх суспільних і державних інститутів, адекватного поведіння кожної окремої людини. Інформація необхідна кожній людині як умова, так і засіб її існування у суспільстві [41], [44].

На сучасному етапі швидко зростає значення непрямих (м'яких) методів впливу на перебіг політичних та економічних процесів в державах [1], [4], [5], [10], [13]. Провідне місце серед, так званих м'яких методів впливу звісно посідають інструменти несилового (інформаційного) впливу [86]. І в цьому основна тенденція розвитку суспільства – перехід від фізичних способів ведення воєнних дій (знищення або примус), до несилової зміни відношення людей до ворогуючої сторони – від ненависті до прийняття. Подібна тенденція спостерігається в усьому світі [4], а 95% всіх підіривних зусиль за відношенням до іншої держави, займає інформаційна війна.

Впливам на масову та індивідуальну свідомість присвячена значна кількість наукових праць в різних сферах діяльності людства [14], [16], [18], [34], [35], [46], [51], [52], [53], [54], [60], [62], [63], [69], [76], [80], [89], [92], [94], [95], [96]. Приділяється значна увага створенню власних систем впливу на супротивника та захисту союзників, власного народу і армії від дії спеціальних інформаційних операцій інших держав [20], [27], [28], [32], [38], [45], [64], [67], [68], [71], [72], [74], [75], [79].

З давніх часів було відомо, що справжньою перемогою є лише така, що не містить у собі зерен реваншу. Після неї немає руйнувань, а супротивник не

відчуває себе переможеним. «Найкраще з найкращого – перемогти супротивника без боротьби» [42].

Запорукою такої перемоги є успіх у боротьбі за свідомість людей (супротивників, союзників та власного народу і армії). Саме цю мету передбачають дії, що отримали останніми кількома роками назву спеціальних інформаційних операцій.

Загальновідомим є те, що вплив на масову та індивідуальну свідомість реалізують за допомогою методів пропаганди [54].

Провівши аналіз, можна стверджувати, що під час здійснення спеціальних інформаційних операцій активно використовуються пропагандистські методи, але арсенал спеціальних інформаційних операцій вони не вичерпують. Насамперед суттєвим є те, що до цього арсеналу входить і організація подій. Не тільки псевдо, а й так званих реальних [76].

Поступові зміни у суспільстві ведуть до радикальних перетворень механізмів соціального контролю. Замість традиційних методів та механізмів, що базуються на прямому застосуванні або загрозі застосування насильства, дедалі більшої ваги набувають м'які методи, тісно пов'язані з використанням засобів впливу на свідомість [57], [66].

Дослідники вважають, що інформаційні операції у межах концепції «м'якої сили» (“SoftPower”) набувають значення одного з найважливіших інструментів у вирішенні сучасних, а тим більш майбутніх конфліктів [5].

Останніми роками неабиякої популярності набули дослідження проблем створення та застосування інформаційної зброї, а також захисту від неї. Спеціальні інформаційні операції зараз визнаються багатьма дослідниками як невід'ємний, навіть ключовий елемент доктрини інформаційних воєн. Так само розглядає тематику спеціальних інформаційних операцій і нова доктрина Пентагона «Інформаційні війни» [2].

Цікаві думки щодо місця спеціальних інформаційних операцій у загальному контексті інформаційних воєн репрезентує Л.С.Джонсон [4]. Згідно з його твердженнями, суттю будь-якої інформаційної війни є реалізація впливу на

інформаційний масив. Інформаційний масив можна розглядати як певну сукупність повідомлень. Ще з часів К.Шеннона (середина XX ст.) відомо, що впливи можуть бути двох основних типів: вплив безпосередньо на повідомлення, на їхню форму, механізми передачі, збереження, обробку тощо; вплив на зміст повідомлень.

Спеціальні інформаційні операції реалізують впливи другого типу [22].

На військовому рівні інформаційні операції являють собою комплекс заходів, які проводяться у масштабах збройних сил, їх видів, і є складовою частиною воєнної кампанії. Вони спрямовані на досягнення інформаційної переваги над противником (у першу чергу – в управлінні військами) та на захист своїх систем управління.

Базовим офіційним документом з проблематики, що досліджується, у США є польовий статут Збройних Сил США FM 33-1 «Психологічні операції» [69]. У ньому наведено таке визначення спеціальних інформаційних операцій: «У широкому розумінні ПсО - це сплановане використання засобів, форм і методів поширення інформації для певного впливу на настанови та поведінку людини. У вузькому розумінні ПсО використовуються збройними силами для деморалізації та дезорієнтації супротивника». Як відзначається у матеріалах Армії США, «основна мета спеціальних психологічних операцій полягає у забезпеченні змін поведінки союзників і супротивників США у сприятливому для країни напрямі» [14].

Управління стратегічних служб, попередник ЦРУ, мало у своєму штаті відділ інформаційних операцій. Діяльність цього підрозділу була спрямована насамперед проти гітлерівської Німеччини та виявилася вельми ефективною на останньому етапі війни [95].

Перша масова операція, що мала назву психологічної, була здійснена Збройними силами США на підтримку військ ООН у Корейській війні (1950-1953 рр.) У 1951 р. у Міністерстві армії було створено Управління психологічних операцій, що в 1955 р. реформувалося в Управління спеціальних методів війни. Тоді ж розпочалася підготовка спеціальних кадрів [89]. Масштабно

застосовувалися війська ПсО у Панамі і у Перській Затоці, де американські фахівці здійснювали інформаційні операції проти режиму Саддама Хусейна, спрямовані на захист курдського населення, а також мусульман-шиїтів від політики Багдада [62].

Масштабні ПсО було здійснено й у межах операцій «Морський ангел» і «Підтримка демократії» (Гаїті, 1991, 1994 рр.), «Відродження надії» та «Спільний щит» (Сомалі, 1992-1995 рр.) [10], «Спільні зусилля» (Боснія, 1996 р.) [54]. Практично всі миротворчі компанії, в яких беруть участь США, супроводжуються психологічними операціями [58]. З них лише операція в Сомалі не досягла поставленої мети.

З 1996 р. США послідовно здійснюють низку спеціальних інформаційних операцій на Балканах. У цій операції активно використовують різноманітну символіку, наполегливо підкреслюється приналежність американської воєнної уніформи [35]. Активність американських спеціальних підрозділів на Балканах достатньо висвітлюється у різних джерелах, зокрема в Інтернеті [13].

За даними журналу «Мілітарірев'ю», якщо у Першій світовій війні один журналіст припадає на 20 тисяч, то під час операції в Боснії - на 500 військовослужбовців [18].

Нині у США діють системи здійснення спеціальних психологічних операцій у межах як ЦРУ, так і Міністерства оборони (Об'єднане командування спеціальних операцій). У країні створено струнку систему підготовки кадрів для ведення інформаційно-психологічної війни. Діють системи перепідготовки та підвищення кваліфікації, заохочується навчання офіцерів у магістратурі (докторантурі) [16].

Основним підрозділом інформаційних операцій в ЗС США є батальйон, що налічує від 200 до 400 чоловік і складається з груп спеціалістів радіо, телемовлення, підготовки листівок, пропагандистських текстів, спецефектів, планування, розвідки, допоміжних служб тощо. Цікавим прикладом подібного підрозділу було 193 спеціальне оперативне крило національної гвардії штату Пенсільванія [1]. Основним його завданням було здійснення певних

інформаційних операцій з застосуванням спеціальних літаків, радіо і телетрансляторів на базі С-130 (С-130Е/RR).

СРСР також мав певну традицію ведення інформаційних воєн. Початок використання так званих «активних заходів» радянською розвідкою офіційно датується 11 січня 1923 р., коли за поданням заступника Голови ДПУ І. С. Уншлихта було ухвалено рішення Політбюро ЦК РКП(б) про створення спеціального міжвідомчого Бюро з дезінформації [60].

Одним з непрямих свідчень ефективності дій цього підрозділу є той факт, що діяльність Бюро «не тільки практично не залишила в архівах розвідки жодних слідів з описами заходів, а й навіть опосередкованих посилок на тих, хто тією чи іншою мірою мав відношення до їх розробки» [60].

Активно діяли підрозділи спецпропаганди (вони входили до складу Головного політичного управління Червоної армії та НКВС СРСР) під час Великої Вітчизняної війни. Як свідчать сучасні дослідники, на другому етапі війни (після битви на Курській дузі) радянські інформаційні операції, спрямовані проти німецької армії, були досить ефективними [51].

Під час «холодної війни» у складі ПГУ КДБ СРСР (зовнішня розвідка) діяло Управління «А» [92], що виконувало завдання здійснення «активних заходів» (одним із напрямів цих заходів були спеціальні інформаційні операції) [52].

Як свідчать матеріали російської та іноземної преси, матеріали аналітиків, подібні підрозділи активно діють у ФСБ РФ і по сьогоднішній день [80]. Зокрема, великого розголосу набуло малоефективне застосування федеральними військами методів спеціальних інформаційних операцій у Чечні. Яскравим прикладом цього стала публікація книги «Інформаційна війна у Чечні» [35].

Події літа-осені 1999 р. у Дагестані продемонстрували, що Росія дійшла певних висновків з програшу у війні, що була в Чечні [96]. За короткий проміжок часу було організовано практично повну інформаційну блокаду чеченсько-дагестанських бойовиків, налагоджено достатньо оперативне висвітлення подій з театру воєнних дій. Але вже на початку вересня з'явилися ознаки можливості ісламістських екстремістів добитися переламу в інформаційному протиборстві.

Про це свідчить, наприклад, тон редакційного коментаря в «Общей газете» від 9 вересня 1999 р., оперативно розміщеного на сайті М.Удугова [94].

Системи здійснення спеціальних інформаційних операцій існують не тільки в США і Росії, а й у багатьох інших країнах, зокрема в Індії. У 1990 р. у Міністерстві оборони цієї країні було створено спеціальну службу інформаційних операцій. Свою роботу служба координує з комітетом начальників штабів ЗС Індії, військовою розвідкою, МЗС тощо [63].

Підрозділи спеціальних психологічних операцій у складі армій і спецслужб існують у Німеччині, Великобританії, Ізраїлі та інших розвинутих країнах.

Отже інформаційно-психологічний вплив є цілеспрямованою психологічною атакою на конкретні сфери психіки людини, групи осіб або суспільну свідомість у цілому. Вплив може здійснюватися засобами інформаційних подразників з використанням усього спектру методів і форм технічного, візуального, звукового, медикаментозного, фізичного, больового, віртуального придушення волі.

Актуальність безпеки нашої держави саме у цій, інформаційній сфері, підтверджує прийняття Верховною Радою України Закону України «Про основи національної безпеки України» (ВВР, 2003 № 39, ст. 351), який визначає протидію інформаційній експансії іноземних держав, однією з форм якої і є спеціальні інформаційні операції як один з напрямів політики національної безпеки [72]. Ця проблема - одна з ключових у контексті гарантування інформаційної безпеки держави.

1.2. Технології супроводження інформаційних війн

Динамічний розвиток інформаційних технологій призвів до появи інформаційної зброї та ведення інформаційних війн, які на сьогодні стають найнебезпечнішим інструментом ведення протистояння між державами [59], [65]. За допомогою інформаційної зброї здійснюється вплив на інформаційні ресурси протилежної держави та суспільну свідомість її населення [33]. Відповідно до

цього, за цільовою ознакою вона класифікується на інформаційно-технічну зброю, яка впливає на інформаційні ресурси, мережі і системи державного і військового управління та інформаційно-психологічну, яка впливає на психіку, свідомість, підсвідомість, морально-психологічний стан людини, соціальних груп та суспільства в цілому. Разом з тим, види цієї зброї визначаються засобами, які можуть застосуватися. Так, виходячи із засобів інформаційно-технічної зброї, вона поділяється на алгоритмічну, програмну і апаратну, а інформаційно-психологічна зброя – на пропагандистську, психофізичну, нейролінгвістичну, психотропну, психотронну, психогенну і психоаналітичну .

1.2.1. Класифікація інформаційної зброї

Провідний експерт Міністерства оборони України О.Л. Левченко в своїй роботі [50] пропонує найбільш узагальнене визначення цього терміну. *Інформаційна зброя* – це сукупність способів, прийомів, засобів і технологій інформаційного впливу на інформаційну інфраструктуру супротивної держави та психіку, свідомість і підсвідомість її населення та особового складу збройних сил.

Зазначена сукупність поділяється за різними ознаками, які пропонуються у відомих дослідженнях [15], [78], [79], [82]. Однією з найбільш повних можна вважати таку класифікацію інформаційної зброї: за метою застосування, за об'єктами впливу, за механізмами реалізації впливу, за реалізованими методами впливу, за характером впливу на інформацію та інформаційні процеси, за масштабом вирішуваних бойових завдань, за терміном дії. Разом з тим найбільш важливою у поділі інформаційної зброї на види, класи, групи тощо вбачається цільова ознака.

Відповідно до цільового призначення інформаційна зброя поділяється на інформаційно-технічну та інформаційно-психологічну. *Інформаційно-технічна зброя* – це зброя, яка впливає на інформаційні ресурси, мережі і системи державного і військового управління [50]. *Інформаційно-психологічна зброя* – це

зброя, яка впливає на психіку, свідомість, підсвідомість, морально-психологічний стан людини, соціальних груп та суспільства в цілому [23], [50].

1.2.2. Інтернет, як арена інформаційного протистояння

Людство щодня отримує інформацію з Інтернету, преси, радіопередач, телебачення. Перебуваючи тривалий час у світі відірваних від реальності символів, людина може навіть піти проти своїх власних інтересів, оскільки, реальність витісняється на другий план, відіграючи підлеглу роль. Втрачаючи зв'язок з реальним світом, людина втрачає свободу. Тим більше, вже відпрацьовано низку способів ефективного інформаційного впливу на неї. Існує такий термін — «Brainwashing» — «промивання мізків». За допомогою такого «промивання» може здійснюватися «зомбування» людей, формування пасивної й слухняної істоти, перетворення народу на легко керовану масу. У цьому сенсі, розмови про свободу, демократію, вільні вибори є містифікацією.

Засоби масової комунікації формують «масову» людину нашого часу. У той же час вони роз'єднують людей, витісняють традиційні безпосередні контакти, замінюючи їх телебаченням і комп'ютерами. Одночасне поширення суперечливих та взаємовиключних суджень ускладнює адекватну орієнтацію, породжує байдужість й апатію, породжує некритичність, викликає соціальну дезорієнтацію [37].

Американський дослідник Гарольд Ласуел виокремив чотири основні функції засобів масової інформації [43]: спостереження за світом (збір і поширення інформації); «редагування» (відбір і коментування інформації); формування суспільної думки; поширення культури.

Сукупність, спрямованих на підвищення ефекту мовного впливу, комунікативних засобів одержала назву «переконуючої комунікації». Г.Ласуелом, була запропонована модель комунікативного процесу [43]:

Хто? (передає повідомлення) — комунікатор.

Що? (передається) — повідомлення (текст).

Як? (здійснюється передача) — канал.

Кому? (спрямоване повідомлення) — аудиторія.

З яким ефектом? — ефективність.

Ключовою схемою для побудови PR-технологій залишається комунікаційна формула, запропонована Г. Ласуеллом. З метою розробки PR-програми, необхідно проаналізувати й оцінити комунікатора, зміст повідомлень, засоби комунікації, характеристики аудиторії й зміни у свідомості в результаті впливу повідомлень [43].

Мета будь-якої війни полягає в зміні поведінки супротивника, його силовому переміщенні до того «місця» структури міжнародної політики, яке йому відводиться переможцем. Однак, якщо всі попередні війни провадились шляхом знищення чи загрози знищення ворога до політичного моменту досягнення бажаного результату, то, за умов інформаційних воєн, протиборство може тривати як завгодно довго та з мінімальним застосуванням насильства [77].

Переможцем інформаційної війни стає та сторона, яка повніше здатна змоделювати поведінку супротивника в різних ситуаціях, визначити власний алгоритм поведінки, нарешті, реалізувати його. Максимально всеосяжне моделювання поведінки супротивника означає, у якомога більших обсягах, збирати, зберігати й обробляти інформацію про нього; а також знати й розуміти його історію, культуру, релігію, побут. Загальний алгоритм інформаційної війни [77] показаний на рисунку 1.1.

Для вирішення цього завдання найкращими інструментами є засоби обчислювальної техніки з відповідним програмним забезпеченням [39], [81]. Ситуаційне моделювання в режимі реального часу сьогодні цілком доступне високопродуктивним комплексам; проблема лише в реалізованій поведінковій моделі конкретних соціальних об'єктів та конкретних людей [36], [61]. І проблема ця тим краще вирішується, чим більше інформації є про об'єкти, які аналізуються й моделюються.

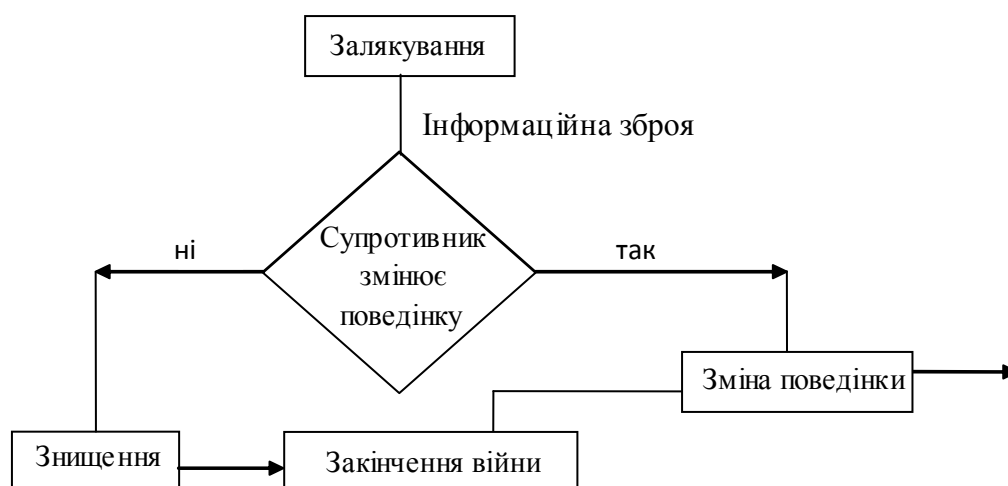


Рис.1.1. Узагальнена схема війни

1.3. Управління інформаційним супроводженням процесів впливу на противника

1.3.1. Інформаційні системи що самонавчаються

Кожна інформаційна система, залежно від її власної структури, має різну кількість базових елементів та зв'язків між ними.

Конкретні прийоми інформаційного впливу й типова стратегія інформаційної війни [77] відображені на рис. 1.2:

1 — здатність інформаційної системи, що самонавчається, цілеспрямовано перепрограмувати іншу подібну систему;

2 — для перепрограмування системи необхідно знайти в навколишньому світі або спеціально створити інформаційну систему, на яку б дана система була схожою, причому, обидві системи повинні бути «розуміючими» одна одну;

3 — перепрограмувати інформаційну систему — це значить підібрати для неї такі вхідні дані, які відповідають меті перепрограмування;

4 — за всіх часів найбезпечніше транслювати на оточення інформацію про переваги власного способу життя;



Рис. 1.2. Типова стратегія інформаційної війни

5 — підібрати вхідні дані для системи відповідно до заданої мети перепрограмування значить змусити інформаційну систему «дивитися на світ чужими очима», очима тієї інформаційної системи, на яку дана система повинна стати схожою, тобто очима еталона;

6 — «розуміючі» інформаційні системи формуються однаковиими емоційними впливами, як правило, минаючи засоби захисту, засновані на логіці;

7 — задля швидкого й масового перепрограмування народу, найбільш ефективними є прийоми, котрі мають емоційне забарвлення і належать до таких сфер, як: масова культура, мистецтво, релігія, що робить діячів мистецтва,

культури, релігійних служителів, політичних коментаторів пріоритетними об'єктами інформаційних впливів;

8 — чим більша потужність базових елементів та зв'язків між ними, тим система стійкіша до цілеспрямованого інформаційного впливу;

9 — ефективне перепрограмування стійких та стабільних систем передбачає попереднє приведення їх у хаотичний стан шляхом руйнування усталених зв'язків і знищення найбільш важливих базових елементів;

10 — за будь-якого серйозного інформаційного впливу на суспільство, головним напрямком інформаційного удару завжди будуть молоді члени суспільства, тобто об'єкти, котрі мають максимальний ресурс для перепрограмування.

Отже, аналіз основних теоретико-методологічних підходів до дослідження поняття інформаційних війн, дозволяє виділити два напрямки, що затвердилися в сучасній науковій літературі. Перший з них виходить із опису явища інформаційної війни через її вплив на масову свідомість, маніпулятивний потенціал і психологічний вплив інформаційних повідомлень. Другий підхід розглядає явище інформаційної війни як автономну систему в сучасному суспільстві за допомогою технічного та математичного понятійного апарата.

1.3.2. Комп'ютерні мережі та геоінформаційні системи в процесах інформаційної підтримки військ (сил)

Так, на даний час існує багато напрямів використання глобальної комп'ютерної мережі Інтернет в інтересах інформаційного протиборства. Тому варто розглянути найважливіші з цих напрямів.

Найпоширенішим напрямком використання глобальної мережі в інтересах військово-політичного протиборства є заміна вмісту сайтів, що полягає в підміні сторінок або їхніх окремих елементів шляхом злому. Такі диверсійні дії, переважно, здійснюються з метою привернення уваги до атакуючої сторони, демонстрації її можливостей, зрештою, способом задекларувати певну політичну

позицію. Крім прямої підміни сторінок, широко використовується реєстрація в пошукових системах сайтів протилежного змісту за однаковими ключовими словами, а також переспрямування (підміна) посилань на іншу адресу, що призводить до відкриття спеціально підготовлених конфронтуючою стороною сторінок [25].

Нині Інтернет дедалі активніше й масштабніше використовується в інтересах інформаційного протиборства сторін, які є учасниками різних конфліктів. Він створює широкі можливості для формування суспільної думки; впливу на прийняття політичних, економічних і воєнних рішень; дії на інформаційні ресурси супротивника й поширення спеціально підготовленої інформації (дезінформації).

Так в США був розроблений Національний план захисту інформаційних систем США та відкрита Комп'ютерна судова лабораторія Міністерства оборони (DefenseComputerForensicsLaboratory, DCFL) — одна з найсучасніших структур, призначена для обробки комп'ютерних доказів у розслідуванні злочинів та шахрайств, а також для надання експертної допомоги у проведенні контррозвідувальних заходів у випадку всіх організацій, що здійснюють кримінальні й контррозвідувальні дослідження. Ця лабораторія забезпечує підтримку ФБР з питань розслідування комп'ютерних злочинів [58].

Також значних успіхів в інформаційних технологіях людство досягло в застосуванні *геоінформаційних систем* (ГІС) [19], [25], [70]. Сучасні ГІС у збройних силах також знайшли широке застосування в оперативній підготовці органів військового керування, інформаційному забезпеченні бойових дій, уточненні топографічних карт, визначенні місця положення військ і окремих військовослужбовців, а також в інших сферах діяльності військ.

На даний час у війська за заявками керувань (служб) видів і родів військ постачається ГІС - «Інтеграція», бо жодна система високоточної зброї (ВТЗ) не може діяти без надійної системи навігації й топоприв'язки. Будь-який носій ВТЗ до його застосування повинен з певною точністю вийти в район пуску. У воєнних

діях у зоні Перської затоки СНС GPS надійно забезпечувала вихід авіації й корабельних засобів поразки в заданий район і точне наведення на ціль.

Як свідчить досвід проведення АТО, в сучасних умовах успіх має той, хто в найкоротший термін приймає правильні рішення. Одним із механізмів скорочення цих термінів є використання даних дистанційного зондування земної поверхні, цифрових (електронних) карт і геоінформаційних технологій за найкращими світовими стандартами. Так нашими науковцями було розроблено основу автоматизованої системи управління військами «Славутич», яка базується саме на геоінформаційній системі. Це електронна карта місцевості, яка в режимі реального часу, за допомогою електронних обчислювальних засобів, здатна визначити чимало параметрів. Наприклад, оптимальну траєкторію польоту вертольота з урахуванням полів ураження засобів ППО противника, а також використання захисних властивостей місцевості. Можливості цієї АСУ вже змогли оцінити під час випробувань у зоні проведення АТО та в Головному командному центрі Збройних Сил України [24].

Реалізація і впровадження ГІС дозволяє значно підвищити оперативність роботи органів державного і військового управління, спрощує роботу вищого командного складу різного рівня, а також значно підвищує ефективність виконання бойових завдань частинами і підрозділами Збройних Сил [24].

1.4. Аналіз сучасних технологій управління інформаційним супроводженням в процесах обробки природномовних текстів

Вважаючи, що інформація про те, кому направити повідомлення, є в самому повідомленні, а адресат повідомлення може бути визначений із самого повідомлення, що необхідною і достатньою умовою, задача управління інформаційним супроводженням трансформується в задачу обробки природномовних текстів, але з деякими особливостями, а саме:

1. Потрібно визначати не зміст (як робить більшість природномовних систем), а того адресата повідомлення, для якого ймовірність потрібно реакції збільшиться;

2. Потрібно «вміти» відсіювати повідомлення, в яких не міститься інформація про адресата, на якого ця інформація найбільше вплине.

З метою визначення спроможності існуючих засобів автоматичного визначення змісту природномовного тексту перейдемо до аналізу таких.

1.4.1. Аналіз існуючих інформаційно-аналітичних систем збирання, структуризації та аналітичної обробки неструктурованої інформації

В даний час в світі існують і активно розвиваються системи аналітичного (смыслового) пошуку в базах даних, які підтримуються провідними фірмами - виробниками серверів баз даних, наприклад Oracle, Microsoft, IBM і ін.

Наведемо декілька зразків використання сучасних інформаційних технологій у практиці інформаційно-аналітичної діяльності за Муковським І.Т. [55], ст. 112-114]:

Система моніторингу на базі WEB-OBSERVER являє собою автоматизовану систему збирання й структуризації інформації із відкритих Інтернет-джерел і корпоративних сховищ.

Основними функціями системи є: оперативне збирання інформації з підключених джерел; розподіл отриманої інформації за рубриками; сповіщення про місце знаходження інформації (по e-mail або SMS); експорт вибраних публікацій в Microsoft Word для надання звітності; якісно-кількісний аналіз інформації; ведення інформаційного архіву; надання можливості ефективного пошуку і обробки інформації в накопиченому архіві публікацій; робота з єдиним інформаційним простором всіма співробітниками незалежно від територіального розташування; автоматичне створення стрічок профільних новин на веб-сайті.

Інформаційно-аналітична система «АСТРА». ІАС «Астра» призначена для роботи підрозділів аналітичних служб компаній і державних структур,

діяльність яких пов'язана із стратегічним плануванням, маркетингом, обробкою і аналізом великих обсягів текстової інформації. У сучасному ІАС «Астра» застосовується в якості аналітичної системи підтримки прийняття рішень і моніторингу інформації.

Комплекс ІАС «Астра» вирішує такі завдання: безперервного інформаційного моніторингу зовнішнього середовища підприємства; тематичної фільтрації інформації.

Функції ІАС «Астра»: отримання інформації з великої кількості різноманітних джерел; автоматична систематизація даних за допомогою рубрикатора, підготовленого експерта; тематична фільтрація пошуку текстових повідомлень; повнотекстова індексація рубрикованих матеріалів, розміщення інформації в базі даних, що забезпечує швидкий та зручний пошук; автоматичне створення дайджестів з можливістю автонотованих матеріалів; статистичний аналіз за часом і за тематикою інформації, яка перебуває в базі даних.

Корпоративна експертна система «Аналітик-2». Система призначена для вирішення широкого кола завдань, пов'язаних із аналітичною обробкою неструктурованої інформації, зокрема, інформації із мережі Інтернет. Інструменти, які представлені в системі, дозволяють вирішувати весь спектр аналітичних завдань від збору і аналітичної обробки до групової роботи експертів в корпоративній базі знань і підготовки звітності: моніторинг ресурсів мережі Інтернет, контекстний пошук, аналітична обробка інформації.

Спектр завдань, які вирішуються за допомогою системи «Аналітик-2»: конкурентна розвідка і аналіз ринку, моніторинг цін і ринкових пропонувань; дослідження нових ринкових галузей при підготовці бізнес-проектів; організація доступу до корпоративних архівів інформації; організація групової роботи спеціалістів в організації; безперебійне забезпечення необхідною інформацією кожного співробітника організації.

Система InfoStream [88]. Призначена для знаходження в мережі Інтернет новин, що цікавлять користувача тематиками, оперативної доставки результатів пошуку, надання користувачеві одночасного доступу в режимі пошуку до

інформації з багатьох Web-сайтів, смислової обробки і, внаслідок цього, мінімізації зусиль користувача на відсіювання дублюючої інформації, шуму. Система InfoStream забезпечує: доступ до оперативної інформації з єдиного інтерфейсу (в міру її появи в Мережі) в пошуковому режимі з урахуванням можливого дублювання та семантичної близькості документів, мовних версій, розмірів документів їх цифрової насиченості і т. д .; доступ до унікального ретроспективному фонду, що перевищує 80 млн. записів; підтримку аналітичної роботи в режимі реального часу: побудова сюжетних ланцюжків, дайджестів, діаграм виявлення й таблиць взаємозв'язків понять, медіа-рейтингів.

1.4.2. Аналіз існуючих програмних засобів обробки природномовних текстів

Слідє також зазначити що такими **програмними засоби є засоби обробки природномовних текстів**, які дозволяють в автоматичному режимі ідентифікувати в досліджуваних масивах текстової форми представлення потрібні одиниці інформації (словоформи, словосполучення і ін.) і знаходити та зберігати їх взаємозв'язок. Такими системами є KNIME, Orange, GATE, RCO Fact Extractor SDK, TextAnalyst, PROMT Analyser та багато інших. Розглянемо декілька з них та визначимо найбільш приближену за необхідністю виконання покладених на нас задань.

KNIME - система інтелектуального аналізу даних містить плагін для обробки тексту з нехитрим назвою KNIME Text Processing. Плагін, як і вся система, має відкритий код і підтримує шестиступеневий процес обробки тексту - від читання і синтаксичного аналізу через розпізнавання сутностей, фільтрації і маніпуляції до підрахунку кількості слів, виділення ключових понять і, нарешті, візуалізації [6]. Все це дає користувачеві широкі можливості роботи з текстом, однак він знайде у KNIME пару істотних недоліків. Наприклад, KNIME не читає дані з MS Excel (хоча для тексту це не критично) і не працює з технологією OLAP

Orange - інструмент для інтелектуального аналізу даних включає в себе розширення для роботи з неструктурованими масивами даних - в тому числі, з текстами [8]. При цьому широкі можливості візуалізації Orange використовуються в цілях text mining. Розширення подібного стилю зручні тим, що можна не відмовлятися від звичного ПО, коли з'являються нові завдання. Зручний графічний користувальницький інтерфейс і інструменти візуального програмування роблять Orange привабливим для користувачів, проте його «зав'язка» на Python не всім може припасти до душі.

General Architecture for Text Engineering (GATE, програма) - система обробки природної мови з відкритим вихідним кодом, яка використовує набори компонентів на мові Java. Система спочатку була розроблена в Університеті Шеффілда і розвивається з 1995 року [3].

За допомогою GATE реалізуються завдання, де потрібно виявити смисловий зміст тексту і кодувати його в структурованому вигляді шляхом додавання анотацій до сегментів тексту. Система застосовується для добування інформації, ручний і автоматичної семантичної анотації, аналізу кореферентності, роботи з онтологіями (наприклад, WordNet), машинного навчання (Weka, RASP, MAXENT, SVM Light), аналізу потоку повідомлень в блогах (наприклад, Twitter).

RCO Fact Extractor – це інтелектуальна програма для комп'ютерного аналізу тексту російською мовою, яка знаходить в ньому опис фактів потрібного типу, наприклад, «зустрічі», «домовленості», «придбання власності», класифікує і впорядковує їх [11]. Основна сфера застосування програми - аналітичні завдання з області комп'ютерної розвідки, що вимагають високоточного пошуку інформації, наприклад, автоматичний підбір матеріалу до досьє на цільовий об'єкт або моніторинг певних сторін його активності, що висвітлюватимуться в ЗМІ.

TextAnalyst® інструмент аналізу символічних текстів, що дозволяє виявити ключові поняття тексту в їх взаємозв'язках, реалізувати анотування текстів і їх смислове порівняння (класифікацію), дозволяє побудувати семантичну мережу понять, виділених в оброблюваному тексті, з посиланнями на контекст [12]. Є можливість смислового пошуку фрагментів тексту з урахуванням прихованих в

тексті смислових зв'язків зі словами запиту. Дозволяє аналізувати текст шляхом побудови ієрархічного дерева тем/підтем, порушених у тексті. Також є можливість реферування тексту. До основних можливостей відносяться: аналіз змісту тексту з автоматичним формуванням семантичної мережі з гіперпосиланнями - отримання смислового портрета тексту в термінах основних понять і їх смислових зв'язків; розумовий пошук з урахуванням прихованих смислових зв'язків слів запиту зі словами тексту; автоматичне реферування тексту - формування його смислового портрета в термінах найбільш інформативних фраз; ранжування всіх видів інформації про семантику тексту за «ступенями значимості» з можливістю варіювання детальності її дослідження.

Очевидно, що програмний продукт з такими широкими можливостями знайде своє застосування в процесі нашого дослідження. Особливо хочеться підкреслити, що результати подібної автоматичної обробки тексту дозволять виявити семантичні зв'язку, які мозок і мовна свідомість кожної окремої людини виявляє досить суб'єктивно, ґрунтуючись на особистому мовному і культурному досвіді.

PROMT Analyser - аналізує будь-які тексти або документи, виділяє в ньому сутності (персоналії, організації, географічні назви, геополітичні суті і ін.), а також визначає співвідносні з цим сутностями дії, дату і місце вчинення дії, формує цілісний образ документа [9]. Система виконує тонкий морфологічний, синтаксичний і семантичний аналіз, що дозволяє максимально точно отримувати інформацію з неструктурованих текстових даних на різних мовах, взаємодіючи навіть з такими морфологічно багатими, як російська і німецька. PROMT Analyser має велику базу даних, але головним його перевагою є те, що, завдяки інноваційним лінгвістичним розробкам, він виділяє в текстах також суті, не представлені в базах. Ще однією перевагою програми є проста настройка - шляхом введення значення для нових типів сутностей.

Як видно із наведених прикладів ринок послуг щодо збору інформації, її обробки, зберігання, аналітики крокує в ногу з нашим інформаційним часом та насичений інформаційно-аналітичними та експертними системами, система

моніторингу та інтелектуального аналізу даних [40], роботи з природномовними текстами. Це все те, що знаходиться у відкритому доступі. А направлене це все на інформаційну розвідку та несилевий вплив в умовах гібридної війни.

Отримана від роботи таких систем інформація обробляється та в підготовленому вигляді надається аналітикам для їх подальшої роботи щодо підготовки звітності та планування подальшої діяльності заказчика цієї інформації [93].

Але наряду з величезною кількістю позитивно вирішених задач у цих системах та програмних засобах ефективність реферування тексту, що обробляється, коливається в діапазоні від 65-70% правильно визначеної суті тексту. Даний показник необхідно та можливо покращити, що в результаті повинно дати можливість більш точно та результативно інформувати користувачів та відповідно змінювати стан їхньої інформованості (обізнаності) за суттю повідомлення. Якщо ж повідомлення буде мати високий показник ймовірності впливу на контрагента та ціле орієнтовано йому надане, то можна буде говорити про підвищення ефективності автоматизованого розподілу інформаційних потоків та ефективному інформаційному впливі на об'єкт інформаційного впливу (контрагента взаємодії).

1.5. Гібридна війна

Сьогодні людство стоїть перед викликом гібридних війн. Саме такі війни породжують формування нового гібридного світу, або, точніше, – гібридного світоустрою. І ми мусимо адекватно відреагувати на цей виклик, описати його не заперечуючи, але приймаючи реальність такою, яка вона є [26].

В результаті поєднання несилевого впливу під час інформаційно-психологічного протистояння з силовим впливом при проведенні традиційних збройних конфліктів, воєнні конфлікти набрали нового вигляду. Їх виділяє особлива послідовність, зазвичай, вони розпочинаються з несилевих антиурядових мітингів, що перетворюються у громадянське протистояння, і

завершуються порушенням державних кордонів військовими формуваннями країни-агресора.

Як показав проведений аналіз, традиційним збройним силам все частіше відводиться допоміжна роль, а основа роль для ведення війн нового типу покладено на сили спеціальних операцій, інформаційного протиборства та психологічних операцій, підрозділи інформаційно-аналітичного забезпечення, РЕБ, розвідки і управління, кібервійська, інформаційні війська, тощо.

Автором терміну «гібридна війна» є відомий теоретик в галузі збройних конфліктів та військово-політичної стратегії Френк Г. Хоффман, колишній офіцер морської піхоти, науковий співробітник міністерства оборони США.

Хоффман зазначає [7], що конфлікти будуть мультимодальними (тобто такими, що ведуться різними способами) та багатоваріантними, що не входять в межі простої конструкції ведення збройного конфлікту чи війни. За Хоффманом майбутні загрози можуть в більшій мірі бути охарактеризованими як гібридне співвідношення традиційних та нерегулярних стратегій і тактик, це децентралізоване планування та виконання, участь недержавних акторів з використанням одночасно простих та складних технологій.

Змістом воєнних дій у війні цього типу стає не фізичне знищення збройних сил супротивника, а деморалізація й нав'язування агресором своєї волі всьому населенню держави. Жертвами ведення такої війни, зазвичай, стають мирні жителі, передусім найбеззахисніші категорії населення – люди похилого віку, жінки й діти [75].

Прикладом таких воєн в найближчих до нас регіонах є:

- війна в Карабаху - роздмухування конфлікту, а потім негласна участь радянських, а з часом і російських військ у Карабаського конфлікту між Вірменією і Азербайджаном на кінці 1980-х - початку 1990-х років;

- Лівансько-ізраїльська війна 2006 року - в якому Хізбалла боролася із військово сильнішим противником Ізраїлем із використанням класичних військових дій, нерегулярних збройних формувань та інформаційних методів

ведення війни, завдавши Ізраїлю, на думку деяких експертів, стратегічної поразки;

- Російсько-грузинська війна 2008 року - одночасно із застосуванням офіційної армії, Росія вела інформаційну, кібер- та економічну війну;

- І звичайно те, що відбувається навколо нас - Російсько-українська війна починаючи з 2014 року і по сьогоднішній день [28], [74].

На думку кандидата наук із соціальних комунікацій, керуючого партнера PR-агенції «АНТ», фахівця із стратегічних комунікацій Олександра Курбана на відміну від двох попередніх, третя світова війна має специфічний характер - вона є гібридною. Вона використовує принципово нову зброю, яку за масштабністю та наслідками можна прирівняти до зброї масового знищення [48].

Характерними ознаками третьої світової війни стали: психологічний геноцид, тероризм, економічна агресія, кіберзлочинність, психотропна агресія. Прояви цих явищ ми бачимо впродовж останніх двох років не тільки в Україні. Полем бою стали країни Сходу (Ізраїль, Сирія, Ірак, Саудівська Аравія, Туреччина), ЄС (Франція, Німеччина, Фінляндія, Нідерланди, Словаччина, Румунія та ін.), ну і, ясна річ, Росія (власне населення) [48].

Базові складові частини російської стратегії і тактики сучасної гібридної війни були сформульовані ще у 2013 році начальником генерального штабу Збройних Сил Російської Федерації В. Герасимовим (рис.1.3) [47].

Саме на основі цих принципів було сплановано та реалізовано напад на Україну, захоплення Криму та розв'язання війни на Донбасі. Серед ключових складових російської концепції зазначається збільшення ролі невійськових методів тиску на противника, насамперед за допомогою політичних (дипломатичних), економічних і гуманітарних елементів.

Інформаційна складова визначалася як основа діяльності на всіх етапах конфлікту від його підготовки до постконфліктного періоду. Особлива увага приділяється «асиметричним заходам», до яких були віднесені: діяльність підрозділів спеціального призначення, підтримка внутрішньої опозиції і

колабораціоністів, а також збільшення цілеспрямованого інформаційного впливу на об'єкт нападу [47].



Рис. 1.3 Схема гібридної війни (російське бачення)

Директор Національного інституту стратегічних досліджень Володимир Горбулін якось сказав, що Україна стала ключовою державою протистояння заходу і Росії [90].

І тут має місце наукова проблема. Як забезпечити ефективну інформаційну дію на широкі верстви населення, дію, яка б дала шанс відновити позитивне відношення населення нашої країни до України як їхньої Батьківщини, Європейської країни? Відповіді на ці питання будуть запропоновані в наступних розділах роботи.

1.6. Постановка задачі досліджень

Як показав проведений аналіз, інформаційне забезпечення (супроводження) проведення бойових дій необхідно розглядати як процес, що характеризується безперервним збором, обробкою, аналізом та розподілом від різних джерел

необхідної інформації з метою якісного виконання поставлених завдань підрозділами ЗС у ході виконання ними відповідних операцій (бойових дій) [21], [49].

Так, не дивлячись на те, що в наукових дослідженнях значна увага приділяється інструментам по збору, обробці, аналізу даних, роботі з природномовною інформацією [16], [26], [7], [84], поки що відсутні рішення, які дозволяють автоматично розподіляти повідомлення в військовій сфері через оцінку інформаційного впливу цих повідомлень на різні верстви населення та війська. Розробки в цій сфері швидше орієнтовані на реалізацію засобів інформаційного впливу [30], [83], [91], а не на вирішення задач управління інформаційним супроводженням. Виходячи з вищевикладеного проглядається практична необхідність в створенні систем і засобів інформаційного супроводження та впливу в умовах гібридної війни з використанням сучасних інформаційних технологій, як в цивільних, економічних, політичних інтересах так і в військовій сфері.

Потрібні:

1. Інформаційні системи і технології, які зможуть оцінити результативність різних способів інформаційного впливу.

2. Інформаційні системи і технології управління реалізацією цих дій.

3. Інформаційні системи здатні автоматично доводити різноманітні повідомлення до найбільш сприятливих до них верств населення і військ.

Для вирішення першої частини завдання в якості науково-методичного базису пропонується використати результати отримані в теорії несилової взаємодії [87], застосовуючи математичний апарат якої можна буде отримати формальні (числові) моделі, які дозволять будувати точні прогнози для управління інформаційною взаємодією людей та на базі цього створити інформаційну технологію інформаційного супроводження.

Для створення такого базису пропонується:

1) Представити в поняттях теорії несилової взаємодії атрибути «м'якої сили». З метою досягнення необхідних дій контрагенту взаємодії необхідно

спочатку змінити його відношення до дійсності, а це досягається зміною його інформованості. В свою чергу для зміни інформованості необхідно, щоб на контрагента здійснювались інформаційні дії.

2) Розрахувати необхідну величину інформаційного впливу на контрагентів взаємодії;

3) Реалізувати методи автоматичного розподілу інформаційних повідомлень з метою максимального несилового впливу на контрагента взаємодії.

Реалізація цих напрямків досліджень буде основним лейтмотивом даної дисертаційної роботи.

На основі вказаних напрямків наукові дослідження будуть присвячені розробці та створенню:

1. Наукових основ побудови інструментів управління інформаційним супроводженням (розділ 2).

2. Математичній моделі супроводження процесів інформаційного впливу на противника (розділ 2).

3. Моделей та методів управління інформаційним супроводженням процесів впливу на контрагентів інформаційної взаємодії (розділ 3).

4. Засобів адресно-орієнтованого управління інформаційним супроводженням (розділ 4).

Висновки до розділу 1

1. Визначена роль інформації в процесах управління військами. Виявлені основні закономірності використання інформації в управлінні інформаційними операціями. Показано, що поняття «інформація» передбачає існування таких об'єктів як джерело інформації, приймач і носій.

2. Проаналізовано інструменти, засоби та методи впливу в інформаційних та гібридних війнах. Розглянуто та наведено найбільш цікаві факти використання інформаційних технологій для супроводження воєнних дій та їх використання, як засіб несилового впливу та супротивника.

3. Розглянуто та наведено поняття інформаційної зброї та її класифікації за метою застосування, за об'єктами впливу, за механізмами реалізації впливу, за реалізованими методами впливу, за характером впливу на інформацію та інформаційні процеси, за масштабом вирішуваних бойових завдань та за терміном дії.

4. Представлені факти застосування глобальної інформаційної мережі Інтернет як арени інформаційного протиборства. Роль та місце геоінформаційних систем в забезпеченні інформаційної підтримки військ.

5. Проведено аналіз існуючих інформаційно-аналітичних систем збирання, структуризації та аналітичної обробки неструктурованої інформації. Наведені приклади розповсюджених та доступних широкому колу інформаційно-аналітичних систем. Проаналізовано існуючі програмні засоби обробки природномовних текстів.

6. Проведено аналіз інформаційної складової гібридної війни. Виявлено основні недоліки в управлінні інформацією під час підготовки та здійснення військових операцій. Вони зводяться до того, що в застосованих інформаційних технологіях аналізу природномовних текстів відсутні рішення, щодо управління інформаційними потоками через автоматичний їх розподіл визначеним адресатам з позиції найбільшої впливовості на них.

7. В результаті проведеного аналізу сформована основна ідея, цілі, направлення, об'єкт і предмет дослідження, поставлено задачі досліджень дисертаційної роботи. Визначена необхідність в розробці моделей і методів, що дозволяють автоматично направляти повідомлення до адресатів, тим самим забезпечуючи оптимізацію доведення інформації до контрагентів та впливаючи на них по суті наданої інформації.

Список використаних джерел

- [1] 193 special operational wing. URL: http://www.state.pa.us/PA_Exec/Military_Affairs/air_national/193fact.html (дата звернення: 19.12.2014).
- [2] Berkowitz B. D. Warfare in Information Age. *Strategy and force planning Faculty, National Security Decision Making Department, Naval War College*. R. M. Lloyd, course director; H. C. Bartlett ... [et al.]. 2nd ed. 1990. P. 465-477. URL: <http://www.dtic.mil/doctrine/doctrine/research/p003.pdf> (дата звернення: 02.03.2015).
- [3] General Architecture for Text Engineering. URL: https://en.wikipedia.org/wiki/General_Architecture_for_Text_Engineering (дата звернення: 02.03.2015).
- [4] Johnson L. S. Toward a Functional Model of Information Warfare. *A Major Intelligence Challenge. Impact of Information Technology*. P. 49-56. URL: <https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol40no5/pdf/v40i5a07p.pdf> (дата звернення: 15.02.2015).
- [5] Jr Nye J. S., Owens W. A.. America's Information edge. *Strategy and force planning Faculty, National Security Decision Making Department, Naval War College*. R. M. Lloyd, course director; H. C. Bartlett ... [et al.], 2nd ed., 1991. P. 630-648. URL: <http://www.dtic.mil/doctrine/doctrine/research/p004.pdf> (дата звернення: 02.03.2015).
- [6] KNIME. URL: <https://www.knime.org/knime-analytics-platform> (дата звернення: 02.03.2015).
- [7] Major Shane R. Reeves, Major Robert E. Barnsby. The New Griffin of War. Hybrid International Armed Conflicts. *Academic journal article "Harvard International Review"*, 2013. Vol. 34. No. 3 URL: <https://www.questia.com/library/journal/1G1-316203914/the-new-griffin-of-war-hybrid-international-armed> (дата звернення: 23.03.2017).
- [8] Orange. URL: <http://orange.biolab.si> (дата звернення: 02.03.2015).
- [9] PROMT Analyser. URL: <http://www.promt.ru/press/news/57586> (дата звернення: 02.03.2015).

- [10] Psychological operations in support of operations “Restore hope“. URL: <https://www.psywar.org/psywar/reproductions/OpRestoreHope.pdf> (дата звернення: 02.03.2015).
- [11] RCO Fact Extractor. URL: <http://www.rco.ru> (дата звернення: 02.03.2015).
- [12] TextAnalys. URL: <http://www.analyst.ru/index.php?lang=eng&dir=content/products/&id=ta>. (дата звернення: 02.03.2015).
- [13] The Balkan Conflict: Stabilization Force (SFOR). URL: www.cybercomm.nl/~stp/b_sfor_update2.html (дата звернення: 13.01.2015).
- [14] U. S. Army Special Operations Command. URL: <http://users.aol.com/armysof1/PSYOPS.html> (дата звернення: 13.01.2015).
- [15] Богуш В. М., Кривуца В. Г., Кудін А. М. Інформаційна безпека: Термінологічний навч. довідник /ред. Кривуци В.Г. Київ: ООО “Д.В.К. ”, 2004. 508 с.
- [16] Большаков М. Подготовка кадров для служб психологических операций и по работе с гражданским населением в США. *Зарубеж. воен. обозрение*, 1998. № 3. С. 9-10.
- [17] Большакова Е. И., Клышинский Э. С., Ландэ Д. В., та ін. Автоматическая обработка текстов на естественном языке и компьютерная лингвистика: учеб. Пособие, Москва, Россия: МИЭМ, 2011. 272 с.
- [18] Бондаренко А. Циклические трансформации нашей "информации", *Независимое военное обозрение*, 1996. №10. С.12.
- [19] Боханов І. Застосування геоінформаційних систем у військовій справі. *Чернігівський наук. часопис, Серія 2, Техніка і природа*, 2011. № 2 (2).
- [20] Бурячок В. Л., Толюпа С. В., Аносов А. О., Козачок В. А., та Лукова-Чуйко Н. В. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник, Київ:ДУТ, 2015. 345 с.
- [21] Визначення цілі та завдання інформаційно-аналітичного забезпечення (ІАЗ). URL: http://pidruchniki.com/15830523/politologiya/viznachennya_tsili_

zavdannya_informatsiyno-analitichnogo_zabezpechennya_iaz (дата звернення: 16.03.2017).

[22] Волковский Н. Л. Силы специальных операций: История, применение, вооружение, оснащение. *воен.-ист. б-ка*, СПб: Полигон, 1996. 368 с.

[23] Воробйова І. В. Інформаційно-психологічна зброя як самостійний засіб ведення інформаційно-психологічної війни, *Сист. озброєння і військ. техніка*, 2010. № 1. С. 141-144.

[24] Воронков С. Система управління військами «Славутич» діє в режимі реального часу. URL: <http://na.mil.gov.ua/32154-cistema-upravlinnya-vijskami-slavutich-diye-v-rezhimi-realnogo-chasu> (дата звернення: 21.03.2017).

[25] Геоінформаційні системи та інформаційні технології у військових і спеціальних задачах. «Січневі ГІСи». Збірка матеріалів, статей, доповідей і тез III науково-практичного семінару 27 січня 2012 року. Львів : АСВ, 2012. 294 с.

[26] Горбулін В. П., Світова гібридна війна: український фронт: монографія, Київ: НІСД, 2017. 496 с.

[27] Горбулін В.П., Додонов О.Г., Ланде Д.В. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія. Київ: Інтертехнологія, 2009. 164 с.

[28] Джердж С. Інформаційна війна Росії проти України: асиметрична відповідь. URL: <http://slovoprosvity.org/2016/04/14/informacijna-vijna-rosii-proti-ukraini-asimetrichna-vidpovid> (дата звернення: 21.11.2016).

[29] Джефф О`Лири, Принципы центуриона: уроки боя для лидеров на линии фронта, Ростов: Феникс, 2005. 296 с.

[30] Дружинін С. В., Климович О. К., Саєнко О. Г. Сучасний стан автоматизації управління військами в Збройних Силах України. *Системи озброєння і військова техніка*, 2010. № 1. С. 60-62.

[31] Ермаков А. Е., Плешко В.В. Семантическая интерпретация в системах компьютерного анализа текста. *Информационные технологии*, 2009. №6. С. 2–7.

[32] Жарков Я. М., Петрик В. М., Присяжнюк М. М. Інформаційно-психологічне протиборство (еволюція та сучасність): *монографія*, Київ: ПАТ «Віпол», 2013. 248 с.

[33] Жук С. Я., Чмельов В. О., Дзюба Т. М. Тенденції та перспективи розвитку інформаційної боротьби й інформаційної зброї, *Наука і оборона*, 2006. №2. С. 35–41.

[34] Знаменский А. Успехи оперативной группы “Орел”, *Независимое военное обозрение*, 1996. № 9. С.2.

[35] Информационная война в Чечне. *Факты, документы, свидетельства*. Ноябрь 1994 - сентябрь 1996. URL: <http://www.internews.ru/books/infowar> (дата звернення: 11.01.2015).

[36] Искусственный интеллект. Справочник в 3-х книгах. Книга 2. Модели и методы, *Под ред. Д.А. Поспелова*, Москва: Радио и связь, 1990. 304 с.

[37] Інформаційна війна в Україні URL: http://revolution.allbest.ru/sociology/00501421_0.html (дата звернення: 07.06.2016).

[38] Інформаційні виклики гібридної війни: контент, канали, механізми протидії : *аналіт. доп., за заг. ред. А.Баровської*, Київ, Україна: НІСД, 2016. 109 с.

[39] Карпенко С. Г., Иванов Є. О. Основи інформаційних систем і технологій: *навч. посіб.* Київ:МАУП, 2002. 264 с.

[40] Козлов А.Н. Интеллектуальные информационные системы: учебник *Мин-во с-х. РФ*, ФГБОУ ВПО Пермская ГСХА. Пермь: Изд-во ФГБОУ ВПО Пермская ГСХА, 2013. 278 с.

[41] Козловський А.В. Комп'ютерна техніка та інформаційні технології: навчальний посібник. 2-ге вид., стер. Київ: Знання, 2012. 463 с.

[42] Конрад Н. И. *Сунь-цзы - Трактат о военном искусстве*. Москва: Ладомир, 1950. 404 с.

[43] Короткий курс лекцій з дисципліни «Теорія комунікації» URL: http://studme.com.ua/10980618/menedzhment/teoriya_kommunikatsii.htm (дата звернення: 27.08.2016).

- [44] Косинський В. І., Швець О. Ф. Сучасні інформаційні технології: *навч. посіб.* Київ: Знання, 2012. 318 с.
- [45] Косошов О. М. Механізми попередження заходам інформаційній кампанії на ранніх стадіях її підготовки. *Системи обробки інформації*, 2016. № 9. С.145-148.
- [46] Кравченко В. О. Основи менеджменту: навч. посібник, Одеса: Атлант, 2012. 211 с.
- [47] Курбан О. Інформаційні війни у соціальних онлайн-мережах. URL: <http://ua.racurs.ua/1063-suchasna-gibrydna-viyna-ta-yiyi-vidobrajennya-u-virtualniy-realnosti-chastyna-2> (дата звернення: 23.03.2017).
- [48] Курбан О. Сучасна гібридна війна та її відображення у віртуальній реальності. URL: <http://ua.racurs.ua/1062-informaciyna-viyna> (дата звернення: 23.03.2017).
- [49] Кучеренко Ю. Ф., Інформаційне забезпечення сучасних бойових дій та його вплив на бойові можливості міжвидового угруповання, *збірник наук. праць ХУПС*, 2009. № 3. С. 2-5.
- [50] Левченко О. В. Класифікація інформаційної зброї за засобами ведення інформаційної боротьби. *Сучасні інформаційні технології у сфері безпеки та оборони*, 2014. № 2. С. 142-146.
- [51] Леонтьєва Л. Є. Історія використання психологічних операцій Німеччиною та Радянським Союзом в роки Другої світової війни (1941-1945 рр.) : автореф. дис. ... канд. іст. наук. 20.02.22 / Держ. ун-т «Львів. політехніка». Ін-т гуманіт. освіти. Львів, 1997. 23 с.
- [52] Любимов М. Деньги на ветер. *Огонек*, 1991. № 41. С. 32.
- [53] Малик Я. Й., Інформаційна безпека України: стан та перспективи розвитку. *Ефективність державного управління*, 2015. № 44(1). С. 13-20.
- [54] Михайлов Б. Психологические операции вооруженных сил США в конфликтах низкой интенсивности. *Зарубеж. воен. обозрение*, 1996. № 8. С. 2-8.

[55] Муковський І. Т., Міщенко А. Г., Шевченко М. М. Інформаційно-аналітична діяльність у міжнародних відносинах: навч. посіб. Київ: Кондор, 2012. 224 с.

[56] Науково-дослідна робота Військового інституту Київського національного університету імені Тараса Шевченка за темою «Автоматизована система розповсюдження інформаційних матеріалів на web-ресурси» Шифр: «Вектор-С» (№ держреєстрації 0101U002293, 2017 р.).

[57] Ожеван М. А. Основні напрями зовнішніх інформаційно-маніпулятивних впливів на суспільні трансформації в Україні: засоби протидії. *Стратегічні пріоритети*, 2011. №3. С. 118–122.

[58] Олійник О.В. Інформаційна безпека США. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*, 2012. № 1 (27). С.280-288.

[59] Онищенко О. С., Горовий В. М., Попик В. І. та ін. Національний інформаційний суверенітет у контексті розвитку новітніх інформаційних технологій: *монографія*, Київ: НБУВ, 2011. 154 с.

[60] Острое оружие дезинформации, *Очерки истории российской внешней разведки: Т. 2. 1917-1933 годы.*, Москва: Междунар. отношения, 1996. 212 с.

[61] Павленко М. А. Разработка процедуры много-этапной формализации знаний для экспертных систем реального времени. *Системи обробки інформації: ХВУ*, 2004. № 9 (37). С. 124-133.

[62] Пашко В. Психологические операции многонациональных сил в Северном Ираке. *Зарубеж. воен. обозрение*, 1995. № 7. С. 12-14.

[63] Пашко В. Силы специальных операций вооруженных сил Индии. *Зарубеж. воен. обозрение*, 1995. № 6. С. 5-7.

[64] Пермяков О. Ю., Сбітнєв А. І. Інформаційні технології і сучасна збройна боротьба, Луганск: Знання, 2008. 204 с.

[65] Пермяков О. Ю., Солонніков В. Г., Прібилєв Ю. Б. Використання інформаційних технологій та застосування космічних систем в інтересах військ (сил) *підручник* Київ: НУОУ ім. Івана Черняхівського, 2014. 208 с.

[66] Петрик В. М., Остроухов В. В. та ін. Сучасні технології та засоби маніпулювання свідомістю, ведення інформаційних війн і спеціальних інформаційних операцій, Київ: Росава, 2006.

[67] Петрик В. М., Присяжнюк М. М. та ін. Сугестивні технології маніпулятивного впливу: навч. посібник 2-ге вид. Київ: ЗАТ Віпол, 2011. 248 с.

[68] Петрик В. М., Прокоф'єва К. О. До питання про застосування методів НЛП в інформаційно-психологічних операціях, *Інформаційна безпека людини, суспільства, держави*, 2009. № 2. С. 71-76.

[69] Полевой устав Армии США FM 33-1. Психологические операции URL: <http://psyfactor.org/lib/fm-33-1.htm> (дата звернення: 17.01.2015).

[70] Попов М. О., Серединін Є. С. Геоінформаційні системи та технології в завданнях оборони й національної безпеки. *Наука і оборона*, 2009. №3. С. 49-55.

[71] Про внесення змін до деяких законів України щодо Сил спеціальних операцій Збройних Сил України: Закон України від 07.07.2016 р. № 1437-VIII. Дата оновлення: 07.07.2016. URL: <http://zakon3.rada.gov.ua/laws/show/1437-19> (дата звернення: 12.11.2016).

[72] Про основи національної безпеки України: Закон України від 19.06.2003 р. № 964-IV. Дата оновлення: 16.07.2015. URL: <http://zakon3.rada.gov.ua/laws/show/964-15> (дата звернення: 08.09.2015).

[73] Про розвідувальні органи України: Закон України від 22.03.2001 р. № 2331-III. Дата оновлення: 07.07.2016. URL: <http://zakon0.rada.gov.ua/laws/show/2331-14>. (дата звернення: 12.11.2016).

[74] Протидія інформвійні в Україні. URL: <http://chornomorka.com/archive/a-6445.html> (дата звернення: 17.10.2016).

[75] Радковець Ю. Ознаки технологій «гібридної війни» в агресивних діях Росії проти України. *Наука і оборона «Техніка»*, 2014. №3. С. 36 – 42.

[76] Раскин А. В. Освещение президентских выборов в Южной Африке американской компанией ABC (“Псевдособытие” как попытка разрешения общественного конфликта). *Вестник МГУ. Сер. 10. Журналистика*, 1996. № 2, С.51–56.

[77] Расторгуев С.П. Информационная война. - М.: Радио и связь. 1998.
URL: <http://evartist.narod.ru/text4/54.htm> (дата звернення: 01.02.2015).

[78] Рось А. О., Замаруєва І. В. Забезпечення інформаційної безпеки держави у воєнній сфері при запобіганні і стримуванні воєнного конфлікту. *Вісник Київського націон. унів-ту ім. Тараса Шевченка. Військово-спеціальні науки*. 2012, №28. С.12-15.

[79] Рось А. О., Замаруєва І. В., Петров В. Л. Концептуальні засади моделювання інформаційної боротьби. *Наука і оборона*, 2000. № 2. С. 47–53.

[80] Савченко И. Черноморский флот, Москва: Новое время, 1997.

[81] Світ телекомунікації та інформатизації: *матеріали Міжнародної науково-технічної конференції студентства та молоді* (м. Київ, 24 груд. 2015 р.). Київ: ДУТ, 2015. 220 с.

[82] Словник основних термінів у галузі інформаційної безпеки держави у воєнній сфері, уклад. А. Рось та ін., за ред. В. М. Телелима. Київ: НУОУ, 2012.

[83] Таїров А. І. Інформаційне забезпечення функціонування органів державної влади: автореф. дис. ... канд. політ. наук: 23.00.02, Київ, 2010. 23с.

[84] Тарануха В. Ю. Інтелектуальна обробка текстів: навч. посібник, Київ: електронна публікація на сайті факультету, 2014. 80 с.

[85] Телешун С. О. та ін. Політична аналітика в системі публічного управління, Київ: НАДУ, 2008. 228 с.

[86] Тесля Ю. Н. Введение в информатику природы, Киев: Маклаут, 2010. 255 с.

[87] Тесля Ю. Н. Несиловое взаимодействие, Киев: Кондор, 2005. 196 с.

[88] Технология мониторинга новостей. URL: <http://infostream.ua> (дата звернення: 05.02.2017).

[89] Токов Е., та Касюк А. Психологические операции ВС США в войнах и конфликтах 20 века. *Зарубеж. воен. обозрение*, 1997. №6. С. 12-17.

[90] УКРІНФОРМ. URL: <https://www.ukrinform.ua/rubric-politycs/2170805-volodimir-gorbulin-direktor-nacionalnogo-institutu-strategicnih-doslidzen.html> (дата звернення: 07.02.2017).

[91] Флегонтов А. В., Фомин В.В. Система интеллектуальной обработки данных. *Известия Рос. гос-ного педагог. ун-та им. А. И. Герцена*, 2013. №154. С. 41–48.

[92] Шebarшин А. Рука Москвы: записки начальника советской разведки. Москва, Россия: Центр-100, 1992. URL: <http://lib.ru/MEMUARY/SHEBARSHIN/rukamoskwy.txt> (дата звернення: 13.01.2015).

[93] Юдаков В. О., Загорка О. М., Тимошенко Р. І., Колесніков В. О. Інформаційно-аналітичне забезпечення процесу прийняття рішення органом військового управління на операцію (бойові дії). *Сучасні інформаційні технології у сфері безпеки та оборони*, 2010. №1(7). С.17-21.

[94] Я так считаю: ред. коммент., общ. газ. 1999.

[95] Яковлев Н. Н. ЦРУ против СССР. 3-е. Киев: Политиздат Украины, 1983. 298 с.

[96] Ярошенко В. Информационная война в Дагестане, *Зеркало недели*, 1999. URL: https://zn.ua/ARCHIVE/rossiya_beret_revansh_za_chechnyu.html (дата звернення: 13.01.2015).

РОЗДІЛ 2

МЕТОДОЛОГІЧНІ ОСНОВИ ТЕХНОЛОГІЇ УПРАВЛІННЯ ІНФОРМАЦІЙНИМ СУПРОВОДЖЕННЯМ

Однією з найважливіших задач в управлінні інформаційним супроводженням (забезпеченням) є задача оцінки інформації, яка найбільш впливає на контрагента взаємодії, з обов'язковим визначенням величин, змісту наповнення та методів її надання.

Цим питанням приділено увагу в значній кількості досліджень в області управління впливами. Але, якщо викладаються способи управління інформацією під час проведення впливу, то майже не приділяється увага впливу цієї інформації на осіб, що приймають рішення, і на самі рішення [9], [10], [11], [14], [19], а якщо досліджуються питання прийняття оптимальних рішень, то не приділяється увага питанням управління інформацією [1], [2], [12], [16]. Рішення ж формується в значній мірі не особою, що приймає рішення, а особами що надають інформацію йому для прийняття рішень.

Проведений аналіз вказав, на, поки що, відсутність робіт, в яких розглядалось би якісне управління інформаційним супроводженням з позицій впливу на контрагента взаємодії (противника), що дозволить оптимізувати процеси інформаційної взаємодії в умовах гібридної війни. Аналіз останніх досліджень і публікацій виявив, що конче необхідно розглянути питання управління інформацією не з позицій максимального інформування контрагентів взаємодії, а з позицій потрібної інформаційного впливу на них. При цьому потрібно врахувати не тільки засоби отримання інформації, а й специфіку методів надання інформації, орієнтованих на інформаційну дію на контрагентів взаємодії.

Наявність невирішеної частини проблеми в цій сфері висуває об'єктивну потребу в розробці технологій управління інформаційними процесами впливу на контрагентів взаємодії, як проміжної ланка між базою знань та засобами інформаційного впливу.

2.1. Термінологічний базис досліджень. Основні поняття та визначення

Понятійний простір роботи формується на перетині кількох наукових дисциплін. Це і інформаційні технології, і психологія, і теорія інформації, і теорія інформаційної взаємодії. Це пов'язано з тим, що **інформаційне супроводження** це, по перше, процеси формування інформаційного ресурсу впливів. По друге, технології та методики представлення інформації в системі управління впливами. По третє, це простір інформаційної взаємодії контрагентів взаємодії та його вміст. По четверте, це цілепокладання та цілеорієнтація сторони, що здійснює вплив. По п'яте – науково-методичний базис формування та використання інформованості в управлінні впливами.

Дамо основні визначення дисертаційної роботи, які утворюють понятійний простір досліджень.

Визначення 2.1. Науково-методичний базис управління інформованістю при здійсненні впливів – загальний набір моделей, методів, правил, алгоритмів, прийомів та теоретичних узагальнень, направлених на вивчення та виділення важливої для здійснення впливу інформації та її перетворення в інформованість контрагентів взаємодії.

Визначення 2.2. Методика управління інформацією в системі управління впливами – упорядкований набір правил та алгоритмів, застосування яких забезпечує оперативний доступ до бази даних системи управління впливами та надання контрагентам впливу отриманої інформації в зручному для сприйняття та найбільш інформативному вигляді.

В основі управління інформацією, і інформованістю як частиною інформаційного середовища впливів, знаходиться цілеорієнтована інформаційна взаємодія об'єктів управління впливами. При цьому в основі цієї взаємодії знаходяться різноманітні повідомлення – носії інформації.

Визначення 2.3. Цілеорієтована інформаційна взаємодія об'єктів управління впливами – процес формування у контрагентів взаємодії необхідного (продиктованого цілями) відношення до об'єктів та процесів шляхом

надання відповідної усної інформації чи повідомлень на твердому носії чи в електронному вигляді.

Визначення 2.4. Відношення до процесів, агентів та контрагентів впливу – суб’єктивна оцінка відповідності процесів, об’єктів та суб’єктів впливу цілям впливу та особи, яка оцінює таку відповідність.

Така суб’єктивна оцінка може бути виражена термінами: відповідає (міра відповідності), не відповідає (міра невідповідності), подобається (міра позитивної емоційної оцінки), не подобається (міра негативної емоційної оцінки) і т.п.

Визначення 2.5. Повідомлення – графічне зображення, текст, звуки, відчуття, які формують у спостерігача уявлення (інформованість) про сутність об’єктів чи процесів, що протікають в предметній області впливів.

Визначення 2.6. Клас повідомлень – множина однотипних повідомлень (наприклад, звітів по ситуації в АТО).

Визначення 2.7. Форма впливу – представлений в узагальненому вигляді (графічному, аудіо, текстовому та іншому) клас повідомлень.

Визначення 2.8. Зміст форми впливу – семантико-прагматична інформація, що передається контрагенту впливу повідомленням і формує у нього нову інформованість.

Визначення 2.9. Засіб впливу – визначений класом повідомлень механізм впливу на контрагента впливу, який відображає вибрану методичку управління інформованістю та являє собою програмно-інформаційний модуль чи інструменти формування форм впливу.

Для ефективного управління інформованістю при здійсненні впливу дуже важливо спочатку визначити, яка інформація і яку дію здійснить на контрагента впливу. Чи відповідатиме ця дія цілям впливу. Іншими словами спочатку необхідно ідентифікувати стан контрагентів взаємодії, їх відношення до дійсності і визначити, яка інформаційний вплив змінить це відношення у відповідності з цілями впливу.

Визначення 2.10. Ідентифікація необхідного відношення до отриманої інформованості - визначення фактичної готовності контрагенту впливу прийняти

ті чи інші рішення в тій чи іншій ситуації в напрямку бажаному стороні, що проводить вплив.

Визначення 2.11. Ідентифікація форм, методів і змісту інформаційного впливу на контрагентів взаємодії - визначення способів надання інформації та змісту самого повідомлення, який забезпечить цілеорієнтований вплив на контрагентів взаємодії у відповідності з цілями впливу. Контрагенту впливу потрібно надавати і хибну інформацію також, якщо вона так вплине на нього, що він прийме потрібне (відповідне цілям впливу) рішення.

Визначення 2.12. Управління інформованістю у впливах - організація, планування та верифікація таких інформаційних дій на об'єкт впливу, які зможуть сформувати у нього адекватне цілям впливу відношення до фактичних та прогнозованих ситуацій. Що в свою чергу збільшить ймовірність прийняття правильних рішень.

Визначення 2.13. Інформаційна технологія управління інформаційним супроводженням (далі – ІТ УІС) - сукупність методів, процесів і програмно-технічних засобів, інтегрованих з метою збирання, опрацювання, зберігання, розповсюдження, показу і використання інформації в інтересах інформаційної підтримки власних військових підрозділів і сил та впливу на противника.

Визначення 2.14. Контрагент взаємодії – об'єкт несилового (інформаційного) впливу, на який в поточний момент часу здійснюється інформаційний вплив з метою спонукання його до певної поведінки і дій, зміни відношення до попередньо набутого світосприйняття.

Визначення 2.15. Інформаційне супроводження в умовах гібридної війни – комплекс заходів направлених на інформаційну підтримку підготовки та проведення військових операцій шляхом автоматизованого визначення цілеспрямованих інформаційних впливів на визначені класи контрагентів взаємодії за критерієм підвищення адресної ймовірності їх бажаної реакції на військову ситуацію в цілому (або окремі її аспекти, складові) за рахунок адресного відбору повідомлень, які мають найбільшу цілеспрямовану інформаційну дію.

2.2. Концептуальна модель визначення необхідних інформаційних впливів на контрагентів взаємодії

Технології інформаційної ери зробили можливою теоретичну і практичну можливість - пряме маніпулювання інформацією противника. Інформація з'являється на основі подій навколишнього світу. Події повинні бути сприйняті якимось чином і проінтерпретовані, щоб стати інформацією. Тому інформація це результат двох речей - сприйнятих подій (даних) і команд, необхідних для інтерпретації даних і зв'язування з ними значення. Відзначимо, що це визначення абсолютно не пов'язано з технологією. Тим не менш, що ми можемо робити з інформацією і як швидко ми можемо це робити, залежить від технології. А якість інформації – це показник труднощі в веденні війни. Чим більше якісною інформацією володіє командир, тим більші в нього переваги в порівнянні з його ворогом [13].

Так у повітряних силах багатьох держав аналіз результатів розвідки і прогнозу погоди є основою для розробки польотного завдання. Точна навігація збільшує ефективність виконання завдання. Всі разом вони є видами військових інформаційних функцій, які збільшують ефективність бойових операцій. Тому дамо визначення **військовим інформаційним функціям** - це будь-яка діяльність, пов'язана з отриманням, передачею, зберіганням і трансформацією інформації, що забезпечує або поліпшує вирішення військами своїх бойових завдань. Інформаційна зброя впливає на інформацію, якою володіє ворог і його інформаційні функції. При цьому наші інформаційні функції захищаються, що дозволяє зменшити його волю або можливості вести боротьбу [13].

Беручи до уваги попередній досвід у впливах на супротивника, в проведенні спеціальних інформаційних операцій та інформаційних війн в умовах гібридного протистояння (розділ 1), пропонується науково-методичний базис для розробки інструментів управління впливами, які можна було б застосувати в управлінні інформаційним супроводженням в процесах підготовки та проведення впливів на контрагента взаємодії (противника). **Основна ідея** цього базису – обґрунтувати та

формально представити такі науково-методичні інструменти управління впливами, які забезпечать значне покращення інформаційно-аналітичного забезпечення військ, шляхів підготовки і проведення операцій з інформаційного впливу на контрагента, здійснення контрзаходів та будуть максимально інформативно зрозумілі, прості, результативні і мінімально затратні.

Для побудови ефективних інформаційних технологій управління інформаційним супроводженням процесів впливами, на думку автора, пропонується, провести таку **підготовчу роботу**:

- вивчити об'єкт і ситуацію, в якій здійснюється вплив;
- вибрати стратегію, тактику та засоби впливу;
- визначити найбільш впливові на контрагента форм представлення інформації та розробити моделі і методи їх формування з допомогою всіх наявних засобів подання (доведення) інформації;
- проаналізувати взаємозв'язок між інформацією, яка надається для впливу та інформованістю об'єкта, на який здійснюється вплив;
- розробити систему аналізу ефективності здійснюваного впливу та його корекції у разі недостатньої дії на контрагента впливу;
- організувати протидію контрагенту впливу, якщо від нього здійснюються контрзаходи.

Вимоги до інформаційної технології супроводження процесів впливу на контрагентів інформаційних взаємодій базуються на розумінні умов, в яких знаходяться об'єкти впливу, джерел та якості отримуваної інформації, а також способів формування різноманітних повідомлень. Виходячи з цього, такими вимогами є: простота, багатогранність, алгоритмічна чіткість, можливість автоматизації основних процесів управління інформацією, захищеність від несанкціонованого доступу, інтелектуальність.

Для забезпечення цих вимог необхідно:

1. Розробити методи автоматичного визначення найбільш впливових шляхів представлення інформації (простота, інтелектуальність).

2. Застосувати різні інструменти попередньої обробки інформації (різні джерела інформації, різні її представлення), управління впливами (вибір яких буде залежати від інформаційних потреб щодо результатів впливу) (багатогранність).

3. Формальними методами представлення інструментів супроводження процесів впливу (алгоритмічна чіткість).

4. Розробкою стандартів інформаційної взаємодії, орієнтованої на перетворення представленої інформації в інформованість контрагентів взаємодії (можливість автоматизації основних процесів обробки інформації).

5. Можливістю доступу до засобів надання інформації тільки заданому кругу користувачів (захищеність від несанкціонованого доступу).

Наведені принципи створення системи відбору інструментів впливу є концептуальною основою наукових досліджень, що проведені автором.

Виходячи із наведених завдань, вимог та принципів побудови інформаційної технології супроводження процесів впливу на контрагентів інформаційної взаємодії можна запропонувати концептуальну модель інформаційного впливу на контрагента взаємодії (рис.2.1).

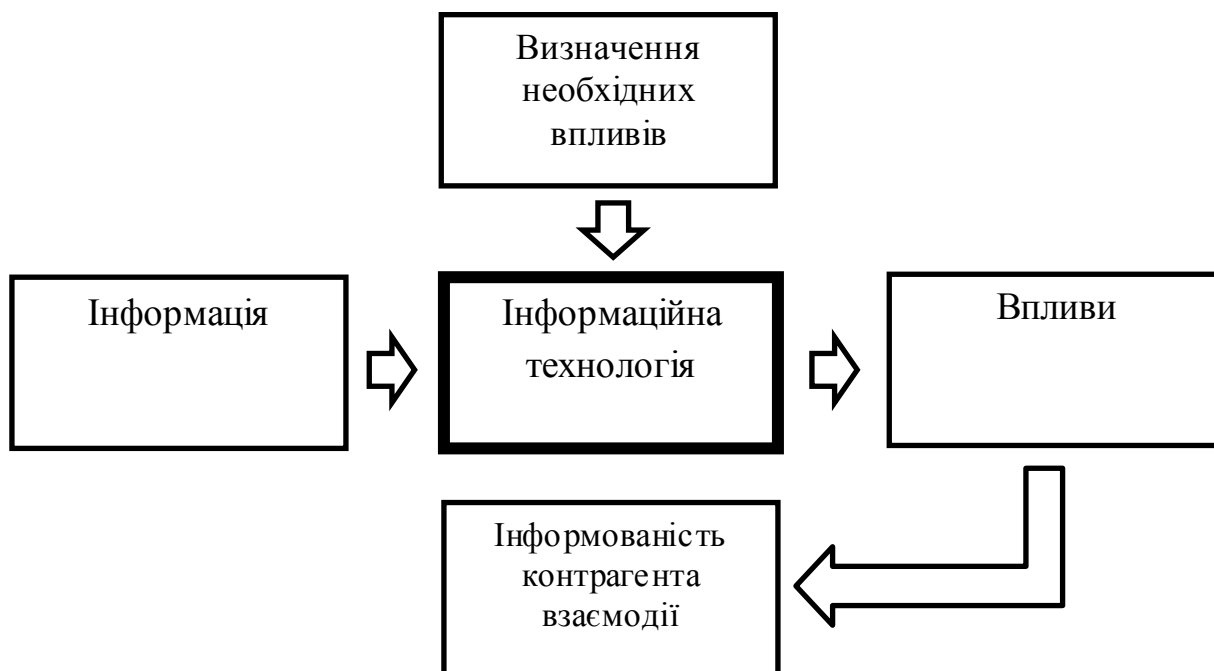


Рис.2.1 Концептуальна модель інформаційного впливу на контрагента взаємодії

Виходячи з трьох наведених на рис.2.1 досить складних задач інформаційного впливу (ідентифікації потрібного відношення до отриманої інформації у контрагентів взаємодії, визначення способів впливу на контрагентів взаємодії, наповнення повідомлення потрібною інформацією), запропонована схема зв'язку між інструментами управління впливами на контрагентів інформаційної взаємодії (рис.2.2).

Виходячи з схеми (рис.2.2) в задачі створення інструментів управління інформованістю і впливами можна виділити дві основні частини: створення інструментів визначення інформованості контрагента впливу, а також створення інструментів інформаційного впливу на нього. Об'єднує ці інструменти інформаційна технологія супроводження процесів впливу на контрагента впливу.

За науково-методичний базис для вирішення першого завдання пропонується взяти теорію інформаційної (несилової) взаємодії. В рамках цієї теорії не тільки створений апарат прогнозування розвитку систем, в основі яких знаходиться взаємодія людей, а й надано математичний апарат для формалізації м'якого компонента, також породжуваного діяльністю людей. На сьогоднішній час, по мимо управління розвитком складних систем, теорія також використовується і для управління підприємствами [10], програмами і проектами [4], щодо побудови систем підготовки прийняття рішень, діагностиці серцево-судинних захворювань [18], в системах голосового управління технічними пристроями [17] й інше. Саме тому, застосовуючи математичний апарат теорії несилової взаємодії в управлінні «м'яким» компонентом, можна досягти поставленої мети, тобто можна буде отримати формальні (числові) моделі, які дозволять будувати точні прогнози про результат інформаційного впливу та розподіляти інформацію по контрагентам з метою вироблення у них потрібної для наших військ реакції.

Для цього необхідно стандартизувати бачення різноманітних компонентів впливу, і особливо, їх взаємозв'язок з баченням сторони, що впливає, того результату, який заданий цілями цього впливу.

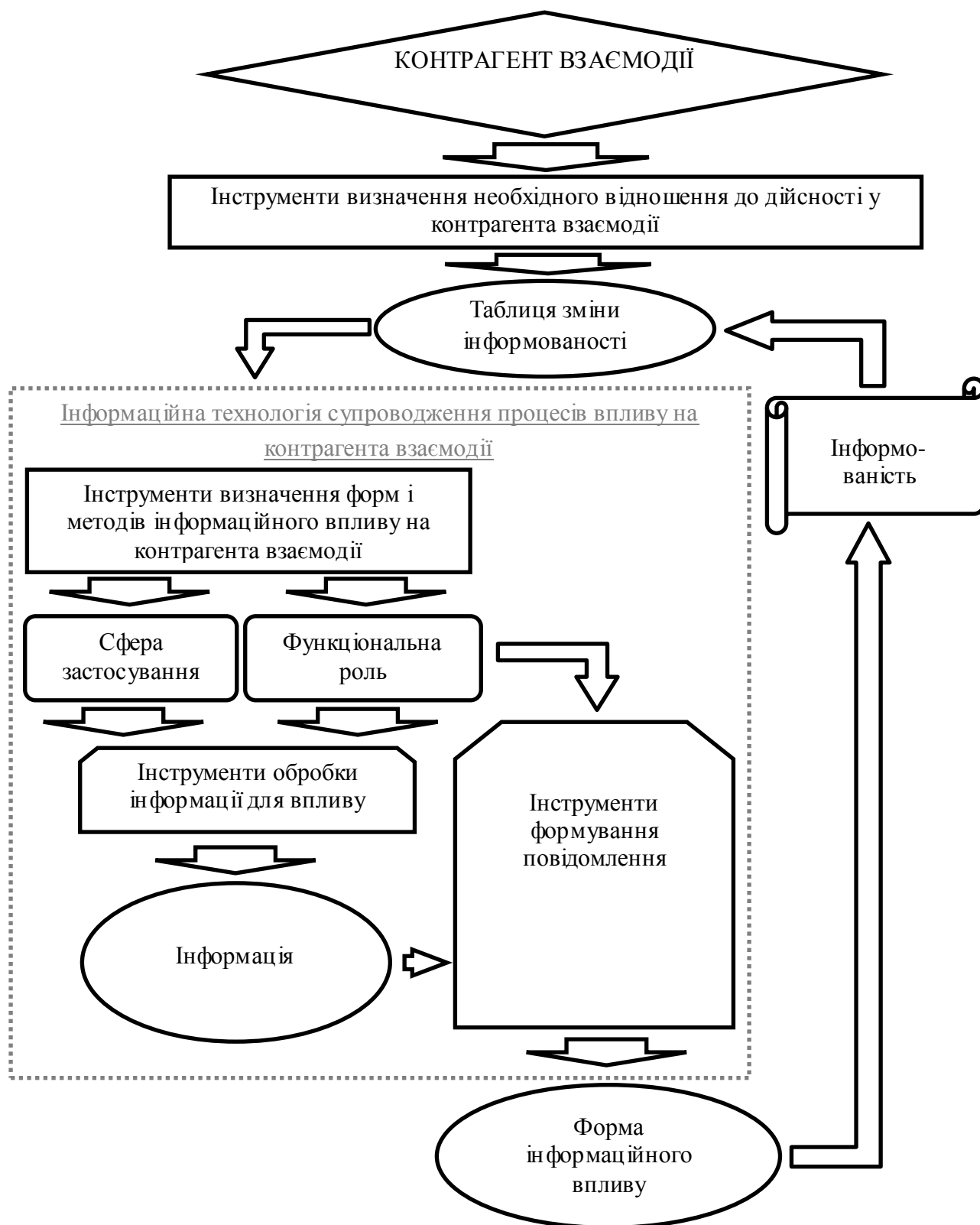


Рис.2.2. Схема зв'язку між інструментами управління впливами на контрагентів інформаційної взаємодії

Інструменти інформаційного впливу на контрагентів взаємодії включатимуть в себе способи отримання потрібної інформації та наповнення цією інформацією форм впливу. Вирішення цієї задачі дозволить досягти мети роботи – ефективно управляти інформованістю через засоби інформаційного впливу. Її реалізація потребує визначити:

1. Як і яка інформованість (відношення до дійсності) позитивно вплине на результати інформаційного впливу;
2. Який інформаційний вплив необхідний, щоб сформувати це відношення до дійсності.

Перейдемо до розгляду першого питання.

2.3. Модель впливу на контрагентів взаємодії

Для забезпечення найкращого інформаційного впливу необхідно не тільки вміти його формувати в процесі управління, але і визначати, яка інформація буде мати найбільший вплив на контрагента впливу, і у якому вигляді її краще надати. Необхідно якісно і ефективно управляти необхідною мірою і змістом інформації, для прийняття оптимального рішення.

2.3.1. Атрибути процесів впливу на контрагентів взаємодії під час підготовки та проведення інформаційного впливу

Реалізація потрібного інформаційного впливу насамперед потребує визначення задач, підбору виконавців (команди), детального вивчення контрагентів взаємодії, визначення термінів виконання та інше. Тобто кожна діяльність в цьому напрямку повинна бути заздалегідь продумана, спроектована, адже реалізація будь якої системи впливів на контрагента взаємодії є проектом, який вимагає якісного управління на базі повного і своєчасного інформаційного забезпечення.

Нехай стан контрагента взаємодії є результатом фізичних чи інформаційних впливів (2.1):

$$J = \{j_e\}_{e=1, n}, \quad (2.1)$$

де J – множина впливів;
 j_e – вплив;
 n – кількість впливів.

В свою чергу кожен вплив характеризується (2.2):

$$j_e = \langle U_e, m_e, R_e, W_e, S_e, S_e^* \rangle, \quad (2.2)$$

де U_e – об'єкт впливу;
 m_e – мета впливу;
 R_e – ресурс впливу (інформація);
 W_e – витрати на вплив;
 S_e – бажаний результат впливу;
 S_e^* – фактичний результат впливу.

Визначення 2.15. Результат впливу – чисельна чи якісна інформаційна характеристика деякого об'єкта, яка формується заданим впливом.

Визначення 2.16. Інформація про результати впливу – відображений в різноманітних документах, інтелектуальному апараті людини, електронних носіях результат впливу.

Визначення 2.17. Інформованість контрагента впливу – кількісна міра всіх впливів на нього.

Визначення 2.18. Визначеність контрагента впливу – міра переважності одних впливів над іншими.

Визначення 2.19. Ресурс впливу – інформація, що призводить до змін в поведінці контрагента впливу.

Будемо вважати, що оцінка впливу j_e на контрагента взаємодії (противника) буде позитивною, якщо його фактичний результат впливу буде відповідати бажаному

$$S_e^* \equiv S_e. \quad (2.3)$$

Тотожність бажаного і фактичного результату впливу може бути визначена із характеристик стану контрагента взаємодії:

$$U_e = \{x_{ei}, i = \overline{1, k_e}\}, \quad (2.4)$$

де x_{ei} – характеристика стану контрагента взаємодії U_e ;

k_e – кількість характеристик контрагента взаємодії U_e , за якими оцінюється результат впливу на нього.

Тоді бажане і фактичне значення характеристики можна представити виразами

$$\begin{aligned} S_e &= \{s_{ei}, i = \overline{1, k_e}\}; \\ S_e^* &= \{s_{ei}^*, i = \overline{1, k_e}\}, \end{aligned} \quad (2.5)$$

де S_{ei} – бажане значення характеристики x_{ei} об'єкта впливу U_{ei} ;

S_{ei}^* – фактичне значення характеристики x_{ei} об'єкта впливу U_{ei} .

Кожна характеристика об'єкта впливу U_e може бути представлена кортежем:

$$x_{ei} = \langle o_{ei}, \pi_{ei}, z_{ei}, z_{ei}^* \rangle, \quad (2.6)$$

де o_{ei} – оцінка характеристичного значення (1 – чим більше, тим краще; -1 – чим менше, тим краще) i -го елемента компоненту впливу j_e ;

π_{ei} – вага i -го елемента характеристики x_{ei} контрагента взаємодії U_{ei} ;

z_{ei} – бажане значення характеристики x_{ei} контрагента взаємодії U_{ei} ;

z_{ei}^* – фактичне значення характеристики x_{ei} контрагента взаємодії U_{ei} .

Тоді оцінка впливу може бути отримана через співставлення бажаних і фактичних значень характеристики x_{ei} контрагента взаємодії U_{ei} . Для цього

спочатку отримаємо міру відповідності бажаного та фактичного результату для окремої характеристики контрагента взаємодії:

$$\lambda_{ei} = \begin{cases} 1, & \text{якщо } o_{ei} \cdot z_{ei}^* \geq o_{ei} \cdot z_{ei}, \\ 0, & \text{якщо } o_{ei} \cdot z_{ei}^* < o_{ei} \cdot z_{ei} \end{cases} \quad (2.7)$$

де $\lambda_{ei}(t)$ – відповідність фактичного значення бажаному для характеристики x_{ei} контрагента взаємодії U_{ei} .

Тоді результативність впливу виглядатиме наступним чином:

$$v_e = \frac{\sum_{i=1}^{k_e} \lambda_{ei} \cdot \pi_{ei}}{\sum_{i=1}^{k_e} \pi_{ei}}, \quad (2.8)$$

де v_e – результативність впливу j_e .

π_{ei} – вага i -го елемента характеристики x_{ei} контрагента взаємодії U_{ei} .

Визначення 2.20. Оптимальним впливом є такий, для якого

$$v_e = 1.$$

Визначення 2.21. Успішним будемо вважати такий вплив на контрагента взаємодії, для якого $v_e > v_{\text{дон}}$,

де $v_{\text{дон}}$ – допустима міра відхилень у діях контрагента взаємодії під час здійснення впливу j_e .

Кожен вплив на контрагента взаємодії реалізується множиною дій, які визначають можливість реалізації впливу (технологія збору і обробки інформації для реалізації впливу), так і безпосередньо несилкових (інформаційних) дій на нього

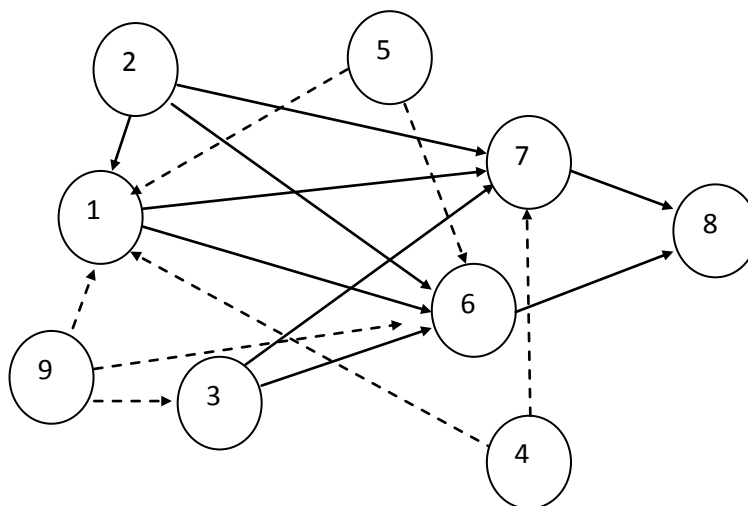
$$j_e = \{h_{ei}, \dots\} = \overline{1, n_e}, \quad (2.9)$$

де h_{ei} – дія по підготовці чи реалізації впливу j_e ;

n_e – кількість дій по підготовці чи реалізації впливу j_e .

Зазвичай дії виконуються у відповідності з деякою сітьовою моделлю. Це обумовлюється як причинно-наслідковими зв'язками між результатами дій (наприклад, спочатку отримати деяку інформацію, проаналізувати, сформулювати

необхідне для несилового впливу повідомлення), так і неможливістю у взаємодії з противником відразу отримати необхідну для нас реакцію (наприклад, звільнення ним зайнятих територій тільки з допомогою одного звернення до нього). Зокрема, якщо компонент «фінансування впливу» буде оптимальним, то ймовірність того, що компонент «час реалізації впливу» теж буде успішним вища, ніж якщо він буде не успішним. Такий взаємозв'язок різних впливів можна представити орієнтованою сітьовою моделлю, ребра якої відповідають каузальним відношенням відносно цих впливів. І лише реалізація всіх впливів може забезпечити досягнення мети у інформаційній війні з ворогом, що відображено на рисунку 2.3.



Позначення

- | | |
|--|---|
| 1 – професіоналізм підрозділу впливу; | 5 – інформаційний вплив звірств противника; |
| 2 – фінансування операції; | 6 – якість впливу; |
| 3 – затверджений план заходів; | 7 – час реалізації впливу; |
| 4 – контрінформаційний вплив противника; | 8 – результативність; |
| | 9 – обман, підкуп, тощо; |

Рис. 2.3. Приклад взаємозв'язку впливів (суцільні лінії – позитивний вплив, пунктирні лінії – негативний вплив)

Визначення 2.22. Доцільною будемо вважати таку дію на контрагента взаємодії, яка збільшить оцінку відповідності бажаному результату впливу як в поточний момент часу, так і по завершенню цього впливу.

$$v(t / h_{ei}(t)) > v(t / \overline{h_{ei}(t)}) \& v(\infty / h_{ei}(t)) > v(\infty / \overline{h_{ei}(t)}),$$

де $v(t / h_{ei}(t))$ – відповідність результату впливу його плану в момент часу t при умові реалізації дії $h_{ei}(t)$ в момент часу t ;

$v(t / \overline{h_{ei}(t)})$ – відповідність результату впливу його плану в момент часу t при умові НЕ реалізації дії $h_{ei}(t)$ в момент часу t ;

$v(\infty / h_{ei}(t))$ – відповідність результату впливу його плану в момент закінчення при умові реалізації дії $h_{ei}(t)$ в момент часу t ;

$v(\infty / \overline{h_{ei}(t)})$ – відповідність результату впливу його плану в момент закінчення при умові НЕ реалізації дії $h_{ei}(t)$ в момент часу t .

Визначення 2.23. Оптимальною будемо вважати ту доцільну дію на контрагента взаємодії, для якої не існує в даний момент часу жодної іншої дії, яка ще більше збільшує оцінку відповідності бажаному результату впливу як в поточний момент часу, так і по завершенню цього впливу

Визначення 2.24. Раціональною будемо вважати ту доцільну дію на контрагента взаємодії, для якої не існує в даний момент часу жодної іншої дії, яка ще більше збільшує оцінку відповідності бажаному результату компонентів впливу по завершенню цього впливу

Визначення 2.25. Діяльність контрагента взаємодії будемо називати оптимальною, якщо він завжди приймає рішення, які відповідають очікуваному результату здійсненого впливу.

Визначення 2.26. Діяльність контрагента взаємодії будемо називати доброю, якщо він приймає рішення, що забезпечують оптимальний та раціональний результат здійснюваного впливу.

Визначення 2.27. Діяльність контрагента взаємодії будемо називати доцільною, якщо він завжди приймає рішення, що забезпечують доцільний, але не завжди оптимальний чи раціональний результат здійснюваного впливу.

Визначення 2.28. Діяльність контрагента взаємодії будемо називати задовільною, якщо він завжди приймає рішення, що забезпечують доцільний, але ніколи оптимальний чи раціональний результат здійснюваного впливу.

Визначення 2.29. Діяльність контрагента взаємодії будемо називати незадовільною, якщо він ніколи приймає рішення, що не забезпечують доцільний результат здійснюваного впливу.

Для того щоб діяльність контрагента взаємодії була оптимальною чи доброю він завжди повинен володіти максимальною інформацією, що направлена на забезпечення виконання плану здійсненого впливу. З точки зору створення системи управління впливами потрібно реалізовувати трішки іншу формулу інформаційного забезпечення контрагентів взаємодії.

Визначення 2.30. Для того щоб діяльність контрагента взаємодії була оптимальною чи раціональною, необхідно реалізувати таку інформаційну дію на нього, щоб сформована в цьому процесі інформованість привела до прийняття ним рішення, які призведуть до оптимальних чи раціональних бажаних дій.

Знаючи, яка інформованість забезпечить оптимальну діяльність контрагента взаємодії можна перейти до розгляду необхідних інформаційних дій на нього.

2.3.2. Управління інформованістю контрагентів взаємодії

Для вирішення задачі визначення потрібної інформованості контрагента впливу виділимо в ній конкретизовані компоненти (отриману інформацію, знання) [5], що може бути представлена виразом 2.10:

$$I = \{I_j\}, j = \overline{1, q}, \quad (2.10)$$

де I_j – конкретизована інформованість;

I – інформованість, потрібна для здійснення оптимальних дій для найкращого результату впливу;

q – кількість конкретизованих інформованостей.

Під інформованістю розуміється і теоретичний матеріал, і досвід роботи, і інформація, яку має контрагент взаємодії та яка стосується тієї задачі, що поставлена для здійснення впливу на нього. Вся ця інформація формує у нього те чи інше відношення до дійсності. А відношення до дійсності (світогляд) лежить в основі прийнятих ним рішень та дій, які заплановані до його виконання за планом впливу, що на нього здійснюється. Це і є концептуальною основою управління інформованістю у впливах через засоби надання інформації. Виходячи з вище зазначеного отримаємо

$$I = I_1 \cup I_2 \cup I_3 \cup I_4 \cup I_5,$$

де I – інформованість (світогляд), необхідні контрагенту впливу для прийняття ним оптимальних для плану впливу рішень;

I_1 – теоретична інформованість, що розкриває сутність речей, явищ та подій;

I_2 – практична інформованість, що включає переважно відомості про використання тих чи інших предметів і ситуацій з конкретною метою;

I_3 – його особиста професійна інформованість;

I_4 – інформованість відносно дій контрагента взаємодії;

I_5 – власні інтереси.

Готовим до виконання поставленої впливом задачі будемо вважати такого контрагента впливу, який володіє всіма перерахованими компонентами (знаннями)

$$I^k = I,$$

де I^k – інформованість, яка є у контрагента впливу k .

Утворюємо матрицю ймовірностей дій в залежності від інформованості контрагента взаємодії:

$$P = \{p_{ij}\}, i = \overline{1, n_J}, j = \overline{1, n_I} \quad (2.11)$$

де P – матриця ймовірностей дій після зміни інформованості контрагента взаємодії;

- n_j – кількість можливих дій;
- n_I – кількість конкретизованих компонентів інформованості, які необхідні для досягнення мети впливу;
- p_{ij} – суб'єктивна ймовірність вибору дії контрагентом впливу h_i , як результат нової інформованості.

В процесі управління інформованістю потрібно так сформулювати матрицю відношень між інформованістю та діями, щоб суб'єктивна ймовірність прийняття рішень по реалізації оптимальних дій дорівнювала 1. А всі інші ймовірності дорівнювали б 0. Але на практиці це неможливо. Потрібно враховувати фактор достовірності інформації, що формує знання, її неповноту, динамічний характер середовища і оточення. Тому суб'єктивні ймовірності, в загальному випадку, не будуть дорівнювати ні 0, ні 1.

Визначені засоби надання інформації є тим носієм інформаційного впливу, який визначає наповнення матриці (2.11). Зрозуміло, що вплив на контрагента впливу визначеними повідомленнями (засобами надання інформації) призведе до змін в матриці P (2.11). Доцільними будемо вважати ті зміни, які призводять до збільшення ймовірностей оптимальних (визначення 2.23) чи раціональних (визначення 2.24) дій, і зменшенню ймовірностей дій, які не підпадають під визначення доцільних (визначення 2.22).

Нехай задана матриця початкової інформованості p контрагента впливу M_k (табл.2.1).

Таблиця 2.1

Матриця ймовірностей дій контрагента впливу h_i в залежності від початкової його інформованості

	j_1	j_2	j_{n_j}
I_1	p_{11}	p_{12}	p_{n_j1}
I_2	p_{12}	p_{22}	p_{n_j2}
.....
I_{n_I}	p_{1n_I}	p_{2n_I}	$p_{n_jn_I}$

Після отримання контрагентом впливу h_i деякого повідомлення B^L матриця ймовірностей дій зміниться (табл.2.2).

Таблиця 2.2

**Матриця ймовірностей дій контрагента впливу h_i
після отримання ним повідомлення B^L**

	j_1	j_2	j_{n_j}
I_1	p_{11}^L	p_{21}^L	$p_{n_j 1}^L$
I_2	p_{12}^L	p_{22}^L	$p_{n_j 2}^L$
.....
I_{n_i}	$p_{1n_i}^L$	$p_{2n_i}^L$	$p_{n_j n_i}^L$

Загальна величина відхилень в суб'єктивних ймовірностях може характеризувати величину впливу форми впливу B^L на контрагента h_i .

Тоді вплив повідомлення B^L на інформованість контрагента впливу в конкретній ситуації може бути оцінено за формулою

$$\Delta\theta^{ou}(B^L) = \sum_{i=1}^{n_I} \left[\psi(h_i) \cdot \sum_{j=1}^{n_J} w(p_{ij}, p_{ij}^L) \right], \quad (2.12)$$

де $\Delta\theta^{ou}(B^L)$ – оцінка інформаційного впливу повідомлення B^L на контрагента впливу h_i ;

$w(p_{ij}, p_{ij}^L)$ – оцінка впливу, який призводить до відхилення між початковою (до впливу) та кінцевою (після впливу) суб'єктивними ймовірностями дії h_i ;

$\psi(h_i)$ – оцінка важливості дії контрагента взаємодії h_i , спрямованої на виконання задуму сторони, що впливає.

Оцінка важливості дії контрагента взаємодії, спрямованої на виконання задуму сторони, що впливає повинна відповідати наступній умові:

- для класів дій: оптимальні, раціональні, доцільні - $\psi(h_i) > 0$;

- для класів дій: не доцільні - $\psi(h_i) \leq 0$.

Тоді можна говорити про оптимізацію впливу на контрагента взаємодії. Цільова функція повинна відображати необхідність найбільш значного впливу на контрагента взаємодії (2.13):

$$\sum_{B^L} \Delta \theta^{ou}(B^L) - \Delta S \rightarrow \max, \quad (2.13)$$

при обмеженнях

$$\Delta S \leq S_{\max};$$

$$B^L,$$

де S_{\max} – бюджет проекту інформаційного супроводження впливу на контрагента взаємодії;

ΔS – фактичні витрати на проект інформаційного супроводження впливу на контрагента взаємодії;

B^L – повідомлення.

Залишилось вирішити ще два питання. Оцінка дій завжди залежить від деякої ситуації. І на практиці ця оцінка може бути отримана тільки експертним шляхом. Розглянемо ці питання.

2.3.3. Вплив поточної ситуації на інформаційну взаємодію з контрагентом взаємодії

Як було вже раніше сказано на контрагента взаємодії в кожен момент часу діє не тільки та інформація, яка визначена в процесі взаємодії, але й різноманітні фактори, які не пов'язані безпосередньо з цілеспрямованою дією на нього, тобто йдеться про вплив поточної ситуації на будь якого контрагента інформаційної взаємодії. Тому черговим кроком до створення інформаційної технології супроводження процесів впливу на контрагента взаємодії є необхідність визначення впливу поточної ситуації на хід інформаційної взаємодії з ним [6].

Дамо ряд визначень, які розкривають суть впливу поточної ситуації на хід інформаційної взаємодії з контрагентом.

Визначення 2.30. Поточна ситуація – стан контрагента взаємодії на поточний момент часу.

Визначення 2.31. Контрагент інформаційного впливу – це особистість або група людей (суспільство, армія, тощо) на яких здійснюється цілеспрямований вплив із використанням інформаційних технологій з метою досягнення потрібної вигоди чи переваги.

Під перевагами, у воєнній сфері, будемо розуміти більш глибоке усвідомлення й розуміння ситуації на полі бою, більш точне з'ясування своїх переваг і недоліків противника, здатність їх реалізувати у своїх цілях, випереджальне прийняття й негайне доведення рішень, повністю адекватних обставині, що склалась, та безперервний контроль їхнього виконання. Основна перевага при застосуванні інформаційної технології управління інформаційним супроводженням бачиться в максимальному зменшенні термінів циклів управління підлеглими військами в зоні ведення бойових дій в ході зміни оперативної обстановки, за рахунок чого забезпечується інформаційна перевага над противником.

Визначення 2.32. Агент інформаційного впливу – індивід чи організована група людей, які здійснюють цілеорієнтований інформаційний вплив на контрагентів впливу з використанням інформаційних технологій з метою досягнення потрібної вигоди чи переваги над ними.

Поточною ситуацією може бути і інформаційний вплив, яку зумовлюють «звірства» щодо полонених, інформаційний вплив (реакція) населення тимчасово окупованих територій на санкції міжнародної спільноти щодо Російської Федерації, інформаційний вплив на населення, щодо пониження підтримки своєї армії (висвітлення недобрих фактів, перекручування інформації, відкрита брехня) та багато інших факторів, які вносять свої корективи в очікуваний результат. Поточна ситуація, зазвичай, призводить до відхилення «фактичних» результатів впливу, від «запланованих».

Вплив поточної ситуації треба враховувати при розрахунку результату цілеспрямованої інформаційного впливу на контрагента взаємодії. Якщо

цілеспрямована інформаційний вплив направлена на вироблення у противника потрібної реакції з максимальною ймовірністю, то поточна ситуація може призвести до збільшення чи зменшення такої ймовірності.

Нехай ймовірність потрібної реакції противника (наприклад: відступ, роззброєння, проведення мирних переговорів, відступ, зневіра у власних силах та ін.) дорівнює p_0 . Тоді цілеспрямована інформаційний вплив на нього повинна приводити до збільшення цієї ймовірності:

$$p(L) \gg p_0$$

де p_0 – ймовірність потрібної реакції противника;

$p(L)$ – ймовірність цілеспрямованої інформаційного впливу на противника.

Ідеальний варіант, коли $p(L)=1$. В свою чергу представимо інформаційну дію L через множину повідомлень, доведених до противника

$$L = \bigcup_i B_i^L,$$

де B_i^L – повідомлення.

Тоді ймовірність потрібної реакції противника від впливу поточної ситуації W в загальному випадку буде відрізнятися від $p(L)$:

$$p(W) \neq p(L),$$

де $p(W)$ – ймовірність потрібної реакції від впливу поточної ситуації W .

І зазвичай вона буде менша від $p(L)$, оскільки в протилежному випадку цілеспрямована інформаційний вплив буде просто-напросто шкідливою, а не корисною:

$$p(W) < p(L)$$

Якщо поєднати і вплив поточної ситуації з цілеспрямованим впливом на контрагента взаємодії (противника), то ймовірність потрібної реакції, в загальному випадку, буде знаходитись між вказаними значеннями

$$p(W) \leq p(W \cup L) \leq p(L),$$

де $p(W \cup L)$ – ймовірність потрібної реакції при поєднанні впливу поточної

ситуації з цілеспрямованим впливом на противника.

Оскільки поточна ситуація завжди багатогранна, включає безліч подій та їх оцінок, то серед них завжди можна знайти такі, які в тій чи іншій мірі збільшують ймовірність потрібної реакції противника. І використати їх як зброю проти нього.

$$W = W^+ \cup W^-, \quad (2.14)$$

де W^+ – поточна ситуація, яка збільшує ймовірність потрібної реакції противника;

W^- – поточна ситуація, яка зменшує ймовірність потрібної реакції противника.

Виходячи з (2.14)

$$p(W^-) \leq p(W) \leq p(L) \leq p(L \cup W^+), \quad (2.15)$$

де $p(W)$ – ймовірність поточної ситуації, яка зменшує потрібну реакцію противника;

$p(L \cup W^+)$ – ймовірність потрібної реакції при поєднанні впливу поточної ситуації, яка збільшує ймовірність потрібної реакції противника з цілеспрямованим впливом на нього.

Виходячи з формули (2.15) при реалізації інформаційної технології супроводження несилових впливів на контрагента взаємодії необхідно відібрати і довести до нього ті події, факти, що відносяться до поточної ситуації, і які максимально збільшують ймовірність потрібної реакції. Але тут виникає проблема. Доведення деякої інформації до противника вимагає значних витрат. Витрат, які несумірні з вирашем від такого впливу.

Пропонується на підставі цього представити цільову функцію інформаційного впливу форми повідомлення на контрагента впливу в наступному вигляді

$$\theta_{(L \cup W_i^+)} \rightarrow \theta_{\Phi_0} \rightarrow S \rightarrow S \rightarrow W_i^+ \rightarrow \max, \quad (2.16)$$

при обмеженнях

$$S(L, Y, W_i^+) \leq S_{\max};$$

$$W;$$

$$L,$$

- де $\theta(L, Y, W_i^+)$ – оцінка ймовірності потрібної реакції при поєднанні впливу поточної ситуації, яка збільшує ймовірність потрібної реакції контрагента з цілеспрямованим впливом на нього;
- θp_0 – оцінка початкової ймовірності потрібної реакції контрагента;
- $S(L)$ – витрати на реалізацію інформаційної дії;
- $S(W_i^+)$ – витрати на використання поточної ситуації, яка збільшує ймовірність потрібної реакції контрагента;
- S_{\max} – бюджет проекту інформаційного супроводження впливу на контрагента.

Оскільки поточна ситуація представляється множиною впливів, то в рамках інформаційної технології управління супроводженням процесів впливу на контрагентів взаємодії необхідно визначити ті впливи, які максимізують цільову функцію (2.16). Тому є необхідність в розробці спеціального методу визначення найбільш інформативних впливів (дій) на контрагентів взаємодії і за окремими діям на них визначати оптимальну реакцію в тій чи іншій ситуації.

З цією метою перш за все сформуємо модель інформаційних дій на контрагентів взаємодії.

2.3.4. Оцінка інформаційних дій на контрагентів взаємодії

Однією з основних науково-методологічних задач роботи є визначення системи інформаційних впливів на контрагентів взаємодії, яка забезпечить досягнення мети (задуму) впливу [7]. Дамо нові визначення.

Визначення 2.33. Інформаційний вплив на контрагентів взаємодії, це цілеорієнтоване надання їм різноманітних повідомлень з метою виробки в них

необхідного відношення до дійсності, що призведе до виконання ними дій запланованих ініціаторами впливу.

Визначення 2.34. Контрагент взаємодії – індивід, група людей, інформаційні ресурсу, що об'єднують групу користувачів та багато іншого, які можуть стати об'єктом вирішення завдань, що ставляться іншими групами людей, користувачами інформаційного простору.

Визначення 2.35. Повідомлення – письмові, усні чи електронні повідомлення, екземпляри документів.

Для того, щоб визначити найбільш потрібну дію на контрагента взаємодії розглянемо суперпозицію функцій:

$$\eta(D, S, Z, C, B, X, t) = f(\eta^1(D), \eta^2(S), \eta^3(Z), \eta^4(C), \eta^5(B), \eta^6(X), \eta^7(t))$$

де $\eta^1(D)$ – інформаційний вплив на контрагентів взаємодії, що визначається діями зі сторони керівництва держави;

$\eta^2(S)$ – інформаційна вплив на контрагентів взаємодії, що визначається діями зі сторони міжнародної спільноти;

$\eta^3(Z)$ – інформаційна вплив, який зумовлюють «звірства» щодо полонених;

$\eta^4(C)$ – інформаційний вплив на населення тимчасово окупованих територій, що визначається санкціями міжнародної спільноти щодо країни-агресора;

$\eta^5(B)$ – інформаційний вплив на населення, щодо пониження підтримки своєї армії (висвітлення недобрих фактів, перекручування інформації, відкрита брехня);

$\eta^6(X)$ – інформаційний вплив, як контрзахід противника;

$\eta^7(t)$ – інформаційний вплив часу t .

Модель, запропонована в теорії несилової взаємодії, дає можливість отримати за результатами спостереження проявів окремих об'єктів, чи за окремими експертними оцінками, їх спільну дію на прийняті рішення за результатами здійсненого впливу. Нехай методами експертної оцінки [15], чи з

застосуванням статистичних методів отримані суб'єктивні ймовірності, чи оцінки вибору (в межах 0÷1) тих чи інших впливів на контрагентів взаємодії в залежності:

1. Від відхилення мети впливу зі сторони керівництва держави

$$p_{ej}^1 = f_1 \quad \eta^1 \quad D = F_j , \quad (2.17)$$

де F_j – інформаційний вплив на контрагента (вид повідомлення, час чи періодичність подання, рівень представлення, форма представлення, коментарі, джерело, очікування); $p_{ej}^1 = f_1 \quad \eta^1 \quad D = F_j$ – оцінка того, які зміни в впливі на контрагента вносить керівництво держави, при бажаному впливі F_j .

2. Від стану контрагента взаємодії

$$p_{ej}^2 = f_2 \quad \eta^2 \quad S = F_j , \quad (2.18)$$

де $p_{ej}^2 = f_2 \quad \eta^2 \quad S = F_j$ – оцінка того, які зміни в впливі на контрагента вносить реакція чи відношення до того, що відбувається, міжнародної спільноти, при бажаному впливі F_j .

3. Від того, як на контрагента діє інформація про порушення женецьких конвенцій щодо прав та свобод людини в зоні дії конфлікту

$$p_{ej}^3 = f_3 \quad \eta^3 \quad Z = F_j , \quad (2.19)$$

де $p_{ej}^3 = f_3 \quad \eta^3 \quad Z = F_j$ – оцінка того, як вплине на контрагента інформація щодо «звірств» над полоненими в зоні дії конфлікту при бажаному впливі F_j .

4. Від того, як на контрагента діє інформація щодо санкцій міжнародної спільноти щодо країни-агресора

$$p_{ej}^4 = f_4 \quad \eta^4 \quad C = F_j , \quad (2.20)$$

де $p_{ej}^4 = f_4 \eta^4 C = F_j$ – оцінка того, як вплине на контрагента інформація щодо санкцій міжнародної спільноти на країну-агресора при бажаному впливі F_j .

5. Від того, як на контрагента діє інформація направлена на пониження підтримки своєї армії (висвітлення недобрих фактів, перекручування інформації, відкрита брехня)

$$p_{ej}^5 = f_5 \eta^5 B = F_j, \quad (2.21)$$

де $p_{ej}^5 = f_5 \eta^5 B = F_j$ – оцінка того, як вплине на контрагента інформація направлена на пониження підтримки своєї армії при бажаному впливі F_j .

6. Від контрінформаційних заходів направлених на зрив запланованих заходів впливу

$$p_{ej}^6 = f_6 \eta^6 X = F_j, \quad (2.22)$$

де $p_{ej}^6 = f_6 \eta^6 X = F_j$ – оцінка того, як впливатимуть контрзаходи на хід виконання запланованого впливу при бажаному впливі F_j .

7. Від того, на якій стадії знаходиться вплив

$$p_{ej}^7 = f_7 \eta^7 t_e = F_j, \quad (2.23)$$

де $p_{ej}^7 = f_7 \eta^7 t_e = F_j$ – ймовірність того, що на фазі виконання впливу t_e буде інформаційний вплив F_j ; t_e – фаза впливу.

По суті цими функціями (2.17 – 2.23) задана випадкова поведінка системи інформування контрагента K , відносно компоненту впливу j_e , де з ймовірностями, які відповідають оцінкам $p_{ej}^k K$, $k = \overline{1,7}$ реалізується вибір виду дії (впливу) на нього F_j . Тепер необхідно оцінити визначеність (пріоритетність, важливість, першочерговість) інформаційного впливу F_j при всіх 7-х діях на систему. Це питання буде розглянуто в розділі 3, після того, як визначено буде характеристики можливих дій на контрагента впливу (форм інформаційного впливу) F_j .

2.4. Математична модель взаємозалежності впливів та поведінки контрагента взаємодії

Поведінка будь якого контрагента (в тому числі ворога) визначається впливами на нього (рис.2.4). Таким чином, для вироблення потрібної поведінки контрагента взаємодії (реакції) необхідно підібрати відповідні впливи. Для цього пропонується модель розрахунку потрібної реакції контрагентів взаємодії.

Будемо виходити з позиції, що будь який інформаційний вплив призводить до збільшення чи зменшення ймовірності потрібної реакції

$$p(R_i) \neq p(R_i / A_j), \quad (2.24)$$

де $p(R_i)$ – безумовна ймовірність реакції (поведінки) R_i у контрагента (визначена його початковою інформованістю);

$p(R_i / A_j)$ – ймовірність реакції (поведінки) R_i у контрагента після впливу A_j (визначена його новою інформованістю).

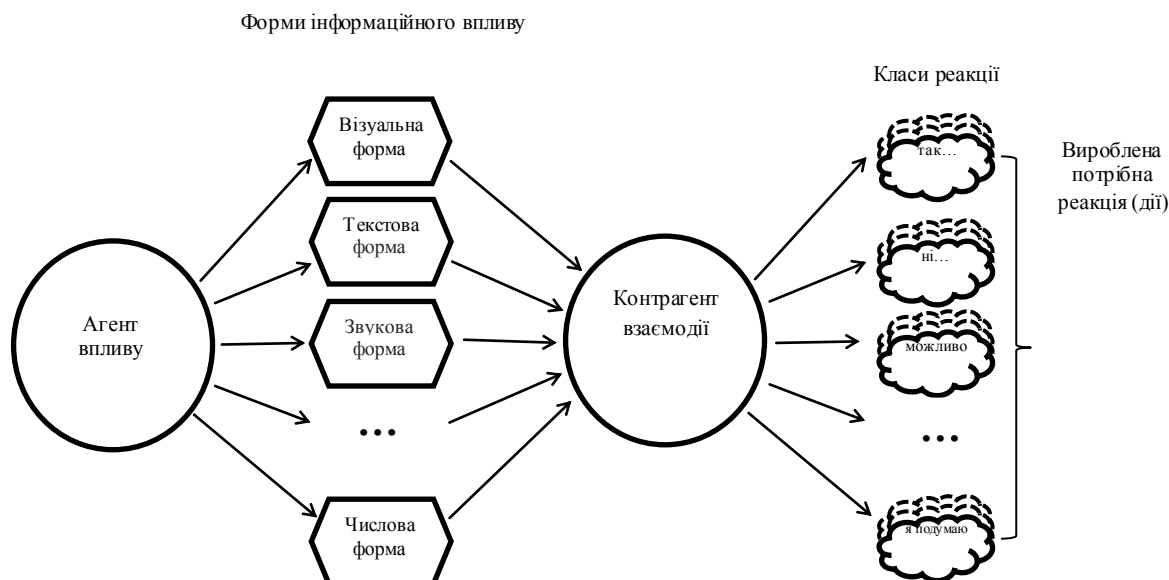


Рис. 2.4. Схема інформаційного впливу з метою вироблення потрібної реакції (дії)

Тоді, якщо реакція бажана, то необхідно підібрати такі впливи, які збільшують її ймовірність. Якщо існують підмножини

$$A^+ = \{A_{j_k}\}, k = \overline{1, n^+};$$

$$A^- = \{A_{j_l}\}, l = \overline{1, n^-},$$

де $p(R_i / A_{j_k}) > p(R_i)$; $p(R_i / A_{j_l}) \leq p(R_i)$;

n^+ – кількість «позитивних» впливів;

n^- – кількість «негативних» впливів.

Тоді для формування потрібної реакції у противника необхідно підібрати ті впливи, які є найбільш значними.

$$p(R_i / A_{j_k}) \gg p(R_i)$$

Вплив на контрагента вимірюватимемо величиною (зростання) ймовірності безумовної події та визначаємо через відхилення умовної ймовірності, від безумовної. Представимо таку оцінку формулою

$$w(R_i / A_{j_k}) = \frac{p(R_i / A_{j_k}) \cdot \overleftarrow{(-p(R_i))}}{\overleftarrow{(-p(R_i / A_{j_k}))} \cdot \overrightarrow{p(R_i)}}, \quad (2.25)$$

де $w(R_i / A_{j_k})$ – оцінка величину впливу A_{j_k} на реакцію R_i .

Перейдемо від величини впливу до ймовірності реакції R_i при багатьох впливах. Для цього пропонується наступна формула

$$w(R_i / A^+) = \sum_{k=1}^{n^+} \left[w(R_i / A_{j_k}) - 1 \right] + 1, \quad (2.26)$$

де $w(R_i / A^+)$ – оцінка величини всіх позитивних впливів на реакцію R_i .

Тепер використовуючи формули (2.25) і (2.26) можна перейти до нової ймовірності реакції:

$$p(R_i / A^+) = \frac{w(R_i / A^+) \cdot p(R_i)}{1 + p(R_i) \cdot (w(R_i / A^+) - 1)}, \quad (2.27)$$

де $p(R_i / A^+)$ – ймовірності реакції R_i після всіх позитивних впливів на контрагента взаємодії A^+ .

Потрібно також враховувати таке важливе явище, як довіра до джерела інформації [3], тобто, якщо невідоме або джерело до якого у вас втрачена довіра намагатиметься хоч багато раз достукатися до вашої свідомості надаючи правдиву і підтверджену інформацію, сам факт недовіри до джерела справить на вас протилежну, щодо очікуваної, дію. І навпаки, якщо джерелу ви довіряєте завдяки внутрішньому настрою, зовнішнім чинникам чи іншим моральним, сердечним та іншим факторам, то таке джерело є найкращим модулятором вашого відношення до дійсності, навіть коли вона не відповідає реалії. Виходячи з цього опишемо сутність довіри до джерела інформації та дамо оцінку цьому впливу на хід проведення запланованого інформаційного впливу.

Насамперед **довіра** це певний стан психологічного внутрішнього спокою, що проявляється за відсутності подразників та переживань. Коли людина довіряє вона робить це добровільно, свідомо, ставлячи своє благополуччя у залежність від зовнішнього фактору і в першу чергу іншій людині, яка викликає довіру [20].

Позначимо D^+ джерело інформації таким, що викликає довіру у контрагента взаємодії, та D^- джерело інформації, яке збуджує у контрагента взаємодії лише негативні спогади, втрачено довіру.

Якщо джерело впливу дає інформацію, яка збігається з відношенням до дійсності у контрагента взаємодії, то довіра збільшується. І навпаки, коли надана інформація не збігається з відношенням до дійсності контрагента, то довіра, відповідно, зменшується. Тому кінцева формула зазнає коректив з застосуванням довіри.

Якщо $p(R_i / A_{j_k}) \gg p(R_i)$, то

$$p(R_i / A_{j_k} (D^+)) > p(R_i / A_{j_k} (0)) \gg p(R_i) > p(R_i / A_{j_k} (D^-)),$$

де $p(R_i / A_{j_k} (D^+))$ – оцінка ймовірності реакції R_i від впливу, який формується джерелом, що викликає довіру $A_{j_k} (D^+)$;

$p(R_i / A_{j_k} (D^-))$ – оцінка ймовірності реакції R_i від впливу, який формується джерелом, що не викликає довіру $A_{j_k} (D^-)$;

$p(R_i / A_{j_k} (0))$ – оцінка ймовірності реакції R_i від впливу, який формується невідомим джерелом (не викликає ні довіри, ні недовіри).

Якщо у джерела, що надає інформацію відсутня довіра, то щоб досягти поставленої мети йому необхідно надавати недостовірну інформацію (протилежну задуму), яка буде спонукати контрагента до протилежних надаваній інформації діям, що в свою чергу буде відповідати реакції щодо задуму впливу.

$$p(R_i / A_{j_l} (D^+)) < p(R_i / A_{j_l} (0)) \ll p(R_i) < p(R_i / A_{j_l} (D^-)),$$

де $p(R_i / A_{j_l} (D^+))$ – оцінка ймовірності реакції R_i від негативного впливу, який формується джерелом, що викликає довіру $A_{j_l} (D^+)$;

$p(R_i / A_{j_l} (D^-))$ – оцінка ймовірності реакції R_i від негативного впливу, який формується джерелом, що не викликає довіру $A_{j_l} (D^-)$;

$p(R_i / A_{j_l} (0))$ – оцінка ймовірності реакції R_i від негативного впливу, який формується невідомим джерелом (не викликає ні довіри, ні недовіри).

Розраховуючи результати різноманітних впливів з використанням наведеної моделі можна визначити стратегію поведінки власних сил інформаційного впливу з тим, щоб застосувати такий набір несилкових дій та засобів їх надання, які забезпечать потрібну реакцію противника (відведення військ, перекидання їх на другорядні напрямки, відміна наступу і т.п.). Схема залежності результату впливу від ступеня довіри до джерела інформаційного впливу представлена на рис.2.5.

Щоб визначити необхідну величину інформаційного впливу на контрагента взаємодії з використанням наведеної моделі потрібно вирішити такі основні задачі: визначити найвпливовішу на контрагента взаємодії інформацію, виділити можливі впливи та шляхи їх реалізації; експертно оцінити результати цих впливів; підібрати таку комбінацію впливів, яка забезпечить необхідну реакцію контрагента взаємодії; реалізувати підібрані впливи.



Рис. 2.5. Схема залежності результату впливу від ступеня довіри до джерела інформаційного впливу

Метою використання наведеної моделі є створення методу для:

1. Пошуку слабких місць в ідеології противника та вплив на населення таким чином, щоб воно перестало його підтримувати.
2. Контролю власного інформаційного простору, захист його від противника (контрінформованість).
3. Ведення інформаційних атак на ворога.
4. Підвищення загальної ефективності збройних сил за допомогою повсюдного використання інструментів інформаційного (несилового) впливу на противника.

Цьому буде присвячено наступний розділ дисертації.

Висновки до розділу 2

1. З'ясовано, що загальноприйняті підходи не дозволяють ефективно керувати процесами цілеорієнтованих інформаційних взаємодій в управлінні впливами, не дозволяють ціленаправлено змінювати інформованість контрагента взаємодії з метою прийняття ними оптимальних для виконання плану впливу рішень. В зв'язку з цим запропоновано концепцію управління інформованістю через поєднання принципів впливу на об'єкти впливу (війська, народ, розвідку, тощо) з визначеними (як найбільш впливовими) формами надання інформації з метою формування необхідного відношення (інформованості) у них.

2. Надано основні визначення дисертаційної роботи, які утворюють понятійний простір досліджень.

3. Розроблено та описано концептуальну модель визначення необхідних інформаційних впливів на контрагента взаємодії. Наведено принципи створення системи відбору інструментів впливу, що є концептуальною основою наукових досліджень.

4. Запропоновано математичну модель визначення потрібної інформованості контрагентів взаємодії. Та зазначено, що для забезпечення найкращого інформаційного впливу необхідно не тільки вміти його формувати в процесі управління, але і визначати, яка інформація буде мати найбільший вплив на контрагента впливу, і у якому вигляді її краще надати. Необхідно якісно і ефективно управляти необхідною мірою і змістом інформації, для прийняття оптимального рішення.

5. Визначені характеристики контрагентів взаємодії на які впливає наша інформація. Запропонована оцінка впливу, яка базується на тому на скільки фактичне значення відповідає бажаному.

6. Запропоновано модель розрахунку величини впливу та оцінки цього впливу на контрагента взаємодії (противника) та цільову функцію в основі якої різниця між вигодою, яка буде отримана від впливу на контрагента і витратами на ці впливи.

7. Формалізовано та складено структуру процесу визначення впливу поточної ситуації у впливах на прийняття контрагентом необхідного, у відповідності з планом, рішення. Показано, що вплив на контрагентів взаємодії визначається відхиленнями в результаті інформаційного впливу на них впливу зі сторони керівництва держави, впливами зі сторони міжнародної спільноти, інформаційного впливу, яку зумовлюють «звірства» щодо полонених, на санкції міжнародної спільноти щодо країни-агресора, інформаційного впливу на населення, щодо пониження підтримки своєї армії (висвітлення недобрих фактів, перекручування інформації, відкрита брехня), інформаційного впливу, як контрзахід

противника.

Список використаних джерел

- [1] Бушуев С. Д. та ін. Креативные технологии управления проектами и программами, Київ: Саммыт-Книга, 2010. С. 5–8.
- [2] Горбулін В. П., Биченок М. М. Проблеми захисту інформаційного простору України: монографія. Київ: Інтертехнологія, 2009. 136 с.
- [3] Кривошея Т., Ятвецька Г., Сербіна Ю., Шелест Г., Рівень довіри населення до різних джерел інформації та новин: Прикордонні райони Одеської області. Соціологічний аналіз: Українська миротворча школа, 2016, URL: <http://peace.in.ua/wp-content/uploads/2016/01/Zvit-info1.pdf>. (дата звернення: 05.06.2016).
- [4] Кубявка Л. Б. Управління проектами впливів у програмах інформатизації вищих навчальних закладів: автореф. дис... канд. техн. наук: 05.13.22, Київ. нац. ун-т буд-ва і архітектури. Київ, 2015. 20 с.
- [5] Кубявка М. Б. Інформаційні дії по формуванню необхідної інформованості контрагента впливу. *Телекомунікаційні та інформаційні технології*. 2016. №4. С. 24–28.
- [6] Кубявка М. Б. Управління інформаційними впливами на противника з врахуванням поточної ситуації. *Збірник наук. праць Військового інституту Київського націон. ун-ту ім. Шевченка*. 2016. №53. С. 99–104.
- [7] Кубявка М. Б., Кубявка Л. Б. Модель інформаційної дії на контрагентів впливу. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2016. № 3(27). С. 54–58.
- [8] Ларичев О. И. Теория и методы принятия решений. 2-е изд., перераб. и доп. Москва: Логос, 2002. 392 с.
- [9] Левченко О. В. Класифікація інформаційної зброї за засобами ведення інформаційної боротьби. *Сучасні інформаційні технології у сфері безпеки та оборони*, 2014. № 2. С. 142–146.

[10] Медведєва О. М. Особливості застосування положень теорій несилового взаємодії для системного вирішення завдань діяльності за проектом сприяння процесам розвитку організації. *Управління проектами та Розвиток виробництва: вид-во СНУ ім. В.Даля*, 2010. № 2 (34). С. 122–132.

[11] Морозов А. А. Ситуационные центры. Понятия и определения. *Математичні машини і системи*, 2016. № 1. С. 48–54.

[12] Нейтан Яу. Искусство визуализации в бизнесе. Как представить сложную информацию простыми образами, Манн: Иванов и Фербер, 2013. 338 с.

[13] Расторгуев С. П. Информационная война. Москва: Радио и связь. 1998. URL: <http://evartist.narod.ru/text4/54.htm> (дата звернення: 21.02.2015).

[14] Рачинський А. П. Стратегічне управління персоналом в органах державної влади (теоретико-методологічний аналіз): монографія, Київ: НАДУ, 2009. 316 с.

[15] Самохвалов Ю. Я., Науменко Е. М. Экспертное оценивание. Методический аспект, Київ: Видавництво ДУІКТ, 2007. 264 с.

[16] Соловцов Н. Е., Глазов Б. И., Ловцов Д. А. Классификация и способы применения “информационного оружия”. *Стратегическая стабильность*, 1999. №4. С. 17–22.

[17] Тесля Ю. Н. Рефлекторная система обработки естественно-языковых текстов в АСУ строительством сложных энергетических объектов. *Радиоэлектроника и информатика*, 1998. №4. С.52-55.

[18] Тесля Ю. Н., Решотько Д. А. Теория несилового взаимодействия и ее приложения к диагностике сердечно-сосудистых заболеваний. *Управління розвитком складних систем*, 2012. №12. С. 111-115.

[19] Черноручкий И. Г. Методы принятия решений. СПб.: БХВ-Петербург, 2005. 416 с.

[20] Що таке довіра та кому довіряти. URL: <http://www.etica.in.ua/shho-take-dovira-ta-komu-doviryati>. (дата звернення: 05.06.2016).

РОЗДІЛ 3

МОДЕЛІ ТА МЕТОД УПРАВЛІННЯ ІНФОРМАЦІЙНИМ СУПРОВОДЖЕННЯМ

«У наш час ми страждаємо не стільки із-за браку інформації, скільки від надлишку зайвої, непотрібної інформації, що не має ніякого стосунку до виходу з кризових ситуацій. Знайдіть можливості відокремити марне від важливого, і ви відчуєте, що володієте ситуацією» [2].

3.1. Управління інформаційним супроводженням процесів впливу на контрагента взаємодії

Система управління інформаційним супроводженням повинна забезпечити постійну наявність релевантної інформації, що володіє такими характеристиками, як адресність, своєчасність, достовірність, повнота.

Релевантна інформація важлива для прийняття управлінських рішень тому, що вона містить дані, які слід використовувати для розрахунків при підготовці інформації що буде надаватися контрагентам взаємодії. Нерелевантна інформація - це несуттєві, надлишкові дані, які не несуть корисного впливу на контрагента взаємодії. Використання нерелевантної інформації може призвести до пониження рівня впливу або ж його унеможливлення [1].

Однією з найбільш складних завдань при створенні такої системи управління [5] є перетворення неявних (імпліцитних) знань контрагентів в явні (експліцитні). Що досягається за умови використання лише релевантної інформації з обов'язковим визначенням кінцевих цілей впливу.

Основною ж задачею цієї роботи є створення інформаційної технології, яка буде знаходити необхідну (релевантну) інформацію, яка б відповідала критеріям найбільш впливової дії на контрагента взаємодії та здійснювала надання цієї інформації з урахуванням його особистих уподобань та індивідуальних морально-психологічних якостей, тобто створити інформаційну технологію управління

3.1.1. Класифікація контрагентів взаємодії за особливостями сприйняття ними інформації

Для ефективного управління знаннями у контрагента взаємодії необхідно визначити, яка інформація і як вплине на його рішення, відібрати найбільш впливову інформацію та розглянути найкращі шляхи представлення цієї інформації. Для вирішення цієї задачі класифікуємо об'єкти впливу за специфікою сприйняття інформації та заздалегідь відомим відношенням до неї [1]. Тобто інформація, надана мусульманину, про те, що християнство - єдина правильна релігія, викличе максимум так це бурю виплеснутих емоційних переживань та ще одне підтвердження правоти ведення тисячолітніх війн між «істинними» віруючими та «невірними».

Виходячи з цього, виділеними ознаками, що забезпечать класифікацію для пошуку і надання інформації є:

1. Національна належність. Національно-психологічні особливості становлять особливий інтерес для фахівців інформаційно-психологічної війни. Вони є найважливішою характеристикою, специфіку якої необхідно враховувати для досягнення максимального ефекту інформаційно-психологічного впливу, тому що, якщо способи інформаційно-психологічного впливу на війська і населення противника, зміст і форма подачі агітаційно-пропагандистських матеріалів не відповідають національно-психологічним особливостям об'єкта, то сам цей вплив виявиться або даремним, або призведе до протилежного результату [7]. Так російські маркетологи встановили, що один і той же рекламний ролик позитивно впливає на росіян, але у українців (як приклад) викликає інше відношення до продукції, що рекламується.

2. Належність за статтю. Практично не існує такого явища, з приводу якого чоловіки і жінки зійшлися б у думках. Ми залишаємося загадкою один для одного і, по суті, живемо в двох відокремлених, лише зрідка перетинаючих один одного, реальностях, відповідно вплив на жінок та чоловіків повинен дещо відрізнятися;

3. Вікова належність [6], с. 39]. Нині прийнята наступна вікова періодизація: дитинство (від народження до 1 року); перед дошкільне дитинство (1-3 роки); дошкільне дитинство (3-6 років); молодший шкільний вік (6-10 років); підлітковий вік (10-15 років); юність: перший період (старший шкільний вік 15-17 років), другий період (17-21 рік); зрілий вік: перший період (21-35 років), другий період (35-60 років); літній вік (60-75 років); старечий вік (75-90 років); довгожителі (90 й вище) і для кожного вікового періоду найбільш прийнятна інформація повинна мати свій специфічний «смак» чи «колір», ми ж до подальшої роботи визначимо інший варіант, який визначається сьогоденням: діти; молодь, що навчається; молодь, що працює; підприємці; працівники; військовослужбовці; пенсіонери.

4. Належність за сприйняттям інформації [3].

Усі люди сприймають і запам'ятовують інформацію по-різному. Так, ті, хто отримує інформацію через слуховий канал, називаються **аудіалами**. Вони прекрасні слухачі, що запам'ятовують подробиці розповіді та сприймають інтонацію, тембр мови, мають гострий слух і чудову пам'ять.

Візуали - це людина, яка сприймає більшість інформації з допомогою зору 30% населення.

Кінестетики - той, хто сприймає інформацію через інші відчуття (дотик, нюх тощо) 40% населення.

Є також люди, у яких сприйняття інформації відбувається через логічне осмислення, з допомогою цифр, знаків, логічних доказів, вони називаються **дискрети**.

Зрозуміло, що будь-яка людина протягом свого життя використовує різні канали сприйняття. Вона може бути за своєю природою візуалом, та це не значить, що інші органи чуттів у неї практично не працюють. Чим більше каналів відкрито для прийняття інформації, тим ефективніше відбувається процес сприйняття.

5. Рід діяльності, робота, хоббі чи спосіб життя.

Наведена вище класифікація допоможе нам зрозуміти особливий підхід до кожного людського створіння, як до особистості, а в подальшому перенести ці знання на сім'ю, групу, країну, можливо світ.

3.1.2. Класи повідомлень з заданим впливом на контрагента взаємодії

Найбільш **важливими властивостями** інформації, які ми всі добре знаємо є: об'єктивність та суб'єктивність, повнота, достовірність, адекватність, доступність, актуальність, точність, цінність.

Давно вже визначено, що **основними видами** повідомлень є: графічна, звукова, текстова, числова та відеоінформація.

А найбільш розповсюдженими **способами подачі** інформації є: мова (усний обмін інформацією), писемність, преса, книги, радіо, кіно, телебачення, комп'ютер.

Використовуючи вище наведені властивості інформації, специфічність людської сутності до сприйняття інформації та на основі проведених досліджень здійснено класифікацію змісту повідомлень з заданим впливом на контрагента взаємодії з урахуванням вікової та ділової належності за критеріями максимальної реакції (зміні світогляду) [1].

1. Зміст повідомлень прийнятний для дітей:
 - 1.1. Що несе похвалу;
 - 1.2. Що несе покарання;
 - 1.3. Про розважальні заходи та свята;
 - 1.4. Про отримання високу оцінку успішності;
 - 1.5. Про улюблені страви та уподобання;
 - 1.6. Щодо несправедливості по відношенню до них;
 - 1.7. Щодо невиконання даних обіцянок;
 - 1.8. Про кумирів та улюбленців;
 - 1.9. Про необхідність виконання домашніх та шкільних обов'язків;
 - 1.10. Про загрозу життю та здоров'ю близької людини.

2. Зміст повідомлень прийнятний для молоді, що працює:

2.1. Що несе похвалу, або позитивну оцінку праці;

2.2. Що несе покарання, або негативну оцінку праці;

2.3. Про стан здоров'я близьких;

2.4. Про рівень заробітної плати;

2.5. Про рівень плати за ЖКХ;

2.6. Про коливання курсу валют та цін на продукти і товари;

2.7. Про стан справ в зоні проведення АТО;

2.8. Про санкції світової спільноти до держави-агресора;

2.9. Про діяльність керівництва держави та високу боєздатність армії щодо забезпечення захисту країни;

2.10. Про «звірства» щодо полонених зі сторони терористичних формувань на сході країни;

2.11. Про «недобрі» факти з життя своєї армії (їх перекручення, відкрита брехня);

2.12. Про загрозу життю та здоров'ю близької людини.

3. Зміст повідомлень прийнятний для молоді, що навчається:

3.1. Що несе похвалу, або позитивну оцінку навчання;

3.2. Що несе покарання, або негативну оцінку навчання;

3.3. Про зміни в освітній програмі студентів;

3.4. Про стан стипендій та плати за гуртожиток;

3.5. Про громадсько-розважальні заходи та заклади;

3.6. Про національну свідомість та самовизначеність;

3.7. Про стан справ в зоні проведення АТО;

3.8. Про санкції світової спільноти до держави-агресора;

3.9. Про діяльність керівництва держави та високу боєздатність армії щодо забезпечення захисту країни;

3.10. Про «недобрі» факти з життя своєї армії (їх перекручення, відкрита брехня);

- 3.11. Про можливість самореалізації після навчання;
- 3.12. Про загрозу життю та здоров'ю близької людини.

4. Зміст повідомлень прийнятний для підприємців:

- 4.1. Що несе позитивну оцінку підприємницької діяльності;
- 4.2. Що несе негативну оцінку підприємницької діяльності;
- 4.3. Про стан здоров'я дітей та близьких;
- 4.4. Про стан справ та ріст доходів підприємства;
- 4.5. Про рівень плати за ЖКХ;
- 4.6. Про коливання курсу валютного ринку;
- 4.7. Про стан справ в зоні проведення АТО;
- 4.8. Про санкції світової спільноти до держави-агресора;
- 4.9. Про діяльність керівництва держави та високу боєздатність армії щодо забезпечення захисту країни;
- 4.10. Про «звірства» щодо полонених зі сторони терористичних формувань на сході країни;
- 4.11. Про «недобрі» факти з життя своєї армії (їх перекручення, відкрита брехня);
- 4.12. Про загрозу життю та здоров'ю близької людини.

5. Зміст повідомлень прийнятний для працівників:

- 5.1. Що несе похвалу, або позитивну оцінку праці;
- 5.2. Що несе покарання, або негативну оцінку праці;
- 5.3. Про стан здоров'я дітей та близьких;
- 5.4. Про заробітну плату;
- 5.5. Про рівень плати за ЖКХ;
- 5.6. Про коливання курсу валют та цін на продукти і товари;
- 5.7. Про стан справ в зоні проведення АТО;
- 5.8. Про санкції світової спільноти до держави-агресора;

5.9. Про діяльність керівництва держави та високу боєздатність армії щодо забезпечення захисту країни;

5.10. Про «звірства» щодо полонених зі сторони терористичних формувань на сході країни;

5.11. Про «недобрі» факти з життя своєї армії (їх перекирення, відкрита брехня);

5.12. Про загрозу життю та здоров'ю близької людини.

6. Зміст повідомлень прийнятний для військовослужбовців:

6.1. Що несе похвалу, або позитивну оцінку службової діяльності;

6.2. Що несе покарання, або негативну оцінку службової діяльності;

6.3. Про стан здоров'я дітей та близьких;

6.4. Про грошове забезпечення;

6.5. Про рівень плати за ЖКХ;

6.6. Про коливання курсу валют та цін на продукти і товари;

6.7. Про стан справ в зоні проведення АТО;

6.8. Про санкції світової спільноти до держави-агресора;

6.9. Про діяльність керівництва держави та високу боєздатність армії щодо забезпечення захисту країни та рівня соціального забезпечення військовослужбовців;

6.10. Про «звірства» щодо полонених зі сторони терористичних формувань на сході країни;

6.11. Про «недобрі» факти з життя своєї армії (їх перекирення, відкрита брехня);

6.12. Про загрозу життю та здоров'ю близької людини.

7. Зміст повідомлень прийнятний для пенсіонерів:

7.1. Що несе похвалу;

7.2. Що несе покарання;

7.3. Про стан здоров'я дітей, внуків та близьких;

- 7.4. Про стан пенсійного забезпечення та соціального забезпечення;
- 7.5. Про рівень плати за ЖКХ;
- 7.6. Про коливання курсу валют та цін на продукти і товари;
- 7.7. Про стан справ в зоні проведення АТО;
- 7.8. Про санкції світової спільноти до держави-агресора;
- 7.9. Про діяльність керівництва держави та високу боєздатність армії щодо забезпечення захисту країни;
- 7.10. Про «звірства» щодо полонених зі сторони терористичних формувань на сході країни;
- 7.11. Про «недобрі» факти з життя своєї армії (їх перекручення, відкрита брехня);
- 7.12. Про загрозу життю та здоров'ю близької людини.

3.2. Інформаційне середовище впливу на контрагента взаємодії

Наведений зміст повідомлень повинен застосовуватися вибірково та дозовано, в залежності від функціональних ролей та у відповідності з функціональними задачами в компонентах впливу. Але саме головне, він повинен представлятися у вигляді деяких інформаційних моделей, які дозволяють формально оперувати з ними в системі управління інформованістю (відношенням до дійсності), що в свою чергу дозволить приймати рішення, які призведуть до оптимальних і раціональних дій контрагента взаємодії. Розглянемо класи повідомлень в розрізі функціональних ролей впливу (табл.3.1).

Такий розріз необхідний тому, що зміст повідомлення конкретизується тими даними, які найбільш відповідають суті задачі управління впливами, що розв'язується.

Для успішного використання повідомлень інформації необхідно щоб ця модель мала зручний та понятійний вигляд, а інформованість контрагента відбувалася поступово, не нав'язливо з максимальним інформуванням.

Функціональні ролі форм впливу

Функціональна роль форм впливу	Як забезпечити
Викликати почуття віри та надії	1. Використати джерело, що заслуговує довіру; 2. Надати інформацію, що переплітається з знаннями контрагента.
Викликати почуття любові та радості	1. Задоволення своїми діями або спільними діями групи людей (перемога улюбленої спортивної команди, перемога бажаного кандидата на виборах і тому подібне);
	2. Оскільки радість може виникати в результаті ослаблення болю, нервової напруги і негативних емоцій, вона здібна викликати ваблення або прив'язаність до об'єкта, який допоміг усунути ту чи іншу негативну емоцію.
Викликати ентузіазм та сміливість	1. Навіть маленьке заохочення може викликати невичерпний ентузіазм, як реакцію на щось прекрасне, чуттєво піднесене; 2. Розвивати національний бойовий дух, який базуватиметься на високих моральних цінностях та усвідомлення ролі чоловіка, жінки, як окремої частинки суспільства.
Викликати почуття колективізму та національної свідомості	1. Проведення заходів щодо національного виховання; 2. Підвищення моралі шляхом заохочення до усвідомлювання та підтримки національних цінностей.
Викликати почуття впевненості	1. Забезпечити стабільність отримання ЗП; 2. Проведення заходів щодо національного виховання.
Викликати почуття захищеності	1. Забезпечити стабільність отримання ЗП; 2. Заходи щодо національного виховання.
Викликати почуття забезпеченості	1. Забезпечити стабільність отримання ЗП; 2. Підвищення моралі шляхом навіювання національних цінностей.
Привити порядність та здержаність	1. Підвищення моралі шляхом навіювання високих моральних цінностей; 2. Використати джерело, що заслуговує довіру.
Привити повагу до людей та Батьківщини	1. Навіювання високих національних цінностей; 2. Використати джерело, що заслуговує довіру. 3. Формувати загальну ідеологію нації.

Таблиця 3.1 (продовження)

Функціональна роль форм впливу	Як забезпечити
Викликати почуття тривоги	1. Використати джерело, що не заслуговує довіру; 2. Надати інформацію, що іде в розріз з знаннями контрагента.
Викликати байдужість та черствість, брехливість та вульгарність, грубість (брутальність), жорстокість та агресивність, лінивість	1. Пониження моралі шляхом навіювання хибних цінностей; 2. Штучний розділ єдиного суспільства на «білих» і «чорних», «власних» і «хлопів» і т.д. 3. Заниження цінності життя людини, як життю необхідної частинки нації, суспільства, світу в цілому.
Привити підозрілість (недовірливість)	1. Надати життєвий досвід «бути обманутим». 2. Пониження моралі шляхом навіювання хибних цінностей.
Привити жадібність, розвивати схильність до шахрайства	1. Надати життєвий досвід «бути обманутим», стимулювати вислів «менше народа – більше кислорода»; 2. Пониження моралі шляхом навіювання хибних цінностей.
Привити лихослівність та нескромність	1. Пониження моралі шляхом навіювання хибних цінностей; 2. «Словесний бруд» навколо нас.
Викликати боягузтво та ненадійність	1. Надати життєвий досвід «бути зрадженим»; 2. Пониження моралі шляхом навіювання хибних цінностей.
Стимулювати нахабність та невічливість	1. Пониження моралі шляхом навіювання хибних цінностей; 2. Зниження етики поведінки та спілкування.

3.3. Метод адресно-орієнтованого управління інформаційним супроводженням

Під управлінням інформаційним супроводженням в дисертаційній роботі розуміється адресація тієї чи іншої інформації конкретним споживачам.

Визначення 3.1. Під інформацією, яка направляється споживачам (контрагентам) будемо розуміти деяке повідомлення, яке несе нову інформацію і призводить (може призвести) до змін у проявах цих споживачів.

Під повідомленням будемо розуміти будь яку інформацію (телепередачі, газетні статті, Інтернет замітки і т.п.), яка буде направлятися споживачам. Які її отримавши приймуть (можуть прийняти) необхідні для нас рішення. За ідеєю весь потік інформації (всі повідомлення), що використовуються і технології супроводження процесів впливу на контрагента взаємодії потрібно розподілити по адресатам. Вище було визначено як класи контрагентів взаємодії (споживачів інформації), та які класи повідомлень будуть оброблятися в названій технології. Будемо вважати, що інформація про те, кому направити повідомлення, є в самому повідомленні.

Визначення 3.2. Адресат повідомлення може бути визначений із самого повідомлення. Це є необхідною і достатньою умовою визначення інформації про те, кому направити повідомлення.

Таким чином задача перетворюється в задачу обробки природномовних текстів, але з такими особливостями:

1. Потрібно визначати не зміст (як робить більшість природномовних систем), а того адресата повідомлення, для якого ймовірність потрібної реакції збільшиться (2.24).

2. Потрібно «вміти» відсіювати повідомлення, в яких не міститься інформація про адресата, на якого ця інформація найбільше вплине.

Ці задачі дуже складні і не мають поки що задовільного рішення в наукових дослідженнях. Для їх розв'язання пропонується застосувати ідеї теорії несилової взаємодії, а саме ті, що пов'язані з побудовою рефлекторних інтелектуальних систем [9]. Будемо вважати, що будь яка комбінація букв (слів) повідомлення з різними ймовірностями визначає адресатів повідомлення. Наприклад, слово «мир» збільшує ймовірність того, що ця інформація повинна бути направлена матерям солдатів. А слово «гроші» - бізнесменам. Звичайно ця ймовірність ніколи не буде одиничною.

Для вирішення цієї задачі скористаємось наступною формалізацією. Наведені задачі є наслідком тих, що вирішувались в розділі 2. В підрозділі 2.4 була побудована математична модель впливу на контрагента взаємодії, з

використанням якої розрахувати, як ті чи інші повідомлення змінять його. Відповідно, можна перейти до вирішення основної задачі інформаційного супроводження процесів впливу на контрагента взаємодії, а саме, визначення адресатів повідомлення. В підрозділі 2.4 побудована модель, яка визначає вплив повідомлень на контрагентів. При цьому контрагенти змінюють свою поведінку. У них з'являються реакції, бажані для того, хто надсилає (генерує) ці повідомлення. Повідомлення ж, в свою чергу, можуть бути отримані різними верствами населення, і мати різний вплив на них. Ці класи були розглянуті теж в розділі 2. Щоб визначити, які повідомлення яким класам контрагентів необхідно відправляти перейдемо в формулах (2.24)-(2.27) від знеособлених контрагентів, до уособлених.

Евристика підходу, що пропонується, є визнання факту, що будь який інформаційний вплив призводить до збільшення чи зменшення ймовірності потрібної реакції у деяких класів користувачів

$$p_k(A_l) \neq p_k(A_l / I_j), \quad (3.1)$$

де A_l – реакція (поведінка) контрагентів взаємодій;

I_j – інформаційний вплив;

$p_k(A_l)$ – безумовна ймовірність реакції (поведінки) A_l у класу контрагентів взаємодій Q_k , якщо на цей клас не буде здійснюватися інформаційний вплив;

$p_k(A_l / I_j)$ – ймовірність реакції (поведінки) A_l у представників класу контрагентів взаємодій Q_k після впливу I_j .

Тоді, на відміну від задачі по визначенню впливу на противника, необхідно підібрати для кожного повідомлення такі класи контрагентів, на які вплив буде максимальний. А саме, для заданих I_j і A_l підібрати такий клас контрагентів Q^* , для якого $p_k(A_l / I_j)$ буде максимальною:

$$Q^* = \max_k \{ p_k(A_l / I_j) \}$$

де Q^* – обраний для реалізації впливу клас контрагентів взаємодії.

Таким чином, виникає задача знаходження функції, що визначає різницю між ймовірністю реакції R_i для класу контрагентів Q^* без впливу, і якщо реалізовано вплив A_j .

Рішення цієї задачі можливе при повторюваності інформаційних впливів, але на практиці такого, практично, не буває. Кожен вплив є комбінаторним, і, як правило, складається з багатьох окремих, інколи незначних елементів. Тоді концептуально цю задачу пропонується вирішити наступним чином. Якщо деяке повідомлення інформативне і значно підвищує ймовірність деякої реакції, то це означає, що і фрагменти повідомлення (окремі речення, слова, комбінації букв) є носіями впливу на контрагента. При появі таких фрагментів ймовірність його реакції змінюється. Як було сказано вище повідомлення, в цілому, не повторюються, але однозначно повторюються їх фрагменти. Наприклад, слова «противник», «ДНР», «зброя» і т.п. Тому можна оцінити зміну ймовірності цієї чи іншої реакції не від усього повідомлення, а від деякого його фрагменту.

Для отримання цієї інформації пропонується наступний експертний метод.

1. Експерту надається текст повідомлення і перелік класів контрагентів із їхніми властивостями.

2. Експерт оцінює інформацію і надає для таких повідомлень найбільш ймовірних адресатів (адресатів, у яких, на його думку, найбільш зміниться ймовірність потрібної реакції).

3. Накопичується статистика за такими експертними оцінками, в тому числі завдяки залученню багатьох експертів.

4. На основі отриманої статистики розраховуються адресати для нових повідомлень.

Для вирішення задачі 4 необхідна розробка методу, в якому на основі експертної оцінки відправки повідомлень адресатам визначаються адресати для нових повідомлень. Існуючі методи вирішення цієї задачі досить складні, вимагають застосування інструментів лінгвістичного аналізу, які для повідомлень різного спрямування використати практично неможливо, або їх створення буде занадто дорогим, адже зазвичай лінгвістичні системи створюються під окремі класи текстів.

Одним із різновидів інтелектуальних систем є рефлекторні інтелектуальні системи [8], які є не чим іншим, як програмними або технічними системи, що формують реакції на несилкові впливи, в основі функціонування яких знаходиться рефлекторний алгоритм, який працює за принципом формування реакції-відповіді (рефлексу) на набір вхідних даних (зовнішній вплив). Але цей підхід поки що ніким не використовувався для визначення адресатів повідомлення. Тому для розв'язання поставленої задачі пропонується використати ймовірно-рефлекторний підхід. В основі рефлексів полягає наступний тезис: якщо це вже було, і деяка реакція була позитивно підкріплена, то необхідно зробити теж саме.

Рефлекторний підхід забезпечує вибір найбільш ймовірної реакції на нескінченність вхідних впливів, при відомих ймовірностях вибору реакції на кожний вхідний вплив, а також на деякі комбінації вхідних впливів.

Схема методу управління інформаційним супроводженням:

1. По різниці між умовною і безумовною ймовірністю появи реакції після появи деякого фрагменту тексту визначається величина впливу на клас контрагентів взаємодії саме цього фрагменту тексту: формули (3.8)-(3.9).

2. Враховуючи всі фрагменти тексту, визначається загальний вплив на клас контрагентів взаємодії: формула (3.10).

3. По величині загального впливу оцінюється (а не визначається) ймовірність потрібної реакції: формула (3.11).

4. Вибираються ті класи контрагентів взаємодії, для яких ймовірність потрібної реакції більше порогового значення (зазвичай – 0,5).

Розглянемо реалізацію методу підбору класів контрагентів взаємодії, для яких ймовірність потрібної реакції більше граничного значення. Метод базується не на розрахунку ймовірностей переадресації повідомлень, а оцінці цієї ймовірності за відхиленнями умовних та безумовних ймовірностей такої адресації від фрагментів природномовного тексту. Використання інформаційно-понятійних і змістовно-релевантних форм в методі, як і засобів інформаційного впливу є взаємодоповнюючим, а не альтернативним. Це теж накладе деякі особливості застосування методу підбору потрібної цілеорієнтованої інформації для

проведення розрахунку величини інформаційного впливу на контрагента взаємодії.

Визначення 3.3. Метод адресації повідомлень для здійснення інформаційного впливу на контрагента взаємодії - метод здійснення пошуку, відбору та представлення потрібної релевантної інформації конкретному класу контрагентів, застосування якої, в рамках зміни інформованості (світогляду) контрагентів взаємодії, приведе до необхідних проявів в їх поведінці.

Під реакцією будемо розуміти правильне визначення адресності інформації.

Адреса інформації – результат, який продукується інтелектуальним апаратом людини. Семантична складова інформації, яка є суттю і продуктом процесів несилової (інформаційної) взаємодії в інтелектуальному апараті людини, визначає її адресність.

Визначення 3.4. Адресність повідомлення – визначений клас контрагентів, для яких зростання безумовної ймовірності події буде найбільшим.

Адресність передбачає розуміння того, кому призначена це повідомлення.

В процесі визначення адресності вироблена реакція вже може і не бути правильною. Точніше, той же результат (оцінка тієї чи іншої адресності) може відповідати дійсності, а може і не відповідати.

При використанні ймовірнісно-рефлекторного підходу необхідно визначити, що є впливом, а що є рефlekсами в засобах інформаційної технології.

З визначення 3.2 впливом є саме повідомлення, а з визначення 3.3 слідує, що реакцією є клас контрагентів взаємодій. Тоді можливості отримати правильного адресата можна представити через певну ймовірність.

$$p_i \approx b_i / k_i, \quad (3.2)$$

де p_i – ймовірність того, що вироблений рефлекс дасть потрібний результат (правильно адресоване повідомлення);

b_i – кількість випробувань, коли було правильно визначено необхідну адресність інформації;

k_i – загальна кількість випробувань.

Визначення адресності інформації на основі оцінки результатів минулих дій можна представити в наступному вигляді табл. 3.2.

Спочатку необхідно визначитись, а що впливає на адресність. Визначення 3.1 і 3.2 дають відповідь на це питання – повідомлення. А значить, і фрагменти природномовного тексту, що переносять це повідомлення. Такі фрагменти будемо називати елементарною одиницею впливу.

Таблиця 3.2

Статистичні дані вироблення рефлексів з визначення адресата повідомлення

Адресність	Скільки разів визначалася адресність інформації	Скільки разів був отриманий необхідний результат
A_1	k_1	b_1
A_2	k_2	b_2
Λ	Λ	Λ
A_i	k_i	b_i
Λ	Λ	Λ
A_m	k_m	b_m

Визначення 3.5. Елементарною одиницею впливу будемо вважати окремий символ, буквосполучення, склад, слово, фразу, речення, уривки тексту, зображення, висловлювання, звук тощо, ту найменшу частинку інформації, що надається контрагенту до сприймання, сприймається ним та приводить до елементарних коректив його світогляду.

Наступним кроком за частотами появи фрагментів в повідомленнях, які адресовані тим чи іншим класам контрагентів, необхідно оцінити ймовірність направлення повідомлення цим контрагентам.

За основу розв'язання цієї задачі взято числову міру впливу на характеристики визначення адресності інформації. В основі розрахунку інформаційного впливу покладено правильно визначена адресність (цілеорієнтація) інформації. Для формалізації цього відслідкуємо різноманітні впливи на процес ідентифікації адресності інформації, що дозволить отримати

залежність відхилення автоматично визначеної адресності інформації від адресності, визначеної експертом.

Для оцінки ймовірності правильно визначеного адресата інформації необхідно:

1. Повідомлення розкласти на множину фрагментів:

$$I = \{i_f, j\} = \overline{1, g}, \quad (3.3)$$

де I – Інформація (повідомлення);

i_f – фрагмент, який часто повторюється;

g – кількість фрагментів.

2. На основі частоти успішних визначень потрібної адресності інформації, можна визначити приблизні значення ймовірності кожного із класів адресності інформації за умови, що фрагмент нової адресності в цей момент теж був присутнім:

$$\forall A_j \in A, i_f \in I : p(A_j / i_f) \approx n(A_j / i_f) \quad (3.4)$$

де $n(A_j / i_f)$ – частота визначення адресності A_j за умови, що фрагмент i_f в тексті був присутнім;

$p(A_j / i_f)$ – ймовірність визначення адресності A_j за умови, що фрагмент i_f в тексті був присутнім.

3. По адресності A_j за її безумовною ймовірністю $p(A_j)$ і частковими умовними ймовірностями $p(A_j / i_1), \dots, p(A_j / i_i), \dots, p(A_j / i_g)$ необхідно оцінити сумісну умовну ймовірність:

$$p(A_j / i_1, \dots, i_i, \dots, i_g) = p(A_j / I) \quad (3.5)$$

Методами теорії ймовірності [4] вирішити задачу знаходження сумісної умовної ймовірності правильно визначеної адресності інформації, за частковими умовними і безумовною ймовірностями, не є можливим. Тому необхідно сформулювати задачу, як оцінити сумісну умовну ймовірність за частковими. Тобто застосувати такий метод оцінки сумісної умовної ймовірності за

частковими, який дозволить вибрати ту адресність, яка була б визначена і експертом. А саме:

$$\forall A_j \in A \exists A_h \in A : p_{M_o}(A_h / I) \geq \eta_{M_o}(A_j / I) / p(A_h / I) \geq p(A_j / I) \approx 1, \quad (3.6)$$

де $\eta_{M_o}(A_h / I)$ – оцінка сумісної умовної ймовірності адресності A_h в інформації I , яка була отримана методом оцінки сумісної умовної ймовірності за частковими;

$\eta_{M_o}(A_j / I)$ – оцінка сумісної умовної ймовірності адресності A_j в інформації I , яка була отримана методом оцінки сумісної умовної ймовірності за частковими;

$p(A_h / I)$ – сумісна умовна ймовірність адресності A_h в інформації I ;

$p(A_j / I)$ – сумісна умовна ймовірність адресності A_j в інформації I ;

M_o – метод оцінки сумісної умовної ймовірності за частковими;

$p_{M_o}(A_h / I) \geq \eta_{M_o}(A_j / I) / p(A_h / I) \geq p(A_j / I)$ – умовна ймовірність

того, що якщо умовна ймовірність визначення адресності A_h інформації максимальна, то і оцінка сумісної умовної ймовірності цієї адресності A_h максимальна.

Вираз (3.6) показує що, якщо сумісна умовна ймовірність визначення адресата A_g максимальна, то майже завжди і максимальна її оцінка. Оптимальний метод M_o завжди дає найвищу оцінку найбільшій сумісній умовній ймовірності.

Відхилення виразу (3.6) від одиниці буде критерієм ефективності методу оцінки сумісних умовних ймовірностей за частковими:

$$p(\eta_{M_o}(A_h / I) \geq \eta_{M_o}(A_j / I) / p(A_h / I) \geq p(A_j / I)) \rightarrow \max, \quad (3.7)$$

при обмеженнях:

1. Інформація I містить множину фрагментів $I = \{i_1, \dots, i_f, \dots, i_g\}$.

2. $\forall A_j \in A$ задано $p(A_j / i_1), \dots, p(A_j / i_f), \dots, p(A_j / i_g)$;

3. $\forall A_j \in A \exists A_h \in A : p(A_h / I) \geq p(A_j / I)$;

4. $\forall A_j \in A : p(A_h / i_1), \dots, p(A_j / i_2), \dots, p(A_j / i_j) \xrightarrow{M_o} \eta_{M_o}(A_j / I)$;

Застосуємо для вирішення цієї задачі математичну модель, представлену в підрозділі 2.4 але вже не за відношенням до впливу на контрагента, а за відношенням до визначення адресата інформації.

Підставивши вирази з таблиці 3.2 в формулу (2.25) отримаємо формулу для оцінки величини впливу деякого фрагменту i_f на адресність повідомлення A_j :

$$1. \text{ Якщо } k_j > b_j \wedge b_j > 0: \quad w(A_j/i_f) = \frac{b_j \cdot \overbrace{(-p(A_j))}^{\sim}}{\overbrace{(j-b_j)}^{\sim} p(A_j)}, \quad (3.8)$$

$$2. \text{ Якщо } k_j = b_j \vee b_j = 0: \quad w(A_j/i_f) = \frac{(b_j + 1) \cdot \overbrace{(-p(A_j))}^{\sim}}{\overbrace{(j-b_j+1)}^{\sim} p(A_j)}, \quad (3.9)$$

де $w(A_j/i_f)$ – оцінка величину впливу фрагменту повідомлення i_f на реакцію (вибір адресата) A_j .

Але в кожному повідомленні багато фрагментів. Тоді сумарний вплив визначимо з формули (2.26):

$$w(A_j/I) = \sum_{f=1}^g \left[w(A_j/i_f) - 1 \right] + 1, \quad (3.10)$$

де $w(A_j/I)$ – оцінка величини всіх впливів на вибір адресата.

Тепер використовуючи формули (3.9) і (3.10) можна перейти до оцінки нової ймовірності вибору адресата A_j :

$$\eta(A_j/I) = \frac{w(A_j/I) \cdot p(A_j)}{1 + p(A_j) \cdot (w(A_j/I) - 1)}, \quad (3.11)$$

де $\eta(A_j/I)$ – оцінка ймовірності вибору адресата A_j .

Оскільки адресатів багато, то така ймовірність розраховується для кожного адресата. І вибираються адресати, оцінка ймовірності для яких більше 0,5:

Направлення повідомлення адресатам, для яких $\eta(A_j/I) \geq 0,5$.

Але для вирішення цієї задачі потрібна експертна інформація про те, наскільки пов'язані класи повідомлень з адресатами (класами контрагентів). Розглянемо це питання.

3.4. Експертний аналіз зв'язку класів контрагентів інформаційної взаємодії з класами повідомлень

Для визначення кількісної міри впливу класів повідомлень (форм) на класи контрагентів взаємодії було проведено експертний аналіз процесів, які супроводжують прийняття рішення по застосуванню повідомлень в різноманітних компонентах впливу і при виконанні різноманітних функціональних ролей. Для цього експертам пропонувалось вказати суб'єктивну ймовірність вибору тієї чи іншої форми повідомлень в різноманітних компонентах впливу і при реалізації різноманітних функціональних ролей.

Визначення 3.6. Суб'єктивна ймовірність – експертна оцінка ймовірності настання тієї чи іншої події.

На основі проведеного соціологічного опитування, яке обіймало дітей шкільного та дошкільного віку та психологів в цих навчальних закладах, аналізу соціальних опитувань в мережі Інтернет та ЗМІ щодо вказаних питань, опитування людей студентського та похилого віку, а також експертів в області соціологічних досліджень сформована інтегрована експертна оцінка суб'єктивної ймовірності реалізації одного із атрибутів моделі при умові, що буде реалізовано інший. За цими ймовірностями можна судити про суб'єктивне відношення експертів до застосування різноманітних форм повідомлень в різних умовах.

В процесі аналізу було виявлено суб'єктивно-ймовірнісні показники застосування:

- класу повідомлень в застосовності до дітей (додаток Б, табл. 1);
- класу повідомлень в застосовності до молоді, що працює (додаток Б, табл. 2);
- класу повідомлень в застосовності до молоді, що навчається (додаток Б, табл. 3);
- класу повідомлень в застосовності до підприємців (додаток Б, табл. 4);
- класу повідомлень в застосовності до працівників (додаток Б, табл. 5);

- класу повідомлень в застосовності до військовослужбовців (додаток Б, табл. 6);
- класу повідомлень в застосовності до пенсіонерів (додаток Б, табл. 7).

Проведений аналіз дозволив створити базис для оцінки важливості інформаційних дій в процесі управління впливами. Що в свою чергу дозволить визначити ті форми повідомлень, які максимально ефективно можуть забезпечити реалізацію цих дій на контрагентів взаємодії.

По суті інформація, що наведена в додатку Б таблиці 1-7, є основою для визначення потрібних для формування оптимальних, раціональних чи доцільних інформаційних впливів на контрагентів взаємодії засобами повідомлень. Для ефективного реалізації інструментів повідомлень необхідно розробити методи ідентифікації інформаційних дій, і потрібних форм повідомлень виходячи із отриманих суб'єктивно-ймовірнісних характеристик сфери застосування.

В результаті вирішення поставленої задачі, інформаційним базисом чого є наведені таблиці, при виникненні тієї чи іншої ситуації, при існуванні проблеми чи її відсутності в процесі управління впливами, при бажанні оцінити один з компонентів впливу та знаючи вид інформації (функціональну роль), яка в даний момент часу найбільш потрібна контрагенту можна буде легко визначити найбільш зручне і інформативне повідомлення. Простішими словами підібрати таку інформацію, яка сформує необхідне відношення до дійсності (необхідні знання) у контрагентів взаємодії. Саме використання вище наведеного методу дозволяє вирішити цю дещо некоректно поставлену задачу. Від визначення адресата повідомлення, до визначення повідомлення, яке потрібно направити вказаному адресату.

Висновки до розділу 3

1. Показано, що інформування контрагентів взаємодії повинне бути таким, щоб забезпечити своєчасне прийняття ними потрібних рішень.

2. Класифіковано контрагентів взаємодії за індивідуальними особливостями їх до сприйняття інформації, дано класифікацію повідомлень з заданим впливом на контрагента взаємодії.

3. Описано інформаційне середовище в процесах управління впливами та розглянуто класи повідомлень в розрізі функціональних ролей впливу. Такий розріз необхідний тому, що зміст повідомлення конкретизується тими даними, які найбільш відповідають суті задачі управління впливами, що розв'язується.

4. Дано основні визначення. Зазначено, що інформація про те, кому направити повідомлення є в самому повідомленні. Визначено, що таким чином задача трансформується в задачу обробки природномовних текстів. Висвітлено дві досить складні задачі визначення адресата повідомлення та відсіювання тих повідомлень в яких не міститься інформація про адресата, на якого ця інформація найбільше вплине.

5. Визнано факт, що будь який інформаційний вплив призводить до збільшення чи зменшення ймовірності потрібної реакції у деяких класів користувачів.

6. Запропоновано використання рефлекторно-ймовірнісного підходу, який поки що не використовувався для визначення адресатів повідомлення. Він базується на інтроформаційних методах і розраховує адекватну вхідним впливам реакцію інтелектуальної системи, характеризується описом поведінки системи на основі рефлексів. В основі рефлексів полягає наступний тезис: якщо це вже було, і деяка реакція була позитивно підкріплена, то необхідно зробити теж саме. Рефлекторний підхід забезпечує вибір найбільш ймовірної реакції на безліч вхідних впливів, при відомих ймовірностях вибору реакції на кожний вхідний вплив, а також на деякі комбінації вхідних впливів.

7. Розглянуто реалізацію методу підбору класів контрагентів взаємодії, для яких ймовірність потрібної реакції більше граничного значення. Метод базується не на розрахунку ймовірностей переадресації повідомлень, а оцінці цієї ймовірності за відхиленнями умовних та безумовній ймовірностей такої адресації від фрагментів природномовного тексту.

8. Проведено експертне оцінювання класів повідомлень. В результаті чого побудовано експертні таблиці залежності класу повідомлень в застосовності до: дітей, до молоді, що навчається, до підприємців, до працівників, до військовослужбовців, до пенсіонерів.

Список використаних джерел

[1] Kubiavka N. The control of information support of the processes of influence on the opponent. *Збірник наук. праць Військового інституту Київського націон. ун-ту ім. Шевченка*, 2016. №54. С. 171-178.

[2] Джефф О`Лири, Принципы центуриона: уроки боя для лидеров на линии фронта, Ростов: Феникс, 2005. 296 с.

[3] Для вчителів та батьків: Типи сприйняття інформації. URL: <http://dnevnik.bigmir.net/groups/article/20340> (дата звернення: 10.09.2016).

[4] Колмогоров А. Н. Проблемы теории вероятностей и математической статистики. *Вестник АН СССР*, 1965. № 5. С. 95.

[5] Комашинский В. И., Смирнов Д.А. Нейронные сети и их применение в системах управления и связи, Москва: Горячая линия – Телеком, 2003. 94 с.

[6] Крутецкий В. А. Основы педагогической психологии, Москва: Просвещение, 1972. 253 с.

[7] Крысько В. Г. Секреты психологической войны (цели, задачи, методы, формы, опыт), Минск: Харвест, 1999. 448 с.

[8] Тесля Ю. М., Каюк П. В., Чернова М. Л. Операции над содержательной информацией в рефлекторных интеллектуальных системах. *Управління розвитком складних систем*, 2010. №2. С. 31-36.

[9] Тесля Ю. Н. Рефлекторная система обработки естественно-языковых текстов в АСУ строительством сложных энергетических объектов. *Радиоэлектроника и информатика*, 1998. №4. С.52-55.

РОЗДІЛ 4

РЕАЛІЗАЦІЯ ТЕХНОЛОГІЇ УПРАВЛІННЯ ІНФОРМАЦІЙНИМ СУПРОВОДЖЕННЯМ

До інформаційних технологій (ІТ) нового покоління належать системи підтримки прийняття рішень [16], [18] та інформаційні технології [5], побудовані на штучному інтелекті (інтелектуальні інформаційні системи) [8], [9], [10], [12], [21], [23], [26].

За основні принципи, базуючись на яких буде побудовано надійну та функціональну технологію супроводження процесів впливу, можна вважати:

- спільність інформаційних масивів, тому що функціонування інформаційної технології повинне здійснюватися на базі єдиних даних інформації;
- комплексність інформації, потрібна для прийняття раціональних управлінських рішень;
- адаптивність до реалізації нових форм і методів інформаційного забезпечення;
- ефективність, тобто отримання таких результатів, які можуть бути використані в управлінні інформаційним супроводженням з позитивним результатом;
- типізація й стандартизація, що дозволяють використовувати стандартне програмне й загальносистемне математичне забезпечення.

Інформаційна технологія управління інформаційним супроводженням (далі – ІТ УІС) [14] повинна створювати умови для розробки прогнозів, моделювання, формування, ведення та актуалізації бази необхідних інформаційних впливів в сучасних умовах інформаційних протиборств. Основною суттю цієї технології є розподіл інформації по кореспондентам.

4.1. Структура технології інформаційного супроводження

Першочерговим кроком до розробки технології інформаційним супроводженням потрібно поєднати вимоги, які частіше всього висуваються до аналогічних систем. Взагалі такі вимоги поділяють на функціональні і не функціональні.

Функціональними вимогами до розробки ІТ УІС є [27]:

- ІТ повинна мати інтуїтивно зрозумілий інтерфейс для зручної роботи з нею;
- трудомісткість обробки даних не повинна перевищувати квадратичну;
- ІТ повинна підтримувати збереження семантики даних при їх імпорті та експорті.

До основних нефункціональних вимог можна віднести [27]:

- ІТ повинна бути розроблена згідно з діючими правилами та стандартами на розробку програмного забезпечення;
- відсутність необхідності змінювати програмний код при зміні структури даних;
- можливість обслуговувати запити, що надходять та забезпечувати надання потрібної інформації.

Вказані вимоги ляжуть в основу проектування та реалізації модулів ІТ управління інформаційним супроводженням.

Основними критеріями якості функціонування ІТ управління інформаційним супроводженням будемо вважати [19]:

- розвинену комунікативну здатність;
- здатність вирішувати слабо організовані задачі;
- здатність до самонавчання;
- здатність обробки великих масивів природномовних текстів;
- можливість застосування технології в різних сферах життєдіяльності;
- здатність прогнозування ймовірності реакції при певному виборі повідомлення;

- здатність до адаптації.

В ході розв'язання основної задачі була розроблена структура інформаційної технології супроводження процесів впливу, логічна і фізична моделі та алгоритм і програмні засоби цієї технології рисунку 4.1.



Рис.4.1. Узагальнена структура інформаційної технології супроводження впливу

Інформаційна технологія включає:

1. Блок додавання інформаційного повідомлення до бази даних дозволяє додати назву повідомлень та самі інформаційні повідомлення, до кожного з них, введені в базу в текстовому представленні.
2. Блок додавання адресата інформаційного повідомлення до бази дозволяє ввести нових адресатів або вибрати їх із уже існуючого списку.
3. База даних створена для зберігання повідомлень та інформації про їх адресність.
4. База адресності повідомлень призначена для зберігання ймовірних адресатів повідомлень, що зберігається в базі даних.

5. Блок введення параметрів для розрахунку дозволяє проводити маніпуляції щодо знаходження максимальної реакції на наданий Зміст повідомлень повідомлення в природномовному тексті.

Кінцевим результатом є розподіл інформації по адресатам.

Для побудови даної інформаційної технології були використані моделі та методи розроблені в розділах 2 та 3 цієї роботи.

4.2. База даних інформаційної технології управління інформаційним супроводженням

Загальна структура інформаційної технології СПВ представлена у вигляді схеми даних на рисунку 4.2., яка відображає взаємозв'язки між реляційними таблицями.

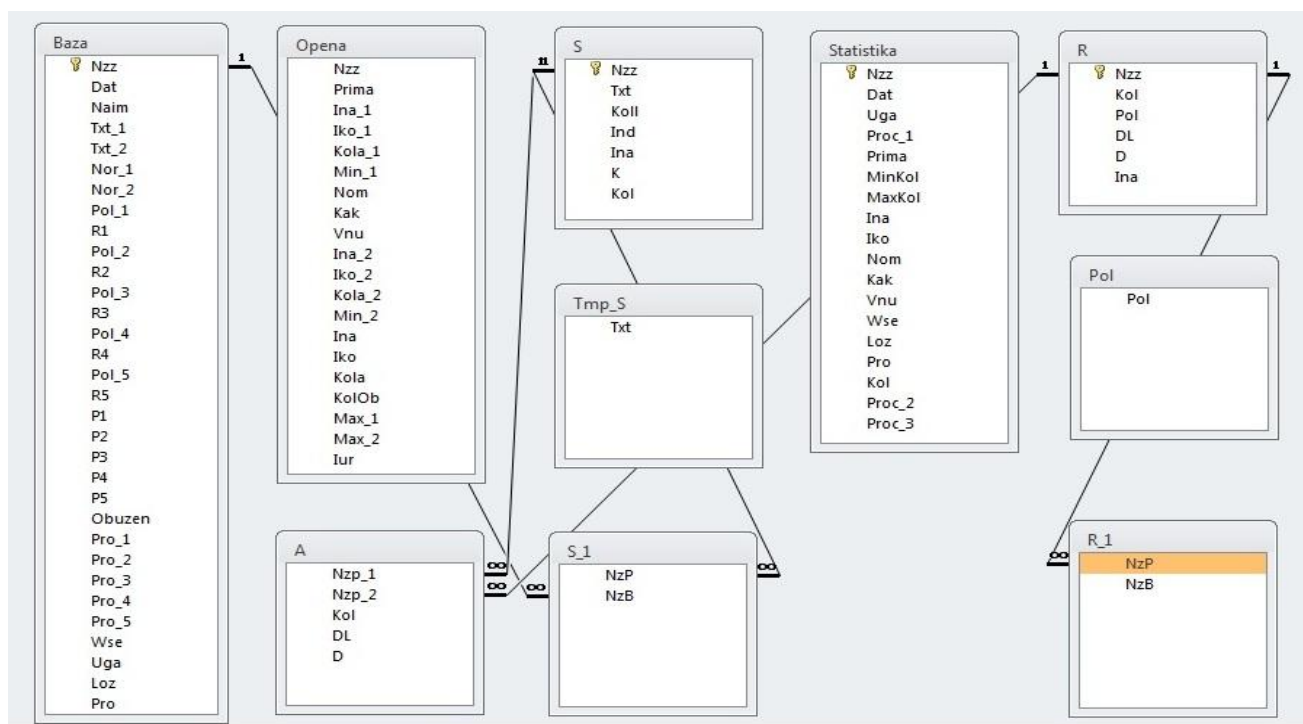


Рис.4.2. Загальна схема даних інформаційної технології супроводження процесів впливу

При організації бази даних ІТ УІС застосовано тип зв'язків між таблицями 1:М – «один-до-багатьох» (є найбільше часто вживаним типом зв'язку між таблицями, дозволяє уникнути повторень однотипної інформації), тобто запису в таблиці Vaza може відповідати кілька записів у таблиці S_1, але запис у таблиці S_1 не може мати більш одного відповідного йому запису в таблиці Vaza [20]. Зв'язок між іншими таблицями організовано за тією ж аналогією, що і попередньо описаний зв'язок.

Схема даних є найбільш приближеною до формату, в якому вона зберігається в комп'ютері. Для кожної таблиці визначаються первинні ключі. До загальної схеми даних предметної області відносяться наступні таблиці нашої інформаційної системи: A, Vaza, Opepa, PoI, R, R_1, S, S_1, Statistika, Tmp_S.

Першим кроком розробки інформаційного забезпечення даної інформаційної технології є побудова інформаційної моделі предметного середовища. Метою її побудови є виявлення основних сутностей, які входять в предметне середовище, їх атрибутів, та зв'язків між сутностями. Інформаційне забезпечення зводиться до розробки форм та методів інформаційного відображення організації в системі та здійснення ефективного обміну інформацією між системою та об'єктом управління.

До складу інформаційного забезпечення включено: дані, засоби їх формалізованого опису та програмні засоби.

Засоби формалізованого опису включають в себе використовувані системні кодування класифікації даних та інформаційні мови. Сутність служить для представлення набору реальних або абстрактних предметів (людей, місць, подій і т.п.), які мають загальні атрибути або характеристики. Сутність – «логічний» об'єкт, який у фізичному середовищі СУБД представлений таблицею. Сутності, атрибути та ідентифікатори елементів інформаційної технології представлені в таблиці (табл. 4.1)

Таблиця 4.1

Сутність	Атрибути сутності	Ідентифікатор
Інформаційні повідомлення_База	Код речення	Nzz
	Дата додавання інформаційного повідомлення до бази даних	Dat
	Назва інформ-го повідомлення	Naim
	Текст речення 1	Txt_1
	Текст речення 2	Txt_2
	Нормалізоване речення 1	Nor_1
	Нормалізоване речення 2	Nor_2
	Адресат речення 1	Pol_1
	Визначеність відносно адресата 1	R1
	Адресат речення 2	Pol_2
	Визначеність відносно адресата 2	R2
	Адресат речення 3	Pol_3
	Визначеність відносно адресата 3	R3
	Адресат речення 4	Pol_4
	Визначеність відносно адресата 4	R4
	Зміст речення 5	Pol_5
	Визначеність відносно адресата 5	R5
	Відсоток правильно визначеного програмою адресату тексту	P1
	Відсоток правильно визначеного програмою адресату тексту	P2
	Відсоток правильно визначеного програмою адресату тексту	P3
	Відсоток правильно визначеного програмою адресату тексту	P4
	Відсоток правильно визначеного програмою адресату тексту	P5
	Логічна функція	Obuzen
	Адресат тексту 1, визначений програмою	Pro_1
	Адресат тексту 2, визначений програмою	Pro_2
	Адресат тексту 3, визначений програмою	Pro_3
	Адресат тексту 4, визначений програмою	Pro_4
	Адресат тексту 5, визначений програмою	Pro_5
Кількість проаналізованих речень	Wse	
Кількість правильно визначених системою речень	Uga	
Кількість хибної тривоги	Loz	
Кількість пропусків цілі	Pro	

Таблиця 4.1 (продовження)

Сутність	Атрибути сутності	Ідентифікатор
OPENA	Код речення Назва експерименту Мінімальне значення довжини фрагменту Максимальне значення довжини фрагменту Режим перебору речень Мінімальна статистика Мінімальна довжина фрагмента Мінімальне значення довжини фрагменту Логічна функція Мінімальне значення довжини фрагменту Максимальне значення довжини фрагменту Режим перебору речень Мінімальна статистика Мінімальне значення довжини фрагменту Максимальне значення довжини фрагменту Кількість нових фрагментів за 1 цикл навчання Кількість речень в навчальній вибірці Максимальна статистика Максимальна статистика Рівень прийняття адресності	Nzz Prima Ina_1 Iko_1 Kola_1 Min_1 Nom Kak Vnu Ina_2 Iko_2 Kola_2 Min_2 Ina Iko Kola KolOb Max_1 Max_2 Iur
R	Код речення Кількість проаналізованих речень (без навчальної вибірки) Упорядкування відносно адресата Довжина фрагменту Визначеність Мінімальне значення довжини фрагменту	Nzz Kol Pol DL D Ina
A	Код фрагменту Кількість фрагментів в тексті Кількість проаналізованих речень (без навчальної вибірки) Довжина фрагменту Визначеність	Nzp_1 Nzp_2 Kol DL D

Таблиця 4.1 (продовження)

Сутність	Атрибути сутності	Ідентифікатор
S_1	Код слова Кількість слів	NzP NzB
Statistika	Код речення Кількість правильно визначених речень Відсоток правильно визначених адресатів тексту Тип експерименту Дата додавання речення до бази даних Режим перебору речень Режим перебору речень Максимальна довжина фрагмента Максимальне значення довжини фрагменту Мінімальне значення довжини фрагменту Логічна функція Загальна кількість проаналізованих речень Загальна кількість хибної тривоги Пропуск цілі Кількість проаналізованих речень (без навчальної вибірки) Середній показник хибної тривоги Середній показник пропусків цілі правильно визначити адресата речення	Nzz Uga Proc_1 Prima Dat MinKol MaxKol Nom Ina Iko Kak Vnu Wse Loz Pro Kol Proc_2 Proc_3
S	Код речення Фрагмент речення Кількість виділених фрагментів в реченні Кількість фрагментів, які зустрічаються в реченні Максимальна довжина фрагмента Кількість фрагментів, які зустрічаються в тексті Кількість проаналізованих речень (без навчальної вибірки)	Nzz Txt Koll Ind Ina K Kol
TMP_S	Тимчасові значення	Txt
R_1	Код речення Кількість речень	NzP NzB
Адресат	Назва адресату	Pol

4.2.1. Логічна модель бази даних інформаційної технології управління супроводженням процесів впливу

Після нормалізації відношень йде побудова логічної моделі БД. Логічна модель є основою бази даних, вона повинна відображати взаємозв'язки між реляційними таблицями. До **логічної моделі** предметної області відносяться наступні таблиці нашої інформаційної системи між якими існують зв'язки, а саме: A, Baza, R, R_1, S, S_1. Логічна модель ІТ УІС наведена на рисунку 4.3.

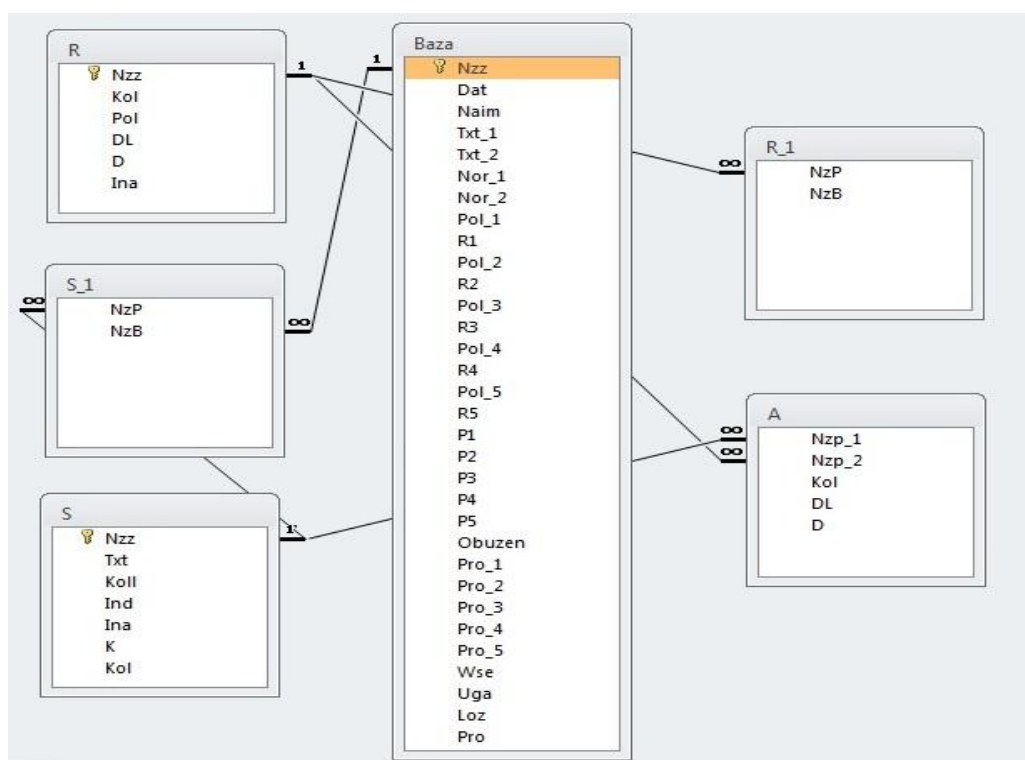


Рис.4.3. Зв'язок між таблицями в інформаційній технології супроводження процесів впливу

При побудові логічної моделі ІТ УІС між таблицею Baza і таблицею S_1 створено зв'язок один до багатьох тому, що між полем Nzz і полем NzB в кожному реченні тексту таблиці Baza є безліч фрагментів, які розбиваються на ці фрагменти та заносяться в таблицю S_1. За аналогією з попередньо описаним у таблиці S, де зберігаються фрагменти речень, в наявності два зв'язки, з таблицею

S_1, яка є робочою для формування фрагментів речень і слів та таблицею A, яка відповідає за зв'язок між реакціями (визначеними адресатами повідомлень) і фрагментами речень. Такий самий зв'язок має і таблиця R, яка зберігає інформацію про реакції (адресатів) кожного із фрагментів речень, довжину фрагментів та визначеність реакції відносно довжини цих фрагментів, з таблицею A та таблицею R_1, яка, в свою чергу, є робочою для формування реакції.

4.2.2. Фізична модель бази даних інформаційної технології управління супроводженням впливу

Фізичні моделі баз даних визначають способи розміщення даних у середовищі зберігання й способи доступу до цих даних, які підтримуються на фізичному рівні.

Фізична модель даних описує дані засобами конкретної СУБД. Відношення, які були розроблені на стадії формування логічної моделі даних, перетворюються в таблиці, атрибути стають стовпцями таблиць, для ключових атрибутів створюються унікальні індекси, домени перетворюються у типи даних, прийняті в конкретній СУБД. Нагадаємо, що в даній роботі для створення інформаційної технології було застосовано СУБД Access.

Фізична модель інформаційної технології представлена в додатку В табл. В.1 - В.9.

4.3. Алгоритм визначення адресності повідомлення у інформаційній технології супроводження процесів впливу

На рисунку 4.4. представлено алгоритм визначення адресата повідомлення, який відображає послідовність дій для здійснення процесу визначення адресата повідомлення.

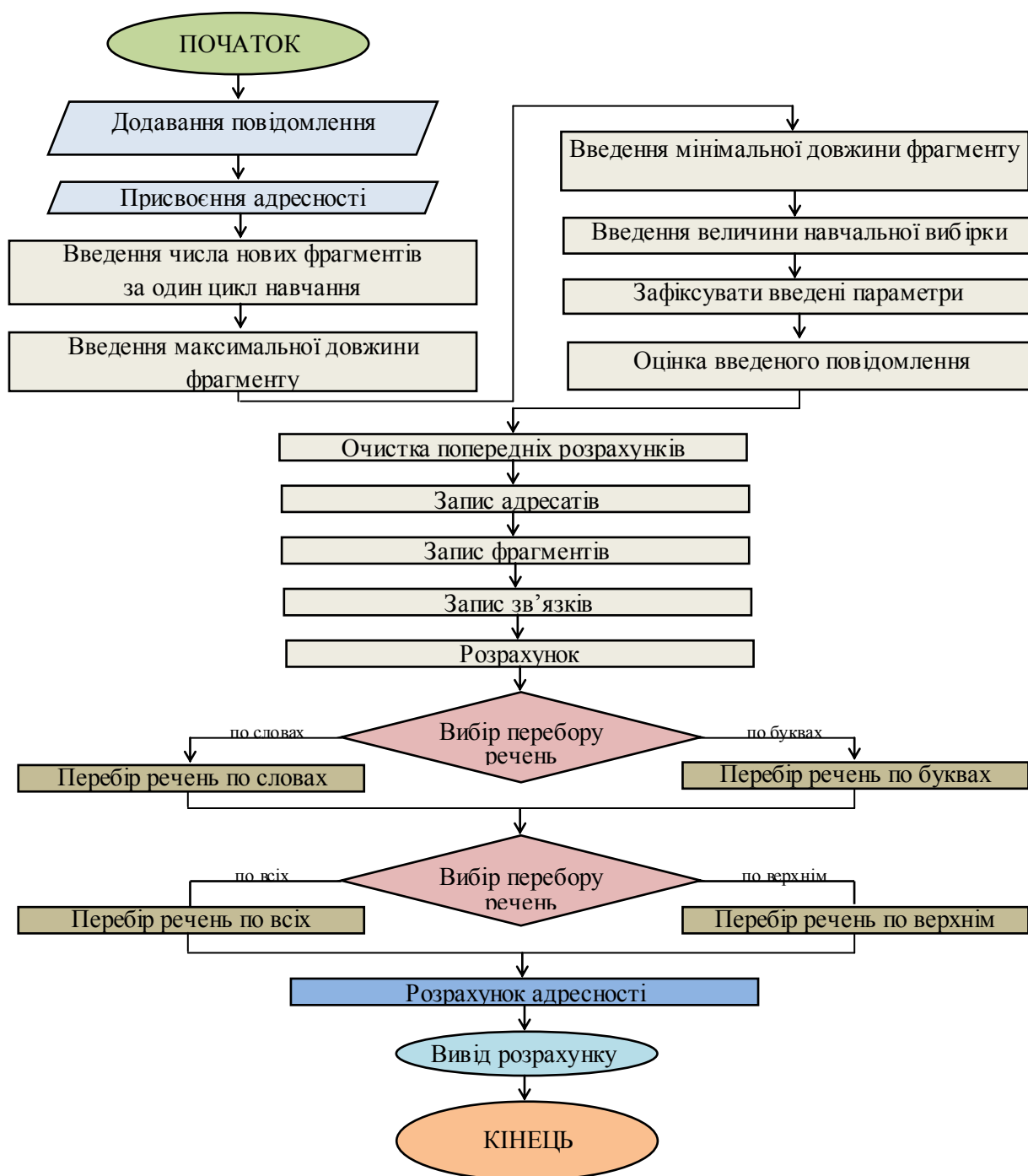


Рис. 4.4. Алгоритм визначення адресата повідомлення при роботі ІТ управління супроводженням процесів впливу

Одним із складових інформаційної технології супроводження процесів впливу є модуль навчання.

Вхідними даними до модулю навчання є інформаційні повідомлення в текстовій формі та список адресатів цих повідомлень.

З метою навчання інформаційної технології було закладено вибірку навчальних інформаційних повідомлень. Навчальна вибірка використовується лише для проведення процесу навчання ІТ УІС. Програма навчається на прикладі наданому їй експертом, а після закінчення фази навчання може узагальнювати отримані в подальшому дані сама.

Більш детально розглянемо процеси в системі на прикладі роботи функції «Розрахунок адресності» та функції запису інформації до таблиці S «Запис фрагментів».

На рисунку 4.5. представлено алгоритм дії функції «Розрахунок адресності».

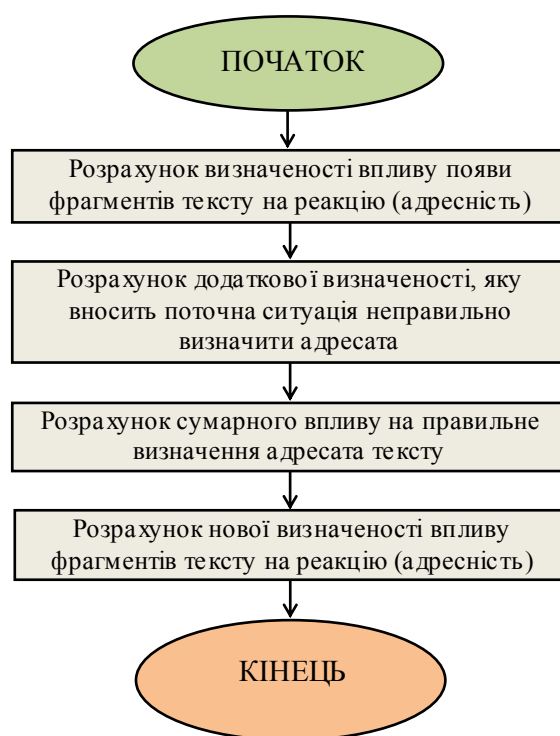


Рис. 4.5. Алгоритм дії функції «Розрахунок адресності»

Дана функція реалізує розроблені в роботі моделі та метод адресно-орієнтованого управління інформаційним супроводженням процесів впливу на контрагентів взаємодії:

1. Розраховуються визначеності впливу появи фрагментів тексту на реакцію (адресність);

2. Розраховується додаткова визначеність, яку вносить поточна ситуація неправильно визначити адресата;
3. Розраховується сумарний вплив на правильне визначення адресата тексту;
4. Розраховується нова визначеність впливу фрагментів тексту на реакцію (адресність).

В основі розрахунку даної функції покладена правильно визначена адресність (цілеорієнтація) інформації. Вона відслідковує різноманітні впливи на процес ідентифікації адресності інформації та оцінює залежність відхилення автоматично визначеної адресності інформації від адресності, визначеної експертом.

На рисунку 4.6. представлено алгоритм роботи функції «Запис фрагментів» добавлення фрагментів речень до таблиці S.

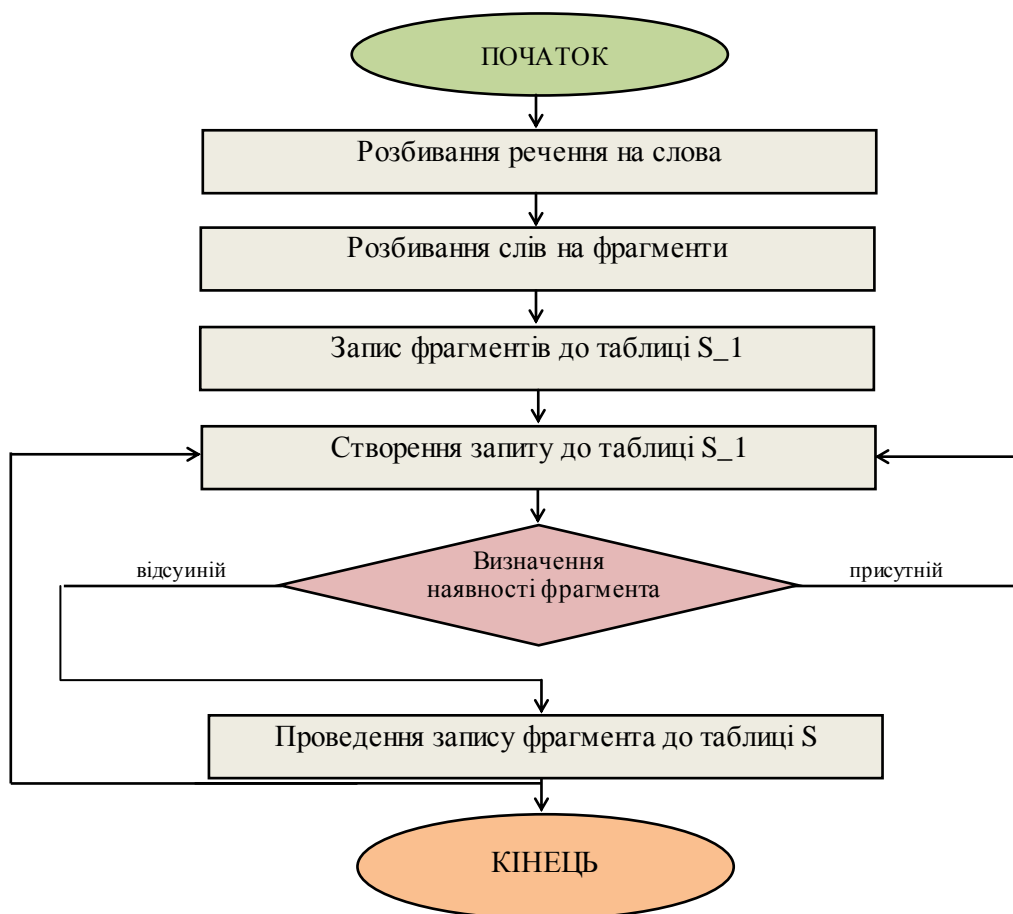


Рис. 4.6. Алгоритм роботи функції «Запис фрагментів» занесення фрагментів тексту до реляційної таблиці S

Txt	Koll	Ind	Ina	K	Kol
Асо	7	0	<input checked="" type="checkbox"/>	4	7
Асоц	7	0	<input checked="" type="checkbox"/>	5	7
Асоці	7	0	<input type="checkbox"/>	6	7
Асоціа	7	0	<input type="checkbox"/>	7	7
Асоціац	7	0	<input type="checkbox"/>	8	7
Асоціаці	7	0	<input type="checkbox"/>	9	7
Асоціаціє	1	0	<input type="checkbox"/>	10	1
Асоціації	1	0	<input type="checkbox"/>	10	1
асоціацію	4	0	<input type="checkbox"/>	10	4
Асоціація	1	0	<input type="checkbox"/>	10	1

Рис. 4.7. Приклад знаходження фрагментів слів в таблиці S

При створенні запиту до таблиці S_1 відбувається порівняння з фрагментами в таблиці S_1 і вже наявними фрагментами в таблиці S, якщо в ній присутній наданий фрагмент то він не повторюється, а функція проводить повторний запит до таблиці S_1. За умови відсутності в таблиці S наданого фрагмента він заноситься до неї, а функція переходить до подальшого перебору вмісту таблиці S_1.

4.4. Програмне забезпечення інформаційної технології управління інформаційним супроводженням

Базуючись на засобах програмування, які доступні в Access 2010, була розроблена інформаційна технологія, програмне середовище якої написано з використанням коду VBA (Visual Basic for Applications) та яка здатна аналізувати інформаційні текстові представлення на природній мові та їх адресувати.

Microsoft Access - повнофункціональна реляційна СУБД, яка надає засоби розробки та управління СУБД. Access може сама організувати доступ до даних що зберігається в файлах с розширенням * .mdb, при цьому всі об'єкти однієї бази

даних зберігаються в одному файлі (деякі СУБД використовують безліч файлів для зберігання об'єктів).

Створення бази даних в Access забезпечує найбільш бюджетне рішення для створення інформаційної технології і забезпечення спільної роботи з даними. Розглянемо докладніше принцип роботи розробленої програми Adres.

4.4.1. Головне меню програмного засобу інформаційної технології управління супроводженням процесів впливу

Для більш зручного користування програмою Adres передбачено головне меню, яке складається: із можливості вибору назви інформаційного повідомлення, вкладки додавання інформації до бази даних, вкладки інформаційного повідомлення, яка за своєю суттю є відображенням створеної бази даних, вкладки навчання системи та вкладки виводу результатів роботи системи.

У списку назв інформаційних повідомлень є можливість вибору існуючого в базі потрібного набору повідомлень, або створення нового.

Вкладка «Адресати» містить в собі суть інформаційного повідомлення, можливість відобразити навчальну вибірку текстової інформації, на основі якої проводилося навчання системи, а також присутня можливість упорядкування інформації за адресністю та відношенням системи до цієї інформації (результатом проведеного системою аналізу). Присутній також опис повідомлення, якому присвоюється його направленість (адресність). Тобто кому це інформаційне повідомлення (новини) адресувати, щоб викликати найбільшу ймовірність потрібної реакції. Це визначають експерти в галузі управління впливами.

Вкладка «Маніпулятор» містить вибір кількості нових фрагментів за один цикл навчання (зазамовчуванням 500), вибір максимальної довжини фрагмента (зазамовчуванням 10), вибір мінімальної довжини фрагмента (зазамовчуванням 2) та вибір навчаючої вибірки (при кількості інформаційних повідомлень – 1000, найкращий результат навчання дала навчальна вибірка, що складається з 750 повідомлень).

Вкладка вміщує також робочі програмні кнопки:

1. Зафіксувати – використовується при зміні кількості інформаційних представлень навчальної вибірки;
2. Оцінка тексту – застосовується при внесенні змін до бази даних та, або зміні кількості повідомлень;
3. Очистити - слугує для очищення таблиці попередніх розрахунків;
4. Запис адресатів – заносить до таблиці реакції адресатів;
5. Запис фрагментів – розбиває та заносить до таблиці фрагменти текстів;
6. Запис зв'язків - заносить до таблиці дані зв'язку між фрагментами тексту і реакцією за кількістю їх збігів;
7. Розрахунок – функціональна кнопка розрахунку значень у таблицях.

В наявності також можливість вибору максимальної і мінімальної довжини фрагмента «з» та «по» відрізків, виведення даних розрахунку лише за верхніми фрагментами або всі дані, виведення розрахунку або за буквами, або за словами і встановлення фактору «прийняття» до розгляду системою повідомлення, якщо система сумнівається в його адресаті. Показник прийняття за замовчуванням складає 0,4. Закінчує даний перелік функціональна кнопка «Розрахунок адресності» та можливість його зупинки, призначення цього елемента говорить саме за себе.

Вкладка «Аналіз», яка представляє собою узагальнену інформацію про результати роботи системи, що відображаються в одноіменному вікні за наступними показниками:

- кількість проаналізованих понять;
- кількість правильно визначених системою понять;
- кількість хибної тривоги;
- кількість пропусків цілі правильно визначити зміст речення;
- кількість проаналізованих речень (без навчальної вибірки);
- середній показник хибної тривоги;
- середній показник пропусків цілі правильно визначити зміст речення;
- відсоток правильно визначених системою адресатів.

І останній елемент програми Adres вкладка «Добавити» являє собою елемент програми, в який вноситься суть повідомлення (на прикладі було внесено новини світу та України в текстовому представленні).

Структура меню програми Adres показана на рис. 4.8.

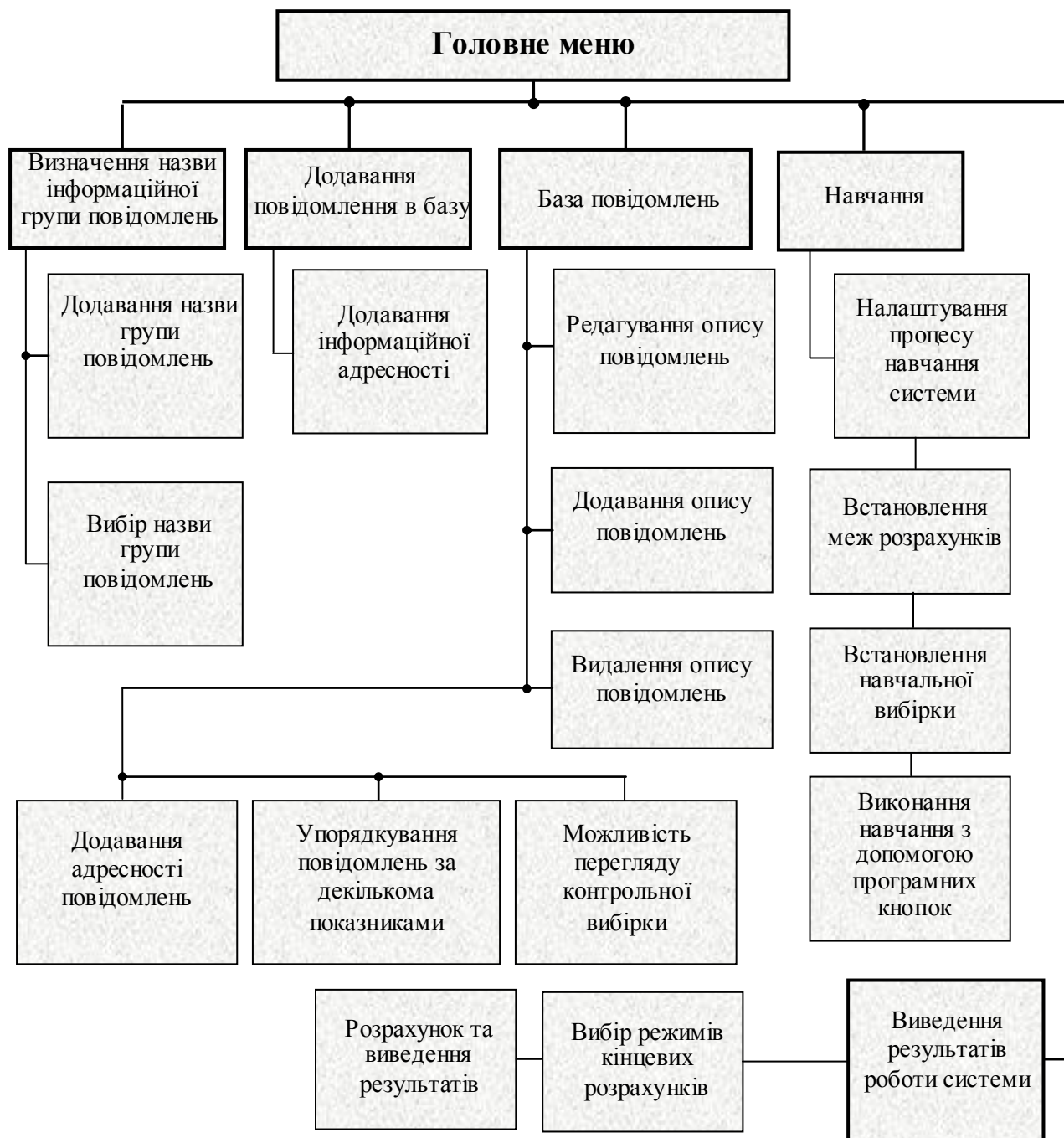


Рис. 4.8. Структурна схема робочого меню програми Adres

4.4.2. Процес навчання програми Adres

В процесі навчання програми виділяються дві похибки:

- 1) похибка навчання;
- 2) похибка узагальнення.

Похибка навчання — це помилка, яка допущена програмою на фазі навчання по навчальній вибірці. На кожній ітерації навчання для неперервної вхідної змінної вона розраховується як середньоквадратична похибка.

Похибка узагальнення — це помилка, яка отримана на фазі аналізу тестових прикладів, обчислюється за тими ж формулами, але для тестової множини [22].

Якщо в процесі навчання була отримана достатньо мала похибка як на навчальній, так і на тестовій вибірці, то можна зробити висновок, що модель набула властивість узагальнення.

Розміри навчальної і тестової вибірки залежать від конкретної задачі. Навчальна множина повинна бути більша, ніж тестова, і містити достатньо даних для якісного навчання моделі. Розмір тестової множини визначається запасом даних навчальної вибірки. Якщо даних мало, то тестову вибірку беруть по менше — 5 % від загального об'єму вибірки. Якщо навчальна вибірка має достатній запас, то тестову множину можна брати 20–30 %.

Для експериментального прикладу визначення адресності повідомлень навчальна вибірка буде становити 75%.

Процес навчання моделі є задачею мінімізації функції вихідної похибки $E(t)$, де t — номер ітерації навчання. В процесі навчання похибка навчання монотонно зменшується.

Для створення навчальної вибірки здійснено заповнення, через вкладку «Добавити» бази даних інформаційними повідомленнями представленими в текстовій формі (для експериментального прикладу взято новини світу та України) (Рис. 4.9).

СИСТЕМА ВИЗНАЧЕННЯ АДРЕСАТІВ ІНФОРМАЦІЙНОГО ВПЛИВУ			ВИХІД	
Адресати	Маніпулятор	Аналіз	Добавити	
<input type="checkbox"/> Контрольна вибірка <input type="checkbox"/> Порядок			Рішення експерта	Рішення системи
Служба безпеки України запобігла другій спробі викрадення і вбивства колишнього співробітника ФСБ РФ Іллі Богданова, який перейшов на бік України у 2014 році і воював у зоні АТО в складі добровольчого батальйону			Військовим	
Очільник Центру визволення військових полонених «Офіцерський корпус» Володимир Рубан розповів, що незадовго після підписання Мінських угод було виявлено близько 3 провокаційних груп, які намагалися створити умови щодо порушення перемир'я з обох сторін			Військовим	
Бойовики "ДНР" застосовують проти мирного населення в околицях Маріуполя, зокрема, селища Саргана, Гнутово, Новоселівка, вилосковані російські наскетні боєприпаси для установок БМ-21 Град - Торнадо-Р			Військовим	
Третя світова війна може початися в Латвії піше Пол Міллер у своїй статті, на черзі країни Балтії, вони стануть одними із перших і найбільших випробувань для новообраного президента Дональда Трампа			Військовим	

Рис. 4.9. База інформаційних повідомлень (новини світу та України)

Наступним кроком є визначення адресності повідомлень експертом в галузі управління впливами (Рис. 4.10).

СИСТЕМА ВИЗНАЧЕННЯ АДРЕСАТІВ ІНФОРМАЦІЙНОГО ВПЛИВУ			ВИХІД	
Адресати	Маніпулятор	Аналіз	Добавити	
<input type="checkbox"/> Контрольна вибірка <input type="checkbox"/> Порядок			Рішення експерта	Рішення системи
Служба безпеки України запобігла другій спробі викрадення і вбивства колишнього співробітника ФСБ РФ Іллі Богданова, який перейшов на бік України у 2014 році і воював у зоні АТО в складі добровольчого батальйону			Військовим	
Очільник Центру визволення військових полонених «Офіцерський корпус» Володимир Рубан розповів, що незадовго після підписання Мінських угод було виявлено близько 3 провокаційних груп, які намагалися створити умови щодо порушення перемир'я з обох сторін			Військовим	
Бойовики "ДНР" застосовують проти мирного населення в околицях Маріуполя, зокрема, селища Саргана, Гнутово, Новоселівка, вилосковані російські наскетні боєприпаси для установок БМ-21 Град - Торнадо-Р			Військовим	
Третя світова війна може початися в Латвії піше Пол Міллер у своїй статті, на черзі країни Балтії, вони стануть одними із перших і найбільших випробувань для новообраного президента Дональда Трампа			Військовим	

Рис. 4.10. Визначення експертом адресата інформаційного посилу

Адресатом повідомлення може бути будь-що, або будь-хто нашого світу. Експерт проводить роботу по визначенню адресата (в рамках нами вибраного розподілу таких, або ж вносить на розгляд системі нового адресата) конкретного повідомлення інформаційний посил змісту якого призведе до найбільшої реакції зі сторони вибраного адресата та призведе до запланованих ним дій. В ході роботи експерта не виключається визначення декількох адресатів повідомлення по мірі зменшення інформаційного впливу повідомлення на них.

Ефективність функціонування будь-якої системи, що навчається істотно залежить від якості тих даних, на яких проходить навчання. Застосування неякісного матеріалу, яким проводиться навчання системи не тільки позначиться на функціонуванні інформаційної технології в майбутньому, але може привести і до неможливості навчитися в принципі. Широке поширення в різних предметних областях отримали моделі, що навчаються, побудовані з використанням штучного інтелекту. Як і будь-яка інша система, що здатна навчатися, ІТ УІС повинна бути забезпечена вхідними даними для навчання, що формують її навчальну вибірку.

В процесі обробки вхідних даних відбувається оцінка повідомлення, тобто здійснюється виділення та поділ введеного інформаційного повідомлення в текстовому представленні на слова і інші послідовності символів, до яких належать також і знаки пунктуації та символи початку абзацу.

У вікні процесу навчання системи виставляються основні параметри для проведення навчання (Рис.4.11).

Параметрами, які застосовуються для проведення навчання системи є:

кількість нових фрагментів за 1 цикл навчання;

максимальна та мінімальна довжина фрагменту;

кількість інформаційних повідомлень в навчальній вибірці.

Далі проводиться сам процес навчання системи шляхом почергового натискання функціональних кнопок: Зафіксувати, Оцінка тексту, Очистити, Запис адресатів, Запис фрагментів, Запис зв'язків та Розрахунок.

СИСТЕМА ВИЗНАЧЕННЯ АДРЕСАТІВ ІНФОРМАЦІЙНОГО ВПЛИВУ

ВИХІД

Адресати Маніпулятор Аналіз Додати

Нових фрагментів за 1 цикл навчання

Максимальна довжина фрагмента

Мінімальна довжина фрагмента

НАВЧАЮЧА ВИБІРКА

Довжина фрагмента з	10
Довжина фрагмента по	10
Мінімальна статистика	20
Максимальна кількість	50 20

1. Зафіксувати

5. Запис фрагментів

2. Оцінка тексту

6. Запис зв'язків

3. Очистити

7. Розрахунок

4. Запис адресатів

Режим

Рівень прийняття

Зупинити

Розрахунок адресності

Всі

Всі по верхнім

Рис. 4.11. Вікно введення параметрів та здійснення навчання системи

У вікні виведення результату роботи системи (Рис.4.12) відбувається останнє виставлення параметрів: перша строчка, від якої довжини, друга – по яку довжину фрагментів ведеться обробка тексту при визначенні його адресату. Наприклад: 2 – 3, 8-10. Означає що будуть розглядатися перший раз фрагменти тексту довжиною від 2 до 8 символів, потім від 2 до 9, потім від 2 до 10, потім від 3 до 8, потім від 3 до 9, і нарешті від 3 до 10 символів. При кожній довжині фрагментів статистичні результати розрахунку будуть виводитись в вікно «Статистика». Але довжина фрагментів враховується лише коли ви вибрали в полі Режим значення «по буквам». Якщо вибрали «по словам» - довжина фрагментів не враховується. Потім вибираємо режим перебору повідомлень (за словами, за буквами), виставлення рівня прийнятності визначення системою вірного адресату та вивід результату.

Основними причинами неправильності визначення системою адресата повідомлення є:

недостатня навчальна вибірка бази даних повідомлень (чим більша навчальна вибірка на вході, тим більше, так мовити досвід у системи і як результат більш точніший результат на виході);

некомпетентність експерта (Зміст повідомлень повідомлень з однаковим явним адресатом визначає надати то одному, то іншому адресату – заплутує систему);

занадто велика база даних слів при відносно невеликій базі даних адресно виражених понять.

The screenshot shows a web application interface for 'СИСТЕМА ВИЗНАЧЕННЯ АДРЕСАТІВ ІНФОРМАЦІЙНОГО ВПЛИВУ'. At the top, there are navigation tabs: 'Адресати', 'Маніпулятор', 'Аналіз', and 'Добавити'. A 'Вихід' button is located in the top right corner. The main content area is titled 'Результат роботи системи' and contains the following data points, each with an adjacent input field:

Метрика	Вхідне поле
Кількість всього проаналізованих повідомлень	<input type="text"/>
Кількість правильно визначених системою повідомлень	<input type="text"/>
Кількість хибної тривоги	<input type="text"/>
Кількість пропусків цілі правильно визначити зміст речення	<input type="text"/>
Кількість проаналізованих речень (без навчальної вибірки)	<input type="text"/>
Середній показник хибної тривоги	<input type="text"/>
Середній показник пропусків цілі правильно визначити зміст речення	<input type="text"/>
Відсоток правильно визначених системою адресатів	<input type="text"/>

Рис. 4.12. Вікно виводу результатів роботи системи

4.5. Експериментальне дослідження інформаційної технології управління інформаційним супроводженням

Інформаційна технологія супроводження процесів впливу має забезпечити особовому складу аналітичних груп та експертам в області інформаційно-психологічного впливу сил спеціальних операцій можливість наповнювати і редагувати базу даних та отримувати дані розрахунків.

Як і будь-яка комп'ютерна програма, дана інформаційна технологія обробляє вхідні дані і виводить результат у вигляді вихідних даних.

Вхідними даними для інформаційної технології управління інформаційним супроводженням впливу є найрізноманітніша інформація використання якої дасть

можливі переваги в ході проведення спеціальних військових операцій з інформаційного впливу на противника та досягненням застосування якої буде отримання переваги над ним в інформаційному просторі в умовах гібридної війни.

4.5.1. Експериментальне визначення адресатів повідомлень ІТ УІС

З метою перевірки працездатності системи до бази інформаційних повідомлень було введено новин світу та України різноманітного характеру з основних порталів новин нашої країни. Чим більше інформаційно-змістовних новин в базі даних тим точніше отримується результат. Тому мінімальна кількість введених речень для отримання адекватних результатів – 1000 речень. Максимальна кількість речень в ході експериментів становила 5000 речень.

Вікно введення інформаційного повідомлення в текстовому представленні у базу даних наведено на рис. 4.13.

СИСТЕМА ВИЗНАЧЕННЯ АДРЕСАТІВ ІНФОРМАЦІЙНОГО ВПЛИВУ ВИХІД

Адресати | Маніпулятор | Аналіз | Добавити

Добавити інформаційний зміст в базу даних

Штрафи за несплату або несвоєчасну сплату єдиного соціального внеску можуть застосовуватися лише у разі його несплати підприємцем на загальній системі оподаткування до 10 лютого року, наступного за звітним. У разі зміни місцезнаходження господарської діяльності – платників податків сплата податків і зборів після реєстрації здійснюється за місцем попередньої реєстрації до закінчення поточного бюджетного періоду. Українські заробітчани роблять значний вклад в економіку нашої країни, справно постачаючи її валютою. Щороку українці переказують з-за кордону суму, співмірну з третиною Державного бюджету України. Затверджено новий Порядок отримання з Державного реєстру фізичних осіб - платників податків даних про заробітну плату (дохід) для призначення пенсії у разі втрати документів про її нарахування та виплату.

Рис. 4.13. Введення інформаційного повідомлення у базу даних

Першочерговим кроком програми є розподіл інформаційного повідомлення на окремі блоки обсягом не більше 255 знаків, які заносяться в базу даних

інформаційної технології. Експерт в галузі управління впливами аналізує введену інформацію та опираючись на свої знання, свій життєвий досвід визначає кому адресувати те чи інше повідомлення (новини). Це буде навчальною вибіркою системи. Приклад інформаційних повідомлень та адресатів з навчальної вибірки наведений на рис. 4.14

СИСТЕМА ВИЗНАЧЕННЯ АДРЕСАТІВ ІНФОРМАЦІЙНОГО ВПЛИВУ				ВИХІД
Адресати	Маніпулятор	Аналіз	Добавити	
<input checked="" type="checkbox"/> Контрольна вибірка		від вгаданих		
			Рішення експерта	Рішення системи
▶	Експерти програми допомоги НАТО "Удосконалення військової освіти" "DEEP" високо оцінили зміни в системі військової освіти України		Військовим	56% Військовим
			Молоді, що навчається	48% Молоді, що навчається
				17% Підприємцям
				12% Населенню ЛДНР, Криму
				8% Держслужбовцям
	В окупованих бойовиками районах Донбасу відкрили пункти мобілізації добровольців, яких відправлять в Сирію		Військовим	62% Військовим
			Населенню ЛДНР, Криму	47% Населенню ЛДНР, Криму
				16% Молоді, що навчається
				9% Держслужбовцям
				8% Всім
	Найбільша проблема у розслідуванні справи Януковича – це свідки.		Всім	48% Всім
			Держслужбовцям	44% Держслужбовцям
				23% Військовим
				20% Молоді, що навчається
				6% Населенню ЛДНР, Криму
	Співробітники Служби інформації і безпеки Молдови затримали 22-річного молдаванина, який воював на Донбасі на стороні проросійських бойовиків		Населенню ЛДНР, Криму	62% Населенню ЛДНР, Криму
			Військовим	55% Військовим
				18% Держслужбовцям
				12% Молоді, що навчається
				6% Підприємцям

Рис. 4.14. Вікно з фрагментом навчальної вибірки

При розрахунку експериментального прикладу вводилися наступні параметри:

- кількість нових фрагментів за 1 цикл навчання: 500;
- мінімальна та максимальна довжина фрагменту: 2 та 10 відповідно;
- кількість речень в навчальній вибірці: 750 із 1000;
- мінімальна довжина фрагменту з 2 по 10;
- максимальна довжина фрагменту з 5 по 10;
- рівень прийняття системою проаналізованих інформаційних повідомлень: 0,4;
- тип експерименту та режиму перебору речень: новий експеримент, з режимом перебору за словами.

Вікно з введеними параметрами для розрахунку наведено на рис. 4.15, а отриманий результат роботи системи показано на рис. 4.16.

СИСТЕМА ВИЗНАЧЕННЯ АДРЕСАТІВ ІНФОРМАЦІЙНОГО ВПЛИВУ ВИХІД

Адресати | Маніпулятор | Аналіз | Додати

Нових фрагментів за 1 цикл навчання
 Максимальна довжина фрагмента
 Мінімальна довжина фрагмента

НАВЧАЮЧА ВИБІРКА

Довжина фрагмента з	2	2,10
Довжина фрагмента по	5	5,10
Мінімальна статистика	1	1,20
Максимальна кількість	1	0,50 20

1. Зафіксувати 5. Запис фрагментів

2. Оцінка тексту 6. Запис зв'язків

3. Очистити 7. Розрахунок

4. Запис адресатів

Розрахунок адресності

Режим
 Рівень прийняття
 Зупинити

Всі
 Всі по верхнім

Рис. 4.15. Вікно введення параметрів для розрахунку статистики

СИСТЕМА ВИЗНАЧЕННЯ АДРЕСАТІВ ІНФОРМАЦІЙНОГО ВПЛИВУ ВИХІД

Адресати | Маніпулятор | Аналіз | Додати

Результат роботи системи

Кількість всього проаналізованих повідомлень	<input type="text" value="133"/>
Кількість правильно визначених системою повідомлень	<input type="text" value="122"/>
Кількість хибної тривоги	<input type="text" value="969"/>
Кількість пропусків цілі правильно визначити зміст речення	<input type="text" value="27"/>
Кількість проаналізованих речень (без навчальної вибірки)	<input type="text" value="250"/>
Середній показник хибної тривоги	<input type="text" value="3,876"/>
Середній показник пропусків цілі правильно визначити зміст речення	<input type="text" value="0,108"/>
Відсоток правильно визначених системою адресатів	<input type="text" value="91,73%"/>

Рис. 4.16. Вікно з результатами роботи системи

В даному прикладі експерименту був використаний режим перебору за буквами, який і дав цей показник правильно визначених системою адресатів. В системі також є можливість здійснювати перебір речень за словами, а також змінювати кількість речень в навчальній вибірці і рівень прийняття системою правильно визначених інформаційних змістів повідомлень. Чим більша навальна вибірка, об'єм інформаційної бази, тим, дійсно, інформаційна технологія більш точно визначає адресатів повідомлень.

В ході проведення дослідження було отримано результат який становить 91,73% правильно визначених адресатів інформаційних повідомлень, що є високим показником в порівнянні з іншими інтелектуальними системами з цього напрямку. Вказаний показник дає значну перевагу у використанні даної інформаційної технології в процесі автоматизації ідентифікації адресатів повідомлень з метою не максимального інформування контрагентів взаємодії, а ціленаправленою (вибірковою) інформаційною дією на них.

Для визначення адресатів повідомлень використано метод описаний в розділі 3, який забезпечує розрахунок несилового впливу фрагментів речень на вибір адресата на якого вони справлять найбільш ефективний інформаційний вплив. Суть даного методу полягає в проведенні визначення умовної ймовірності появи адресних понять при умові, що у вхідному повідомленні (тексті) є деякий фрагмент (буквосполучення), а відхилення умовної ймовірності від абсолютної ймовірності появи цього адресного поняття свідчить про несильний (інформаційний) вплив інтелектуального апарату людини, який визначив появу цього фрагменту на виникнення образу, що відповідає адресному поняттю. За максимальною сумою таких впливів вибирається адресність повідомлення.

Шляхом зміни рівня прийняття визначених системою правильних адресатів повідомлень з порогом в 0,05 досягнуто деякого обсягу різних показників в кількості проаналізованих системою понять та відсотком правильно визначених системою адресатів, які зведені до загальної таблиці (таб. 4.2) на основі якої побудовано графік залежності відсотку правильно визначених системою адресатів від кількості всього проаналізованих понять, графік залежності відсотку

правильно визначених системою адресатів від рівня прийняття проаналізованих понять та графік залежності кількості всього проаналізованих понять від рівня їх прийняття системою, які представлені в додатку Д рис. Д.1 - Д.3.

Таблиця 4.2

Результати аналізу роботи програми Adres

Рівень прийняття	Відсоток правильно визначених системою адресатів	Кількість всього проаналізованих повідомлень
0,3	83,18%	214
0,35	88,17%	169
0,4	91,73%	133
0,45	97,27%	110
0,5	98,85%	87
0,55	100,00%	60
0,6	100,00%	44
0,65	100,00%	25
0,7	100,00%	18
0,75	100,00%	9

Сумістивши два отриманих графіки залежності відсотку правильно визначених системою адресатів від рівня прийняття проаналізованих понять та залежності кількості всього проаналізованих понять від рівня їх прийняття системою було отримано оптимальне значення рівня прийняття правильно відібраних інформаційних змістів повідомлень (додаток Д рис. Д.4)

В ході проведення подальших експериментальних досліджень по працездатності запропонованої системи управління інформаційним супроводженням впливу вона показувала в більшості випадків більш точніше визначення адресатів повідомлень, ніж експерт в галузі управління впливами. Що показало спроможність системи навчатися читати природномовні тексти, аналізувати їх, та розуміти краще, в деяких випадках, ніж людина. Але самим цікавим в роботі цієї системи є таке звичайне людське поняття, як «невпевненість», саме так, той Зміст повідомлень повідомлення який система невпевнена кому адресувати, вона віддає на перегляд експерту. Так на цьому етапі

система близько 60 відсотків адресатів визначає сама, а решту відсотків обробленої інформації, в якій не впевнена, віддає на корекцію людині. В цьому і є одне із інноваційних досягнень даної системи, вона знає що віддати оператору на доопрацювання (перегляд), а що самій розподілити до контрагентів взаємодії.

Здатність інформаційної технології до навчання та отримання високих результатів експериментів в цьому напрямку є одним із кроків в створенні штучного інтелекту.

4.5.2. Порівняльний аналіз роботи інформаційної технології супроводження процесів впливу

Представлена в даній роботі ІТ УІС за своєю суттю є системою інтелектуального аналізу природномовних текстів, тому для повноти оцінки її роботи необхідно проаналізувати отриманий результат в порівнянні з іншими існуючими на теперішньому етапі розвитку суспільства аналогічними системами [2], [3], [4], [7], [11], [17]. Для цього, із наведених в першому розділі цієї роботи існуючих систем, які можна б було використати та вже застосовуються для здійснення пошуку (розвідки) і інформаційного (несилового) впливу, виберемо найбільш адаптовану до нашої задачі та проведемо порівняльний аналіз, попередні результати якого наведено в таблиці 4.3.

Так, проаналізувавши розглянуті на нинішньому ринку технологічні послуги по аналізу природномовних текстів найбільшу увагу привертає програмний засіб TextAnalyst - інструмент аналізу символічних текстів [1]. В ньому реалізована технологія автоматичної смислової обробки текстів, що має найбільш приближену сторону схожості з ІТ УІС в аналізі текстів незалежно від мови і предметної області. Обсяг прийняття тексту контролюється за допомогою семантичної граничної величини, а пошук інформації здійснюється на основі аналізу природної мови на наявність важливих слів і витяг релевантних пропозицій з бази даних текстових документів.

Таблиця 4.3

TextAnalyst	Adres
Аналізує природно мовний текст	Аналізує природно мовний текст
Проводить статистичний аналіз	Використовує статистичні дані
Проводить семантичний аналіз	Застосовує рефлекторний метод
Використав лише 106 вагомих речень для визначення суті змісту тексту, що склало 65%	Використав 133 речення, в яких з загальною ймовірністю 91,73% вказано їх адресата
Визначає найбільш вагомі речення за частотою повторень їх фрагментів	Визначає адресата речення за оцінкою ймовірності найбільш важливості того повідомлення що йому надається
З допомогою реферування забезпечує користувача потрібною для нього інформацію	З допомогою розроблених моделей та методів забезпечує користувача потрібною для нього інформацію
TextAnalyst формує семантичну мережу - інтегральне уявлення сенсу тексту, що служить основою для всіх видів подальшого аналізу	Adres розподіляє повідомлення за їх адресатами за рахунок повторення закладеного шаблону сутності повідомлення визначеної семантичною мережею експерта
Умовно визначає адресата речень в утвореному рефераті	З високою ймовірністю визначає адресата окремого повідомлення в тексті

Основні можливості програмного засобу TextAnalyst:

- аналіз змісту тексту з автоматичним формуванням семантичної мережі з гіперпосиланнями - отримання смислового портрета тексту в термінах основних понять і їх смислових зв'язків;
- аналіз змісту тексту з автоматичним формуванням тематичного древа з гіперпосиланнями - виявлення семантичної структури тексту у вигляді ієрархії тем і підтем;
- розумовий пошук з урахуванням прихованих смислових зв'язків слів запиту зі словами тексту;
- автоматичне реферування тексту - формування його смислового портрета в термінах найбільш інформативних фраз;
- кластеризація інформації - аналіз розподілу матеріалу текстів за тематичними класами;
- автоматична індексація тексту з перетворенням в гіпертекст;

- ранжування всіх видів інформації про семантику тексту за «ступенем значимості» з можливістю варіювання детальності її дослідження;

- автоматичне формування повнотекстової бази знань з гіпертекстової структурою і можливостями асоціативного доступу до інформації.

Для експериментального прикладу було взято повну текстову базу новин, що використана для визначення працездатності ІТ УІС в кількості 250 окремих повідомлень. Цей текст новин введено в відповідне поле програмного засобу TextAnalyst v.2.01. В налаштуваннях програми виставлено аналогічні показники рівню прийняття повідомлень, як і в ІТ УІС, в розмірі 40 відсотків ваги речень (Рис. 4.17).

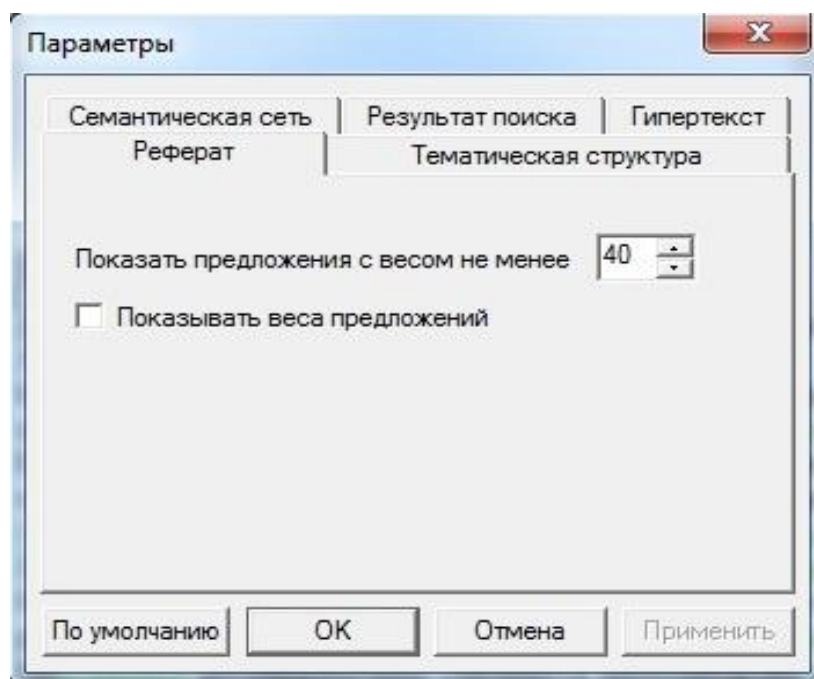


Рис. 4.17. Вікно налаштування параметрів системи TextAnalyst v.2.01

При аналізі програмою TextAnalyst v.2.01 текстової бази та створення реферату системою було виділено 65% тексту та ключові слова в 106 змістовних реченнях (Рис. 4.18).

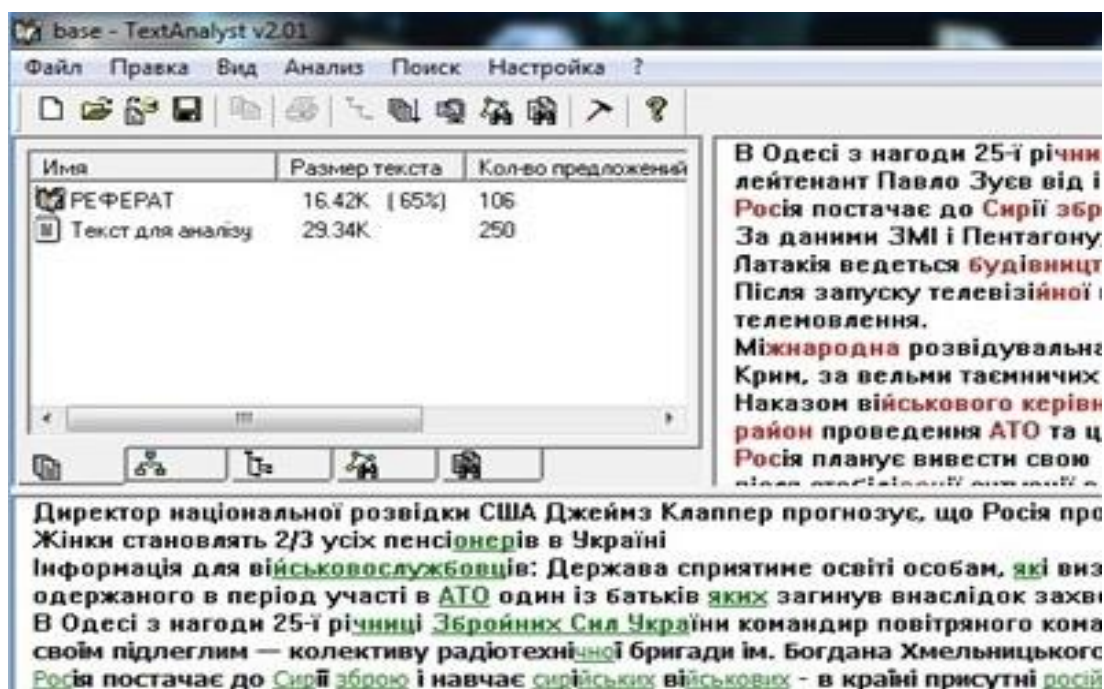


Рис. 4.18. Результат аналізу тексту новин та реферування нейромережевої технології TextAnalyst

Що в порівнянні з роботою ІТ УС (рис. 4.16), яка базується на розроблених в дисертації методах, при показниках 122 правильно визначених речень та процентом правильно визначених понять 91,73% показало значно гірший результат.

Проведено подальші дослідження при незмінному об'ємі бази новин в кількості 250 змістовних речень та різних показниках прийняття повідомлень від 0,3 до 0,75 з інтервалом в 0,05 частини. Отримані показники аналізу тексту програмою TextAnalyst v.2.01 занесені до таблиці 4.4.

На основі даної таблиці побудовано графік залежності відсотку реферування від кількості всього проаналізованих речень, графік залежності відсотку реферування від рівня прийняття проаналізованих понять та графік залежності кількості всього проаналізованих речень від рівня їх прийняття системою, які представлені в додатку Г рис. Г.5 - Г.8.

Знаючи, що реферування це одна з найбільш широко розповсюджених письмових форм отримання інформації, яка дозволяє у короткий термін *надати* потрібну спеціалісту інформацію, проведено наступне порівняння.

Таблиця 4.4

Результати аналізу роботи програми TextAnalyst

Рівень прийняття	Відсоток реферування системою TextAnalyst v.2.01	Кількість всього проаналізованих речень
0,3	63%	123
0,35	59%	114
0,4	55%	106
0,45	55%	104
0,5	50%	95
0,55	46%	87
0,6	44%	82
0,65	41%	75
0,7	38%	70
0,75	31%	58

Взято 250 повідомлень попередньо описаної контрольної вибірки, переведено на рідну мову програми TextAnalyst v.2.01, введено до неї та утворено реферат. В результаті реферування програмою TextAnalyst v.2.01 виділено 63 речення, що склало 34% від загальної кількості введених повідомлень, що видно на рисунку 4.19.

Попередній перегляд реферату дав враження про те, що із різних і непов'язаних речень TextAnalyst вибрав лише адресовані для військових.

На основі отриманого реферату експертом проведено розподіл 63 речень по найбільш ймовірним їх адресатам, що в результаті із них склало 47 речень адресованих для військових, 14 речень для населення окупованих територій і 38 речень для всіх класів.

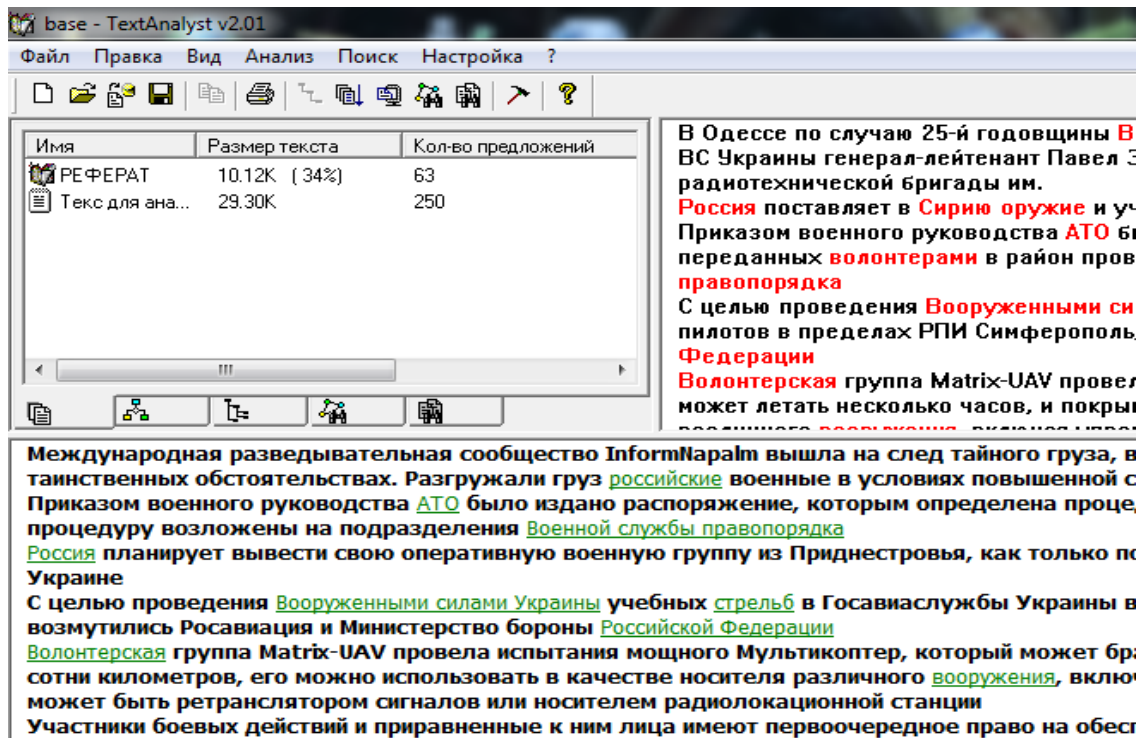


Рис. 4.19. Повторний результат аналізу тексту новин та реферування нейромережевої технології TextAnalyst

Далі ці 63 реферовані речення були проаналізовані в програмному засобі Adres, який визначив, з ймовірністю більше ніж 50%, що адресувати потрібно військовослужбовцям лише 57 речень. Тобто ймовірність визначення адресата речення експертом по реферату склала 74%, а за допомогою програми Adres – 90%, що в черговий раз підтверджує ефективність розробленої програми більш ніж на 16% в порівнянні з аналогічними рішеннями щодо аналізу природномовного тексту.

На основі проведених експериментів і отримання результатів, можна вважати, що застосування ІТ УІС «Adres» є актуальним в усіх галузях, де є необхідність управління персоналом, ведення заходів несилового впливу на противника чи контрдій по захисту від такого [17], а також, адаптувавши систему, застосувати її для спеціальної техніки читання будь-яких текстів, яка базується на розуміння змісту тексту за допомогою змістовних понять.

Використання рефлекторного алгоритму [15], який застосований в ІТ УІС, дає певні можливості, що є перевагами в порівнянні з іншими аналогічними системами, а саме:

- здатність до вирішення широкого кола завдань в області супроводження управління впливами;

- здатність витягати знання з даних і представляти їх в обсязі бажаному виключно заданим адресатам, з метою не максимального інформування контрагента взаємодії, а потрібного і достатнього інформаційного впливу на нього;

- простота використання;

- інтуїтивно зрозумілий інтерфейс;

- моделювання механізмів інтелектуальної діяльності людини;

- можливість інтегрувати інформаційну технологію та застосувати рефлекторні методи в будь-якій галузі управління [25] та насамперед в отриманні переваг в ході постійної негативної інформаційного впливу на населення країни в умовах гібридної війни [15].

Висновки до розділу 4

1. Сформульовані основні принципи побудови інформаційної технології та визначено, що інформаційна технологія супроводження процесів впливу повинна створювати умови для розробки прогнозів, моделювання, формування, ведення та актуалізації бази необхідних інформаційних впливів в сучасних умовах інформаційних протиборств. Основною суттю цієї технології є розподіл інформації по кореспондентам.

2. Наведені критерії якості функціонування інформаційної технології супроводження процесів впливу та визначено, що вона повинна мати розвинену комунікативну здатність, здатність вирішувати слабо організовані задачі, мати здатність до самонавчання, обробки великих масивів природномовних текстів, прогнозування ймовірності реакції при певному виборі повідомлення, мати

можливість бути застосованою в різних сферах життєдіяльності людства та бути спроможною до адаптації.

3. Розроблена загальна схема даних інформаційної технології супроводження процесів впливу, яка включила в себе блок додавання інформаційного повідомлення до бази даних, блок додавання адресата інформаційного повідомлення до бази, відповідно і саму базу даних та базу адресності, а також блок введення параметрів для розрахунку та блок виведення результатів цих розрахунків.

4. Розроблена логічна та фізична моделі інформаційної технології супроводження процесів впливу та описано зв'язки між реляційними таблицями в логічній моделі і описано сутність, атрибути сутності та ідентифікатори в фізичній моделі.

5. Розроблений алгоритм визначення адресата повідомлення інформаційною технологією супроводження процесів впливу та описано його роботу;

6. Базуючись на засобах програмування, які доступні в Access 2010, була розроблена інформаційна технологія, програмне середовище якої написано з використанням коду VBA (Visual Basic for Applications) та яка здатна аналізувати інформаційні текстові представлення на природній мові та їх переадресувати. Створена програма стала носієм назви «Adres».

7. Детально описано процес вводу вхідних даних до бази даних програми Adres, введення параметрів розрахунку, а також здійснено її навчання експертом з області управління впливами;

8. Проведено експериментальне порівняння програми Adres з аналогічним зразком програмного забезпечення по аналізу природномовних текстів TextAnalyst та на основі результатів проведених досліджень побудовані графіки залежностей на основі яких виведено оптимальне значення рівня прийняття правильно відібраних інформаційних змістів повідомлень.

Список використаних джерел

- [1] TextAnalys URL: <http://www.analyst.ru/index.php?lang=eng&dir=content/products/&id=ta> (дата звернення: 02.03.2015).
- [2] Акелис Стивен Б. Технический анализ от А до Я: *пер. с англ.*, Москва: Диаграмма, 1999. 376 с.
- [3] Андреев А. М., Березкин Д. В., Брик А. В., Кантонистов Ю. А. Вероятностный синтаксический анализатор для информационно-поисковой системы. URL: http://www.inteltec.ru/publish/articles/textan/1kx5_9.shtml (дата звернення: 14.12.2016).
- [4] Апресян Ю. Д. Исследования по семантике и лексикографии. *Т.1: Парадигматика, Языки славянских культур*. Москва, 2009. 568 с.
- [5] Білик В. М., Костирко В. С. Інформаційні технології та системи: навч. посіб. Київ: Центр навч. літ., 2006. 232 с.
- [6] Большакова Е. И., Клышинский Э. С., Ландэ Д. В., Носков А. А. та ін. Автоматическая обработка текстов на естественном языке и компьютерная лингвистика: *учеб. пособие*, Москва: МИЭМ, 2011. 272 с.
- [7] Ермаков А. Е., Плешко В. В. Семантическая интерпретация в системах компьютерного анализа текста/ *Информационные технологии*, 2009. №6. С. 2–7.
- [8] Змитрович А. И. Интеллектуальные информационные системы Москва: НТООО "ТетраСистемс", 1997. 368 с.
- [9] Катеринчук І. С., Рачок Р. В., Кравчук В. В., Кулик В. М. Інтелектуальна система автоматизованого контролю знань студентів вищих навчальних закладів. *Інформаційні технології в освіті, Вид-во ХДУ*, 2009. № 4. С.139–147.
- [10] Козлов А.Н. Интеллектуальные информационные системы: *учебник Мин-во с-х. РФ*, Пермь: ФГБОУ ВПО Пермская ГСХА, 2013. 278 с.
- [11] Кокорева Л. В., Перевозчикова О. Л., Ющенко Е. Л. Диалоговые системы. Київ: Наук. думка, 1993. 446 с.

[12] Колос П. О., Голуб С. В. Розробка програмно-алгоритмічного забезпечення автоматизованої системи контролю знань. *Звіт про НДР/АПВУ №204-1004*, Хмельницький, 2003. 70 с.

[13] Комашинский В. И., Смирнов Д. А. Нейронные сети и их применение в системах управления и связи. Москва: Горячая линия – Телеком, 2003. 94 с.

[14] Кубявка М.Б., Тесля Ю. М., Кубявка Л. Б. Інформаційна технологія управління інформаційним супроводженням. *Науково-технічний збірник “Управління розвитком складних систем” Київського націон. унів-ту будівництва і архітектури*. 2017. №29. С. 95–102.

[15] Кубявка М.Б., Тесля Ю. М., Кубявка Л. Б. Рефлекторний метод управління інформаційним супроводженням військ (сил). *Збірник наук. праць Харківського націон. унів-ту Повітряних Сил*. 2017. №1(50). С. 48–53.

[16] Ларичев О. И. Теория и методы принятия решений. 2-е изд., перераб. и доп. Москва: Логос, 2002. 392 с.

[17] Ляльководи свідомості URL: <http://gazeta.dt.ua/technologies/lyalkovodi-svidomosti-.html> (дата звернення: 12.01.2017).

[18] Михалевич В. С., Шор Н. З. Вычислительные методы выбора оптимальных проектных решений, Київ: Наук. мысль, 1977. 230 с.

[19] Показники якості функціонування. URL: http://pidruchniki.com/14310927/psihologiya/pokazniki_yakosti_funktsionuvannya.html. (дата звернення: 15.01.2017).

[20] Посібник зі зв'язків між таблицями Access. URL: <https://support.office.com/uk-Посібник-зі-зв-язків-між-таблицями-8a027791-b8a3-4a32-aa99-e06c4e272c45> (дата звернення: 09.01.2017).

[21] Снитюк В. Е. Прогнозирование. Модели, методы, алгоритмы: учебное пособие. Київ: Маклаут, 2008. 366 с.

[22] Струбицький П., Струбицька І. Побудова дискретних моделей як процес машинного навчання. *Актуальні задачі сучасних технологій*: матеріали Міжнар. науково-технічної конф. молодих учених та студентів. (м. Тернопіль, 19-20 груд. 2012 р.). Тернопіль, 2012. С. 229–230.

[23] Тельнов Ю. Ф., Трембач В. М. Интеллектуальные информационные системы: *Учебное пособие*. Москва: МЭСИ, 2009. 202 с.

[24] Тесля Ю. Н. Рефлекторная система обработки естественно-языковых текстов в АСУ строительством сложных энергетических объектов. *Радиоэлектроника и информатика*, 1998. №4. С.52-55.

[25] Тесля Ю. Н., Чёрный А. Ю. Рефлекторная система голосового управления техническими устройствами (РСГУ). *Управління розвитком складних систем*, 2013. № 15. С. 105–110.

[26] Флегонтов А. В., Фомин В. В. Система интеллектуальной обработки данных. *Известия Российского государственного педагогического университета имени А. И. Герцена*, 2013. №154. С. 41–48.

[27] Функціональні та Не Функціональні Вимоги URL: http://lvivqaclub.blogspot.com/2008/10/blog-post_17.html (дата звернення: 27.12.2016).

ВИСНОВКИ

У дисертаційній роботі розв'язане актуальне наукове завдання щодо розробки моделей та методів управління інформаційним супроводженням в умовах гібридної війни.

У процесі цих досліджень було розв'язано наступні наукові завдання:

1. Проведено аналіз інформаційної складової гібридної війни. Проаналізовано сучасні моделі, методи та засоби інформаційного супроводження процесів впливу в інформаційних війнах. Показано, що актуальною задачею є задача автоматичної адресації повідомлень тим адресатам, які їх найбільше потребують. В результаті аналізу виявлено основні недоліки в управлінні інформацією під час підготовки та здійснення військових операцій. Вони зводяться до того, що в застосованих інформаційних технологіях аналізу природномовних текстів відсутні рішення, щодо управління інформаційними потоками через автоматичний їх розподіл визначеним адресатам з позиції найбільшої впливовості на них. Результати аналізу сформулювали необхідність в розробці моделей і методів, що дозволяють автоматично направляти повідомлення до адресатів, тим самим забезпечуючи оптимізацію доведення інформації до контрагентів та впливаючи на них відповідно до змісту наданої інформації.

2. Проаналізовано причинно-наслідкові зв'язки між інформаційним впливом та інформованістю суб'єктів, на які здійснюється вплив, та з'ясовано, що загальноприйняті підходи не дозволяють ефективно керувати процесами цілеорієнтованих інформаційних взаємодій в управлінні впливами. Запропоновано концепцію управління інформованістю контрагентів взаємодії (війська, цивільне населення, розвідку тощо) з метою формування потрібної їх реакції.

3. Визначено та обґрунтовано застосування процесів інформаційного впливу для вдосконалення проведення військових операцій. Рекомендовано до застосування науково-методичний базис управління інформаційним

супроводженням процесів впливу, в якому виокремлено дві частини: пошук шляхів визначення та зміни інформованості контрагентів взаємодії та розрахунок інформаційного впливу на цих контрагентів. Виходячи з цього, запропоновано концепцію несилового впливу на контрагентів взаємодії та запропоновано модель взаємозалежності впливів та поведінки контрагентів взаємодії.

4. Удосконалено модель управління інформаційним супроводженням, яка забезпечує визначення найбільш інформативних повідомлень для груп населення та військових, а також модель визначення найбільш інформативних компонентів природномовного тексту, характерних для гібридної війни, з позиції автоматичної адресації цих повідомлень різним класам контрагентів, що дозволило автоматично визначати адресатів повідомлень.

5. Запропоновано модель оцінки відхилень в умовних та безумовних ймовірностях реакцій контрагентів впливу в залежності від появи в повідомленнях фіксованих фрагментів тексту та розроблено рефлекторний метод реагування на зміст повідомлення, який дозволив автоматично розподіляти повідомлення по найбільш сприятливим до цих повідомлень класам контрагентів інформаційної взаємодії.

6. Розроблено інформаційну технологію управління інформаційним супроводженням в умовах гібридної війни, ядром якої стала програма Adres, яка здатна аналізувати повідомлення на природній мові та автоматично адресувати їх визначеним контрагентам взаємодії. Проведено експериментальні дослідження. Отримані результати (92% правильно адресованих повідомлень) практично довели спроможність програми Adres автоматично ідентифікувати адресатів повідомлень з метою ціленаправленого (вибіркового) інформаційного впливу на контрагентів взаємодії.

Адекватність та достовірність одержаних у роботі результатів підтверджується вибором методів досліджень, використанням сучасного математичного апарату, а також прикладними реалізаціями розроблених моделей, методів та засобів в технології супроводження процесів впливу під час експериментального розрахунку показника правильно визначених адресатів

повідомлень (у відсотковому співвідношенні). Результати роботи програми Adres мають високу збіжність, з математичними розрахунками проведеними в дисертації, що свідчить про адекватність запропонованих математичних моделей і достовірність наукових положень та висновків отриманих в роботі.

Наукові положення, висновки, пропозиції і рекомендації дисертаційної роботи можуть бути використані в науково-дослідній сфері, оскільки результати роботи поглиблюють та узагальнюють існуючі уявлення про інформаційний вплив, можуть стати основою для подальших наукових досліджень відповідної проблематики, в навчальному процесі і при підготовці навчальної та наукової літератури. Також можуть застосовуватися в постійній роботі підрозділів інформаційно-аналітичного забезпечення та підрозділів спеціальних військових операцій для підготовки у здійсненні цілеорієнтованого несилового впливу на визначений клас контрагентів взаємодії. Все вищенаведене надає підстави вважати сформульовану мету роботи досягнутою.

Результати роботи використані у науково-дослідній роботі Військового інституту Київського національного університету імені Тараса Шевченка, впроваджені в інформаційне забезпечення служб Проектного офісу реформ Міністерства оборони України, виробничу діяльність ТОВ «Авіаційна виробнича компанія СГ «Скаетон», постійну роботу служб Управління інформаційних технологій Міністерства оборони України та в навчальному процесі Київського національного університету імені Тараса Шевченка. Акти впровадження наведені в додатку А.

[1]

ДОДАТКИ

ДОДАТОК А -
АКТИ ПРО ВПРОВАДЖЕННЯ РЕЗУЛЬТАТІВ ДИСЕРТАЦІЙНОГО
ДОСЛІДЖЕННЯ

ПРОЕКТНИЙ ОФІС РЕФОРМ
МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ03168, Київ, Україна
Повітрофлотський пр-т, 6

створений наказом Міністра Оборони України №420 від 18.08.2015

Вих. № 71/04-П від 03.04.2017 р.

Довідка

про впровадження результатів дисертаційного дослідження

Кубявки Миколи Богдановича

по темі

**«МОДЕЛІ ТА МЕТОДИ УПРАВЛІННЯ ІНФОРМАЦІЙНИМ
СУПРОВОДЖЕННЯМ В УМОВАХ ГІБРИДНОЇ ВІЙНИ»**

Довідка видана Кубявці М.Б. про те, що в Проектному офісі реформ Міністерства оборони України (далі ПОР МОУ) були використані результати його дисертаційного дослідження з метою інформаційного забезпечення служб.

На основі інструментів, створених в дисертаційній роботі Кубявкою М.Б., визначені:

1. Взаємозалежність впливів та потреб споживачів інформації, що дозволило формалізувати підхід до оцінки корисності інформації, яку необхідно надати її споживачам.

2. Метод та засоби автоматичного реагування на зміст повідомлення, в основу якого покладено рефлекторний підхід, що забезпечило управління інформаційним супроводженням інформаційного впливу. Розроблений метод дозволив автоматично розподіляти повідомлення по споживачам інформації.

3. Спосіб управління інформованістю контрагентів взаємодії, який полягає у визначенні найбільш інформативних повідомлень для споживачів інформації.

4. Найбільш інформативні компоненти природномовного тексту з позиції автоматичної адресації цих повідомлень різним класам споживачів.

В практичній площині Кубявкою М.Б. було виконано впровадження програми А, яка дозволила автоматично розподіляти повідомлення по усім реалізуємих проектам ПОР МОУ. Що значно зменшило час надходження повідомлень до адресатів в зв'язку з тим, що з контуру управління був виключений оператор і повідомлення адресувались автоматично. Дослідна експлуатація впроваджених засобів показала, що близько для 90% повідомлень вибраний адресат підтверджувався і оператором. Крім того, важливим елементом цих засобів є те, що для принципово нових, чи повідомлень в яких важко визначити адресата вказувався в якості адресата сам оператор.

Ці результати дозволили направляти інформацію тільки тим службам, які її потребують, що оптимізувало інформованість підрозділів та послужило основою їх продуктивної роботи з інформацією.

З повагою

Заступник керівника Проектного
Офісу реформ Міністерства
оборони України, к.т.н.Заступник Проектного
Офісу Міністерства
оборони України, к.т.н. П.В. КАЮК

ЗАТВЕРДЖУЮ

Директор ТОВ «Авіаційна виробнича
компанія СГ «Скаетон»М.М. Топтун
2017 року

Акт
впровадження матеріалів і результатів
дисертаційної роботи
**«Моделі та методи управління інформаційним супроводженням
в умовах гібридної війни»**
автор: Кубявка М.Б.

Матеріали і результати, які містяться в дисертаційній роботі Кубявки Миколи Богдановича, знайшли практичне застосування при впровадженні в виробничу діяльність компанії ТОВ «Авіаційна виробнича компанія СГ «Скаетон»». Автором дисертаційної роботи на базі методології управління інформаційними впливами та теорії несилової взаємодії розроблено підходи і технологію управління інформаційним супроводженням інформованістю (знаннями), які застосовані в діяльності компанії з метою підвищення ефективності процесів управління трудовими ресурсами та оптимізації термінів реалізації проектів компанії.

Впровадження дозволило:

- скоротити час надходження розпорядчих повідомлень за рахунок виключення оператора;
- своєчасно використовувати існуючий досвід і технологію компанії при впровадженні методів проектного управління;
- підвищити ефективність доведення необхідної інформації до робочого персоналу компанії та удосконалити контроль за реалізацією проектів з боку керівництва;
- оптимізувати реалізацію проектів за рахунок всебічного, цілеорієнтованого інформування їх виконавців, оптимально завантажити трудові ресурси компанії.

За результатами впровадження в діяльності компанії отримано значне підвищення управління інформаційними потоками. Це дозволило направляти інформацію тільки тим службам, які її потребують, що оптимізувало інформованість підрозділів та послужило основою їх продуктивної роботи з інформацією, стало ключовим моментом суттєвого скорочення витрат і зменшення відхилень за термінами реалізації об'єктів компанії.

Заступник директора з якості

В.А. Литвинов

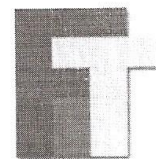
Начальник виробництва

П.М. Деща



КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ



04116, м. Київ, вул. Ванди Василевської, 24; тел.: 481-45-07
Електронна адреса, e-mail: fit_dpt.head@univ.net.ua; Internet: www.fit.univ.kiev.ua

ДОВІДКА

**про впровадження результатів дисертаційного дослідження
Кубявки Миколи Богдановича «Моделі та методи управління
інформаційним супроводженням в умовах гібридної війни»
в навчальний процес**

У результаті проведення дисертаційного дослідження Кубявки М.Б. на тему: «Моделі та методи управління інформаційним супроводженням в умовах гібридної війни» було розроблено, теоретично обґрунтовано та експериментально перевірено авторські моделі та методи інформаційної технології управління інформаційним супроводженням процесів інформаційного впливу. Робота доповнює методологію управління впливами новими науковими положеннями, поняттями, теоретико-методичними побудовами, моделями і методами та результатом якої є розроблений програмний засіб Adres спроможний розподіляти повідомлення по визначеним їх адресатам за критерієм максимального інформаційної дії на них.

Зазначені в роботі положення, поняття, теоретико-методичні побудови, моделі і методи, а також новий підхід до управління впливами були використані у навчальному процесі для студентів V курсу спеціальності «Консолідована інформація» та спеціальності «Інформаційна аналітика та вплив». На основі матеріалів дисертації було розроблено курс лекцій та практичних занять з дисципліни «Методи інформаційної розвідки та впливів», що вплинуло на формування готовності майбутніх спеціалістів в області інформаційної аналітики та консолідованої інформації.

Впровадження результатів дисертаційного дослідження Кубявки М.Б. відбувалося протягом 2016-2017 років на базі факультету інформаційних технологій Київського національного університету імені Т.Шевченка.

Отримані результати дослідження можна рекомендувати до подальшого впровадження: у навчальний процес вищих навчальних закладів України з метою підвищення якісного рівня професійної підготовки майбутніх магістрів.

Заступник декана
з навчально-виховної роботи



М. О. Мостопалова

ЗАТВЕРДЖУЮ

Начальник Управління інформаційних
технологій Міністерства оборони України
полковник

К.О.СОКОЛОВ

2017 року

**АКТ****впровадження результатів дисертаційного дослідження**

Кубявки Миколи Богдановича

по темі «Моделі та методи управління інформаційним супроводженням в умовах гібридної війни»

Акт складений про те, що результати дисертаційного дослідження Кубявці М.Б. були використані в *Управлінні інформаційних технологій Міністерства оборони України* з метою інформаційного забезпечення відділів.

Отримані в роботі інструменти забезпечили:

1. Управління інформаційним супроводженням інформаційного впливу, а саме автоматичний розподіл повідомлень по споживачам інформації. В основу якого покладено метод та засіб автоматичного реагування на зміст повідомлення, що базується на використанні рефлекторного підходу.

2. Визначення найбільш інформативних повідомлень для споживачів інформації на основі розробленого способу управління інформованістю контрагентів взаємодії.

3. Формалізувати підхід до оцінки корисності інформації, яку необхідно надати споживачу в зв'язку з використанням моделі взаємозалежності впливів та потреб споживачів інформації.

Розроблена Кубявкою М.Б. програма Adres дозволила автоматично розподіляти повідомлення по відділам *Управління*, що оптимізувало інформованість підрозділів та послужило основою їх продуктивної роботи з інформацією, дало ряд переваг над іншими аналогічними системами, а саме:

- здатність до вирішення широкого кола завдань в області супроводження управління впливами;

- здатність витягати знання з даних і представляти їх в обсязі необхідному виключно заданим адресатам, з метою не максимального інформування контрагента взаємодії, а необхідної і достатньої інформаційної дії на нього;

- простоту використання;

Додаток А.4 (продовження)

- інтуїтивно зрозумілий інтерфейс;
- моделювання механізмів інтелектуальної діяльності людини;
- можливість інтегрувати інформаційну технологію та застосувати рефлекторні методи в будь-якій галузі управління та на самперед в отриманні переваг в ході постійної негативної інформаційної дії на населення країни в умовах гібридної війни.

На основі проведених експериментів і отриманих результатів, можна вважати, що застосування інформаційної технології управління інформаційним супроводженням інформаційного впливу є актуальним у всіх галузях, де є необхідність управління персоналом, ведення заходів несилового впливу на противника чи контрдії по захисту від такого, а також, адаптувавши систему, є можливість застосувати її для спеціальної техніки читання будь-яких текстів, яка базується на розуміння змісту тексту за допомогою змістовних понять.

Комісія у складі:

голови: начальник відділу інформаційної політики – заступник начальника полковник Галушко С.О.;

членів: старший офіцер відділу інформаційної політики підполковник Ситнік О.Й.;

офіцер відділу інформаційної політики підполковник Віщун В.В.;

офіцер відділу інформаційної політики капітан Горбенко О.В.

установила впровадження в повсякденну діяльність Управління інформаційних технологій Міністерства оборони України.

Голова комісії:

начальник відділу інформаційної політики –

заступник начальника Управління інформаційних технологій
полковник

 ГАЛУШКО С.О.

Члени комісії:

старший офіцер відділу інформаційної політики

Управління інформаційних технологій
підполковник

 СИТНИК О.Й.

офіцер відділу інформаційної політики

Управління інформаційних технологій
підполковник

 ВІЩУН В.В.

офіцер відділу інформаційної політики

Управління інформаційних технологій
капітан

 ГОРБЕНКО О.В.

ДОВІДКА
про впровадження в освітній процес
результатів дисертаційного дослідження
Кубявки Миколи Богдановича «Моделі та методи управління
інформаційним супроводженням в умовах гібридної війни»

У результаті проведення дисертаційного дослідження Кубявкою М.Б. на тему: «Моделі та методи управління інформаційним супроводженням в умовах гібридної війни» було розроблено, теоретично обґрунтовано та експериментально перевірено авторські моделі та методи інформаційної технології управління інформаційним супроводженням процесів інформаційного впливу. Робота доповнює методологію аналізу природномовного тексту новими науковими положеннями, поняттями, теоретико-методичними побудовами, моделями і методами та результатом якої є розроблений програмний засіб Adres спроможний розподіляти повідомлення по визначеним їх адресатам за критерієм максимального інформаційної дії на них.

Зазначені в роботі положення, поняття, теоретико-методичні побудови, моделі і методи, а також засоби аналізу природномовних текстів були використані у навчальному процесі для студентів III курсу Інституту філології, спеціальності 035.10 «Прикладна лінгвістика». На основі матеріалів дисертації було розроблено курс практичних занять, що вплинуло на формування готовності майбутніх спеціалістів в області прикладної лінгвістики.

Отримані результати дослідження можна рекомендувати до подальшого впровадження у навчальний процес вищих навчальних закладів України для студентів філологічних спеціальностей з метою підвищення якісного рівня професійної підготовки студентів.

Директор інституту філології
 Київського національного університету
 імені Тараса Шевченка



ДОДАТОК Б -
ЕКСПЕРТНА ОЦІНКА КЛАСУ ПОВІДОМЛЕНЬ

Таблиця Б.1

Експертна оцінка класу повідомлень в застосовності до дітей

Вплив	Зміст повідомлень прийнятний для дітей									
	Що несе похвалу	Що несе покарання	Про розважальні заходи та свята	Про отримання високої оцінки успішності	Про улюблені страви та уподобання	Щодо несправедливості по відношенню до них	Щодо невиконання даних обіцянок	Про кумирів та улюбленців	Про необхідність виконання домашніх та шкільних обов'язків	Про загрозу життю та здоров'ю близької людини
1	2	3	4	5	6	7	8	9	10	11
Викликати почуття віри та надії	1,0	0,0	0,4	0,9	0,5	0,0	0,0	0,7	0,2	0,0
Викликати почуття любові та радості	1,0	0,0	0,7	0,9	0,7	0,0	0,0	0,6	0,2	0,0
Викликати ентузіазм та сміливість	1,0	0,0	0,6	0,7	0,0	0,1	0,0	0,3	0,3	0,4
Викликати почуття колективізму та національної свідомості	0,5	0,0	0,2	0,3	0,0	0,0	0,0	0,0	0,1	0,0
Викликати почуття впевненості	1,0	0,5	0,4	1,0	0,1	0,0	0,0	0,0	0,3	0,0
Викликати почуття захищеності	1,0	0,0	0,2	0,2	0,3	0,0	0,0	0,0	0,0	0,0
Викликати почуття забезпеченості	1,0	0,0	0,6	0,3	0,6	0,0	0,0	0,0	0,0	0,0
Привити порядність та здержаність	1,0	0,5	0,1	0,6	0,0	0,0	0,0	0,0	0,1	0,0
Привити повагу до людей та Батьківщини	0,9	0,5	0,1	0,2	0,0	0,0	0,0	0,0	0,0	0,0
Привити національну свідомість	0,3	0,0	0,0	0,2	0,2	0,0	0,0	0,1	0,0	0,0

Таблиця Б.1 (закінчення)

1	2	3	4	5	6	7	8	9	10	11
Викликати почуття тривоги	0,0	1,0	0,0	0,1	0,0	0,9	0,9	0,0	0,2	1,0
Викликати байдужість та черствість	0,0	0,7	0,0	0,3	0,0	0,5	0,5	0,0	0,0	0,0
Насадити брехливість та вульгарність	0,0	0,8	0,0	0,0	0,0	0,3	0,6	0,0	0,0	0,0
Заохочувати грубість (брутальність)	0,4	0,8	0,0	0,0	0,0	0,1	0,0	0,0	0,0	0,0
Привити жорстокість та агресивність	0,9	0,9	0,0	0,0	0,0	0,2	0,4	0,0	0,0	0,0
Привити лінивість	0,5	0,4	0,0	0,2	0,0	0,3	0,0	0,0	0,2	0,0
Привити підозрілість (недовірливість)	0,0	0,3	0,0	0,2	0,0	0,2	1,0	0,0	0,0	0,0
Привити жадібність	0,4	0,2	0,0	0,0	0,0	0,0	0,8	0,0	0,0	0,0
Привити лихослівність та нескромність	0,0	0,6	0,0	0,3	0,0	0,0	0,0	0,0	0,0	0,0
Викликати боягузтво та ненадійність	0,0	0,7	0,0	0,0	0,0	0,2	0,7	0,0	0,2	0,8
Стимулювати нахабність та неввічливість	0,0	0,5	0,0	0,0	0,0	0,0	0,5	0,0	0,0	0,0
Заохочувати підлість та невдячність	0,0	0,4	0,0	0,0	0,0	0,2	0,4	0,0	0,0	0,0
Дратувати схильність до вбивства	0,0	0,5	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,4
Стимулювати схильність до перелюбу	0,0	0,2	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Розвивати схильність до шахрайства	0,0	0,4	0,0	0,2	0,0	0,0	0,3	0,0	0,0	0,0
Спонукаати до самогубства	0,0	0,7	0,0	0,0	0,0	0,3	0,0	0,0	0,0	0,1

Таблиця Б.2

Експертна оцінка класу повідомлень в застосовності до молоді, що працює

Вплив	Зміст повідомлень прийнятний для молоді, що працює											
	Що несе похвалу, або позитивну оцінку праці	Що несе покарання, або негативну оцінку праці	Про стан здоров'я близьких	Про рівень заробітної плати	Про рівень плати за ЖКХ	Про коливання курсу валют та цін на продукти і товари	Про стан справ в зоні проведення АТО	Про санкції світової спільноти до держави-агресора	Про діяльність керівництва держави та високу боєздатність армії щодо забезпечення захисту країни	Про «звірства» щодо полонених зі сторони терористичних формувань на сході країни	Про недобрі факти з життя своєї армії (їх перекучення, відкрита брехня)	Про загрозу життю та здоров'ю близької людини
1	2	3	4	5	6	7	8	9	10	11	12	13
Викликати почуття віри та надії	1,0	0,0	0,6	0,9	0,0	0,0	0,5	0,5	0,6	0,0	0,0	0,6
Викликати почуття любові та радості	1,0	0,0	0,5	0,9	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Викликати ентузіазм та сміливість	1,0	0,0	0,3	0,7	0,0	0,0	0,0	0,3	0,5	0,0	0,0	0,0
Викликати почуття колективізму та національної свідомості	0,5	0,0	0,0	0,5	0,0	0,0	0,5	0,2	0,7	0,5	0,3	0,3
Викликати почуття впевненості	1,0	0,5	0,5	1,0	0,0	0,0	0,0	0,3	0,6	0,0	0,0	0,0
Викликати почуття захищеності	1,0	0,0	0,5	0,7	0,0	0,0	0,4	0,2	0,7	0,0	0,0	0,0
Викликати почуття забезпеченості	1,0	0,0	0,5	0,6	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Привити порядність та здержаність	1,0	0,5	0,5	0,6	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Привити повагу до людей та Батьківщини	0,9	0,0	0,0	0,8	0,0	0,0	0,6	0,2	0,8	0,0	0,1	0,0

Таблиця Б.2 (закінчення)

1	2	3	4	5	6	7	8	9	10	11	12	13
Привити національну свідомість	0,7	0,0	0,0	0,5	0,0	0,0	0,5	0,0	0,8	0,0	0,0	0,0
Викликати почуття тривоги	0,0	1,0	0,5	0,5	1,0	1,0	0,8	0,0	0,2	0,9	0,3	1,0
Викликати байдужість та черствість	0,0	0,7	0,0	0,0	0,3	0,3	0,0	0,0	0,0	0,2	0,1	0,0
Насадити брехливість та вульгарність	0,0	0,8	0,0	0,0	0,2	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Заохочувати грубість (брутальність)	0,4	0,8	0,0	0,0	0,8	0,1	0,0	0,0	0,0	0,3	0,0	0,3
Привити жорстокість та агресивність	0,9	0,9	0,0	0,0	0,7	0,1	0,0	0,0	0,0	0,0	0,0	0,4
Привити лінивість	0,5	0,4	0,0	0,5	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Привити підозрілість (недовірливість)	0,0	0,3	0,0	0,0	0,4	0,0	0,2	0,0	0,2	0,0	0,4	0,0
Привити жадібність	0,4	0,2	0,0	0,5	0,8	0,7	0,0	0,0	0,0	0,0	0,0	0,3
Привити лихослівність та нескромність	0,0	0,6	0,0	0,5	0,6	0,2	0,0	0,0	0,0	0,0	0,5	0,5
Викликати боягузтво та ненадійність	0,0	0,7	0,0	0,0	0,0	0,0	0,3	0,0	0,0	0,0	0,0	0,0
Стимулювати нахабність та неvwічливість	0,0	0,5	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,5
Заохочувати підлість та невдячність	0,0	0,5	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,5
Дратувати схильність до вбивства	0,0	0,5	0,0	0,0	0,2	0,0	0,3	0,0	0,0	0,0	0,0	0,5
Стимулювати схильність до перелюбу	0,0	0,5	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,5
Розвивати схильність до шахрайства	0,0	0,5	0,5	0,5	0,7	0,2	0,0	0,0	0,0	0,0	0,2	0,5

Спонукаати до самогубства	0,0	0,5	0,0	0,0	0,6	0,1	0,0	0,0	0,0	0,0	0,0	0,5
---------------------------	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----

Таблиця Б.3

Експертна оцінка класу повідомлень в застосовності до молоді, що навчається

Вплив	Зміст повідомлень прийнятний для молоді, що навчається											
	Що несе похвалу, або позитивну оцінку навчання	Що несе покарання, або негативну оцінку навчання	Про стан здоров'я близьких	Про зміни в освітній програмі студентів	Про стан стипендій та плагіату за гуртожиток	Про громадсько-розважальні заходи та заклади	Про національну свідомість та самовизначеність	Про стан справ в зоні проведення АТО	Про діяльність керівництва держави та високу боєздатність армії щодо забезпечення захисту країни	Про недобрі факти з життя своєї армії (їх перекучення, відкрита брехня)	Про можливість самореалізації після навчання	Про загрозу життю та здоров'ю близької людини
1	2	3	4	5	6	7	8	9	10	11	12	13
Викликати почуття віри та надії	1,0	0,0	0,6	0,9	0,4	1,0	1,0	0,6	0,7	0,0	0,0	0,5
Викликати почуття любові та радості	1,0	0,0	0,5	0,9	0,0	0,8	0,7	0,0	0,0	0,0	0,0	0,0
Викликати ентузіазм та сміливість	1,0	0,0	0,3	0,7	0,4	0,8	0,0	0,4	0,3	0,0	0,0	0,0
Викликати почуття колективізму та національної свідомості	0,5	0,0	0,0	0,3	0,4	0,9	0,0	0,6	0,6	0,0	0,0	0,3
Викликати почуття впевненості	1,0	0,0	0,5	1,0	0,3	0,7	0,0	0,3	0,8	0,0	0,0	0,0
Викликати почуття захищеності	1,0	0,0	0,5	0,2	0,0	0,2	0,0	0,4	0,9	0,0	0,0	0,0
Викликати почуття забезпеченості	1,0	0,0	0,0	0,3	0,5	0,2	0,0	0,0	0,4	0,0	0,0	0,0
Привити порядність та здержаність	1,0	0,5	0,0	0,6	0,0	0,3	0,0	0,0	0,2	0,0	0,0	0,3

Привити повагу до людей та Батьківщини	0,9	0,0	0,3	0,2	0,4	0,4	0,0	0,3	0,9	0,0	0,5	0,5
--	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----

Привити повагу до людей та Батьківщини	0,9	0,0	0,3	0,2	0,0	0,0	0,3	0,0	0,1	0,0	0,5	0,5
--	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----

Таблиця Б.4 (закінчення)

1	2	3	4	5	6	7	8	9	10	11	12	13
Привити національну свідомість	0,7	0,0	0,0	0,2	0,0	0,0	0,7	0,1	0,1	0,0	0,0	0,0
Викликати почуття тривоги	0,0	1,0	0,0	0,1	0,4	0,8	0,5	0,5	0,1	0,9	0,4	0,5
Викликати байдужість та черствість	0,0	0,7	0,0	0,3	0,1	0,0	0,0	0,0	0,0	0,1	0,2	0,0
Насадити брехливість та вульгарність	0,0	0,8	0,0	0,0	0,0	0,0	0,0	0,2	0,0	0,0	0,0	0,0
Заохочувати грубість (брутальність)	0,4	0,8	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,3
Привити жорстокість та агресивність	0,9	0,9	0,0	0,0	0,2	0,0	0,1	0,2	0,0	0,1	0,0	0,0
Привити лінивість	0,5	0,4	0,0	0,2	0,0	0,0	0,0	0,0	0,0	0,0	0,2	0,0
Привити підозрілість (недовірливість)	0,0	0,3	0,0	0,2	0,2	0,4	0,3	0,1	0,3	0,0	0,0	0,0
Привити жадібність	0,4	0,2	0,0	0,0	0,3	0,5	0,0	0,6	0,0	0,0	0,0	0,3
Привити лихослівність та нескромність	0,0	0,6	0,0	0,3	0,2	0,0	0,0	0,2	0,0	0,0	0,5	0,5
Викликати боягузтво та ненадійність	0,0	0,7	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Стимулювати нахабність та неvwчливість	0,0	0,5	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,5
Заохочувати підлість та невдячність	0,0	0,5	0,0	0,0	0,0	0,0	0,0	0,2	0,0	0,0	0,0	0,5
Дратувати схильність до вбивства	0,0	0,5	0,0	0,0	0,0	0,4	0,2	0,0	0,0	0,3	0,0	0,5
Стимулювати схильність до перелюбу	0,0	0,5	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,5
Розвивати схильність до шахрайства	0,0	0,5	0,0	0,0	0,0	0,6	0,0	0,5	0,0	0,0	0,0	0,5

Привити повагу до людей та Батьківщини	0,9	0,0	0,0	0,2	0,0	0,0	0,3	0,0	0,1	0,0	0,5	0,5
--	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----

Таблиця Б.5 (закінчення)

1	2	3	4	5	6	7	8	9	10	11	12	13
Привити національну свідомість	0,7	0,0	0,0	0,2	0,0	0,0	0,7	0,1	0,1	0,0	0,0	0,0
Викликати почуття тривоги	0,0	1,0	0,0	0,1	0,4	0,8	0,5	0,5	0,1	0,9	0,4	0,5
Викликати байдужість та черствість	0,0	0,7	0,0	0,3	0,1	0,0	0,0	0,0	0,0	0,1	0,2	0,0
Насадити брехливість та вульгарність	0,0	0,8	0,0	0,0	0,0	0,0	0,0	0,2	0,0	0,0	0,0	0,0
Заохочувати грубість (брутальність)	0,4	0,8	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,3
Привити жорстокість та агресивність	0,9	0,9	0,0	0,0	0,2	0,0	0,1	0,2	0,0	0,1	0,0	0,0
Привити лінивість	0,5	0,4	0,0	0,2	0,0	0,0	0,0	0,0	0,0	0,0	0,2	0,0
Привити підозрілість (недовірливість)	0,0	0,3	0,0	0,2	0,2	0,4	0,3	0,1	0,3	0,0	0,0	0,0
Привити жадібність	0,4	0,2	0,0	0,0	0,3	0,5	0,0	0,6	0,0	0,0	0,0	0,3
Привити лихослівність та нескромність	0,0	0,6	0,0	0,3	0,2	0,0	0,0	0,2	0,0	0,0	0,5	0,5
Викликати боягузтво та ненадійність	0,0	0,7	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Стимулювати нахабність та неvwічливість	0,0	0,5	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,5
Заохочувати підлість та невдячність	0,0	0,5	0,0	0,0	0,0	0,0	0,0	0,2	0,0	0,0	0,0	0,5
Дратувати схильність до вбивства	0,0	0,5	0,0	0,0	0,0	0,4	0,2	0,0	0,0	0,3	0,0	0,5
Стимулювати схильність до перелюбу	0,0	0,5	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,5
Розвивати схильність до шахрайства	0,0	0,5	0,0	0,0	0,0	0,6	0,0	0,5	0,0	0,0	0,0	0,5

Привити повагу до людей та Батьківщини	0,9	0,0	0,0	0,2	0,0	0,0	0,3	0,0	0,1	0,0	0,5	0,5
--	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----

Таблиця Б.6 (закінчення)

1	2	3	4	5	6	7	8	9	10	11	12	13
Привити національну свідомість	0,7	0,0	0,0	0,2	0,0	0,0	0,7	0,1	0,1	0,0	0,0	0,0
Викликати почуття тривоги	0,0	1,0	0,0	0,1	0,4	0,8	0,5	0,5	0,1	0,9	0,4	0,5
Викликати байдужість та черствість	0,0	0,7	0,0	0,3	0,1	0,0	0,0	0,0	0,0	0,1	0,2	0,0
Насадити брехливість та вульгарність	0,0	0,8	0,0	0,0	0,0	0,0	0,0	0,2	0,0	0,0	0,0	0,0
Заохочувати грубість (брутальність)	0,4	0,8	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,3
Привити жорстокість та агресивність	0,9	0,9	0,0	0,0	0,2	0,0	0,1	0,2	0,0	0,1	0,0	0,0
Привити лінивість	0,5	0,4	0,0	0,2	0,0	0,0	0,0	0,0	0,0	0,0	0,2	0,0
Привити підозрілість (недовірливість)	0,0	0,3	0,0	0,2	0,2	0,4	0,3	0,1	0,3	0,0	0,0	0,0
Привити жадібність	0,4	0,2	0,0	0,0	0,3	0,5	0,0	0,6	0,0	0,0	0,0	0,3
Привити лихослівність та нескромність	0,0	0,6	0,0	0,3	0,2	0,0	0,0	0,2	0,0	0,0	0,5	0,5
Викликати боягузтво та ненадійність	0,0	0,7	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Стимулювати нахабність та неввічливість	0,0	0,5	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,5
Заохочувати підлість та невдячність	0,0	0,5	0,0	0,0	0,0	0,0	0,0	0,2	0,0	0,0	0,0	0,5
Дратувати схильність до вбивства	0,0	0,5	0,0	0,0	0,0	0,4	0,2	0,0	0,0	0,3	0,0	0,5
Стимулювати схильність до перелюбу	0,0	0,5	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,5
Розвивати схильність до шахрайства	0,0	0,5	0,0	0,0	0,0	0,6	0,0	0,5	0,0	0,0	0,0	0,5

Привити повагу до людей та Батьківщини	0,9	0,0	0,0	0,2	0,0	0,0	0,3	0,0	0,1	0,0	0,5	0,5
--	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----

Таблиця Б.7 (закінчення)

1	2	3	4	5	6	7	8	9	10	11	12	13
Привити національну свідомість	0,7	0,0	0,0	0,2	0,0	0,0	0,7	0,1	0,1	0,0	0,0	0,0
Викликати почуття тривоги	0,0	1,0	0,0	0,1	0,4	0,8	0,5	0,5	0,1	0,9	0,4	0,5
Викликати байдужість та черствість	0,0	0,7	0,0	0,3	0,1	0,0	0,0	0,0	0,0	0,1	0,2	0,0
Насадити брехливість та вульгарність	0,0	0,8	0,0	0,0	0,0	0,0	0,0	0,2	0,0	0,0	0,0	0,0
Заохочувати грубість (брутальність)	0,4	0,8	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,3
Привити жорстокість та агресивність	0,9	0,9	0,0	0,0	0,2	0,0	0,1	0,2	0,0	0,1	0,0	0,0
Привити лінивість	0,5	0,4	0,0	0,2	0,0	0,0	0,0	0,0	0,0	0,0	0,2	0,0
Привити підозрілість (недовірливість)	0,0	0,3	0,0	0,2	0,2	0,4	0,3	0,1	0,3	0,0	0,0	0,0
Привити жадібність	0,4	0,2	0,0	0,0	0,3	0,5	0,0	0,6	0,0	0,0	0,0	0,3
Привити лихослівність та нескромність	0,0	0,6	0,0	0,3	0,2	0,0	0,0	0,2	0,0	0,0	0,5	0,5
Викликати боягузтво та ненадійність	0,0	0,7	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Стимулювати нахабність та неввічливість	0,0	0,5	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,5
Заохочувати підлість та невдячність	0,0	0,5	0,0	0,0	0,0	0,0	0,0	0,2	0,0	0,0	0,0	0,5
Дратувати схильність до вбивства	0,0	0,5	0,0	0,0	0,0	0,4	0,2	0,0	0,0	0,3	0,0	0,5
Стимулювати схильність до перелюбу	0,0	0,5	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,5
Розвивати схильність до шахрайства	0,0	0,5	0,0	0,0	0,0	0,6	0,0	0,5	0,0	0,0	0,0	0,5

Спонукаци до самогубства	0,0	0,5	0,0	0,0	0,0	0,3	0,0	0,0	0,0	0,0	0,0	0,5
--------------------------	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----

ДОДАТОК В –
СХЕМАТИЧНЕ ПРЕДСТАВЕННЯ ФІЗИЧНОЇ МОДЕЛІ
ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ УПРАВЛІННЯ ІНФОРМАЦІЙНИМ
СУПРОВОДЖЕННЯМ

Фізична модель інформаційної технології управління інформаційним супроводженням

Таблиця А має п'ять полів числового типу, всі поля не мають умови обов'язкового заповнення.

Таблиця В.1

Опис атрибутів таблиці А

Поле	Тип поля	Розмір поля	Індекс
Nzp_1	Числовий	Довге ціле	
Nzp_2	Числовий	Довге ціле	
Ko1	Числовий	Довге ціле	
DL	Числовий	Подвійне з плаваючою крапкою	
D	Числовий	Подвійне з плаваючою крапкою	

Таблиця S має шість полів типу лічильник, текстовий, числовий та логічний. Всі поля, окрім поля Nzz, не мають умови обов'язкового заповнення. Це поле є первинним ключем, тобто атрибутом, який унікально ідентифікує рядок.

Таблиця В.2

Опис атрибутів таблиці S

Поле	Тип поля	Розмір поля	Індекс
Nzz	Лічильник	Довге ціле	Primary key
Tx	Текстовий	32	
Ko11	Числовий	Довге ціле	
Ind	Числовий	Байт	
Ina	Логічний	Так/ні	
K	Числовий	Байт	
Ko1	Числовий	Довге ціле	

Таблиця S_1 має два поля типу числовий. Всі поля не мають умови обов'язкового заповнення:

Таблиця В.3

Опис атрибутів таблиці S_1

Поле	Тип поля	Розмір поля	Індекс
NzP	Числовий	Довге ціле	
NzB	Числовий	Довге ціле	

Таблиця Ваза має тридцять два поля типу лічильник, дата/час, текстовий, числовий та логічний. Всі поля, окрім поля Nzz, не мають умови обов'язкового заповнення. Це поле є первинним ключем, тобто атрибутом, який унікально ідентифікує рядок.

Таблиця В.4

Опис атрибутів таблиці Ваза (повідомлення)

Поле	Тип поля	Розмір поля	Індекс
Nzz	Лічильник	Довге ціле	Primary key
Dat	Дата/час		
Naim	Текстовий	255	
Txt_1	Текстовий	255	
Txt_2	Текстовий	255	
Nor_1	Текстовий	255	
Nor_2	Текстовий	255	
PoL_1	Текстовий	50	
R1	Числовий	Одинарне з плаваючою крапкою	
PoL_2	Текстовий	50	
R2	Числовий	Одинарне з плаваючою крапкою	
PoL_3	Текстовий	50	
R3	Числовий	Одинарне з плаваючою крапкою	
PoL_4	Текстовий	50	
R4	Числовий	Одинарне з плаваючою крапкою	
PoL_5	Текстовий	50	
R5	Числовий	Одинарне з плаваючою крапкою	
P1	Числовий	Одинарне з плаваючою крапкою	
P2	Числовий	Одинарне з плаваючою крапкою	
P3	Числовий	Одинарне з плаваючою крапкою	
P4	Числовий	Одинарне з плаваючою крапкою	
P5	Числовий	Одинарне з плаваючою крапкою	
Obuzen	Логічний	Так/ні	
Pro_1	Текстовий	50	
Pro_2	Текстовий	50	
Pro_3	Текстовий	50	
Pro_4	Текстовий	50	
Pro_5	Текстовий	50	
Wse	Числовий	Довге ціле	
Uga	Числовий	Довге ціле	
Loz	Числовий	Довге ціле	
Pro	Числовий	Довге ціле	

Таблиця R має шести полів типу лічильник, текстовий, числовий та логічний. Всі поля, окрім поля Nzz, не мають умови обов'язкового заповнення. Це поле є первинним ключем, тобто атрибутом, який унікально ідентифікує рядок.

Таблиця В.5

Опис атрибутів таблиці R

Поле	Тип поля	Розмір поля	Індекс
Nzz	Лічильник	Довге ціле	Primary key
Kol	Числовий	Довге ціле	
Pol	Текстовий	50	
DL	Числовий	Подвійне з плаваючою крапкою	
D	Числовий	Подвійне з плаваючою крапкою	
Ina	Логічний	Так/ні	

Таблиця Statistika має вісімнадцять полів типу лічильник, текстовий, дата/час, числовий та логічний. Всі поля, окрім поля Nzz, не мають умови обов'язкового заповнення. Це поле є первинним ключем, тобто атрибутом, який унікально ідентифікує рядок.

Таблиця В.6

Опис атрибутів таблиці статистики

Поле	Тип поля	Розмір поля	Індекс
Nzz	Лічильник	Довге ціле	Primary key
Uga	Числовий	Довге ціле	
Proc_1	Числовий	Одинарне з плаваючою крапкою	
Prima	Текстовий	255	
Dat	Дата/час		
MinKol	Числовий	Довге ціле	
MaxKol	Числовий	Довге ціле	
Nom	Числовий	Довге ціле	
Ina	Числовий	Довге ціле	
Iko	Числовий	Довге ціле	
Kak	Логічний	Так/ні	
Vnu	Логічний	Так/ні	
Wse	Числовий	Довге ціле	
Loz	Числовий	Довге ціле	
Pro	Числовий	Довге ціле	
Kol	Числовий	Довге ціле	
Proc_2	Числовий	Одинарне з плаваючою крапкою	
Proc_3	Числовий	Одинарне з плаваючою крапкою	

Таблиця R_1 має два поля типу числовий. Всі поля не мають умови обов'язкового заповнення:

Таблиця В.7

Опис атрибутів таблиці R_1

Поле	Тип поля	Розмір поля	Індекс
NzP	Числовий	Довге ціле	
NzB	Числовий	Довге ціле	

Таблиця Орепа має дев'ятнадцять полів типу текстовий, числовий та логічний. Всі поля не мають умови обов'язкового заповнення:

Таблиця В.8

Опис атрибутів таблиці Орепа

Поле	Тип поля	Розмір поля	Індекс
Nzz	Числовий	Довге ціле	
Prima	Текстовий	255	
Ina_1	Числовий	Довге ціле	
Iko_1	Числовий	Довге ціле	
Kola_1	Числовий	Довге ціле	
Min_1	Числовий	Довге ціле	
Nom	Числовий	Довге ціле	
Kak	Логічний	Так/ні	
Vnu	Логічний	Так/ні	
Ina_2	Числовий	Довге ціле	
Iko_2	Числовий	Довге ціле	
Kola_2	Числовий	Довге ціле	
Min_2	Числовий	Довге ціле	
Ina	Числовий	Довге ціле	
Iko	Числовий	Довге ціле	
Kola	Числовий	Довге ціле	
KolOb	Числовий	Довге ціле	
Max_1	Числовий	Довге ціле	
Max_2	Числовий	Довге ціле	
Iur	Числовий	Одинарне з плаваючою крапкою	

Таблиця Pol має одне поле типу текстовий. Поле не має умови обов'язкового заповнення:

Таблиця В.9

Опис атрибутів таблиці адресатів

Поле	Тип поля	Розмір поля	Індекс
Pol	Текстовий	50	

**ДОДАТОК Д –
ГРАФІЧНА ВІЗУАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ПРОВЕДЕНИХ
ДОСЛІДЖЕНЬ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ УПРАВЛІННЯ
ІНФОРМАЦІЙНИМ СУПРОВОДЖЕННЯМ**

**Залежність відсотку правильно
визначених системою адресатів від кількості всього
проаналізованих понять**

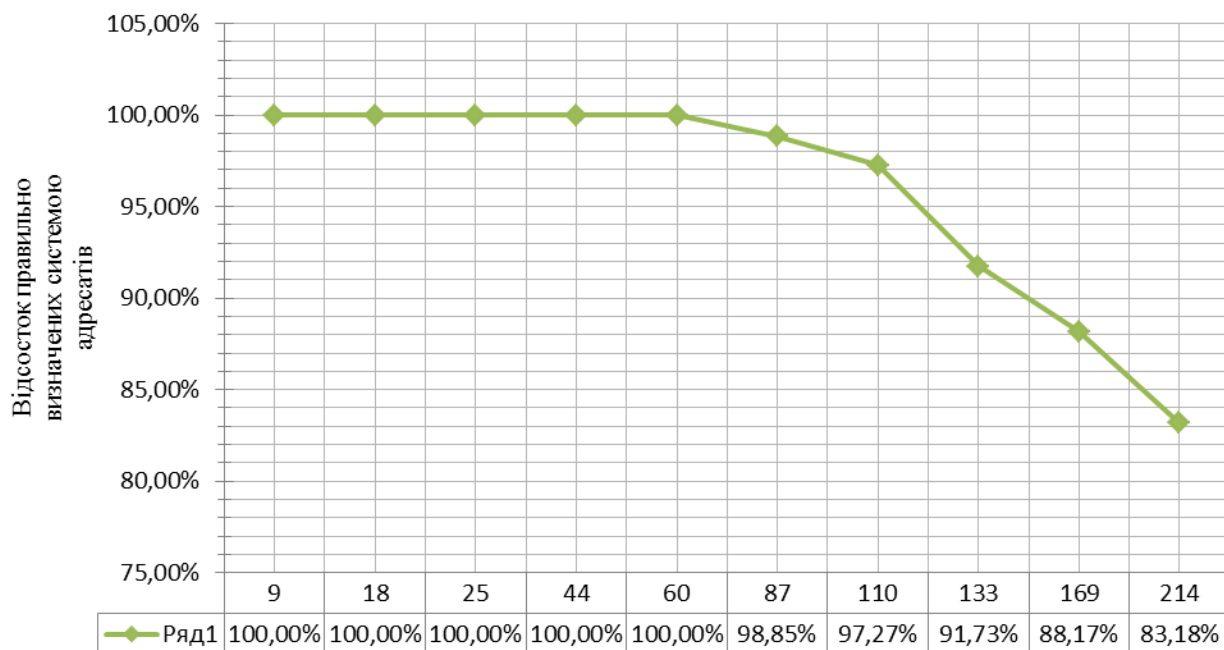


Рис. Д.1 Графік залежності відсотку правильно визначених системою адресатів від кількості всього проаналізованих понять.

**Залежність відсотку правильно
визначених системою адресатів від рівня прийняття
проаналізованих понять**

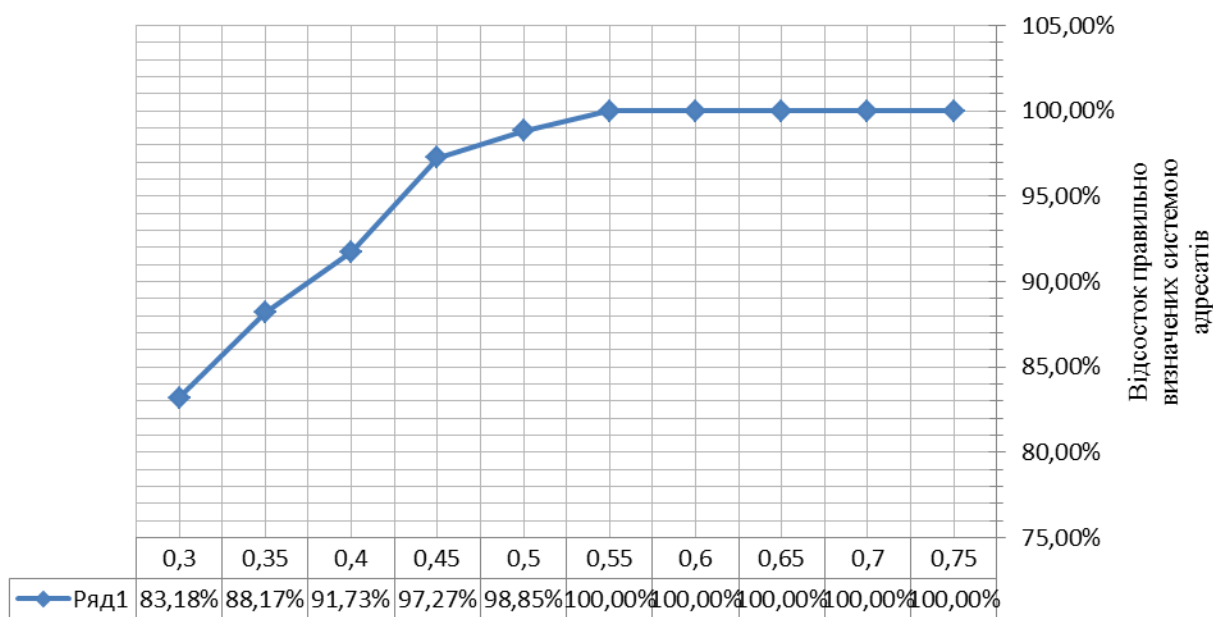


Рис. Д.2 Графік залежності відсотку правильно визначених системою адресатів від рівня прийняття проаналізованих понять.

Залежність кількості всього проаналізованих понять від рівня їх прийняття системою

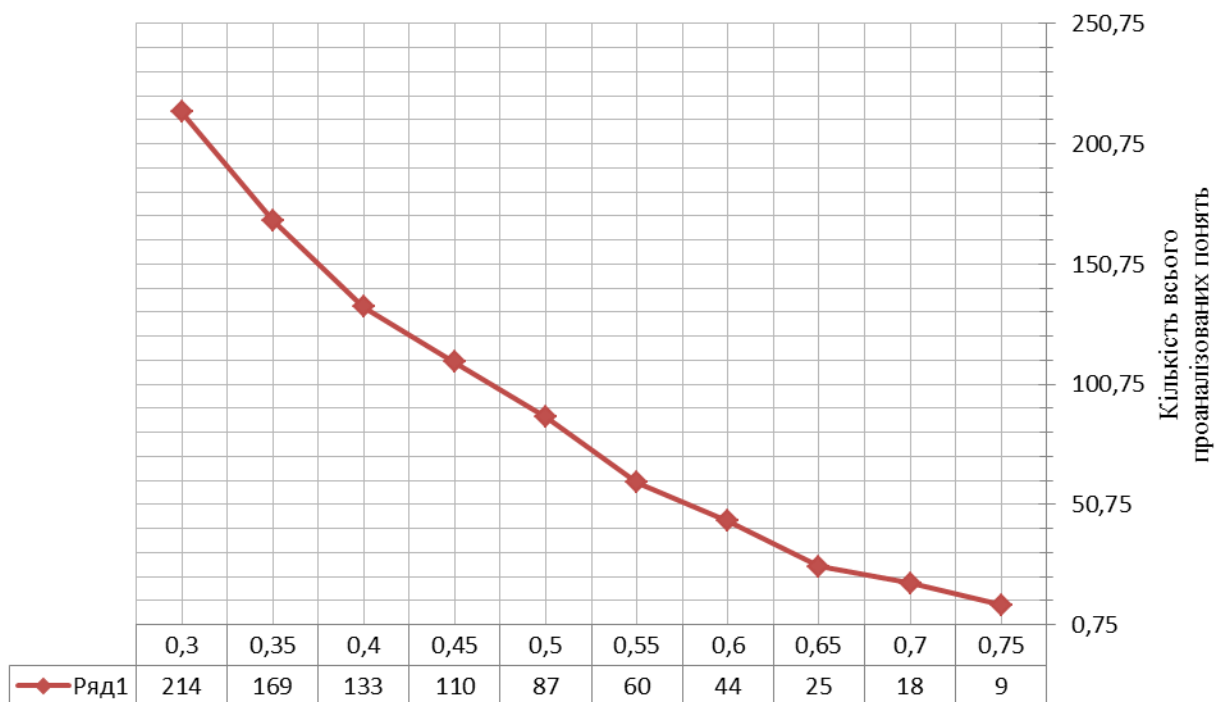


Рис. Д.3 Графік залежності кількості всього проаналізованих понять від рівня їх прийняття системою.

Діаграма правильності розподілу повідомлень

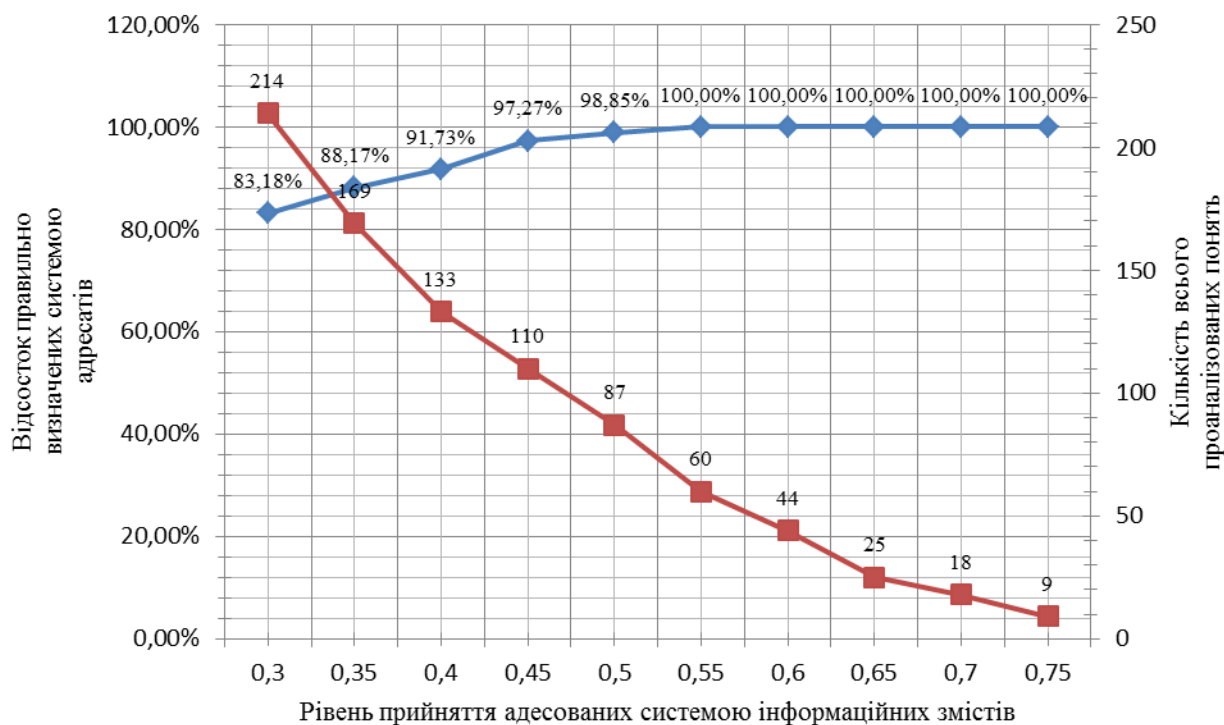


Рис. Д.4 Діаграма правильності розподілу повідомлень.

Залежність відсотку реферування системою TextAnalyst від кількості всього проаналізованих нею речень

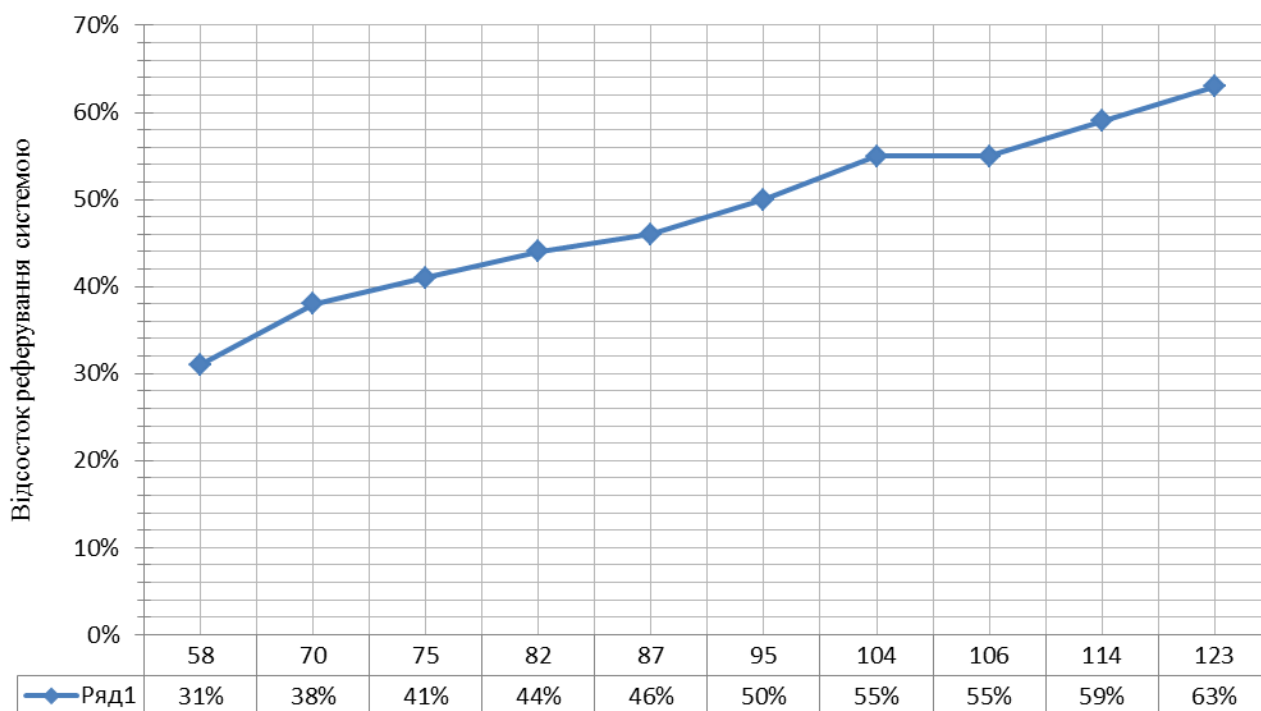


Рис. Д.5 Графік залежності відсотку реферування системою TextAnalyst від кількості всього проаналізованих нею речень

Залежність кількості всього проаналізованих речень системою TextAnalyst від рівня їх ваги

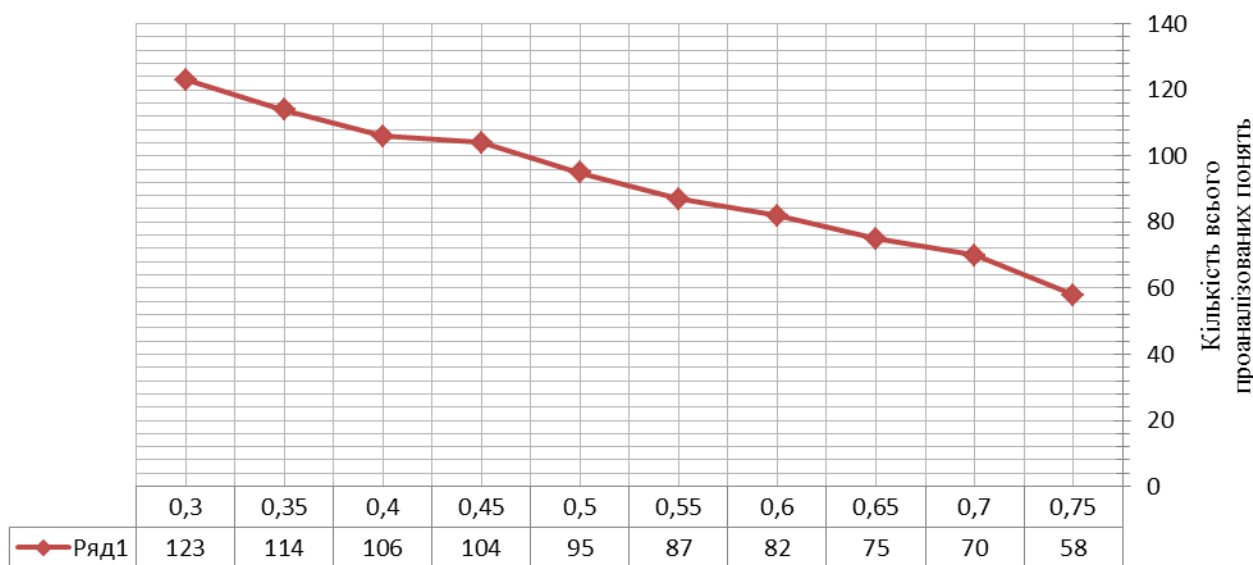


Рис. Д.6 Графік залежності кількості всього проаналізованих речень системою TextAnalyst від рівня їх ваги

Залежність відсотку реферування системою TextAnalyst від рівня рівня ваги речень

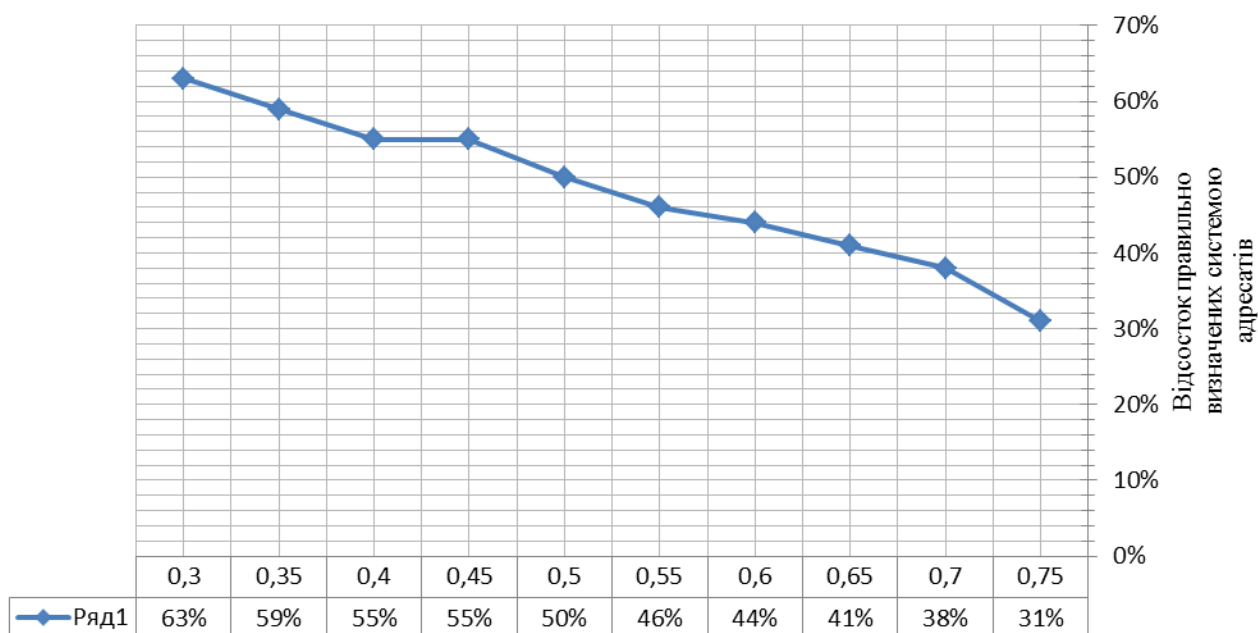


Рис. Д.7 Графік залежності відсотку реферування системою TextAnalyst від рівня ваги речень

Діаграма аналізу тексту системою TextAnalyst

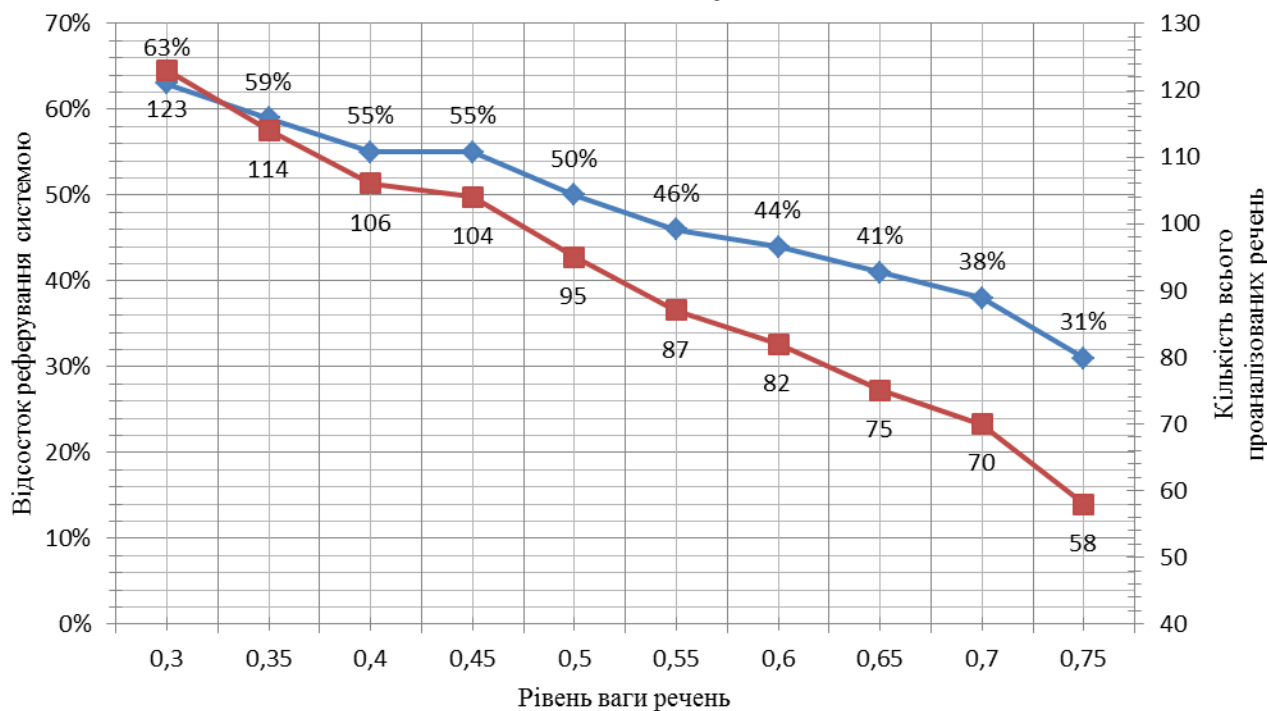


Рис. Д.8 Діаграма реферування тексту системою TextAnalyst

ДОДАТОК Е –
СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ ТА
ВІДОМОСТІ ПРО АПРОБАЦІЮ РЕЗУЛЬТАТІВ ДИСЕРТАЦІЇ

Список публікацій здобувача в яких опубліковані основні наукові результати дисертації:

27. Кубявка М. Б., Кубявка Л. Б. Модель інформаційної дії на контрагентів впливу. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2016. № 3(27). С. 54–58.

28. Кубявка М. Б. Математична модель несилої взаємодії в інформаційній технології інформаційного супроводження. *Information Technology and Security*. 2016. Vol. 4, No. 2 (7). P. 206–212.

29. Кубявка М. Б. Управління інформаційними впливами на противника з врахуванням поточної ситуації. *Збірник наук. праць Військового інституту Київського націон. ун-ту ім. Шевченка*. 2016. №53. С. 99–104.

30. Кубявка М. Б. Інформаційні дії по формуванню необхідної інформованості контрагента впливу. *Телекомунікаційні та інформаційні технології*. 2016. №4. С. 24–28.

31. Кубявка М. Б., Тесля Ю. М., Кубявка Л. Б. Визначення міри впливу на противника в інформаційній технології супроводження процесів підготовки та проведення військових операцій. *Збірник наук. праць Військового інституту Київського націон. ун-ту ім. Шевченка*. 2017. №55. С. 135–144.

32. Кубявка М.Б., Тесля Ю. М., Кубявка Л. Б. Інформаційна технологія управління інформаційним супроводженням. *Науково-технічний збірник “Управління розвитком складних систем” Київського національного університету будівництва і архітектури*. 2017. №29. С. 95–102.

33. Кубявка М.Б., Тесля Ю.М., Кубявка Л. Б. Рефлекторний метод управління інформаційним супроводженням військ (сил). *Збірник наукових праць Харківського національного університету Повітряних Сил*. 2017. №1(50). С. 48–53.

Список публікацій здобувача, які засвідчують апробацію матеріалів дисертації:

34. Кубявка Л. Б., Кубявка М. Б. Протидія впливам в програмах інформатизації вищих навчальних закладів. *Сучасні інформаційні технології в економіці та управлінні підприємствами, програмами, проектами*: матеріали XII Міжнарод. наук.-практ. конф. (м. Харків, 08–12 вересня 2014 р.). Харків, 2014. С.56–58.

35. Кубявка М. Б., Тесля Ю. М. Теорія несилової взаємодії як метод забезпечення інформаційної безпеки військ та держави в цілому. *Information Technologies & Interactions*: матеріали II Міжнарод. конф. (м. Київ, 3-5 листопада 2015 р.). Київ, 2015. С. 229–231.

36. Кубявка М. Б., Тесля Ю. М. Інформаційні технології на захисті інформаційного простору нашої держави. *Молодіжна військова наука у Київському національному університеті імені Тараса Шевченка*: матеріали Всеукр. наук.-практ. конф. молодих вчених, ад'юнктів, слухачів, курсантів і студентів. (м. Київ, 26 квітня 2016 р.). Київ, 2016. С. 64–65.

37. Кубявка М. Б., Кубявка Л. Б. Теорія несилової взаємодії - фундамент для побудови інформаційної технології супроводження процесів впливу на противника. *Інформаційні технології в освіті, науці і техніці*: матеріали III Міжнарод. наук.-практ. конф. (м. Черкаси, 12-14 травня 2016 р.). Черкаси, 2016. С. 63–64.

38. Кубявка М. Б., Тесля Ю. М., Кубявка Л. Б. Information management technology by non-forceful influence on the enemy during the preparation and conduction of military actions. *The 1th IEEE International Conference on Data Stream Mining & Processing*. (м. Львів, 23-27 серпня 2016 р.). Львів, 2016. С. 85–89.

39. Кубявка М. Б., Кубявка Л. Б. Інформаційна технологія формування необхідної інформованості у контрагентів взаємодії. *Спільні дії військових формувань і правоохоронних органів держави: проблеми та перспективи*:

матеріали III Всеукр. наук.-практ. конф. (м. Одеса, 22-23 вересня 2016 р.). Одеса, 2016. С. 151–152.

40. Кубявка М. Б. Поточна ситуація в управлінні інформаційними впливами. *Information Technologies & Interactions*: матеріали III Міжнарод. наук.-практ. конф. (м. Київ, 8-10 листопада 2016 р.). Київ, 2016. С. 85–89.

41. Кубявка М. Б., Кубявка Л. Б. Концептуальна модель визначення необхідних інформаційних впливів на противника. *Національна безпека України: актуальні проблеми та шляхи їх вирішення*: матеріали II Всеукр. курсантсько-студентської наук.-практ. конф. (м. Одеса, 24 листопада 2016 р.). Одеса, 2016. С. 148–150.

42. Кубявка М. Б., Тесля Ю. М. Формування необхідної інформованості контрагента впливу. *Військова освіта і наука: сьогодні та майбутнє*: матеріали XII Міжнарод. наук.-практ. конф. (м. Київ, 25 листопада 2016 р.). Київ, 2016. С. 57.

43. Кубявка М. Б., Кубявка Л. Б. Метод автоматичного визначення адресата повідомлення на основі використання ймовірно-рефлекторного підходу. *Прикладні науково-технічні дослідження*: матеріали I Міжнарод. інтернет-конф., АТН України. (м. Івано-Франківськ, 5 квітня 2017 р.). Івано-Франківськ, 2017. С. 20–21.

44. Кубявка М. Б., Тесля Ю. М., Кубявка Л. Б. Модель визначення найбільш інформативних компонентів природно-мовного тексту з позиції автоматичної адресації цих повідомлень різним класам контрагентів. *Інформаційна безпека та комп'ютерні технології*: матеріали II Міжнарод. наук.-практ. конф. (м. Кропивницький, 20-22 квітня 2017 р.). Кропивницький, 2017. С. 192–193.

45. Кубявка М. Б., Кубявка Л. Б. Рефлекторний метод автоматичного реагування на зміст повідомлення. *Молодіжна військова наука у Київському націон. унів-ті ім. Тараса Шевченка*: Всеукр. наук.-практ. конф. молодих вчених, ад'юнктів, слухачів, курсантів і студентів. (м. Київ, 28 квітня 2017 р.). Київ, 2017. С. 91–92.

Список публікацій здобувача, які додатково відображають наукові результати дисертації:

46. Kubiavka N. B. The control of information support of the processes of influence on the opponent. *Збірник наук. праць Військового інституту Київського націон. ун-ту ім. Шевченка*. 2016. №54. С. 171–178.

47. Кубявка М. Б., Тесля Ю. М., Кубявка Л. Б. Основи інформаційних технологій супроводження процесів впливу на контрагентів взаємодії. *Збірник наук. праць Військового інституту Київського націон. ун-ту ім. Шевченка*. 2016. №52. С. 123–128.

48. Кубявка М. Б., Кубявка Л. Б. Концептуальна модель визначення необхідних інформаційних впливів на противника. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2016. №2(26). С. 44–47.

49. Тесля Ю. М., Кубявка М. Б., Кубявка Л. Б. Можливості застосування теорії несилового впливу в військовій контррозвідці. *Scientific Journal “ScienceRise”*. 2015. №2/1(7). С. 18–22.

50. Кубявка М. Б., Кубявка Л. Б., Миколенко А. О. Інформаційні технології - як засіб несилового впливу під час підготовки та проведення бойових дій. *International Journal “Information Technologies & Knowledge”*. 2014. Vol. 8. No. 4. p. 380–382.

51. Kubiavka L. B., Kolomiets A. S, Kubiavka N. B. Applying the theory of non-forceful cooperation in influence management, on project human resources. *Nauka i Studia*. 2016. No. 20(151). p. 94–99.

52. Тесля Ю. М., Кубявка М. Б., Кубявка Л. Б., Миколенко А. О. Використання технологій інформаційного впливу під час підготовки та проведення бойових дій. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2014. №2 (20). С. 147-152.