МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

Прим. № ___

Кваліфікаційна наукова
праця на правах рукопису

БЕЛІКОВА ТЕТЯНА ВЯЧЕСЛАВІВНА

УДК 621.327: 681.5

ДИСЕРТАЦІЯ

МЕТОДИ ВИЯВЛЕННЯ ДЕСТРУКТИВНОГО ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ВПЛИВУ ДЛЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПІДЛІТКІВ

05.13.06 – інформаційні технології
технічні науки

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
Т.В. БЕЛІКОВА

Науковий керівник
Бараннік Володимир Вікторович,
доктор технічних наук, професор

Черкаси – 2019 рік

АНОТАЦІЯ

Белікова Т.В. Методи виявлення деструктивного інформаційно-психологічного впливу для інформаційних технологій забезпечення безпеки підлітків. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.06 – Інформаційні технології. – Черкаський державний технологічний університет, Черкаси, 2019.

У дисертаційній роботі вирішено науково-прикладне завдання, яке полягає в підвищенні інформаційної безпеки підлітків відносно деструктивних інформаційно-психологічних дій в інфокомунікаційному просторі.

Обґрунтовується, що ключовий ефект в забезпеченні інформаційної переваги і переваги в гібридної війні досягається в разі проведення деструктивних інформаційно-психологічних атак на підліткове покоління. При цьому для них найбільш популярними, затребуваними і системами, що довіряють каналами комунікацій є Інтернет ресурси та в тому чисел, ті які мають законодавче обмеження.

В результаті проведеного аналізу загроз інформаційно-психологічної безпеки підлітків в інфокомунікаційному просторі виявлено концептуальне протиріччя. З одного боку інтеграція України в світовий інформаційний та соціо-технічний простір, розвиток аспектів інформатизації держави, розвиток і взаємна інтеграція різних технологій, а саме інформаційних, комп'ютерних і телекомунікаційних призводять до того, що підвищується рівень інформованості підлітків, підвищується довіра з боку підлітків до таких комунікаційних каналів отримання інформації як Інтернет ресурси. З іншого боку інтеграція України в світовий інформаційний та соціо-технічний простір, розвиток аспектів інформатизації держави призводять до того, що: створюється потенціал для більш швидкого і ефективного проникнення деструктивного інформаційного контенту в інфокомунікаційних простір; створюється потенціал для збільшення охоплення аудиторії підлітків для проведення деструктивного інформаційно-психологічного впливу.

Тоді в умовах наявності безлічі дестабілізуючих внутрішньодержавних

чинників, недостатньої контрольованості такого простору як Інтернет і двох дисбалансів, а саме: на рівні інформаційної культури підлітка; на рівні використання джерел комунікаційних каналів виникають суттєві втрати інформаційно-психологічної безпеки підлітків.

Обґрунтовано і розроблено концептуальну структура інформаційної технології забезпечення інформаційно-психологічної безпеки підлітків щодо впливу інформаційних деструктивних трансформацій на їх підсвідомість і свідомість. На основі системного аналізу базових складових інформаційної технології забезпечення інформаційної безпеки підлітків обґрунтовується, що одним з ключових її технологічних етапів є складова, яка будується з використанням методів виявлення (детектування) наявності інформаційно-психологічних деструкцій в інформаційних ресурсах.

Розробляється система показників якості методів виявлення і детектування інформаційних деструктивних модифікацій в інформаційних ресурсах. Показано що сфера розробки таких технологічних рішень знаходяться в критичному стані. Відповідні технології мають недостатній рівень розвитку, щоб бути адекватними існуючим інформаційно-технологічними можливостями протиборчої сторони щодо організації і проведення деструктивного ІП впливу.

Викладається розробка моделі загроз ІП безпеки особистості в умовах інформаційного протиборства і демократизації соціуму. Обґрунтовується, що найбільш актуальними і значущими загрозами ІП безпеки особистості є сугестивні деструктивні ІП впливи на базі деструктивних інформаційних модифікацій в аудіоконтейнерах і електронних текстових ресурсах.

Обґрунтовано, що інформаційні технології, які відносяться до першого і другого класів представлені дуже широко, однак, не враховують сугестивну складову ІП впливу. Показано, що інформаційні технології, які дозволяють проведення більш глибинного аналізу інформаційних ресурсів, а саме враховують можливість виявлення сугестивного впливу на підсвідомість, характеризуються тим, що мають обмежену можливість щодо використання та проведення досліджень. Доводиться, що відсутність вітчизняних розробок в області інформаційних техноло-

гій забезпечення протидії сугестивним деструктивним ІП атакам на підсвідомість особистості створює критичний рівень загроз порушення національної безпеки держави.

Отже пропонується удосконалити інформаційну технологію забезпечення протидії загрозам інформаційно-психологічної (ІП) безпеки підлітків. З урахуванням чого, ***мета досліджень*** полягає в розробці методів виявлення деструктивної інформаційно-психологічної дії в інфокомунікаційному просторі для інформаційних технологій забезпечення безпеки підлітків.

Стверджується, що існує необхідність в розробці комплексних методів виявлення сугестивних деструктивних ІП впливів на підсвідомість особистості в електронних текстових ресурсах з врахуванням сучасних технологічних аспектів створення інформаційних деструкцій протиборчою стороною. Викладається побудова інформаційної моделі аналізу ТІР на основі формування семантичного диференціала. На основі розробляється метод виділення значущих лінгвістичних біполярних ознак.

1. Розроблено модель загроз ІП безпеки особистості в умовах інформаційного протиборства і демократизації соціуму, коли потрібно забезпечити баланс безпеки особистості одночасно в інформаційно-психологічному та інформаційно-технічному просторах (умова мережецентричності безпеки підлітка в інформаційному просторі). Обґрунтовано, що найбільш актуальними і значущими загрозами ІП безпеки особистості з позиції: виявлення та організації протидії; нанесення шкоди є сугестивны деструктивні ІП впливи. Показано, що одними з ключових ІП атак, які здійснюються в сучасному інформаційно-комунікаційному просторі, є деструктивні інформаційні модифікації в аудіоконтейнерах і електронних текстових ресурсах, а саме: аудіосуггестія, приховані вставки в аудіопотоки; сугестія текстів.

2. Побудовано інформаційна модель аналізу ТІР на основі формування семантичного диференціала. На основі чого було розроблений метод виділення значущих лінгвістичних біполярних ознак на основі представлення фонетичних оцінок звуко-букв алфавіту в речовому нерівноважному позиційному просторі. Ос-

новна відмінність тут полягає в тому, що векторний фонетичний простір лінгвістичної біполярної ознаки по всіх звуко-буквам представляється в раціональному нерівноважному позиційному базисі.

3. Розроблено метод ідентифікації інформаційно-психологічного впливу структурних компонент (слів) текстових інформаційних ресурсів на підсвідомість особи на основі формування векторного семантичного диференціалу. Метод базується на визначенні векторного семантичного диференціалу на основі індентіфікациі інтегрованих фонетичних оцінок по всіх біполярних градаційних шкалах значущих лінгвістичних ознак з врахуванням детектування двунаправленності ІП атак (конструктивні та деструктивні) в двовимірному нерівноважному просторі.

4. Створено комплексний метод виявлення прихованого інформаційно-психологічного впливу в текстовому інформаційному ресурсі на підсвідомість особи в багатовимірному фонетичному просторі з прив'язкою до векторних градаційних двополюсних шкал значущих біполярних лінгвістичних ознак на основі формування семантичного диференціалу слів і обробкою їх за динамічною технологією з накопиченням фрагментарної інформації.

Наукова новизна отриманих результатів.

У рамках дисертаційної роботи отримані основні результати, що мають наукову новизну:

1. Вперше розроблена модель інформаційно-психологічної безпеки особистості на основі мережецентричного підходу.

2. Вдосконалена модель побудови одновимірного семантичного диференціалу для оцінки рівня і напрямку ІП впливу структурних компонент ТІР на основі формування фонетичних оцінок звуко-букв.

3. Вперше розроблено метод ідентифікації ІП впливів структурних компонент ТІР на підсвідомість особи на основі формування векторного семантичного диференціала.

4. Удосконалено інформаційну технологію забезпечення ІП безпеки підлітків на основі виявлення сугестивних інформаційних деструкцій в ТІР.

Новизна отриманих результатів підтверджується відсутністю розроблених моделей і методів в існуючих інформаційних технологіях забезпечення ІП безпеки підлітків.

Практичне значення отриманих результатів.

Інтеграція програмних реалізацій розроблених методів виявлення сугестивних інформаційних деструкцій текстових ресурсів в інформаційну технологію забезпечення ІП безпеки підлітків забезпечує:

1) визначення спрямованості текстового інформаційного ресурсу здійснюється в статичному та динамічному режимах, що дозволяє виявити сугестивний ІП вплив у разі додаткового його маскувння з боку протиборчої сторони в послідовності фрагментів ТІР та врахувати особливості сприйняття інформації підлітками;

2) приріст ефективності виявлення сугестивних інформаційно-психологічних впливів в текстових інформаційних ресурсах на підсвідомість особистості у середньому до 16 % в порівнянні з експертами (підготовленими фахівцями) та у середньому до 59 % в порівнянні з тими, на кого здійснюється такий вплив (підлітками);

3) ефективність виявлення сугестивних ІП впливів на підсвідомість людини в ТІР складає від 98 до 100 %, що на 10 - 17 % більше в прівнянні з відомими методами аналізу на основі ключої інформації, які оцінюють наявність сугестивного ІП впливу на підсвідомість з урахуванням семантичної складової текстів.

Ключові слова: інформаційна безпека, інформаційно-психологічний вплив, сугестивні інформаційні деструкції, інформаційні технології забезпечення безпеки, семантичний діференціал, текстові ресурси.

Список публікацій, в яких опубліковані основні наукові результати дисертації:

1. Беликова Т.В., Баранник В.В. Методы выявления суггестивных воздействий на подсознание человека в текстовых сообщениях в условиях информационно-психологического противоборства. Наукоемкие технологии в инфокоммуникациях: обработка информации, кибербезопасность, информационная борьба:

коллективная монография / под редакцией В.М.Безрука. – Х.: ТОВ Вид. «Лідер», 2017. – С. 435 – 455.

2. Сапрыкина Т.В., Сидченко С.А., Школяренко В.А. Информационная технология тестирования семантической составляющей для выявления суггестивного воздействия методом фонетического анализа накопительным итогом. *Автоматизированные системы управления и приборы автоматики*. 2013. № 165. С. 111 – 117.

3. Saprykina T.V., Sidchenko S.A. Method of complex information and psychological document analysis. *Science-Based Technologies*. 2014. № 1(21). P. 79 – 83.

4. Сапрыкина Т.В., Сидченко С.А., Школяренко В.А. Метод составления текста с заданной суггестивной направленностью контекста. *Системи обробки інформації*. Х.: ХУПС. 2014. № 4(120). С. 96 – 101.

5. Беликова Т.В. Методы выявления деструктивных суггестивных информационно-психологических операций в информационно-социальном пространстве. *Радиоэлектроника и информатика*. 2017. №2. С. 45 – 50.

6. Belikova T.V. The Technology Of Suggestive Information-Psychological Operations Masking In The Infocommunication Space. *Science-Based Technologies*. 2017. № 3. P. 21 – 26.

7. Алімпієв А.М., Бараннік В.В., Белікова Т.В., Сідченко С.О. Теоретичні основи створення технологій протидії прихованим інформаційним атакам в сучасній гібридній війні. *Системи обробки інформації*. Харьков: ХНУПС. 2017. № 4(150). С. 113 – 121.

8. Баранник В.В., Беликова Т.В., Довбенко О.В. Методи виявлення прихованих ої інформаційно-психологічних дій в інформаційному просторі. *Наукоємні технології*. 2018. №3. С. 24 – 30.

9. Бараннік В.В., Белікова Т.В., Капко М.О., Гуржій І.А. Комплексний метод автоматичного фоносемантичного аналізу текстової інформації на основі оцінки вагомих семантичних одиниць в умовах інформаційного протиборства. *Кібербезпека. освіта, наука, техніка*. 2019. №1(1). С. 13 – 22.

Список публікацій, які засвідчують апробацію матеріалів дисертації:

1. Сапрыкина Т.В., Школяренко В.А. Информационная технология выявления суггестивных воздействий на подсознание человека. *Інформаційні технології: наука, техніка, технологія, освіта, здоров'я* (МикроКАД): матеріали XXII Міжн. наук.-практ. конф., тези доп., (Харків, 21-23 травня 2014 р.). Харків, НТУ «ХПІ»., 2014. С. 71.

2. Saprykina T., Komolov Dm., Vlasov A., Sidchenko S. Assessment of Video Information Resource Security of Videoconferencing in Public Administration. *International Symposium «IEEE East-West Design & Test»*, (Kiev, Ukraine, September 26–29, 2014). Kiev: 2014. P. 329 – 331.

3. Баранник В.В., Сидченко С.А., Сапрыкина Т.В. Методология построения стойких к несанкционированной дешифровки изображений на базе систем компактного представления. *Проблеми інформатики та моделювання*: матеріали 15 Міжн. наук.-практ. конф. (Харків - Одеса, 14 - 18 вересня 2015 р.). Харків-Одеса, НТУ «ХПІ», 2015. С. 56.

4. Бараннік В.В., Белікова Т.В., Тупиця І.М. Кластеризація даних вхідного сигналу для підвищення захисту інформаційного ресурсу. *Захист інформації і безпека інформаційних систем*: матеріали V Міжн. наук.-практ. конф., (Львів, 2 - 03 червня 2016 р.). Львів: нац. ун-т "Львівська політехніка", 2016. С. 23 – 25.

5. Barannik V., Belikova T, Komolov D., Krivonos V., Tarnopolov R. Estimate of the capacity of the closed video channel for the method based on the selection of relevant structural units. *International Symposium «IEEE East-West Design & Test*», (Batumi, 2016). Batumi: 2016. P. 325 – 328.

6. Бєлікова Т.В., Баранник В.В. Методика автоматичного підвищення суггестивної спрямованості семантичної складової тексту. *Фізико-технологічні проблеми передавання, оброблення та зберігання інформації в інфокомунікаційних системах*: матеріали V Міжн. наук.-практ. конф., (Чернівці, 3-5 листопада 2016 р.). Чернівці: Чернівецький нац. ун-т імені Юрія Федьковича, 2016. С. 45 – 48.

7. Belikova T., Barannik V., Karpinskyi V. Development of technology analys for the content semantics, *Engineer of XXI Century - We Design the Future*, Bielsko-Biała, Poland: ATH, 2016. P.65 – 72.

8. Barannik V., Belikova T., Podlesny S., Suprun O. The Alignment Method of Code Structures for Enhancing the Information's Reliability in the Infocommunication Networks. *The Experience of Designing and Application of CAD Systems in Microelectronics CADSM'2017*: The 14th International Conference, (Polyana-Svalyava (Zakarpattya), Ukraine, 21-25 February 2017). 2017. P. 29 – 31.

9. Баранник В.В., Беликова Т.В Метод анализа информационных ресурсов с выевлением семантики контента. *Актуальні питання забезпечення кібернетичної безпеки та захисту інформації*: матеріали III Міжн. наук.-практ. конф., (Закарпатська область Міжгірський район село Верхнє Студене, 22-25 лютого 2017 р.). Навчально-науковий інститут права та безпеки підприємництва Європейського університету, 2017. С. 28 – 31.

10. Беликова Т.В. Методы противодействия скрытной информационно-психологическим атакам на социум в инфокомуникационном пространстве. *Обробка сигналів і негаусівських процесів», присвяченій пам'яті професора Кунченка Ю.П.*: матеріали VI Міжн. наук.-практ. конф., (Черкаси, 24 - 26 травня 2017 р.). Черкаси: ЧДТУ, 2017. С. 23 – 24.

11. Баранник В.В., Беликова Т.В., Подлесный С.А., Хаханова А.В. Способ повышения целостности и доступности видеоконтента в условиях проведения кибернетических атак. *ABIA-2017*: матеріали XIII Міжн. наук.-техн. конф., (Київ, 19 - 21 квітня, 2017 р). Київ: НАУ, 2017. С. 40 – 43.

12. Баранник В. В., Белікова Т. В., Довбенко О. В., Сідченко С. О. Виявлення прихованих інформаційних впливів в інформаційно-комунікаційному просторі. *Проблеми кібербезпеки інформаційно-комунікаційних систем (PCSITS)*: матеріали I наук.-практ. конф., (Київ 5–6 квітня. 2018 р.). Київ: нац. ун-т імені Тараса Шевченка, 2018. С. 223 - 226.

13. Бараннік В.В., Белікова Т.В., Довбенко О.В. Методи виявлення прихованих інформаційно-психологічних дій в інформаційному просторі. *Перспективні*

напрямки захисту інформації: матеріали IV Наук. практ. конф., (Одеса, 2 - 6 вересня 2018 р.). Одесса: ОНАЗ, 2018. С. 10 - 11.

14. Бараннік В.В., Белікова Т.В., Довбенко О.В., Сідченко С.О., Слободянюк О.В. Методика автоматизованого виявлення прихованих інформаційно-психологічних впливів. *Фізико-технологічні проблеми передавання, оброблення та зберігання інформації в інфокомунікаційних системах*: матеріали VII Міжн. наук.-практ. конф., (Чернівці, 8 - 10 листопада 2018 р.). Чернівці: Чернівецький нац. ун-т імені Юрія Федьковича, 2018. С. 20 – 21.

15. Belikova T., Dovbenko O., Lekakh A., Dodukh O. Method of Increasing the Capacity of Information Threat Detection Filters in Modern Information and Communication Systems. *on Advanced Information and Communication Technologies, AICT 2019*: 3nd IEEE International Conference, Proceedings, (Lviv, July 2019). Lviv, 2019. P. 188 - 192.

ABSTRACT

Belikova T.V. Methods of detecting destructive information and psychological impact of information technology security of teenagers. - Qualification scientific work as the manuscript.

The Thesis for PhD of Engineering Sciences degree in the specialty 05.13.06 "Information technologies". - Cherkasy state technological university, Cherkasy, 2019.

The dissertation deals with the applied scientific problem, which is to increase the information security of adolescents regarding destructive information and psychological actions in the infocommunication space.

Substantiated that a key effect in providing information superiority and advantages in hybrid warfare is achieved in case of destructive information and psychological attacks on teenager generation. At the same time for them the most popular, in demand, trusted systems communication channels are Internet resources including those that have the legal limitation.

As a result of analysis of threats information and psychological safety of teenagers in infocommunication space the conceptual contradiction is revealed. On the one hand, Ukraine's integration into the global information and socio-technical space, development aspects of informatization, development and mutual integration of various technologies, namely information, computer and telecommunications lead to an increase in the level of awareness teenagers, raising trust from teenagers to such communication channels as the information about Internet resources. On the other hand, Ukraine's integration into the global information and socio-technical space, The development of aspects of informatization of Ukaraine leads to creating capacity for faster and more efficient penetration of destructive information content in infocomm space; creating the potential for increasing coverage of the adolescent audience for the course of the destructive information and psychological influence.

Then, in the presence of many rank-destabilizing domestic workers, insufficient control such space as the internet and two imbalances: At the level of informational culture of a teenager; At the level of the use of sources of communication channels, arise significant losses of information and psychological security.

Proved and developed conceptual structure of information technology providing information and psychological safety of teenagers about the impact of informational destructive transformations in their subconscious and consciousness. Based on system analysis of the basic components of information technology of information security of teenagers substantiated, that one of its key technological stages is the component, which is constructed with use of methods of detection of information and psychological destrucations in information resources.

Developed a system of quality indicators and detection methods for detecting information of destructive modifications to information resources. It is shown that the area of the development of such technological solutions is in a critical condition. Appropriate technologies have an insufficient level of development to be adequate to the existing information and technological capabilities of the opposing side – to the organization and conduct of the destructive IP of influence.

It outlines the development of the threat model of the individual's security in the context of informatational confrontation and democratization of society. The of substantiated that the most relevant and significant threats IP security personality are suggestive destructive IP impacts on the basis of destructive informational modifications in audio containers and electronic text resources.

Proved that information technology relating to the first and second grade are very widely, however, do not include suggestive component of IP impact. It is shown that information technologies that allow carrying out of more depth-analysis of information resources, namely taking into account the possibility of revealing of the subgestal influence on subconscious, characterized by having limited possibility to use and conduct of research. It is proved that the lack of domestic developments in information technologies provide suggestive destructive IP attack on the personality subconscious generates critical level of threats of violation of national security.

Thus, it is proposed to improve information technology for countering threats of information and psychological (IP) security of teenagers. Taking into account what, r***esearch purpose*** consists in developing methods for detecting destructive information and psychological actions in infocommunicational space for information technology to provide safety of teenagers.

It is alleged that there is a need to develop complex methods Detection of suggestive destructive IP attacs on subconscious of personality in electronic text resources taking into account modern technological aspects of creating information destructions opposing side. The building of information model of analysis TIR based on the formation of the semantic differential. Based on the selection method developed significant linguistic bipolar features.

1. Developed a model of threats IP security of the person in the context of information confrontation and democratization of society, when it needs to ensure the balance of personal security at the same time in the information-psychological and information-technical spaces (condition of the network-centric safety of a teenager in the information space). Proved that the most relevant and significant threats to IP security from the position: detection and organization of counteraction; inflicting damage and

suggestive destructive IP attack. It is shown that some of the key IP attacks carried out in the modern information and communication space are destructive information modifications in audio containers and electronic resources, namely audiosuggestation, hidden insertion into audio streams; suggestion texts.

2. Built TIR information analysis model based on the formation of semantic differential. Based on what is the method of allocation of meaningful linguistic bipolar features on the basis of representation of phonetic estimates of the alphabet's sound-letters in the real nonequilibrium positional space is developed. The main difference here is that vector phonetic space of the linguistic bipolar characteristic of all sound-letters is presented in a rational nonequilibrium positional basis.

3. A method of identification of the information-psychological influence of the structural component (words) of textual information resources on the subconscious of a person on the basis of a vector semantic differential is developed. The method is based on the definition of a vector semantic differential based on the indentification of integrated phonetic estimates of all bipolar tonal scales of significant linguistic characteristics, taking into account the detection of bidirectional IP attacks (constructive and destructive) in two-dimensional nonequilibrium space.

4. A complex method of detecting hidden information and psychological impact of a text subliminal information resource person in a multidimensional phonetic space with reference to the vector gradational scales bipolar bipolar significant linguistic features based on the formation of words semantic differential and processing them in a dynamic technology with the accumulation of information fragments.

The scientific novelty of the results.

Within the thesis the main results with contains scientific novelty:

1. The first developed model for information-psychological safety of personality on the basis of network-centric approach.

2. Improved one-dimensional model for constructing semantic differential to assess the level and direction of PI influence of TIR structural component based on the formation of phonetic ratings of sound letters.

3. For the first time the method of identifying IP influences the structural component TIR subliminal person from forming vector semantic differential.

4. Improved the information technology of IP security of teenagers based on the identification of the sugestisive information destrucations in TIR.

Novelty of the obtained results is supported by the lack of developed models and methods in existing information technologies.

The practical significance of the results.

Integration of software implementations of the developed methods of identifying the suggestive information destructions of text resources into the informational technology of the security:

1) The orientation definition of text information resource is carried out in a static and dynamic modes, that allows to reveal the suggestive IP influence in case of additional masking from the opposite side in sequence fragments of TIR and to consider feature of perception of information by teenagers;

2) an increase the effectiveness of detecting suggestive information-psychological influences in textual information resources on the subconscious of the person by an average of 16% compared to experts (trained specialists) and an average of 59% compared to those who are exerted by such influence (teenagers);;

3) the effectiveness of detecting suggestive IPV on the human subconscious in TIR ranges from 98 to 100%, which is 10 - 17% higher compared to known methods of analysis based on key information that assess the presence of suggestive IP influence on the subconscious, taking into account the semantic component of texts.

Keywords: information security, information and psychological influence, suggestive information destruction, Information security technologies, semantic differential, text resources.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

АІР – аудіо інформаційний ресурс

АЯ – алгоритмічне ядро (модуль аналізу тексту)

БД – база даних

ІП – інформаційно-психологічний

ІР – інформаційний ресурс

ІТ – інформаційно-технічний

ЛБ – лінгвістичний біполярний

ЛП – лінгвістичний процесор (модуль перетворення тексту)

МДАНП – метод динамічного аналізу накопичувальним підсумком

ТБ – телебачення

ТІР – текстовий інформаційний ресурс

ВСТУП

Обґрунтування вибору теми дослідження. За сучасних умов інформаційна складова набуває дедалі більшої ваги і стає одним із найважливіших елементів забезпечення національної безпеки. Через це забезпечення інформаційної безпеки являє собою важливу сферу національної безпеки [2, 5-7, 22-27, 29-33, 36, 38-42, 45-52, 55-58, 61, 64-67, 74-76, 83, 92, 96, 97, 101, 103, 105, 106, 112-121, 124, 127, 129]. В загальному випадку інформаційна безпека розглядається в двох сегментах в залежності від об'єктів інтересу, а саме: об'єкти інформаційно-технічного простору; об'єкти інформаційно-психологічного (ІП) простору.

В умовах проведення гібридної та інформаційної війн з врахуванням наявності безлічі внутрідержавних дестабілізуючих чинників ключовий ефект в забезпеченні інформаційної переваги досягається у разі проведення інформаційно-психологічних атак. Це обумовлено наявністю дисбалансу між технологіями і засобами інформаційного протиборства в Україні. Наприклад, інформаційно-пропагандистська експансія в медіа-просторі, просування ідеології в інтересах інших держав призводять до нанесення: більшої втрати національної безпеки, чим безпосередній озброєний конфлікт; більш значущого збитку в порівнянні з кібератаками [24, 25, 34, 38, 42, 46, 48, 50, 51, 55, 61, 64-66, 74-76, 83, 88, 89, 96, 97, 101, 102, 103].

При цьому найуразливішими об'єктами деструктивної інформаційно-психологічної дії є підлітки. Це пояснюється тим, що:

1) з одного боку найбільшим ступенем сприйняття нової інформації і потреби в її отриманні, тобто високим рівнем потреби нових знань і мінімальний час засвоєння нової інформації. Виникають нові, не інституційні канали творчої і комунікативної самореалізації підлітків;

2) з іншого боку найменший ступінь: критичності сприйняття отримуваної інформації, тобто низький рівень критичного аналізу і оцінки інформації, яка надходить; стійкості морально-етичних і психологічних установок.

В теж час ефективність деструктивної інформаційної дії залежить від типу середовища комунікаційних каналів. У разі атак на підлітків і молодь найбільш ефективними каналами комунікаційної дії є Інтернет і телебачення до 48% від загальної маси. Відповідна затребуваність в цих джерелах інформації для підлітків і молоді досягає 70%, а відповідна ступінь довіри – до 60 %. Тут потрібно відзначити, що одними з популярних віртуальних соціальних мереж серед підлітків і молоді не дивлячись на законодавчі обмеження продовжують залишатися: "Вконтакте" (до 82% зареєстрованих); "Одноклассники" (до 62% зареєстрованих); "Мой мир" (до 41% зареєстрованих) [80-82, 84].

З врахуванням чого виникає ***концептуальна суперечність***. Інтеграція України у в світовий інформаційний та соціотехнічний простір, розвиток аспектів інформатизації держави, розвиток і взаємна інтеграція різних технологій, а саме інформаційних, комп'ютерних і телекомунікаційних приводять до того, що: з одного боку *підвищується рівень інформованості підлітків*; з іншого боку *формується множина загроз втрати інформаційно-психологічної безпеці підлітків*. Тоді в умовах наявності множини дестабілізуючих внутрідержавних чинників, недостатньої контрольованості Інтернет-простору і дисбалансів на рівні: інформаційної культури підлітка; на рівні використання джерел комунікаційних каналів - виникають істотні втрати інформаційно-психологічної безпеки підлітків.

Тому ***науково-прикладна задача***, яка полягає в підвищенні інформаційної безпеки підлітків відносно деструктивних інформаційно-психологічних дій в інфокомунікаційному просторі, є ***актуальною***.

Для вирішення сформульованої задачі *пропонується* удосконалити інформаційну технологію забезпечення протидії загрозам інформаційно-психологічної безпеки підлітків [37, 64, 65, 71, 72, 88, 89, 91]. Як показує аналіз базових складових таких інформаційних технологій одним з ключових її технологічних етапів є методи виявлення (детектування) наявності ІП деструкцій в інформаційних ресурсах (ІР). Саме недоліки в процесі виявлення інформаційно-психологічних деструкцій в інформаційних ресурсах неминуче спричиняє зниження ефективності всієї інформаційної технології забезпечення ІП безпеки підлітків.

Питанням розробки та розвитку технологій інформаційної боротьби займається багато вчених. Серед них Додонов О.Г., Ланде Д.В, Толубко В.Б., Горбулін В. П., Богданович В.Ю., Пєвцов Г.В., Почепцов Г.Г., Расторгуев С. П., Руснак І.С., Телелим В.М., Жук С.Я., Косевцов В.О., Юдін О.К. та інши. Серед закордонних дослідників: Дж. Бойд, Гриняев С.Н., Комов С.А., Манойло А.В. та інши.

Проте сфера розробки технологічних рішень в напрямку виявлення ІП впливів знаходяться в критичному стані. Відповідні технології мають недостатній рівень розвитку, щоб бути адекватними існуючим інформаційно-технологічним можливостям протиборчої сторони щодо організації і проведення деструктивної дії ІП. Методи пошуку, аналізу, складання та формування текстових інформаційних ресурсів представлені дуже широко. Але системи, що реалізують ці методи, не завжди придатні для ведення інформаційно-психологічного протиборства. Значним недоліком більшості таких технологій є те що вони є закордонними. При цьому використання закордонних інформаційних технологій протидії деструктивному ІП впливу є обмеженим у зв’язку з тим, що відсутній опис їх математичної бази та існує заборона урядів більшості держав на експорт даних продуктів в повному обсязі [2, 64, 65].

Отже ***тематика дисертаційних досліджень***, яка стосується розробки методів виявлення деструктивної інформаційно-психологічної дії в інфокомунікаційному просторі для інформаційних технологій забезпечення безпеки підлітків є ***актуальною.***

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційні дослідження проводилися відповідно до наступних програм і нормативних документів: Закону України “Про Концепцію Національної програми інформатизації” від 04.02.1998 р. № 75/98-ВР; Постанови Верховної Ради України “Концепція національної безпеки України ” від 16 січня 1997 № 3/97-ВР; Указу Президента України “Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 року “Про нову редакцію Воєнної доктрини України” від 24 вересня 2015 року № 555/2015; Указу Президента України “Про рішення Ради національної безпеки і оборони України “Про Стратегічний оборонний бюлетень України” від

20 травня 2016 року № 240/2016, положення “Стратегії розвитку інформаційного суспільства в Україні” (затверджено Кабінетом Міністрів України від 15 травня 2013 р.); планами наукової, науково-технічної діяльності Черкаського державного технологічного університету, Харківського національного університету Повітряних Сил імені Івана Кожедуба, у рамках яких була виконана НДР “Обґрунтування заходів щодо удосконалення навчального процесу та підвищення якості підготовки військових фахівців”, шифр “Фахівець-2012” (№ 0101U001347), в якій автор дисертації був виконавцем.

Мета і завдання досліджень. Мета дисертаційної роботи полягає в розробці методів виявлення деструктивної інформаційно-психологічної дії в інфокомунікаційному просторі для інформаційних технологій забезпечення безпеки підлітків.

Для досягнення сформульованої мети необхідно вирішити такі завдання:

1. Побудувати модель загроз ІП безпеки підлітків в інфокомунікаційному просторі та обґрунтувати напрямок виявлення прихованих деструктивних інформаційно-психологічних впливів в інформаційних ресурсах для підвищення ефективності інформаційних технологій забезпечення ІП безпеки.

2. Розробити методи виявлення сугестивних деструктивних інформаційно-психологічних атак на підсвідомість підлітків на основі семантичного диференціалу в інфокомунікаційному просторі.

3. Створити методи динамічного аналізу текстових інформаційних ресурсів в багатовимірному фонетичному просторі за лінгвістичними ознаками для виявлення сугестивних інформаційних деструкцій з маскуванням.

4. Розробити програмний продукт для методів виявлення сугестивних деструктивних інформаційно-психологічних впливів в текстових ресурсах та оцінити їх ефективність.

Об'єкт дослідження. Процеси підвищення ефективності інформаційних технологій забезпечення інформаційної безпеки підлітків відносно деструктивних інформаційно-психологічних атак.

Предмет дослідження. Методи виявлення деструктивних інформаційно-психологічних атак для забезпечення інформаційної безпеки підлітків в інфокомунікаційному просторі.

Методи дослідження. Обґрунтування напряму підвищення ефективності функціонування інформаційних технологій забезпечення безпеки підлітків ґрунтується на положеннях теорії інформаційного протиборства та складних систем. Визначення актуальності та значимості загроз ІП безпеки особистості базується на системному підході з використанням положень теорії інформаційної безпеки. Розробка методів виявлення сугестивних інформаційних деструкцій в ТІР проводилось зі застосуванням положень теорії інформації, кодування та інтелектуального аналізу даних. Оцінка адекватності теоретичних і практичних результатів проводилась на основі методів планування експериментів та математичної статистики.

Наукова новизна отриманих результатів досліджень полягає в наступному:

1. Вперше розроблена модель інформаційно-психологічної безпеки особистості на основі мережецентричного підходу. Відмінностями є те, що враховується: сугестивні деструктивні ІП впливи на підсвідомість; наявність дисбалансу з категоріями інформаційної безпеки в інформаційно-технічному просторі. Це дозволяє оцінити значимість і актуальність загроз ІП безпеки особистості в умовах інформаційного протиборства і демократизації соціуму.

2. Вдосконалена модель побудови одновимірного семантичного диференціалу для оцінки рівня і напрямку ІП впливу структурних компонент ТІР на основі формування фонетичних оцінок звуко-букв. Відмінність полягає у використанні для побудови фонетичного простору тільки значущих біполярних лінгвістичних (ЛБ) ознак. Це дозволяє в автоматизованому режимі провести оцінку значущості і наявності прихованих інформаційних деструкцій для структурних компонент ТІР з врахуванням їх залежності від ЛБ ознак.

3. Вперше розроблено метод ідентифікації ІП впливів структурних компонент ТІР на підсвідомість особи на основі формування векторного семантичного

диференціала. Основними відмітними особливостями методу є: визначення рівня та напрямку ІП впливу структурної компоненти ТІР на підсвідомість особи за всіма звуко-буквами в значущому ЛБ просторі, який представляється раціональним нерівноважним базисом; визначення векторного семантичного диференціалу на основі ідентифікації інтегрованих фонетичних оцінок за всіма біполярними градаційними шкалами значущих лінгвістичних ознак з врахуванням детектування двонаправленості ІП впливів в двовимірному раціональному нерівноважному просторі. Це створює умови для підвищення ефективності і автоматичного виявлення сугестивного деструктивного ІП впливу в структурних компонентах ТІР на підсвідомість особи в інфокомунікаційному просторі.

4. Удосконалено інформаційну технологію забезпечення ІП безпеки підлітків на основі виявлення сугестивних інформаційних деструкцій в ТІР. Базові відмінності від існуючих технологій полягають в тому, що: побудований комплексний метод виявлення прихованого ІП впливу в ТІР на підсвідомість особи в багатовимірному фонетичному просторі з прив'язкою до векторних градаційних шкал значущих лінгвістичних ознак на основі формування семантичного диференціалу слів і обробкою їх за динамічною технологією з накопиченням фрагментарної інформації. Це дозволяє підвищити ефективність функціонування інформаційних технологій забезпечення ІП безпеки підлітків в інфокомунікаційному просторі.

Новизна отриманих результатів підтверджується відсутністю розроблених моделей і методів в існуючих інформаційних технологіях забезпечення ІП безпеки підлітків.

Обґрунтованість і достовірність отриманих наукових результатів забезпечується наступним: адекватністю результатів отриманих на основі експертних оцінок та результатів застосування програмної реалізації методів виявлення сугестивних інформаційних деструкцій в ТІР довільного та заданого (еталонного) змісту; не суперечністю отриманих результатів положенням теорії інформації, методам забезпечення інформаційної безпеки.

Практичне значення отриманих результатів отриманих результатів полягає в тому, що інтеграція програмних реалізацій розроблених методів виявлення

сугестивних інформаційних деструкцій текстових ресурсів в інформаційну технологію забезпечення ІП безпеки підлітків забезпечує:

– автоматичне виявлення деструктивних та конструктивних сугестивних ІП впливів на підсвідомість особистості в текстових інформаційних ресурсах лише на основі фонетичної складової текстової інформації без врахування семантичної спрямованості повідомлень;

- визначення спрямованості текстового інформаційного ресурсу здійснюється в статичному та динамічному режимах, що дозволяє виявити сугестивний ІП вплив у разі додаткового його маскування з боку протиборчої сторони в послідовності фрагментів ТІР та врахувати особливості сприйняття інформації підлітками;

– виявлення та оцінку спрямованості сугестивних ІП впливів на підсвідомість особистості в ТІР в реальному часі. Процес виявлення швидше майже в 90 разів в порівнянні з експертами (підготовленими фахівцями).

– приріст ефективності виявлення сугестивних інформаційно-психологічних впливів в текстових інформаційних ресурсах на підсвідомість особистості у середньому до 16 % в порівнянні з експертами (підготовленими фахівцями) та у середньому до 59 % в порівнянні з тими, на кого здійснюється такий вплив (підлітками);

– ефективність виявлення сугестивних ІП впливів на підсвідомість людини в ТІР складає від 98 до 100 %, що на 10 - 17 % більше в порівнянні з відомими методами аналізу на основі ключової інформації, які оцінюють наявність сугестивного ІП впливу на підсвідомість з урахуванням семантичної складової текстів;

– в порівнянні з відомим на даний час програмними засобами (технологія “ВААЛ 2000”) виявлення сугестивних ІП впливів забезпечує істотне розширення функцій аналізу, обробки, редагування текстових документів, відображення інформації й інші функції. При цьому сам процес виявлення конструктивного або деструктивного впливу в розробленої в дисертаційній роботі технології здійснюється швидше за рахунок методу векторного семантичного диференціалу в значимому лінгвістичному біполярному просторі, представленому раціональним нерівноваговим базисом.

Створюється можливість для забезпечення комплексної ІП безпеки підлітків на рівнях: роботи експертів з оцінки та виявленню шкідливих ІП дій; моніторингу інфокомунікаційного простору для виявлення прихованих інформаційних деструкцій в інформаційних ресурсах.

Практична значущість отриманих результатів дисертації підтверджується їх застосуванням при виконанні дослідно-конструкторських робіт щодо розробки методики аналізу ризиків порушення інформаційної безпеки та моніторингу Інтернет ресурсів в управлінні зв'язку та телекомунікації Головного управління національної поліції в Харківській області (акт реалізації від 13.03.2018 р.); в навчальному процесі Харківського національного університету Повітряних Сил імені Івана Кожедуба (акт реалізації від 13.04.2018 р.), Національного університету цивільного захисту України (акт реалізації від 13.02.2018 р.).

Особистий вклад автора. Усі положення, які виносяться на захист, отримано автором особисто. У наукових працях, опублікованих у співавторстві, здобувачеві належить наступне: в працях [1, 18, 87] - викладаються основні етапи створення і будується план проведення експериментів для оцінки ефективності інформаційної технології забезпечення ІП безпеки підлітків в інфокомунікаційному просторі; в працях [15, 85, 110] - розробляється метод векторного семантичного диференціалу в багатовимірному фонетичному просторі по значущих лінгвістичних ознаках; в праці [125] - будується комплексний метод виявлення інформационих деструкцій в ТІР на основі динамічного аналізу в багатовимірному фонетичному просторі значущих лінгвістичних ознак з накопиченням фрагментарної інформації; в працях [14, 17, 86] - створюється метод і здійснюється оцінка ефективності динамічного аналізу ТІР на основі семантичного диференціалу з накопиченням фрагментарної інформації; в працях [8, 11] - висловлюється підхід для оцінки значущості лінгвістичних ознак в нерівноваговому позиційному просторі; в працях [9, 10, 111] - формується технологія ідентифікації рівня і напряму сугестивного ІП впливу на підсвідомість підлітка на основі використання двовимірного раціонального нерівноважного позиційного простору; в працях [12, 126] - пропонується модель оцінки ІП загроз безпеці особи; в працях [13, 107, 108] - прово-

диться оцінка впливу детектування інформаційних деструкцій на характеристики сервісів реального часу в інфокомунікаційних системах; в праці [16] - висловлюється методика проведення тестування груп підлітків для встановлення рівня і направленості сугестивних ІП впливів в ТІР.

Апробація результатів дисертації. Основні результати дисертації доповідались і були схвалені на: XXII Міжнародній науково-практичній конференції, ″Інформаційні технології: наука, техніка, технологія, освіта, здоров'я (МикроКАД)″, (Харків, 21 - 23 травня 2014 р.); International Symposium ″IEEE East-West Design & Test″, (Kiev, Ukraine, September 26 - 29, 2014); 15 Міжнародній науково-практичній конференції, ″Проблеми інформатики та моделювання: матеріали″, (Харків - Одеса, 14 - 18 вересня 2015 р.); V Міжнародній науково-практичній конференції, ″Захист інформації і безпека інформаційних систем″ , (Львів, 02 - 03 червня 2016 р.); International Symposium ″IEEE East-West Design & Test″, (Batumi, 2016); V-а Міжнародна науково-практична конференція, "Фізико-технологічні проблеми передавання, оброблення та зберігання інформації в інфокомунікаційних системах", (Чернівці, 03 - 05 листопада 2016 р.); Engineer of XXI Century - We Design the Future, Bielsko-Biała, Poland: ATH, 2016; 14th International Conference, "The Experience of Designing and Application of CAD Systems in Microelectronics CADSM'2017", (21 - 25 February 2017 Polyana-Svalyava (Zakarpattya), Ukraine); III Міжнародній науково-практичній конференції, "Актуальні питання забезпечення кібернетичної безпеки та захисту інформації", (Закарпатська область Міжгірський район село Верхнє Студене, 22 - 25 лютого 2017 р); VI Міжнародній науково-практичній конференції, «Обробка сигналів і негаусівських процесів», присвяченій пам'яті професора Кунченка Ю.П.″, (Черкаси, 24 - 26 травня 2017 р.); XIII Міжнародній науково-технічній конференції, "ABIA-2017", (Київ, 19-21 квітня, 2017 р.); I науково-технічній конференції "Проблеми кібербезпеки інформаційно-комунікаційних систем (PCSITS)", (Київ 05 - 06 квітня 2018 р.); IV Науково-практичній конференції "Перспективні напрямки захисту інформації", (Одеса, 02 - 06 вересня 2018 р.); VII

Міжнародній науково-практичній конференції "Фізико-технологічні проблеми передавання, оброблення та зберігання інформації в інфокомунікаційних системах", (Чернівці, 08 - 10 листопада 2018 р.); 3rd IEEE International Conference, "on Advanced Information and Communication Technologies (AICT 2019)", (Lviv, July, 2019).

Публікації. Основні положення і результати дисертаційної роботи опубліковано в 24 наукових працях, серед яких одна колективна монографія, 8 статей, зокрема, дві одноосібні статті та сім статей опубліковано в журналах, які входять до міжнародних наукометричних баз. Апробація результатів дисертації відображена у 16 тезах доповідей на міжнародних науково-технічних та науково-практичних конференціях, зокрема 4 публікації у матеріалах конференції, що входять до міжнародної наукометричної бази Scopus.

РОЗДІЛ 1
ОБГРУНТУВАННЯ НЕОБХІДНОСТІ ВДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОЇ БЕЗПЕКИ ПІДЛІТКІВ

Обґрунтовується, що ключовий ефект в забезпеченні інформаційної переваги і переваги в гібридної війні досягається в разі проведення деструктивних інформаційно-психологічних атак на підліткове покоління. При цьому для них найбільш популярними, затребуваними і системами, що довіряють каналами комунікацій є Інтернет ресурси та в тому чисел, ті які мають законодавче обмеження. Доводиться, що в умовах наявності безлічі дестабілізуючих внутрішньодержавних чинників, недостатньою контрольованості такого простору як Інтернет і дисбалансів: на рівні інформаційної культури підлітка; на рівні використання джерел комунікаційних каналів виникають суттєві втрати інформаційно-психологічної безпеки підлітків.

На основі системного аналізу базових складових інформаційної технології забезпечення інформаційної безпеки підлітків обґрунтовується, що одним з її ключових технологічних етапів є виявлення наявності інформаційно-психологічних деструкцій в інформаційних ресурсах.

Розробляється система показників якості методів виявлення і детектування інформаційних деструктивних модифікацій в інформаційних ресурсах. Показано що сфера розробки таких технологічних рішень знаходяться в критичному стані. Відповідні технології мають недостатній рівень розвитку, щоб бути адекватними існуючим інформаційно-технологічними можливостями протиборчої сторони щодо організації і проведення деструктивного ІП впливу.

1.1. Аналіз умов забезпечення національної безпеки держави в інформаційній сфері

Сучасний розвиток України, соціальна і політична стабільність в соціумі, економічне зростання і добробут населення напряму залежить від реалізації аспектів щодо забезпечення Національної безпеки та інформатизації держави. Тут потрібно враховувати наступні фактори (рис. 1.1) [2-7, 22-34, 36, 38-40, 42, 45-69, 73-79, 88, 92-106, 112-122, 124, 127-129]:

1. ***Зовнішні*** чинники, що створюють загрози Національної безпеки:

1) дисбаланс існуючої Концепції колективної безпеки, яка не завжди здатна адекватно реагувати на сучасні виклики. Це загострює протиборство між державами та групами держав. Взаємодія країн в сучасності часі здійснюється в умовах наявності інформаційних війн. Сучасні відношення між державами характеризуються багатовекторністю та багатофакторністю стосунків);

2) негативні наслідки змін геополітичної обстановки для безпеки в різних регіонах світу;

3) боротьба між різними ідеологічними системами;

4) політична, інформаційна, технологічна та економічна експансія розвинених країн по відношенню до менш розвинених країн з метою здобуття переваг;

5) негативні наслідки розширення кооперації у сфері розвитку інформаційної інфраструктури і співпраці із іноземними державами;

6) деструктивні наслідки для національної безпеки обумовлені наявністю протиріч між економічними інтересами держав. Загострення протиріч є наслідком появи на ринку великої кількості вітчизняних та іноземних комерційних структур – виробників і споживачів інформації, засобів інформатизації і захисту інформації, включенням інформаційної продукції в систему товарних відносин;

7) постійний розвиток інформаційно-технічної бази і підвищення доступності засобів для здійснення атак в інформаційно-технічному (вірусні атаки, кібернетичні атаки) та інформаційно-психологічному просторах.

2. ***Внутрішньодержавні*** фактори загроз Національної безпеки:

Рисунок 1.1 – Дестабілізуючі чинники національної безпеки

1) особливе геополітичне розташування України, що обумовлює формування епіцентру конфронтаційних зіткнень інтересів різних супердержав і міжнародних блоків;

2) Україна як держава і соціум є об'єктом для проведення гібридних та інформаційних воєн. Наслідком чого є виникнення затяжних соціально-політичних і військових конфліктів, включаючи конфлікт на Південному Сході країни;

3) використання різними національними політичними силами «брудних» передвиборних технологій, що ініціює зіткнення різних соціальних груп населення;

4) стягування релігійних інтересів в політичне русло, що обумовлює конфесійне протистояння в суспільстві;

5) істотний відтік висококваліфікованих фахівців за кордон;

6) недостатнє фінансування наукомістких інформаційних і технологічних сфер. В результаті утворюється інформаційна і технологічна залежність від інших держав, в тому числі в сегменті обороноздатності і кібербезпеки;

7) критичний стан вітчизняних галузей промисловості, яка виробляє засоби інформатизації, захисту інформації, технології інтелектуальної обробки даних і штучного інтелекту. Використання імпортних технічних і програмних засобів для зберігання, обробки і передачі інформації. Це може супроводжуватися впровадженням в апаратні і програмні вироби компонента, реалізуючи функції, які не передбачені документацією;

8) наявність соціальних, політичних і економічних криз всередині держави, складна криміногенна ситуація;

9) недостатній рівень розвитку державних засобів масової інформації, які призвані відображати та доводити державні інтереси та конструкційну політику до суспільства. Це призводе до достатнього рівня конструктивної інформаційної пропаганди в умовах ведення інформаційних війн;

10) недосконала законодавча база і неопрацьованість механізмів виконання законодавчих актів. Уразливість існуючої міжнародної і національної нормативно-правової бази у сфері регуляції і забезпечення національної та інформаційної безпеки. Недостатня регуляція державою процесів функціонування і розвитку ри-

нку засобів інформатизації, інформаційних продуктів і послуг. Наприклад, відсутня державна програма інформаційної безпеки підлітків. Доречи така програма вже прийнята в багатьох розвинених країнах світу.

11) стихійні лиха (пожежі, повені, снігові затори);

12) Україна є зосередженням великої кількості об'єктів критичної інфраструктури, включаючи атомні, гідро і тепло електростанції, нафтохімічні підприємства, нафтогазова транспортна система, склади з озброєнням і військовою технікою. Така особливість в умовах дестабілізації формує ризики для виникнення техногенних катастроф;

13) негативна дія природних і антропогенних чинників на довкілля. Це призводить до екологічних змін довкілля та впливає на загальний стан захищеності інформаційного середовища.

Звідки ключовими ***пріоритетами*** національної безпеки, що відповідають інтересам суспільного розвитку, є [23, 26, 38, 39, 49-51, 64, 65, 101]: забезпечення територіальної цілісності і прогресивного соціально-економічного розвитку держави; збереження і зміцнення української державності і політичної стабільності суспільства; збереження і розвиток демократичних інститутів суспільства, забезпечення прав та свобод громадян, зміцнення законності і правопорядку; забезпечення гідної ролі України в світовому співтоваристві; збереження та розвиток національних культурних цінностей і традицій; забезпечення національної безпеки в інформаційні сфері, тобто забезпечення інформаційної безпеки.

За сучасних умов інформаційна складова набуває дедалі більшої ваги і стає одним із найважливіших елементів забезпечення національної безпеки. Цьому сприяє використання інформаційних ресурсів та інформаційних технологій в різних сферах життя-діяльності держави. Інформаційний простір, інформаційні ресурси, інформаційна інфраструктура та інформаційні технології значною мірою впливають на рівень і темпи соціально-економічного, науково-технічного і культурного розвитку [3, 4, 28, 50-54, 57-60, 62, 63, 68, 69, 73, 77, 94, 95, 98, 100, 104, 122]. Тим самим створюються передумови для підтримання стабільності суспільства і держави. Отже, рівень розвитку та безпека інформаційного середовища є:

- по-перше системоутворюючим фактором в усіх сферах життя-діяльності та забезпечення національної безпеки;

- по-друге активно впливає на стан політичної, економічної, оборонної та інших складових національної безпеки України.

Через це забезпечення інформаційної безпеки являє собою важливу сферу національної безпеки [2, 6, 22, 26, 27, 38, 39, 46, 50, 55-57, 64-67, 76, 97, 101, 103]. При визначенні поняття «Інформаційна безпека» потрібно врахувати, що інформаційна безпека створює умови для забезпечення інтересів особистості, суспільства (соціуму) та держави, як в інформаційно-технічному, так і в інформаційно-психологічному просторах.

Тому пропонується варіант узагальнення декількох визначень поняття «Інформаційна безпека» [26, 27, 31, 39, 56, 64, 97, 101].

Інформаційна безпека – стан захищеності життєво важливих ***інтересів*** людини, суспільства і держави в інформаційній сфері, при якому як в інформаційно-технічному, так і в інформаційно-психологічному просторах досягається:

1. З одного боку - інформаційний розвиток, а саме: технічний, інтелектуальний, соціально-політичний, морально-етичний.

2. З іншого боку - запобігання нанесення шкоди сторонніми інформаційними впливами через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації.

Відповідний варіант структурного опису представлено на рис. 1.2.

При цьому під *інформаційною сферою* розуміється сфера діяльності суб’єктів, пов’язана із створенням, перетворенням та споживанням інформації.

В загальному випадку інформаційну безпеку можна розглядати в двох сегментах в залежності від об’єктів інтересу (об’єктів захисту, об’єктів, на які здійснюється інформаційний вплив) таких як:

1. Об’єкти інформаційно-технічного простору: інформаційні ресурси (особисті, конфіденційні, власність держави, з обмеженим доступом), науково-технічні засоби та інформаційно-технічні системи і технології.

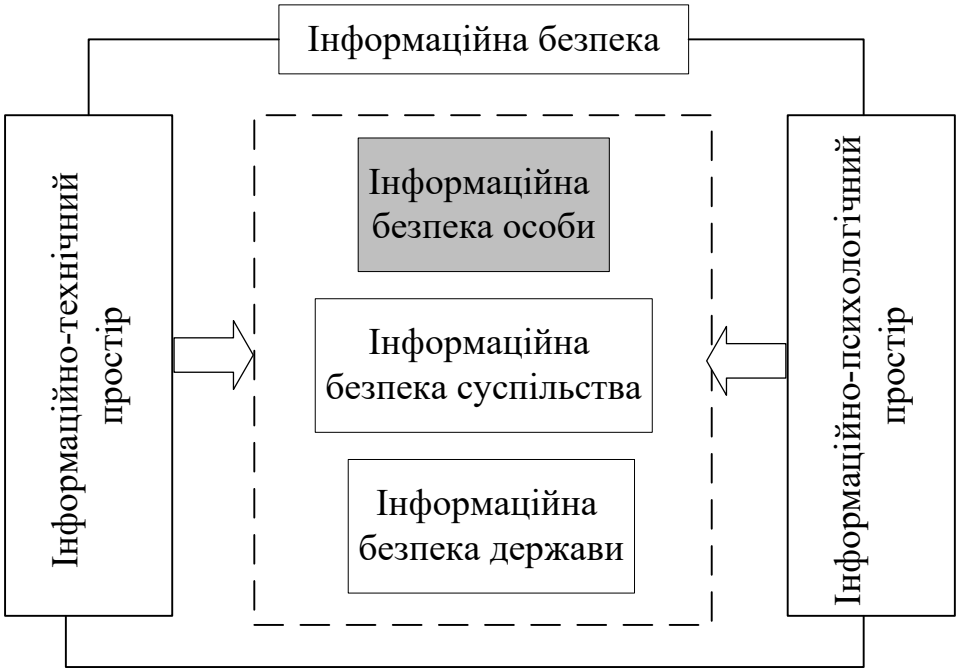


Рисунок 1.2 – Структурний опис інформаційної безпеки

2. Об’єкти інформаційно-психологічного простору: соціосистема, що включає соціальні об’єкти: особистість, соціальна група, соціум; безпосередні об’єкти: свідомість, підсвідомість особистості, власні інформаційні ресурси; соціотехнічні системи: інформаційно-керуючи системи, АСУ, Інтернет, Мобільні мережі.

Тоді інформаційна безпека в залежності від об’єктів деструктивного впливу полягає:

- для інформаційно-технічного (ІТ) простору це по-перше забезпечення безпеки інформаційних ресурсів громадян і держави, автоматизованих та інформаційних систем;

- для інформаційно-психологічного простору це захист свідомості та підсвідомості особистості, а для соціуму – захист його стабільності та прогресивних поглядів відносно деструктивного впливу (атак).

Такий розподіл напрямків забезпечення інформаційної безпеки дозволяє більш ефективно оцінювати загрози та забезпечувати безпеку об’єктів інтересу з врахуванням особливостей: самих об’єктів захисту; відповідних технологій, які використовуються для забезпечення інформаційної безпеки.

В загальному випадку загрозами ***національній безпеці*** України в ***інформаційній сфері*** є сукупність умов та факторів, які становлять небезпеку життєво важливим інтересам держави,суспільства й особи у зв’язку з можливістю негативного інформаційного впливу на свідомість і поведінку громадян, а також інформаційні ресурси й інформаційно-технічну інфраструктуру в табл. 1.1 [26, 27, 31, 39, 50, 56, 64, 65, 76, 97, 101, 103].

Таким чином, за даним матеріалом можна зробити наступний висновок:

1) забезпечення інформаційної безпеки являє собою важливу сферу національної безпеки держави. Особливо це актуально в умовах коли створено ***дисбаланс***, який викликано тим, що: з одного боку здійснюється відкрите або приховане проведення гібридних війн та інформаційного протиборства з врахуванням наявності зовнішніх та внутрішніх дестабілізуючих факторів в різних сферах життєдіяльності країни; з іншого боку формуються протиріччя існуючої концепції колективної безпеки, яка не завжди здатна адекватно реагувати на сучасні виклики;

2) існує ***протиріччя*** обумовлене міжнародною інтеграцією держави у світовий інформаційний та соціотехнічний простір. Це полягає втому, що: з одного боку створюються умови для інтеграції держави у світове співтовариство, а отже, формуються умови для розвитку держави, соціуму і особистості; з іншого боку така інтеграція створює умови для проведення інформаційних атак на ресурси держави, соціуму і особистості;

3) в загальному випадку для підвищення рівня інформаційної безпеки її можна розглядати в двох сегментах, а саме в залежності від об’єктів інтересу таких як: об’єкти інформаційно-технічного простору; об’єкти інформаційно-психологічного простору.

Таблиця 1.1

Узагальнений перелік загроз інформаційній безпеці у різних сферах життя-діяльності держави

Сфери діяльності	Загрози інформаційній безпеці	
	Інформаційно-психологічний простір	Інформаційно-технічний простір
1	2	3
1. Зовнішньо-політична	1.1. Поширення у світовому інформаційному просторі викривленої, недостовірної та упередженої інформації, що завдає шкоди національним інтересам України. 1.2. Зовнішні негативні інформаційні впливи на суспільну свідомість через засоби масової інформації, а також мережу Інтернет.	1.1. Прояви комп'ютерної злочинності, комп'ютерного тероризму, що загрожують сталому та безпечному функціонуванню національних інформаційно-телекомунікаційних систем
2. Державної безпеки	2.1. Негативні інформаційні впливи, спрямовані на підрив конституційного ладу, суверенітету, територіальної цілісності і недоторканності кордонів України. 2.2. Використання засобів масової інформації, а також мережі Інтернет для пропаганди сепаратизму за етнічною, мовною, релігійною та іншими ознаками. 2.3. Інформаційно-психологічний вплив на населення України, у тому числі на особовий склад військових формувань, з метою послаблення їх готовності до оборони держави та погіршення іміджу військової служби	2.1. Несанкціонований доступ до інформаційних ресурсів органів державної влади. 2.2. Розголошення інформації, яка становить державну та іншу передбачену законодавством таємницю, а також конфіденційної інформації, що є власністю держави
3. Внутрішньо- політична	4.1. Недостатня розвиненість інститутів громадянського суспільства, недосконалість партійно-політичної системи, непрозорість політичної та громадської діяльності, що створює передумови для обмеження свободи слова, маніпулювання суспільною свідомістю. 4.2. Негативні інформаційні впливи, в тому числі із застосуванням спеціальних засобів, на індивідуальну та суспільну свідомість. 4.3. Поширення суб'єктами інформаційної діяльності викривленої, недостовірної та упередженої інформації	

Продовження табл. 1.1

1	2	3
4. Економічна		4.1. Відставання вітчизняних наукоємних і високотехнологічних виробництв, особливо у сфері телекомунікаційних засобів і технологій. 4.2. Недостатній рівень інформатизації економічної сфери, зокрема кредитно-фінансової системи, промисловості, сільського господарства, сфери державних закупівель. 4.3. Несанкціонований доступ, порушення встановленого порядку роботи з ІР в галузях національної економіки, викривлення інформації в таких ресурсах. 4.4. Використання неліцензованого і несертифікованого програмного забезпечення, засобів і комплексів обробки інформації
	4.5. Недостатній рівень розвитку національної інформаційної інфраструктури	
5. Соціальна та гуманітарна	5.1. Відставання України від розвинутих держав за рівнем інформатизації соціальної та гуманітарної сфер, насамперед освіти, охорони здоров'я, соціального забезпечення, культури. 5.2. Недодержання прав людини і громадянина на одержання інформації, необхідної для захисту їх соціально-економічних прав. 5.3. Поширення в засобах масової інформації невластивих українській культурній традиції цінностей і способу життя, культу насильства, жорстокості, порнографії, зневажливого ставлення до людської і національної гідності	

Продовження табл. 1.1

1	2	3
	5.4. Тенденція до витіснення з інформаційного простору та молодіжної культури українських мистецьких творів, народних традицій і форм дозвілля. 5.5. Послаблення суспільно-політичної, міжетнічної та міжконфесійної єдності суспільства. 5.6. Відставання рівня розвитку українського кінематографу, книговидання, книгорозповсюдження та бібліотечної справи від рівня розвинутих держав	
6. Науково-технологічна	6.1. Зниження наукового потенціалу в галузі інформатизації та зв'язку. 6.2. Низька конкурентоспроможність вітчизняної інформаційної продукції на світовому ринку. 6.3. Відтік за кордон наукових кадрів та суб'єктів права інтелектуальної власності. 6.4. Недостатній захист від несанкціонованого доступу до інформації внаслідок використання іноземних інформаційних технологій та техніки. 6.5. Неконтрольована експансія закордонних сучасних інформаційних технологій, що створює передумови технологічної залежності України 6.6. Негативні наслідки розширення кооперації у сфері розвитку інформаційної інфраструктури і співпраці із іноземними державами. Уразливість для інформаційної безпеки виникає, як наслідок надання інформаційних майданчиків для засобів мультимедіа інших держав, включаючи Інтернет-ресурси.	
7. Екологічна	8.1. Приховування, несвоєчасне надання інформації або надання недостовірної інформації населенню про надзвичайні екологічні ситуації чи надзвичайні ситуації техногенного та природного характеру.	8.2. Недостатня надійність інформаційно-телекомунікаційних систем збирання, обробки та передачі інформації в умовах надзвичайних ситуацій.
	8.3. Низький рівень інформатизації органів державної влади, що унеможливлює здійснення оперативного контролю та аналізу стану потенційно небезпечних об'єктів і територій, завчасного прогнозування та реагування на надзвичайні ситуації	

1.2. Обґрунтування актуальності та значущості загроз інформаційної безпеки держави, обумовлених деструктивними інформаційно-психологічними атаками

Дослідження особливостей проведення деструктивних інформаційних операцій в рамках гібридної та інформаційних війн, організації вірусних і кібернетичних атак, виявили наступні концептуальні аспекти інформаційної боротьби [2, 5-7, 22-27, 29-33, 36, 38-42, 45-52, 55-58, 61, 64-67, 74-76, 83, 92, 96, 97, 101, 103, 105, 106, 112-121, 124, 127, 129].

І. З одного боку інформаційно-технічні атаки в інформаційної сфері держави і протидія їм характеризуються тим, що:

1.1. Існують відповідні нормативно-правові акти, організаційні механізми та інформаційні технології протидії, які розробляються й удосконалюються протягом значного часу. Вони в достатній степені апробовані та пройшли перевірку практикою та часом.

1.2. Сформовані відповідні органи, відповідаючи за забезпечення інформаційної безпеки в інформаційно-технічному просторі.

1.3. Технології протидії ІТ атакам повністю або їх базові компоненти розробляються вітчизняними компаніями.

1.4. Існують потужні наукові школи та навчальні програми за підготовкою спеціалістів з ІТ безпеки.

1.5. Інформаційно-технічні атаки або проводяться у відкритому режимі або існують відповідні адаптивні технології і методи по виявленню прихованих ІТ атак (кібератаки, вірусні атаки, стеганографія та ін.).

1.6. Такі атаки напряму не здійснюють деструктивного впливу на психологічний стан особистості та соціуму. Тому дія тільки таких атак не може призвести до досягнення остаточної переваги в сучасній гібридній війні.

ІІ. З іншого боку інформаційно-психологічна боротьба в інформаційній сфері держава відрізняється тим, що

2.1. Досягнення ключового паритету в інформаційній війні з використан-

ням інформаційно-психологічних засобів забезпечує фактичну перевагу у всій кампанії. Шкода від дії таких атак може призвести до втрати суверенності держави.

2.2. У гібридній війні інформаційні атаки на населення, ІП вплив на нього займають друге місце за значимістю щодо досягнення кінцевого результату і нанесення збитку після військового конфлікту, тобто після застосування Збройних Сил.

2.3. Інформаційно-психологічні операції більш економічні та політично вигідні за порівнянням з використанням. У цьому випадку очікується значна економічна вигода з мінімальною затратою матеріальних та людських ресурсів.

2.3. У протиборчої сторони існують спеціально розроблені та апробовані інформаційно-психологічні технології для проведення ІП атак.

2.4. Відомі інформаційні технології протидії ІП впливу недостатньо ефективні щодо виявлення інформаційно-психологічних атак і протидії їм. Особливо це проявляється у випадку використання сугестивних інформаційно-психологічних атак.

2.5. Інформаційне середовище держави характеризується відносною неконтрольованістю соціо-технічного простору, в тому числі Інтернет простору. Це спричиняє непоодинокі випадки надання ефірного часу теле- та радіопрограмам, спрямованим на руйнування моральних цінностей, свідомості української нації, підривання морального й фізичного здоров’я громадян. З іншого боку свідомо чи несвідомо ЗМІ створюють додатковий негативний вплив на психіку населення, «готуючи» її до проведення інших заходів прихованого деструктивного іноземного впливу.

2.6. Технології ІП впливу довгий час були якщо незасекречені, то мали обмежену доступність для відкритого доступу, тобто не надавались для загальному аналізу і оцінці.

2.7. Результати ІП впливів можуть проявлятись протягом значного часового періоду. Це створює складність для їх своєчасного виявлення та блокування.

2.8. Прийнято умови щодо обмеженої можливості (на законодавчому рівні) щодо накладення цензури, блокування Інтернету, TV каналів. В іншому випадку

такі радикальні заходи пов'язані з порушенням таких категорій інформаційної безпеки як доступність і своєчасність отримання інформації, тобто немає жорсткої межі між порушенням прав особистості на отримання інформації та порушенням інформаційної безпеки особистості щодо блокування деструктивного на неї впливу.

2.9. Державні засоби пропаганди відрізняються обмеженими можливостями доведення населенню конструктивних морально-ідеологічних норм. Низький загальний рівень інформаційної інфраструктури сприяє експансії іноземними компаніями ринку інформаційних послуг.

На думку українських експертів, саме експансія в інформаційному просторі є однією з найнебезпечніших складових «гібридної» війни проти України. (табл. 1.2.) [1, 38, 61, 64, 65, 83]. Аналіз табл. 1.2 показує, що по експертним оцінками такі ІП атаки, як інформаційно-пропагандистська експансія (диверсії, провокації) в Українському медіа-просторі, просування ідеології «русского мира» забезпечують нанесення: більшої шкоди національній безпеці держави, ніж безпосередньо збройний конфлікт; більш значимого збитку в порівнянні з кібератаками в середньому на 10%.

Отже, по викладеному матеріалу можна стверджувати про наявність дисбалансу між технологіями і засобами інформаційного протиборства в Україні, що представлено в табл. 1.3. Як показано в табл. 1.3 дисбаланс існує по семи категоріях, включаючи: ступінь завдання шкоди, наявність нормативно-правової бази, існування системоутворюючої організаційно-штатної структури, створеної і апробованої науково-фундаментальної і прикладної бази, доступність технологій для широкого кола дослідників, конкурентно-спроможність відповідних технологій протидії, наявність потужних наукових шкіл і навчальних закладів.

У роботі під інформаційно-психологічним впливом (інформаційними атаками в інформаційно-психологічному просторі) будемо розуміти наступне визначення [42, 57, 61, 64-66, 102, 105, 109, 114, 116, 117].

Під ***інформаційно-психологічнім впливом*** розуміється весь спектр технологій, форм, методів і способів цілеспрямованого, усвідомленого, відкритого або прихованого безпосереднього впливу на індивідуальну, групову і суспільну сві-

домість та підсвідомість, психологію і поведінку населення та особистості через зовнішні та внутрішні комунікаційні канали, в тому числі Інтернет ресурси, засоби масової інформації, спеціальні канали комунікації, за допомогою створення та розповсюдження спеціальної інформації для зміни поведінки, мотиваційних установок та морально-етичних норм об'єкту впливу.

Таблиця 1.2

Оцінка рівня небезпеки інформаційно-психологічного простору

Рівні небезпеки інформаційно-психологічного простору	Середній бал
Інформаційно-пропагандистська експансія (диверсії, провокації) в українському медіа-просторі. Просування ідеології «русского мира»	4,4
Ведення інтенсивних бойових дій у Південно-Східному регіоні держави з загрозою їх ескалації	4,3
Шпигунська, агентуро-розвідувальна діяльність російських спецслужб на території України	4,3
Мілітаризація Криму і окремих районів Донецької та Луганської областей	4,3
Підтримка «п'ятої колони» в органах влади, ЗМІ, громадських організаціях в Україні	4,2
Дискредитація України в Європі і світі політико-дипломатичними,інформаційними та ін. засобами	4,2
Диверсійно-терористичні акції на території України	4,0
Підбурювання сепаратистських настроїв в регіонах	4,0
Захоплення українських заручників за сфабрикованими звинуваченнями у шпигунстві, тероризмі тощо.	4,0
Кібератаки на українські комп'ютерні мережі	4,0
Інспірування акцій соціального протесту	3,9
Введення і поширення економічних санкцій проти України	3,4
Використання «енергетичних» засобів тиску	3,4

Таблиця 1.3

Дисбаланс технологій і засобів інформаційного протиборства в Україні

Аспекты	Інформаційно-технічний простір	Інформаційно-психологічний простір
Фундаментальна база створена в державі	Існують відповідні нормативно-правові акти, організаційні механізми і інформаційні технології протидії. Вони в достатній мірі апробовані і пройшли перевірку практикою і часом	Відсутні системні розробки. Створення технологій починалося з початку 2000-х років. Отримало підтвердження актуальності в 2014 році
Організаційно-штатна структура спеціальних органів	Створені центральні та регіональні центри і підрозділи по забезпеченю безпеки в ІТ просторі	Питання ІП впливів покладені на Сили спеціальних операцій Збройних Сил України. Питання протидії негативним ІП впливів делеговані різнорідним структурам без чіткого керівництва і взаємодії
Наявність ІТ і методів протидії	Розроблено і стандартизовані відповідні методики і технології. Існують засоби по виявленню прихованих ІТ-атак	Технології знаходяться на стадії розробки. Відповідні стандарти відсутні
Доступ технологій для досліджень	Методи і базові стандарти викладено у відкритому доступі для всебічної апробації та дослідження широким колом фахівців	Інформація в цій галузі довгий час була обмежена для доступу. Використання відкритих іноземних технологій без адаптації не можливо і не дасть результатів (повний опис технологій у відкритому доступі відсутньо). Нові технології або їх елементи, що розробляються в Україні, знаходяться на стадії апробації і не доведені до остаточного рішення
Наявність наукових шкіл з підготовки фахівців	Існують досить потужні наукові школи та інститути	Проблематикою займаються окремі групи вчених, що працюють в основному в інтересах сектора безпеки і оборони
За ступенем нанесення збитку	Дія тільки таких атак не може привести до досягнення остаточної переваги в сучасній гібридній війні	Вони не призводять до знищення фізичних і матеріальних ресурсів. Основний їх вплив спрямований на зміну (корекцію) мислення особистості (соціуму). Однак, збиток, що наноситься ІП атаками, може бути фатальним для суверенетету і незалежності держави
Порівняння з зарубіжними аналогами	Технології по забезпеченню таких категорій інформаційної безпеки як конфіденційність і цілісність знаходяться на достатньому конкурентному рівні	Технології або відсутні, або неконкурентноспроможні. Існує значне відставання від зарубіжних аналогів

У випадку розгляду інформаційно-психологічного простору, тобто у разі дії деструктивних ІП атак поняття інформаційна безпека набирає більш конкретні визначення. Саме ***пропонується*** ввести поняття «***Інформаційно-психологічна безпека***» та надати визначення на основі модифікації існуючих термінів.

Інформаційно-психологічна безпека особи – це стан захищеності психіки, здоров'я, ідейно-моральних принципів та життя людини від деструктивного інформаційно-психологічного впливу, який призводить до неадекватного сприйняття нею дійсності та (або) погіршення її фізичного стану.

Інформаційно-психологічна безпека суспільства – можливість безперешкодної реалізації суспільством й окремими його членами своїх конституційних прав, пов'язаних із вільним одержанням, обробленням, створенням і поширенням інформації, а також ступінь їх захисту від деструктивного інформаційно-психологічного впливу.

Інформаційно-психологічна безпека держави – це стан її захищеності та інформаційного розвитку, при якому деструктивні інформаційно-психологічні атаки не завдають шкоди національним інтересам.

Для оцінки рівня загроз втрати інформаційної безпеки в ІП просторі пропонується використовувати такі показники якості дії деструктивний ІП атак:

1. Імовірність деструктивної модифікації психологічного стану соціуму $P_{дмс}$ і особистості $P_{дмо}$.

2. Часові затрати $T_{дмс}$ и $T_{дмо}$ на здійснення такої деструктивної модифікації.

3. Об'єм $V_{дмс}$ и $V_{дмо}$ інформаційного ресурсу, який потрібно задіяти для досягнення деструктивної модифікації.

Відповідно ефективність проведення деструктивної ІП атаки з боку протиборчої сторони визначається наступними співвідношеннями:

$$P_{дмс} \rightarrow \max \text{ і } P_{дмо} \rightarrow \max \qquad (1.1)$$

в умовах виконання обмежень

$$T_{дмс} \le T_{дмс/з} \text{ і } T_{дмо} \le T_{дмо/з}; \quad (1.2)$$

$$V_{дмс} \le V_{дмс/з} \text{ і } V_{дмо} \le V_{дмо/з}. \quad (1.3)$$

Тут $T_{дмс/з}$, $T_{дмо/з}$, $V_{дмс/з}$, $V_{дмо/з}$ - обмеження на часові терміни проведення ІП атаки і обсяг інформації на їх проведення відповідно для соціуму і особистості.

Значимість проведених деструктивних ІП атак визначається комплексним показником $\rho_{шк}$ нанесеної шкоди соціуму, особистості і держави. У загальному випадку під збитком розуміється:

- не тільки модифікація психологічного стану особистості та соціуму через його свідомість (колективна свідомість) і підсвідомість в сторону деструктивності, що веде до збитку для його здоров'я і життя та неблагополучного подальшого розвитку;

- але і ті наслідки які будуть відображатися на життєдіяльності всього соціуму і національної безпеки держави.

Такі показники в загальному випадку залежать від:

1) внутрішніх захисних характеристик об'єктів деструктивного ІП впливу, в тому числі наявністю безлічі вразливостей, утому числі: психологічні і інтелектуальні здібності об'єкта ІП впливу, здатність щодо критичного сприйняття і аналізу інформації, тобто інформаційно-психологічна стійкість особистості (об'єкта впливу), ступінь навіюваності особистості; психологічний і моральний стан об'єкта ІП впливу; соціальний характер і соціальна стійкість найближчого середовища впливу на особистість;

2) ефективності технологій і засобів формування деструктивного інформаційно-психологічного впливу, включаючи методи та методики здійснення безпосереднього й опосередкованого ІП впливу. У загальному випадку ІП технологія задається функціоналом $F_{дів}$, використовуваним для здійснення деструктивної ІП атаки, тобто для перетворення множини $W_{поч}$ вихідних психологічних станів підлітка (особистості) в множину $W_{вих}$ станів після деструктивного впливу. Це опи-

сується таким виразом

$$F_{дів} : W_{поч} \rightarrow W_{вих} ; \quad (1.4)$$

3) комунікаційних каналів для проведення ДІП впливу, включаючи:

- характеристики інфокомунікаційного простору, що використовується як технічний канал для реалізації ІП впливу, у тому числі включаючи технічні характеристики інфокомунікаційного простору;

- доступність інфокомунікаційних технологій для об'єкта впливу (засоби масової інформації, Інтернет ресурси, мобільні інфокомунікаційні мережі), як тих що висвітлюють і проводять державну пропаганду, так і тих, що реалізують деструктивні дії;

4) безлічі дестабілізуючих факторів, в тому числі:

- соціальна, економічна, політична обстановка в державі, наявність факторів, що призводять до зневірі і не впевненості в завтрашньому дні;

- наявність затяжних військових конфліктів і терористичних загроз;

5) доступність особистості до інформаційних ресурсів, що здійснює інформаційно-пропагандистську діяльність в інтересах держави.

За викладеного матеріалу можна зробити висновок, що в умовах проведення гібридної і інформаційної війни з урахуванням наявності безлічі внутрішньодержавних дестабілізуючих факторів встановлюється наступне:

а) найбільший ефект в забезпеченні як інформаційної переваги, так і переваги в гібридної війні досягається в разі проведення ІП атак в порівнянні з атаками в інфокомунікаційного просторі;

б) існує дисбаланс, обумовлений відставанням вітчизняних засобів і технологій протидії ІП впливу щодо інформаційно-технологічних можливостей протиборчої сторони в сфері інформаційно-психологічних операцій.

Отже виникає інтерес, щодо оцінки найбільш уразливого сегмента соціуму щодо деструктивного інформаційно-психологічного впливу.

1.3. Обґрунтування актуальності і значущості загроз втрати інформаційної безпеки підлітків обумовлених дією деструктивних інформаційно-психологічних атак

З позиції забезпечення протидії деструктивним ІП атакам необхідно виявити найбільш вразливі сегменти простору об'єктів такого впливу.

Тут потрібно враховувати, що ключовим об'єктом деструктивного інформаційно-психологічного впливу є соціосистема, яка формується на особистостях, соціальних групах і соціумі. При цьому найбільш вразливим сегментом соціуму буде той, для якого характерні:

1) з одного боку найменший ступінь: $\rho_{кв}$ критичності сприйняття одержуваної інформації, тобто низький рівень критичного аналізу і оцінки одержуваної інформації; $\rho_{уст}$ стійкості морально-етичних і психологічних установок;

2) з іншого боку найбільша ступінь $\rho_{вi}$ сприйняття нової інформації і потреби в її отриманні, тобто високий рівень потреби нових знань і мінімальний час $T_{уi}$ засвоєння нової інформації.

Виходячи з таких показників найбільш уразливим з позиції ефективності проведення деструктивного ІП впливу є сегмент населення, який охоплює віковий діапазон від 9 до 16 років. Такий віковий діапазон визначається як підлітковий. Відповідно найбільш уразливими об'єктами деструктивного ІП впливу є підлітки.

В цьому аспекті для підлітків і молоді (від 17 до 25 років) характерним є таке:

1. Відрізняються найбільшим прагненням до свободи, незалежності і найповнішої реалізації своїх здібностей. Один з таких результатів це те, що підлітки і молодь найшвидше групуються в різні віртуальні спільноти. При цьому виникають нові, не інституційні канали творчої та комунікативної самореалізації підлітків.

2. Під впливом інформаційних ресурсів, що надаються соціуму через різні інформаційні канали, формуються поведінкові моделі підлітків, такі як:

1) ставлення до соціально значущих економічних, політичних і інших подій

і явищ, що відбуваються в державі;

2) формування контексту сприйняття поточних подій в індивідуальному та суспільному житті;

3) побудова поточних мотивацій і стратегічних життєвих планів.

Наявність такого дисбалансу для підлітків, а також безліч дестабілізуючих факторів $\Psi_{дф}$ і безліч комунікаційних каналів $\Psi_{ком/к}$ приводить до виникнення множини $\Psi_{вібл}$ вразливостей інформаційної безпеки особистості.

Тоді ймовірність $P_{дмо}$ модифікації психологічного стану підлітка, тобто ймовірність переходу його вихідного психологічного стану $w_{поч}$ в деструктивне $w_{вих}$ за допомогою функціоналу $F_{дів}$, який описує технологію деструктивного ІП впливу, буде найбільшою, тобто:

$$P_{дмо} : w_{поч} \xrightarrow{F_{дів};\, f_{псп}(\rho_{кв};\, \rho_{уст};\, \rho_{ві};\, T_{уі})} w_{вих} \to \max. \qquad (1.5)$$

Тут $f_{псп}(\rho_{кв};\, \rho_{уст};\, \rho_{ві};\, T_{уі})$ - функціонал, що визначає вихідний характеристичний стан підлітка.

Для опису суті процесу модифікації вихідного психологічного стану підлітка пропонується використовувати модель його канально-установочного опису. У цьому випадку використовується набір (множина $\Omega_{уст}$) первинних установок підлітка. *Установка* (орієнтація) – це сформовані під впливом пропаганди, виховання й досвіду відносно стійкі *знання*, *почуття* і *мотиви*, що викликають відповідне відношення людини до ідейних, політичних і суспільних явищ реальної дійсності, що виражаються в дії (у широкому змісті слова). До установок також відносять *генетичну спрямованість* підлітка та *менталітет* ближнього соціального середовища. Установка визначає напрямок дій і одночасно спосіб сприйняття і мислення. Звичайно різні установки не є рівнозначними для детермінації поведінки. Іншими словами установки мають різну вагу в процесі забезпечення стійкості підлітків стосовно деструктивної дії ІП атак.

Орієнтація підлітка залежить від безлічі соціальних установок, що співвідносяться з певними сторонами суспільного буття. Вони мають певну цінність з точки зору їхнього значення для підлітка. Отже на формування цих установок певний вплив відіграє ближня соціальне середовище або внутрішній соціальний канал впливу. Модель розподілу значимості такого впливу наведена на рис. 1.3 [64, 65].

На рис. 1.3 запропоновано модель всебічного впливу на підлітка (цільову групу підлітків), яку розроблено за принципами моделі противника (моделі п’яти кілець), що була розроблена в США полковником ВВС Джоном Уорденом та в подальшому адаптована при проведенні інформаційно-психологічних операцій [64, 65].

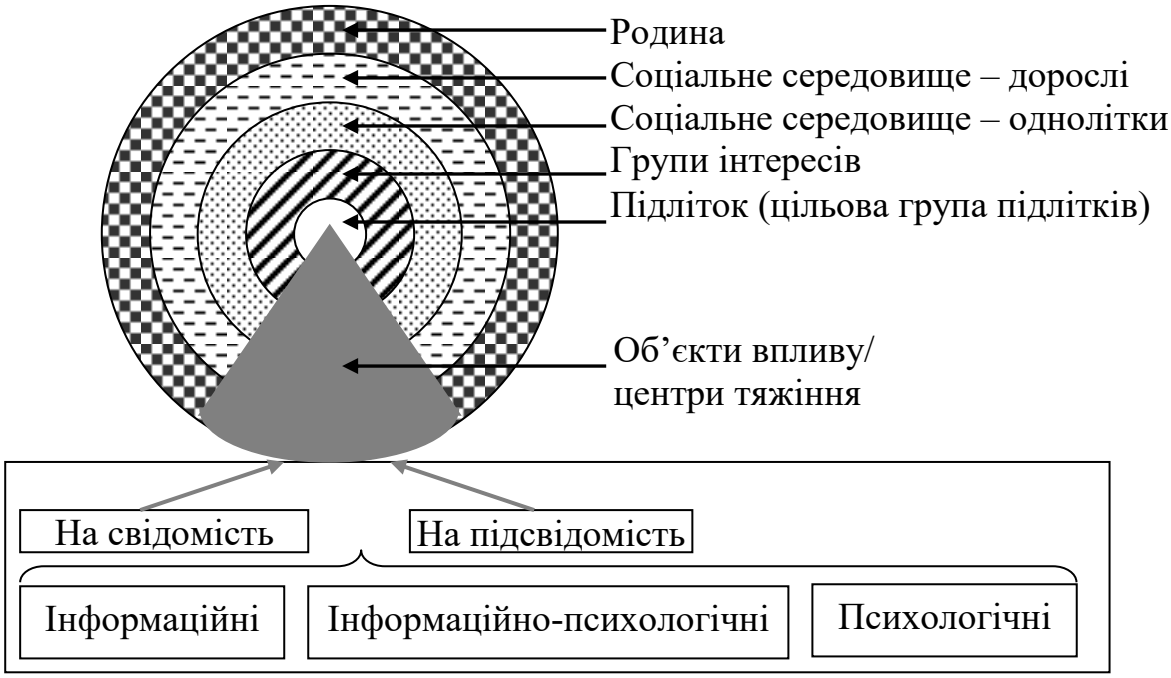


Рисунок 1.3 – Модель всебічного впливу на підлітка (цільову групу підлітків)

Відповідно до концепції моделі п’яти кілець, всі життєво важливі сегменти соціального існування підлітка або цільової групи підлітків можна представити п’ятьма сегментами: безпосередньо підліток або цільова група підлітків; їх групи інтересів, до яких можуть входити соціальні групи за інтересами в соціальних мережах, на Інтернет сайтах та порталах, соціальні групи інтересів в реальному житті тощо; соціальне середовище – однолітки, до якого можуть входити друзі в соціальних мережах, однокласники (однокурсники), друзі та знайомі тощо; соціальне середовище – дорослі, до якого можуть входити вчителя (викладачі), дорослі зна-

йомі, сусіди тощо; родина підлітка (родини підлітків цільової групи).

Щоб змусити об’єкти впливу (підлітка, цільову групу підлітків) змінити поведінку (установки), необхідно вичислити критичні вузли цих сегментів та вивести їх з рівноваги, що дозволить послідовно перевести об’єкти впливу із одного стану $w_{поч}$ до іншого $w_{вих}$, забезпечити сприйняття впливу, відключити підсистеми психологічного захисту особистості і, як результат, змінити поведінку об’єкту впливу.

В загальному випадку структурно-функціональна схема інформаційної технології деструктивного інформаційно-психологічного впливу на підлітка (групу підлітків, населення) представлено на рис. 1.4. В загальному випадку ***інформаційно-психологічні технології*** – це широкомасштабне застосування способів і засобів інформаційної дії на психіку населення протилежної сторони на користь досягнення стороною, що здійснює вплив, політичних, дипломатичних, воєнних, економічних та інших цілей.

Процес деструктивного інформаційного впливу на підлітка ґрунтується на таких етапах, як (рис. 1.4):

1. Перший етап – виявлення інтересів підлітка, сфери його бажань, інтересів та мотивацій. Вивчається потребо-мотиваційна сфера підлітка: знання, переконання, цінності, орієнтації, схильності бажання. На цьому етапі починається втрата цінностей актуальної інформації, яка закладається генетично та під час встановлення початкових установок.

2. Другий етап – інформаційний вплив на підлітка з метою надання йому інформації відповідно до його інтересів. Такий етап впливає на пізнавальну та пізнавально-інтелектуальну сфери підлітка: відчуття, сприйняття, уява, пам’ять, мислення. На цьому етапі здійснюється підготовка підлітка для забезпечення некритичного сприйняття ім інформації та засвоєння будь якої інформації психологічного впливу. Цей етап застосовується для руйнування фільтрів критичного сприйняття інформації підлітком. Змінюється в потрібну сторону уявлення підлітка, характер сприйняття інформації, яка отримується.

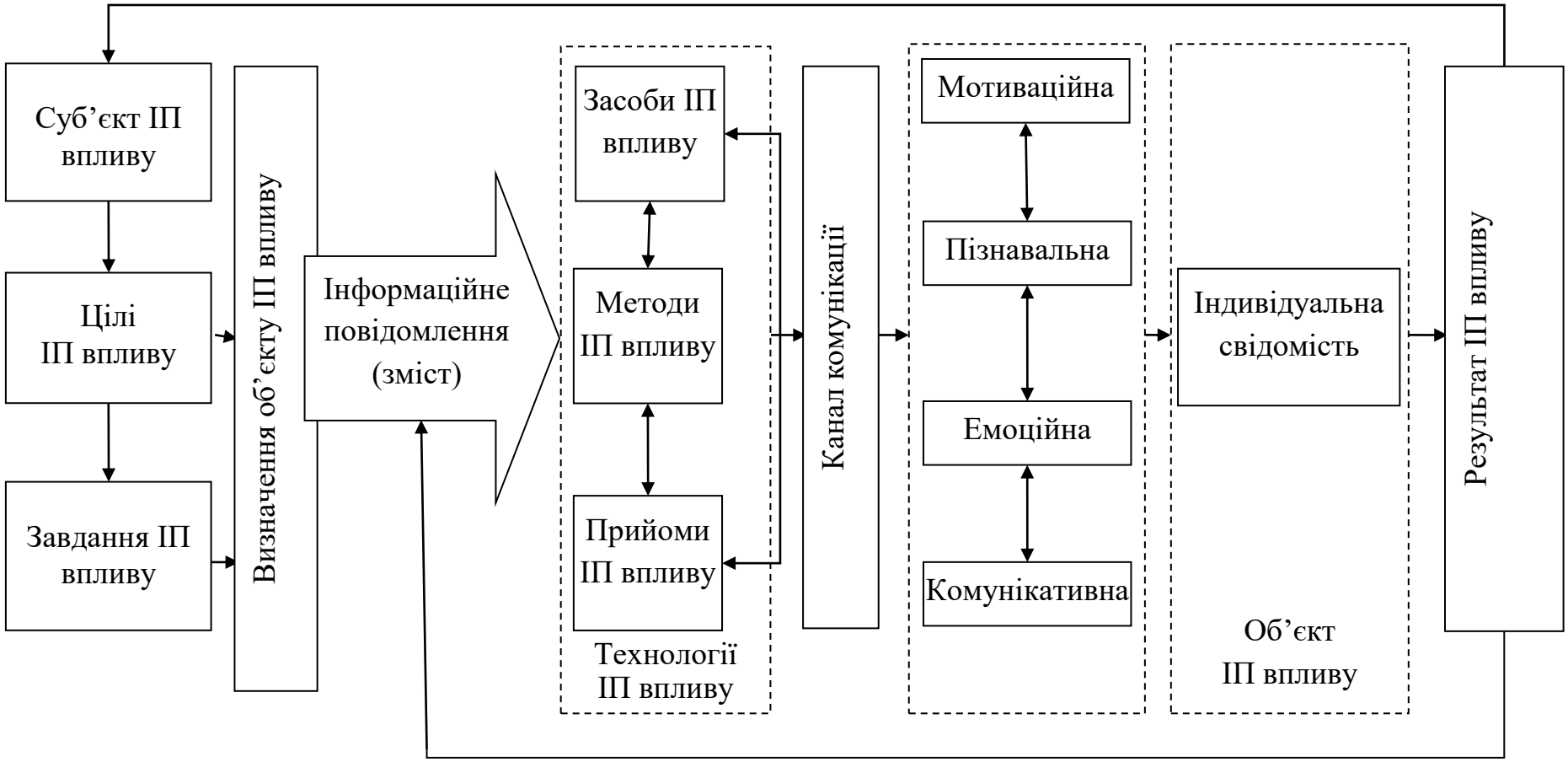


Рисунок 1.4 – Структурно-функціональна схема інформаційної технології деструктивного інформаційно-психологічного впливу

3. Третій етап – перевірка результатів другого етапу, а саме яким чином змінюється мотивація підлітка, його інтереси та поведінка. Даний етап застосовується для оцінки змін емоційно-вольової сфери підлітка, а саме: емоції, почуття, настрої, вольові процеси. Перш за все здійснюється оцінка внутрішніх переживань підлітка.

4. Четвертий етап – інформаційні дії для досягнення необхідних мотиваційних установок підлітка. Цей етап є базовим для внесення негативної деструктивної інформації. Змінюється вольова активність підлітка та закладається фундамент для забезпечення маніпулювання підлітком. Здійснюється оцінка зміни в поведінкової та комутативно-поведінкової сфери діяльності підлітка, тобто характер, особливості спілкування, взаємодії в соціумі та соціальних групах.

У результаті таких дій у підлітка можуть виникнути уявлення, які не відповідають дійсності та створюються сфера для здійснення неадекватних вчинків.

У випадку розгляду інформаційної безпеки підлітка в інформаційно-психологічному просторі, тобто інформаційно-психологічної безпеки підлітка пропонуються наступні визначення.

Інформаційно-психологічна безпека підлітка – це стан захищеності психіки, здоров'я, моральних норм поведінки та життя підлітка від ***усвідомленого*** деструктивного інформаційно-психологічного впливу ***безпосередньо*** на його свідомість та підсвідомість, який призводить до деструктивної модифікації попередніх установок (орієнтацій), деградації морально-психологічного розвитку та неадекватного сприйняття дійсності з послідуючим погіршення його фізичного стану та втратою життя.

Відповідно базовими ***загрозами*** (безліч загроз $\Psi_{зіб}$) інформаційно-психологічної безпеки підлітка, тобто інформаційної безпеки підлітка в інформаційно-психологічному просторі або інформаційної безпеки підлітка стосовно безпосередньої дії усвідомлених деструктивних ІП атак є [42, 57, 61, 64-66, 102, 105, 109, 114, 116, 117]:

– маніпулювання індивідуальною, груповою та масовою свідомістю;

– незаконне використання сучасних інформаційно-технічних та інформаційно-психологічних технологій для коректування життєвих цінностей особистості (підлітка), її психологічного стану;

– надмірне обмеження доступу до відкритих інформаційних ресурсів органів державної влади, органів місцевого самоврядування, архівних матеріалів та іншої суспільно-необхідної інформації;

– протидія, насамперед, з боку недержавних структур, реалізації своїх конституційних прав на особисту та сімейну таємницю, таємницю листування, телефонних переговорів;

– протиправне обмеження свободи совісті і віросповідання;

– поширення в засобах масової інформації агресивної реклами товарів і послуг, що використовує технології нейролінгвістичного програмування та іншого маніпулятивного впливу на свідомість громадян;

– пропаганда, що йде в розріз із прийнятими в суспільстві моральними нормами та розпалює ненависть і ворожнечу в різних формах і проявах, не надання громадянам соціально значимої інформації;

– приховування або перекручування органами державної влади фактів і обставин, що створюють загрозу для психологічного здоров'я людини;

– відсутність дієвого механізму запобігання використанню засобів масової інформації для порушення конституційних прав громадянина, приниження людської гідності, збудження соціальної, расової, релігійної ненависті;

– явне порушення моральних цінностей і етичних норм поводження, прийнятих у суспільстві.

Тоді під ***інформаційно-психологічною атакою*** (впливом) на підлітка будемо розуміти перш за-все стратегічні ***інформаційно-психологічні*** операції, як комплекс безпосереднього та усвідомленого системного інформаційно-психологічного впливу з метою формування у них системи певних поглядів і ціннісних орієнтирів, які спрямовані на руйнування морально-психологічного стереотипу, що сприяє зниженню морально-психологічної стійкості, надійності, рівня морально-психологічного стану.

В загальному випадку стратегічна ІП операція задається безліччю $\Psi_{атк/іп}$ ІП атак на підлітків.

Порушення інформаційної безпеки підлітка полягає у:

1) порушенні стану захищеності психіки та здоров’я людини від деструктивного інформаційного впливу, який призводить до неадекватного сприйняття нею дійсності та (або) погіршення її фізичного стану;

2) руйнуванні моральних цінностей, підрив морального й фізичного здоров’я нації;

3) втрати довіри до влади з боку значної частини населення внаслідок поширення компромату, застосування “брудних” політичних технологій, особливо під час виборчих кампаній.

Результатом (***збитком***, наслідками) дії деструктивного безпосереднього ІП впливу на підлітка в далекій і ближній перспективі може бути:

- формування в інтересах протиборчої сторони (тобто в розріз інтересам суспільства і держави) відповідних стереотипів, переконань, моделей поведінки; зміна світогляду в бік негативних деструкцій;

- формування лояльного ставлення до процесів, явищ, подій, що відбивають або відбуваються в інтересах протиборчої сторони, і відповідно формування деструктивного ставлення до процесів і подій, які відображають інтереси політичних и громадських організацій, держави;

- формування пріоритетів і ціннісних орієнтирів індивіда в напрямку деградації суспільства і ослаблення почуття патріотизму, духовності;

- формування образу мислення сприятливого для здійснення маніпуляцій з боку протиборчої системи;

- відтік інтересів особистості (груп індивідів) від значущих і стратегічно важливих для суспільства і держави відповідних процесів і дій;

- блокування і створення перешкод щодо процесів передачі знань, досвіду, інтеграції особистості в культурно-історичні, соціально-економічні процеси суспільства і держави;

- нав'язування почуття безвиходу і неможливості виходу в складній життєвій ситуації; суїцидальна спрямованість;

- створення умов для підвищення невизначеності соціальної позиції і підвищення ймовірності прийняття рішень, пов'язаних з ризиком для здоров'я і життя підлітка. вчинення правопорушень і іншим протиправним діям;

- формування у особистості негативних переконань, моралі, ідеалів, одним словом, таких цінностей, як індивідуалізм, егоїзм, націоналізм, вживання алкоголю і наркотиків, політичної індиферентності, скепсису і нігілізму.

Тут формується множина $\Psi_{шк}$ збитків як з позиції розвитку особистості підлітків, так і з позиції їх інформаційної безпеки.

На основі викладеного матеріалу можна зробити наступні висновки:

1. Показано, що найбільш вразливим (критичним) сегментом соціуму щодо порушення категорій інформаційної безпеки в наслідку дії деструктивних інформаційно-психологічних атак є підліткове покоління.

2. Обґрунтовано, що деструктивні інформаційно-психологічні атаки на свідомість і підсвідомість підлітків є найбільш актуальними та значущими.

2.1. Найбільша актуальність ДІП атак пояснюється тим, що:

а) по-перше рівень інформаційної затребуваності і засвоєння знань (*інформаційна пропускна здатність по сприйняттю інформації*) у підлітків зростає швидше, ніж рівень їх морально-психологічного стану, соціального інтегрованості, критичного аналізу і осмислення одержуваної інформації (*низький рівень критичної фільтрації інформації*);

б) по-друге на формування морально-етичних, психологічних установок підлітків значущий вплив надає ближня соціальне середовище (сім, друзі, школа, соціальна група), в свою чергу на яку також виявляється деструктивний ІП вплив в умовах значної залежності від дестабілізації соціально політичної сфери діяльності держави;

в) по-третє підліткове покоління відрізняється чутливістю щодо внутрішньодержавних дестабілізуючих чинників.

2.2. Значимість ДІП атак на підлітків обумовлена тим, що в цьому випадку:

- по-перше, в ближній перспективі досягається модифікація психологічного стану підлітка через його свідомість і підсвідомість в сторону деструктивності, що веде до збитку для його здоров'я і життя і неблагополучного подальшого розвитку;

- по-друге, в далекій перспективі утворюються наслідки які будуть відо-

бражатися на життєдіяльності всього соціуму і національної безпеки держави.

3. Показано, що на відміну від інших сегментів соціуму на підліткове покоління реалізація ДІП атак може здійснюватися через більш розширене кількість каналів комунікації: інфокомунікаційної, соціотехнічної і соціального середовища. Тому потрібно виявити найбільш ключові комунікаційні канали, через які здійснюється шкідливий ІП вплив на підлітків, тобто там де існують найбільші ризики для втрати інформаційно-психологічної безпеки підлітків.

1.4 Обґрунтування значущості інфокомунікаційних каналів як інформаційного середовища проведення деструктивних інформаційно-психологічних атак на підлітків

У загальному випадку весь сучасний інформаційний простір (інформаційне середовище) можна розділити на два компоненти:

I. Вербальні канали комунікації.

1. Соціальні канали (канали особистого спілкування), включаючи: соціальні канали ближнього середовища (сім'я, друзі, школа, близьке оточення); соціальні канали далекого середовища (навколишнє населення, соціальні групи агенти впливу, державні структури).

2. Канали друкованої інформації. Друковані інформаційні матеріали, газети, журнали, листівки, рекламні оголошення,

3. Інформаційно-технічні канали, це такі інформаційні канали які формуються з використанням сучасних технічних засобів, включаючи Інтернет, мобільні мережі, TV-канали, радіо,

II. Невербальні канали комунікації. Через поведінку, емоції оточуючих, через умови навколишнього середовища (море, ліс, пустеля, дощ, спека, холод, шум транспорту та ін.)

Можна виділити наступні канали комунікаційного впливу на підлітків у сучасному інформаційному просторі (рис. 1.5).

Як показує практика сучасного розвитку суспільства найбільш затребуваними каналами для комунікаційної взаємодії та отримання інформації підлітками є інфокомунікаційні канали (безліч таких каналів позначається як $\Psi_{ік/к}$). Тут найбільш ефективними каналами комунікаційного впливу є ***Інтернет і телебачення*** (ТБ). Відповідні результати соціологічних опитувань представлені у вигляді кругових діаграм на рис. 1.6. Тут представлені статистичні дані по затребуваності різних джерел інформації [80-82, 84]. Як видно з аналізу діаграм на рис. 1.6 з п'яти найбільш популярних джерел інформації найбільш затребуваними є Інтернет і телебачення (до 48%) [80-82, 84].

Відповідно затребуваність в цих джерелах інформації серед різних вікових категорій нашої держави наведені у вигляді діаграм на рис. 1.7. Звідки можна зробити висновок, що:

- найбільшою (значущою) популярністю Інтернет користується серед підлітків і молоді з віковою категорією від 14 до 20 років. Тут затребуваність Інтернет ресурсів досягає 70%, що є підтвердженням його абсолютної переваги (цінності) щодо інших джерел інформації і свідчить про наростання нових інформаційно-комунікаційних традицій у підліткового покоління.

У міру дорослішими категорії населення зростає популярність TV-каналів, що досягає до 55%. При цьому частка затребуваності Інтернет ресурсів не опускається нижче 35%, тобто залишається значущим джерелом інформації.

Слід також зазначити, що при цьому Інтернет ресурси і TV-канали є джерелами інформації з найбільш високим рівнем довіри (до 60%). Це підтверджується аналізом відповідної діаграми на рис. 1.8 [80-82, 84].

Значить, Інтернет ресурси і TV-канали мають найбільший попит і довіру серед джерел інформації, якими користуються підлітки і молодь.

З аналізу статистичних даних за ступенем доступності до інформаційно-комп'ютерних технологій можна відзначити наступне: доступ до комп'ютерних технологій існує не менше, ніж у 85% підлітків і молоді у віці 12 - 30 років, в тому числі 80% мають комп'ютер вдома, 30% мають доступ до комп'ютера за місцем роботи, до 5% - в Інтернет кафе, клубах [80-82, 84].

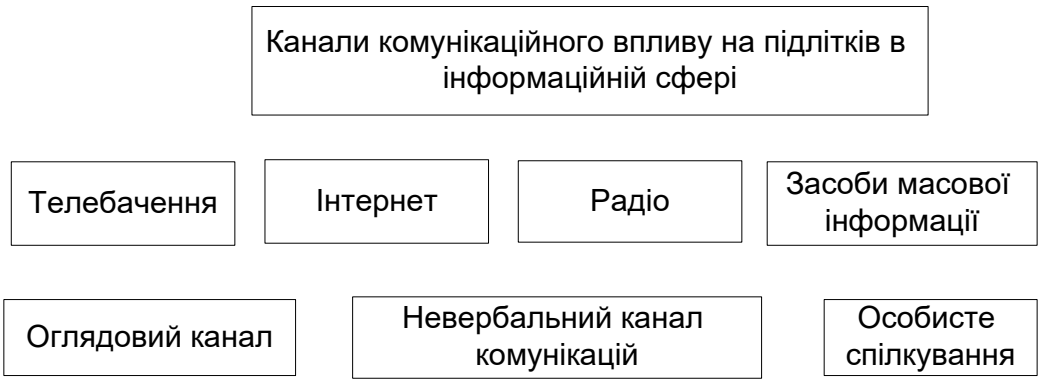


Рисунок 1.5 –Канали комунікаційного впливу на підлітків у сучасному інформаційному просторі

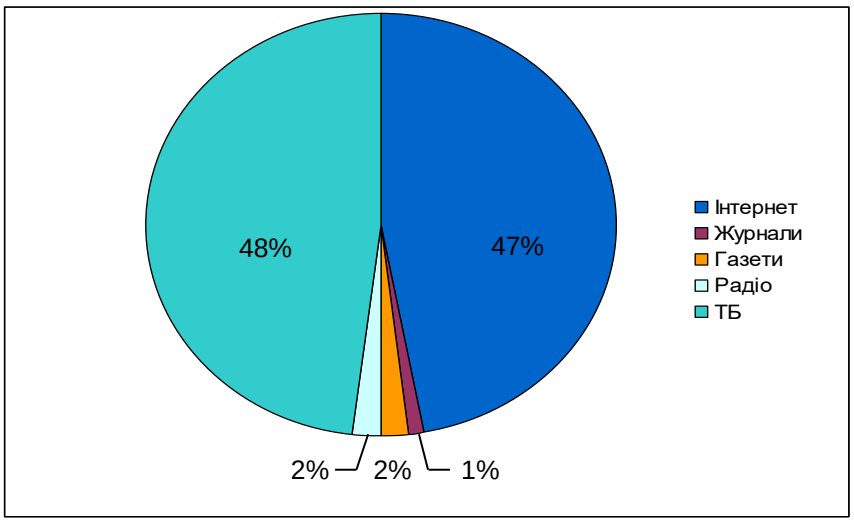


Рисунок 1.6 – Розподіл рівня затребуваності різних джерел інформації

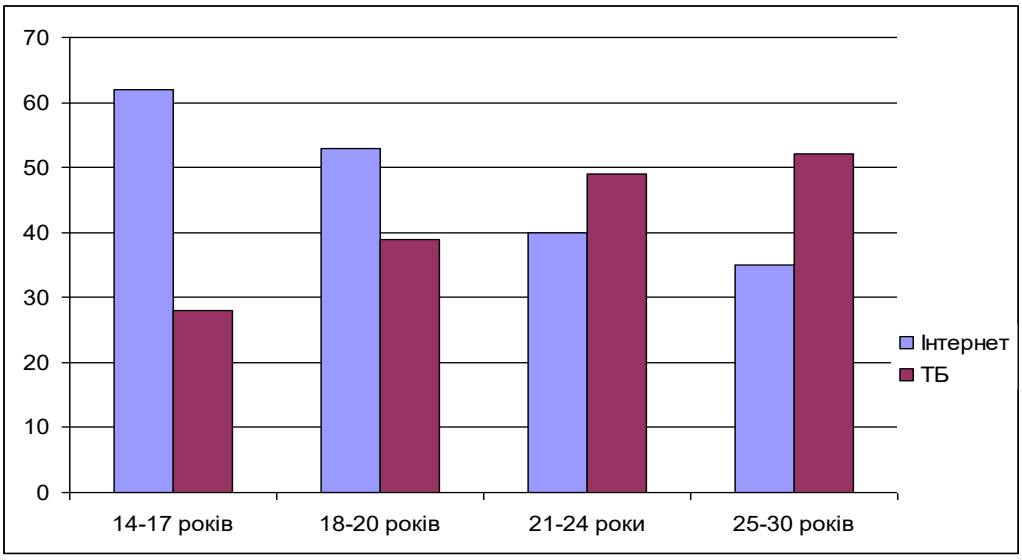


Рисунок 1.7 – Залежність затребуваності Інтернет ресурсів та TV-каналів від вікової категорії населення України

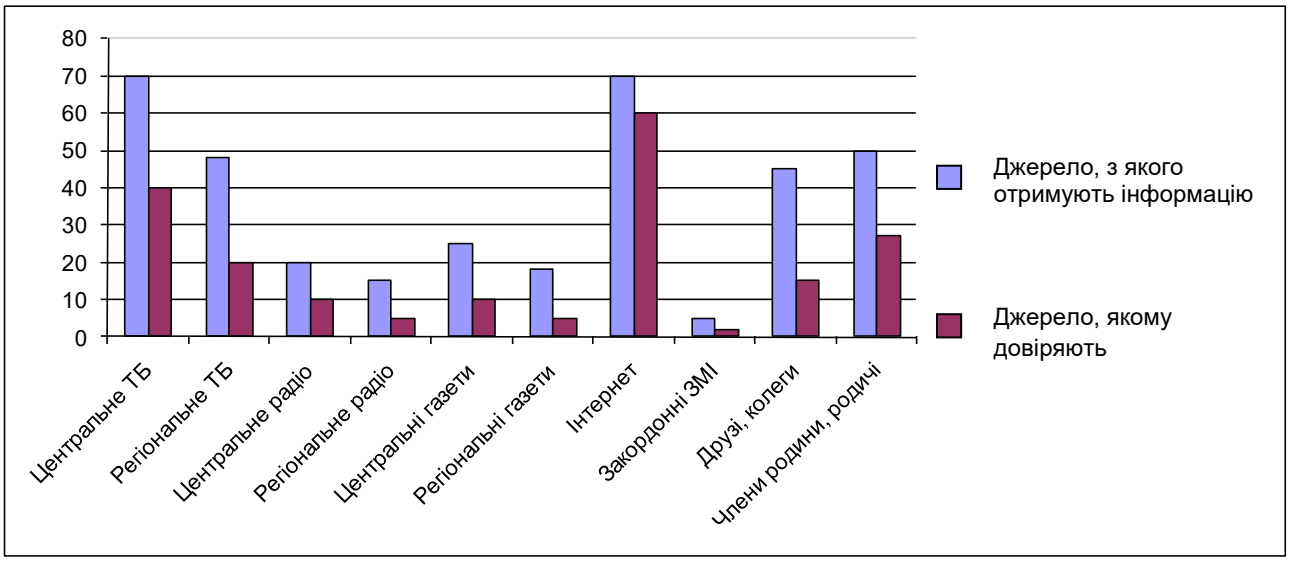


Рисунок 1.8 – Рейтинг довіри джерел інформації

При цьому серед підлітків і молоді у віці від 12 до 30 років, які використовують Інтернет ресурси, частка тих які роблять це: практично щодня досягає 80%, кілька разів на тиждень - 15%; кілька разів на місяць - 3%; не менше разу на півроку - 2% [80-82, 84]. При цьому слід зауважити, що сучасні соціальні мережі стають основним місцем проведення дозвілля, спілкування і розваги підлітків і молоді, а саме 20% юнаків і дівчат весь свій вільний час витрачають на соціальні мережі; 57% проводять там кілька годин в день, 20% респондентів відвідують соціальні мережі декілька разів на тиждень; лише 3% заходять не частіше ніж один раз на місяць. Тут в результаті проведеного дослідження було діагностовано, що найпопулярнішими віртуальними соціальними мережами серед підлітків і молоді незважаючи на законодавче обмеження продовжують залишатися: "ВКонтакте" (82% в ній зареєстровані); "Однокласники" (62% в ній зареєстровані); "Мій світ" (41% в ній зареєстровані). Подальший рейтинг популярності розподілився наступним чином: **YouTube** – до 70% опитаних знають про існування цієї соціальної мережі і 30% респондентів в ній зареєстровані; 40% респондентів знають про існування сайтів знайомств і 10% з них гам зареєстровані і активно спілкуються; 30% респондентів знають про наявність такої соціальної мережі, як "Фотострана", і 15% з них в ній зареєстровані. Також респонденти були інформовані про існування таких мереж, як "Моє коло" (25% знають і 5% зареєстрованих користувачів), **Facebook** (96% знають і 80% зареєстровано) та мережу **Twitter** (10% знають і 3% зареєстровані).

У загальному вигляді розподіл затребуваності підлітків за типами Інтернет ресурсів наведено у вигляді кругових діаграм на рис. 1.9.

Рисунок 1.9 –Розподіл затребуваності Інтернет ресурсів в залежності від їх типів

Звідки провівши аналіз, можна зробити висновок, що соціальні мережі та онлайн ігри займають до 80% питомої затребуваності всіх типів Інтернет ресурсів.

Таким чином, по представленому матеріалу можна зробити висновок, що:

1. Серед всіх комунікаційних каналів Інтернет ресурси і TV-канали мають найбільший попит і являються найбільш довіреними джерелами інформації серед підлітків і молоді, а саме: популярність і затребуваність досягає 70%, а рівень довіри 60%; рівень доступності до таких інформаційних каналів досягає не менше 85%, а тривалість доступу до Інтернет ресурсів в середньому від 5 до 7 годин на добу.

2. Серед різних типів Інтернет ресурсів найбільш популярними і затребуваними є соціальні мережі до 60%. При цьому популярними віртуальними соціальними мережами серед підлітків і молоді незважаючи на законодавче обмеження продовжують залишатися: "ВКонтакте" (рівень використання 82%); "Одноклассники" (рівень використання 62%).

3. Формуються два фундаментальних дисбаланси.

3.1. ***Дисбаланс*** на рівні розвитку інформаційної культури підлітків, а саме ступінь затребуваності нових знань та адаптації до новітніх наукомістких інфокомунікаційних технологій зростає швидше в порівнянні з темпами психологічного розвитку підлітків, їх рівня критичного осмислення інформації.

3.2. ***Дисбаланс*** на рівні використання комунікаційних каналів отримання інформації, обумовлений довірою до таких джерел інформації як Інтернет ресурси, а саме:

1) з одного боку різко зменшується потенціал державних інститутів у формуванні масової свідомості сучасної молоді і підлітків;

2) з іншого боку віртуальний соціокультурний простір в силу своєї доступності і поширеності стає одним з найбільш сприятливих сфер для виникнення нових, ***не інституційних каналів*** творчої та комунікативної самореалізації підлітків.

4. З урахуванням такого дисбалансу виникає ***концептуальне протиріччя*** (рис. 1.10).

I. З одного боку інтеграція України в світовий інформаційний та соціотехнічний простір, розвиток аспектів інформатизації держави, розвиток і взаємна інтеграція різних технологій, а саме інформаційних, комп'ютерних і телекомунікаційних призводять до того, що:

1) інформаційні та комп'ютерні технології стають більш доступними і мобільними. Створюються умови для підвищення інформатизації суспільства, створення комфортних умов для розвитку особистості. Роль масових комунікацій в соціалізації підлітків і молоді, формування її світогляду в умовах інформатизації держави стає ключовою;

2) зростає затребуваність і доступ щодо використання сучасних ІК технологій, включаючи Інтернет ресурси та цифрове TV;

3) підвищується довіра з боку підлітків до таких комунікаційних каналів отримання інформації як Інтернет ресурси та TV-канали.

В результаті підвищується рівень інформованості підлітків.

II. З іншого боку інтеграція України в в світовий інформаційний та соціотехнічний простір, розвиток аспектів інформатизації держави призводять до того, що:

1) створюється ***потенціал*** для більш швидкого і ефективного проникнення деструктивного інформаційного контенту в інфокомунікаційних простір;

2) створюється ***потенціал*** для збільшення охоплення аудиторії підлітків для проведення деструктивного інформаційно-психологічного впливу.

В результаті формується безліч загроз втрати інформаційно-психологічної безпеки підлітка.

Рисунок 1.10 – Структурна схема формування концептуального протиріччя відносно забезпечення інформаційно-психологічної безпеки підлітків в інфокомунікаційному просторі

Тоді в умовах наявності безлічі дестабілізуючих внутрішньодержавних чинників, недостатньою контрольованості такого простору як Інтернет і двох дисбалансів, а саме: на рівні інформаційної культури підлітка; на рівні використання джерел комунікаційних каналів виникають суттєві втрати ІП безпеки підлітків.

Тому ***науково-прикладна задача***, яка полягає у підвищенні інформаційної безпеки підлітків щодо деструктивних інформаційно-психологічних впливів в інфокомунікаційному просторі, ***є актуальною***.

У формалізованому вигляді постановка науково-прикладної задачі з позиції зниження ефективності дії деструктивних інформаційно-психологічних впливів задається наступним виразом. Потрібно мінімізувати ймовірність $P_{дмо}$ модифікації психологічного стану підлітка, тобто ймовірність деструкції його вихідного психологічного стану $w_{поч}$ в деградаційне $w_{вих}$, в слідстві дії безлічі шкідливих ІП впливів $\Psi_{атк/іп}$ в множині $\Psi_{ік/к}$ інфокомунікаційних каналів в умовах наявності множини $\Psi_{зіб}$ загроз ІП безпеки, безлічі дестабілізуючих факторів $\Psi_{дф}$ і множини $\Psi_{вібо}$ вразливостей інформаційної безпеки особистості, а саме:

$$P_{дмо} : w_{поч} \xrightarrow{\{\Psi_{атк/іп};\Psi_{зіб};\Psi_{ік/к};\Psi_{дф};\Psi_{вібо}\}} w_{вих} \to \min, \qquad (1.6)$$

щоб в кінцевому підсумку забезпечити мінімізацію можливих збитків соціуму, особистості і держави, тобто:

$$\rho_{шк} \to \min \qquad (1.7)$$

або

$$\Psi_{атк/іп} : \{\Psi_{дзіб}; \Psi_{вібо}\} \to \Psi_{шк} \to \min. \qquad (1.8)$$

Тут $\Psi_{шк}$ - множина шкоди від дії деструктивних ІП атак; $\Psi_{дзіб}$ - множина джерел загроз інформаційно-психологічної безпеки.

Для вирішення сформульованої науково-прикладної задачі пропонується розробити підхід і інформаційну технологію для забезпечення протидії загрозам інформаційно-психологічної безпеки підлітків.

1.5. Обґрунтування необхідності створення інформаційної технології забезпечення безпеки підлітків

Ключовою складовою попередження, виявлення, ідентифікації, локалізації і протидії загрозам в інформаційно-психологічному просторі є спеціальні державні відомства, включаючи підрозділи сил спеціальних операцій, підрозділи інформаційної пропаганди, засоби масової інформації. Тут частково закриваються питання щодо протидії деструктивному ІП впливу (операціями) в Збройних Силах України. У той час як питанням інформаційної безпеки підлітків і молоді на законодавчому та організаційному рівні приділяється недостатня увага. Відсутні як спеціальні законодавчі акти, так і організаційно-штатні структури, які б займалися таким напрямком. Відсутні також методики і спеціальні інформаційні технології, використання яких дозволить здійснювати ефективну протидію деструктивним ІП атакам. В цьому напрямку необхідно виконати такі заходи:

1. Прийняти закон про інформаційну безпеку дітей, за прикладом як це вже зроблено в розвинутих державах.

2. Створювати спеціалізовані центри ІП підтримки підлітків та молоді, впроваджувати посади спеціалістів з інформаційної безпеки підлітків.

3. Розробляти спеціальні інформаційні технології для підтримки прийняття рішень в процесі моніторингу стану інформаційних ресурсів на предмет наявності шкідливих інформаційних контентів.

4. Забезпечити спеціальними інформаційними технологіями спеціалізовані центри прогнозу та виявлення деструктивностей в поведінці і психологічному розвитку підлітків та молоді.

На всіх рівнях підтримки і прийняття рішень, моніторингу інформаційного та соціального просторів України, важливим постає питання про необхідність розробки і подальшого удосконалення інформаційної технології забезпечення інформаційно-психологічної безпеки підлітків.

Отже необхідно створити ***інформаційну технологію*** забезпечення інформаційної безпеки особистості, використовуючи одночасно як базові складові тех-

нологічні аспекти інформаційно-технічних та інформаційно-психологічних технологій.

Інформаційно-технічні технології, як складова протидії ІП атакам – це комплексне застосування методів та засобів збору, обробки, передачі, аналізу, консолідації та розпізнавання інформації від різних джерел з використанням апаратно-програмних засобів комп'ютерних систем та комунікаційних мереж.

Інформаційно-психологічні технології, як складова протидії ІП атакам – це широкомасштабне застосування методів і засобів виявлення, розпізнавання та блокування деструктивних інформаційно-психологічних атак як на свідомість, так і на підсвідомість особистості.

В процесі розробки і вдосконалення таких інформаційних технологій необхідно враховувати наступні аспекти:

1) необхідність використання в процесі обробки ІР етапів, для яких обробка буде проводитися як в автоматичному, так і в автоматизованому режимах;

2) складність організації фільтрації (детектування, розпізнавання) ІР на наявність в них деструктивного впливу. Це обумовлено необхідністю використання комплексних інформаційно-технологічних фільтрів, які здійснюють перевірку інформаційних потоків на наявність деструктивності з урахуванням таких концептів:

по-перше деструктивна трансформація проводиться одночасно за трьома інформаційними каналами, а саме: на рівні ключових слів; на рівні змісту інформаційного ресурсу; на сугестивному рівні;

по-друге деструктивна модифікація здійснюється в статичному і динамічному розгляді документу;

по-третє в умовах використання протиборчої стороною різних технологій маскування, в тому числі і стеганографічні технології приховування шкідливої інформації. Маскування деструктивних інформаційно-психологічних впливів під інформаційні ресурси конструктивного змісту (використовувані в інтересах державної пропаганди);

по-четверте сама така обробка є наукомісткою (нетривіальною), і пов'язана з необхідністю створення і розвитку спеціального математичного апарату, який

потребує значних витрат інформаційних та обчислювальних ресурсів;

по-п'яте те, що інформаційне протиборство характеризується динамічністю і постійним вдосконаленням технологій противника. Тому інформаційні технології протидії повинні бути адаптивними своєчасно або з випередженням реагувати на впровадження нових засобів і технологій протиборчої стороною.

3) протиборча сторона задіє безліч різних інформаційних і соціо-технічних каналів для здійснення інформаційно-психологічних операцій, включаючи Інтернет ресурси, TV-канали, створення інформаційних каналів (телеграм-канал), і каналів широкоефірної розсилки повідомлень через мобільні мережі, віртуальні спільноти, сім'я , друзі, колектив навчального закладу (школа, інститут), різні агенти впливу;

4) різке зростання кількості різних за своєю природою віртуальних спільнот і сайтів. Відповідно зростання кількості користувачів підліткового віку і часових показників щодо їх знаходження на сайтах різних віртуальних спільнот;

5) проведення ІП операцій з боку безлічі держав, що переслідують свої інтереси, і відповідно використовують на інформаційному просторі нашої держави одночасно сплетення різних інформаційних технологій деструктивного ІП-впливу;

6) обробка в реальному часі інформаційних ресурсів з високою бітовою інтенсивністю, тобто мають значний цифровий обсяг синтаксичного опису;

7) обробка і фільтрація інформаційних потоків від великої кількості джерел інформації.

Таким чином, ефективне вирішення питань протидії ІП впливу противника – це надзвичайно складний, багаторівневий процес. Такі інформаційні технології пропонується формувати з використанням чотирьох мережевих рівнів обробки інформаційних потоків, а саме: мережа засобів виявлення вразливостей; мережа засобів прогнозування, управління та коректування ІП впливом; мережа засобів і технологій і методик реалізації ІП впливу; мережа засобів оцінки деструктивного ІП впливу. Тому до основних функцій інформаційних технологій забезпечення інформаційної безпеки особистості щодо деструктивного ІП впливу відносяться:

- безперервне і періодичне оцінювання стану (моніторинг) інформаційного

простору з позиції наявності деструктивних інформаційних ресурсів та їх джерел;

- збір, прийом, передача, обробка, узагальнення, зберігання, аналіз і відображення інформації про стан інформаційного, соціально-інформаційного простору;

- оперативне відображення і реєстрація відомостей про факти виявлення джерел деструктивних ІП впливів,

- інформаційно-технічна підтримка в автоматичному і автоматизованому режимах процесів виявлення, ідентифікації, блокування і протидії загрозам деструктивного ІП впливу;

- ідентифікація та розпізнавання деструктивних ІП впливів, оцінка їх взаємозв'язків і джерел;

- прогнозування процесів, пов'язаних з одного боку з поширенням шкідливих ІР і оцінки рівня ефективності деструктивного ІП впливу, а з іншого боку з оцінкою ефективності блокування джерел деструктивного ІП впливу;

- адаптація інформаційної технології з урахуванням виявлення нових класів і джерел загроз;

- підготовка даних і організація обміну між суміжними (сусідніми) і вищестоящими рівнями системи забезпечення національної безпеки держави в інформаційній сфері.

Структурно-функціональна схема базового концепту інформаційної технології забезпечення інформаційно-психологічної безпеки підлітків представлена на рис. 1.11.

На рис. 1.11 прийнятті наступні позначення каналів передачі даних:

– інформація щодо аналітичної діяльності;

– інформація стосовно фільтрації (виявлення, детектування наявності інформаційних деструктивних модифікацій інформаційних ресурсів;

– інформація щодо управлінських рішень

Таким чином, розроблена концептуальна структура інформаційної технології забезпечення інформаційно-психологічної безпеки підлітків щодо впливу інформаційних деструктивних трансформацій на їх підсвідомість і свідомість.

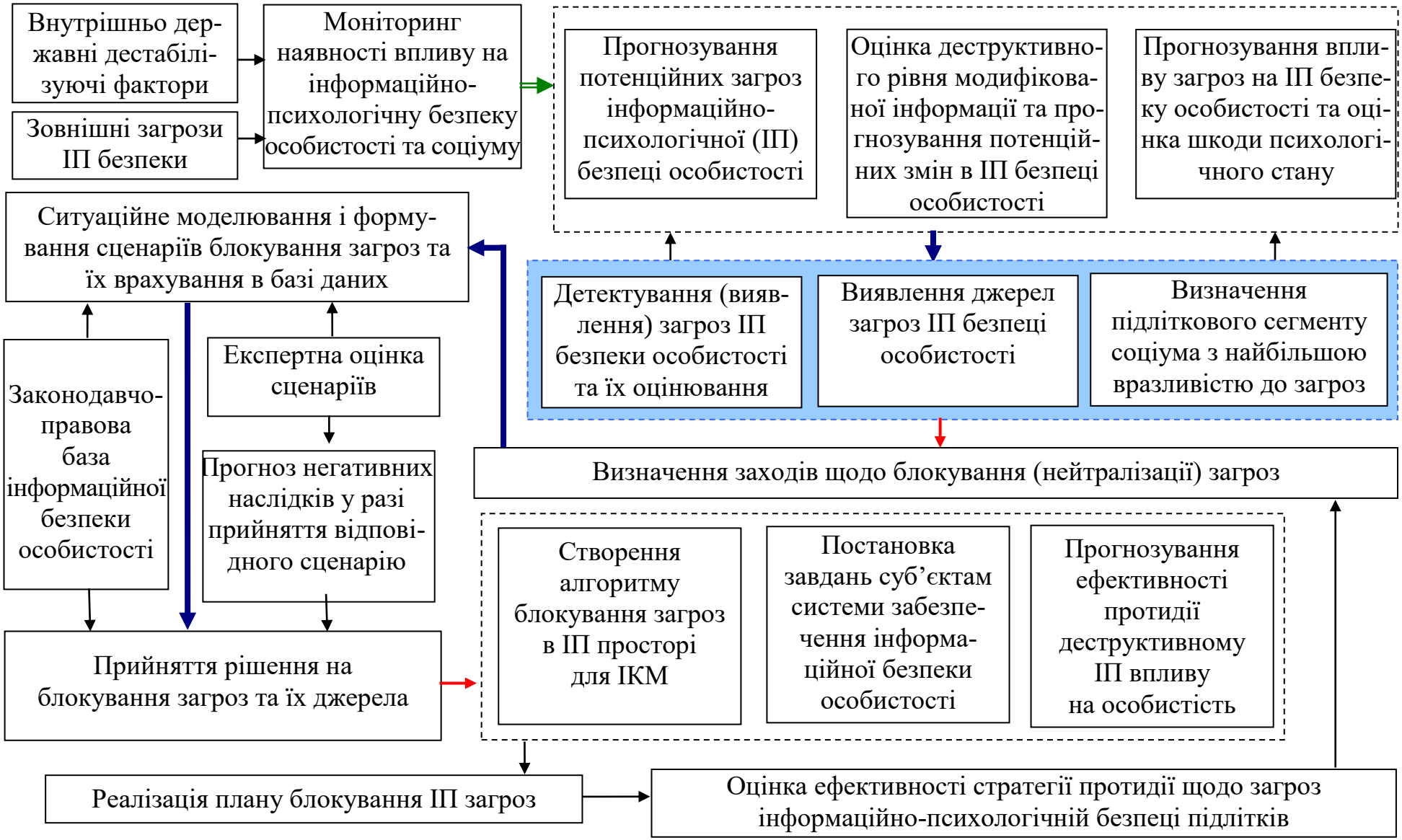


Рисунок 1.11 – Структурно-функціональна схема базового концепту інформаційної технології забезпечення інформаційно-психологічної безпеки підлітків

1.6. Постановка мети і задач на дослідження

Як показує аналіз базових складових інформаційної технології забезпечення інформаційної безпеки підлітків одним з ключових її технологічних етапів є методи виявлення (детектування) наявності ІП деструкцій в інформаційних ресурсах.

Обґрунтування значущості методів виявлення (детектування, фільтрації, розпізнання) наявності деструктивних трансформацій в інформаційних ресурсах наведено на рис. 1.12.

Для оцінки якості функціонування методу виявлення деструктивного ІП впливу пропонується використовувати такі показники:

1. Імовірність $P_{віпв}$ виявлення наявності ІП впливу в інформаціойному ресурсі:

$$P_{віпв} = n_{ірв} / n_{ір}, \tag{1.9}$$

де $n_{ірв}$ - кількість деструктивно-модифікованих ІР, які були виявлені в процесі їх аналізу; $n_{дір}$ - кількість ІР, модифікованих інформаційною деструкцією

$$n_{ір} = n_{дір} + n_{кір} \tag{1.10}$$

$n_{ір}$ - кількість аналізованих інформаційних ресурсів; $n_{кір}$ - кількість конструктивних ІР, тобто кількість ІР незаражених деструктивними модифікаціями.

2. Помилка ν_1 першого роду, тобто ймовірність події, коли ІП атака не була виявлено

$$\nu_1 = \bar{n}_{іпа} / n_{дір}, \tag{1.11}$$

де $\bar{n}_{іпа}$ - кількість невиявлених деструктивних ІП атак.

3. Помилка ν_2 другого роду, тобто ймовірність події, коли за деструкцію була прийнята конструктивна інформація

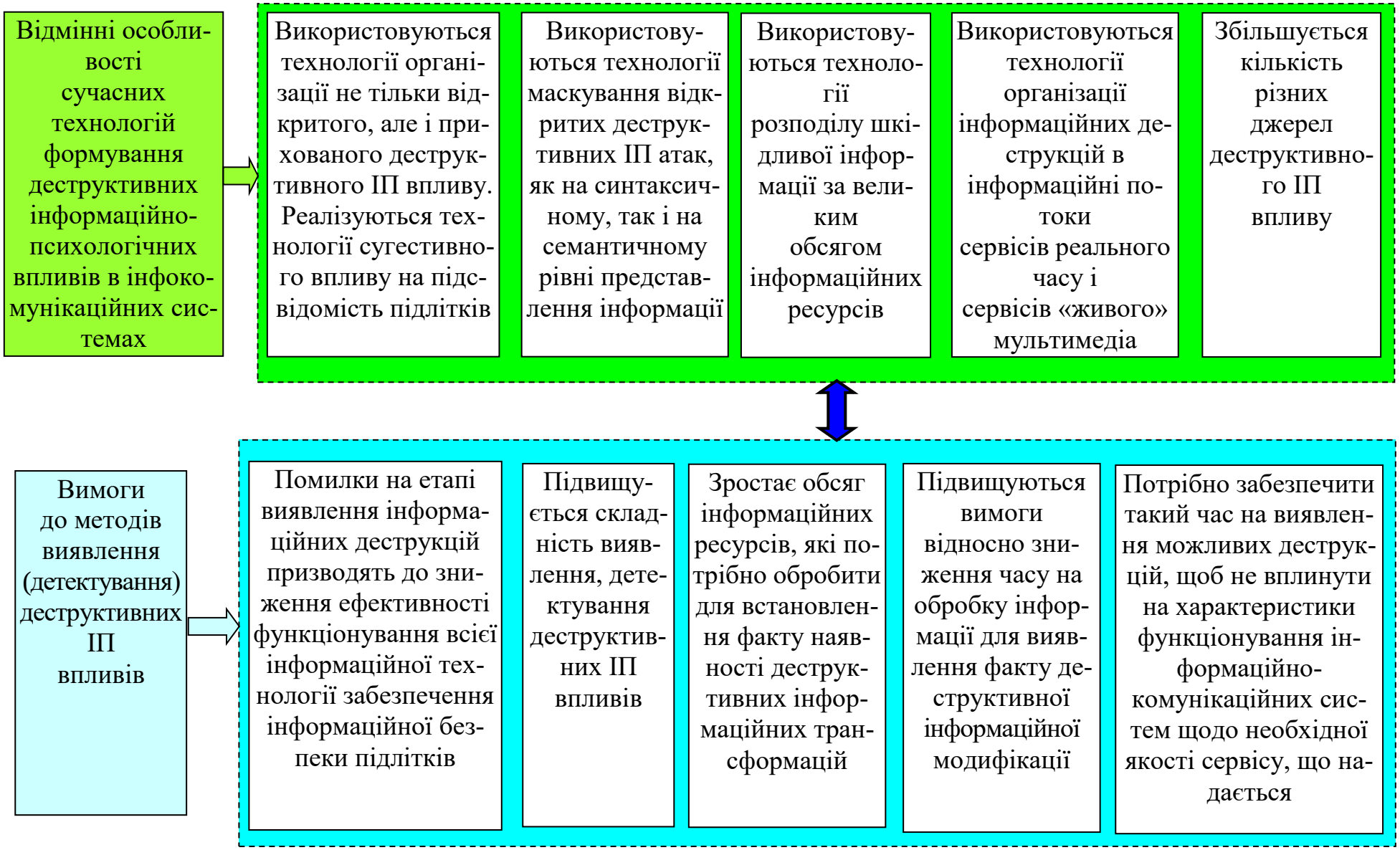


Рисунок 1.12 – Структурна схема обґрунтування значущості методів детектування деструктивних інформаційних модифікацій для інформаційної технології забезпечення інформаційної безпеки підлітків

$$\nu_2 = \bar{n}_{кір} / n_{кір}, \qquad (1.12)$$

$\bar{n}_{кір}$ - кількість конструктивних інформаційних ресурсів, які в процесі аналізу були оцінені як трансформовані інформаційними деструкціями.

4. Часові витрати $t(w_{min})_{обр}$ на обробку інформаційних ресурсів для виявлення деструктивних інформаційних модифікацій, залежне від продуктивності обчислювальних систем і мінімально достатнього об'єму w_{min} інформації, який потрібен для прийняття відповідного рішення.

5. Мінімально необхідний і достатній обсяг w_{min} інформаційного ресурсу для того, щоб забезпечити можливість для його детектування на наявність деструктивних інформаційних трансформацій

Низька якість функціонування методів виявлення (детектування) наявності ІП деструкцій в інформаційних ресурсах неминуче спричинить за собою зниження ефективності всієї інформаційної технології забезпечення ІП безпеки підлітків. Однак сфера розробки таких технологічних рішень знаходяться в критичному стані. Відповідні технології мають недостатній рівень розвитку, щоб бути адекватними існуючим інформаційно-технологічними можливостями протиборчої сторони щодо організації та проведення деструктивного ІП впливу. Наприклад, методи пошуку, аналізу, складання та формування текстів (інформації) представлені дуже широко. Але системи, що реалізують ці методи, не завжди придатні для ведення ІП протиборства. Більшість реалізованих систем, які застосовуються для аналізу та формування текстів із заданими параметрами впливу, орієнтовані на російськомовні тексти і є вузьконаправлені. Ще одним недоліком більшості цих систем є те що вони є закордонними. При цьому використання закордонних інформаційних технологій протидії деструктивному ІП впливу є обмеженні у зв'язку з тим, що для більшості цих систем є відсутність опису їх математичної бази та існує заборона урядів більшості держав на експорт даних продуктів в повному обсязі [2, 36, 64, 65].

Отже в процесі (розробки інформаційної технології) забезпечення інформаційної безпеки підлітків щодо деструктивних ІП впливів в умовах міжнародної інтеграції України в світовий інформаційний простір, інформаційної та гібридних

війн, інформатизації держави і внутрішньодержавних дестабілізуючих факторів існує наступна структура ієрархій ***комплексного протиріччя*** (рис. 1.13):

1. Протиріччя на рівні розвитку і взаємної інтеграцією різних технологій, а саме інформаційних, комп'ютерних і телекомунікаційних. З одного боку інформаційні технології стають більш доступними і мобільними. Створюються умови для підвищення інформаційної безпеки держави, інформатизації суспільства, створення комфортних умов для розвитку особистості. З іншого боку створюються умови для більш швидкого і ефективного проникнення деструктивного інформаційного контенту і охоплення своїм деструктивним ІП впливом набагато більшого сектора соціуму. При цьому для віртуального соціокультурного простору стає характерним витіснення державних інститутів у формуванні масової свідомості сучасної молоді і підлітків на не інституційні канали творчої та комунікативної самореалізації підлітків. Підлітки отримують доступ до віртуальних соціальних просторів, які мають законодавчі обмеження (Однокласники, ВКонтакт). В умовах дисбалансу на рівні інформаційної культури підлітків така ситуація призводить до зростання загроз їх інформаційно-психологічної безпеки до ***критичного рівня***.

Під ***критичним рівнем загроз інформаційно-психологічної безпеки підлітків розуміється стан***, для якого відбувається найбільш висока актуальність і значимість загроз на системному рівні, що в умовах: інформаційної війни, світової інформаційної інтеграції та розвитку інформаційно-технічних засобів для реалізації ІП атак; внутрішньодержавних дестабілізуючих факторів, дисбалансу на рівні розвитку інформаційної культури підлітків, неминуче тягне за собою непоправиму шкоду національній безпеці держави, здоров’ю та життю підлітків.

2. Протиріччя на рівні інформаційно-технологічного розвитку, обумовлене відставанням вітчизняних засобів і технологій протидії деструктивному ІП впливу щодо інформаційно-технологічним можливостям протиборчої сторони. З одного боку (з боку протиборчої сторони) забезпечуються всебічні умови для створення та розвитку інформаційних технологій реалізації операцій деструктивного ІП впливу. З іншого боку рівень розвитку вітчизняних інформаційних технологій протидії, включаючи засоби масової інформації недостатній для організації ефективної інформаційної боротьби.

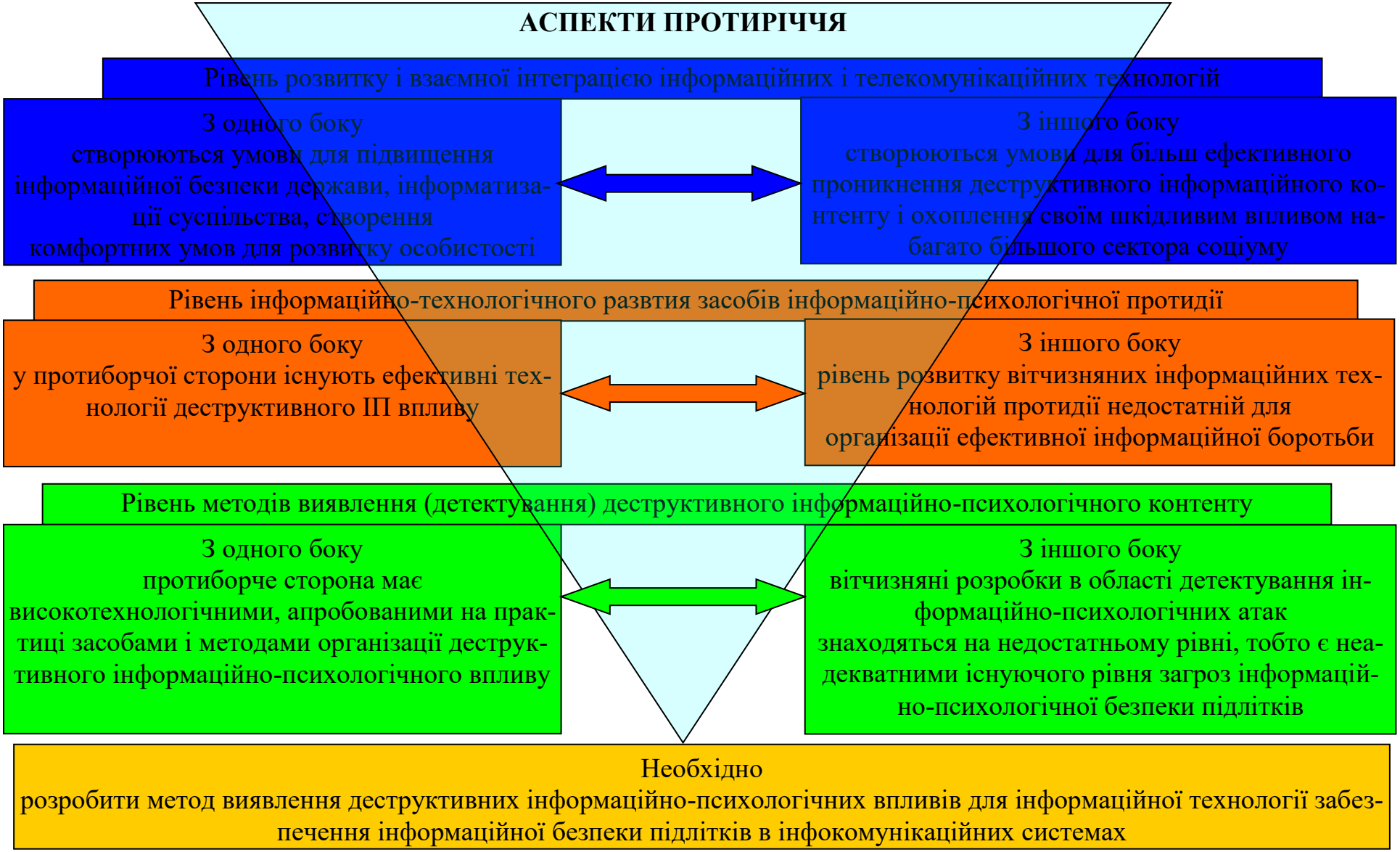


Рисунок 1.13 – Структурна схема ієрархії комплексного протиріччя процесі розробки інформаційних технологій забезпечення інформаційно-психологічної безпеки підлітків

3. Рівень розробки і удосконалення методів виявлення (детектування) ІП атак. З одного боку протиборча сторона має високотехнологічні, апробовані на практиці засоби та методами організації деструктивного ІП впливу. З іншого боку вітчизняні розробки в області виявлення ІП атак знаходяться на недостатньому рівні, тобто є неадекватними існуючому рівню загроз ІП безпеки підлітків.

Отже, можна стверджувати, що розробка методу виявлення деструктивних інформаційно-психологічних впливів для інформаційної технології забезпечення інформаційної безпеки підлітків в інфокомунікаційних системах, є ***актуальною тематикою науково-прикладних досліджень***.

Таким чином, ***ціль досліджень*** полягає в розробки методу виявлення деструктивного ІП впливу в інформаційно-комунікаційному просторі для інформаційних технологій забезпечення безпеки підлітків.

Формалізоване трактування мети науково-прикладних досліджень представлено у наступному вигляді,

Потрібно створити такий метод виявлення деструктивних інформаційних трансформацій, який описується функціоналом $F_{вдіпа}$, щоб забезпечити максимальну ймовірність виявлення шкідливих (негативних) ІП атак (мінімізувати ймовірність $P_{дмо}$ модифікації психологічного стану підлітка):

$$F_{вдіпа} : P_{віпв} = n_{ірв} / n_{дір} \to \max \;\; и \;\; P_{дмо} \to \min \qquad (1.13)$$

при виконанні наступних умов:

$$\begin{cases} t(w_{min})_{обр} \le t_{потр}; \\ w_{min} \le w_{потр}. \end{cases} \qquad (1.14)$$

Тут $t_{потр}$ - обмеження на час виявлення деструктивних ІП атак; $w_{потр}$ - обмеження на мінімально необхідний і достатній обсяг інформаційного ресурсу для виявлення деструктивних трансформацій, коли досягається:

$$\nu_1 = \bar{n}_{\text{іпа}} / n_{\text{дір}} \rightarrow \min \text{ и } \nu_2 = \bar{n}_{\text{кір}} / n_{\text{кір}} \rightarrow \min, \quad (1.15)$$

де ν_1, ν_2 - відповідно помилки першого і другого роду.

Для досягнення мети необхідно вирішити такі завдання:

1. Побудувати модель загроз ІП безпеки підлітків в інфокомунікаційному просторі та обґрунтувати напрямок виявлення прихованих деструктивних інформаційно-психологічних впливів в інформаційних ресурсах для підвищення ефективності інформаційних технологій забезпечення ІП безпеки.

2. Розробити методи виявлення сугестивних деструктивних ІП атак на підсвідомість підлітків на основі семантичного диференціалу в інфокомунікаційному просторі.

3. Створити методи динамічного аналізу текстових інформаційних ресурсів в багатовимірному фонетичному просторі за лінгвістичними ознаками для виявлення сугестивних інформаційних деструкцій з маскуванням.

4. Розробити програмний продукт для методів виявлення сугестивних деструктивних ІП впливів в текстових ресурсах та оцінити їх ефективність.

Висновки за першим розділом

1. Забезпечення інформаційної безпеки є важлива сфера національної безпеки держави. Україна, в силу її геополітичного розташування, є об'єктом інтересів багатьох держав. Це обумовлює велику вірогідність втягування її в інформаційну війну, що останнім часом стає вже реальністю.

2. В умовах проведення гібридної і інформаційної війни з урахуванням наявності безлічі внутрішньодержавних дестабілізуючих факторів встановлюється наступне:

а) найбільший ефект в забезпеченні інформаційної переваги, і переваги в гібридній війні досягається у разі проведення ІП атак в порівнянні з атаками в інфокомунікаційному просторі. Це обумовлено наявністю дисбалансу між техноло-

гіями і механізмами інформаційного протиборства в Україні;

б) існує дисбаланс, обумовлений відставанням вітчизняних засобів і технологій протидії ІП впливу щодо інформаційно-технологічних можливостей протиборчої сторони в сфері інформаційно-психологічних операцій.

3. Показано, що найбільш вразливим сегментом соціуму щодо порушення категорій інформаційної безпеки внаслідок дії деструктивних ІП атак є підліткове покоління.

4. На основі статистичного аналізу результатів соціологічних опитувань і прогнозних моделей, отримані такі результати:

4.1. Серед всіх комунікаційних каналів Інтернет ресурси і TV-канали мають найбільший попит та довіру серед джерел інформації, якими користуються підлітки і молодь, а саме: популярність і затребуваність досягає 70%, а рівень довіри 60%, причому найбільш активна підліткова і молодіжна соціальна група у віці 12 - 22 років; рівень доступності до таких інформаційних каналів досягає не менше 85%, а тривалість доступу до Інтернет ресурсів в середньому від 5 до 7 годин на добу.

4.2. Серед різних типів Інтернет ресурсів найбільш популярними і затребуваними є соціальні мережі до 60%. При цьому найпопулярнішими віртуальними соціальними мережами серед підлітків і молоді незважаючи на законодавче обмеження продовжують залишатися: "ВКонтакте" (рівень використання 82%); "Одноклассники" (рівень використання 62%). Популярність ***Facebook*** досягає рівня 96% використання.

5. В результаті проведеного аналізу загроз інформаційно-психологічної безпеки підлітків в інфокомунікаційному просторі виявлено ***концептуальне протиріччя.***

5.1. З одного боку інтеграція України в світовий інформаційний та соціотехнічний простір, розвиток аспектів інформатизації держави, розвиток і взаємна інтеграція різних технологій, а саме інформаційних, комп'ютерних і телекомунікаційних призводять до того, що підвищується рівень інформованості підлітків, підвищується довіра з боку підлітків до таких комунікаційних каналів отримання інформації як Інтернет ресурси.

5.2. З іншого боку інтеграція України в світовий інформаційний та соціотехнічний простір, розвиток аспектів інформатизації держави призводять до того, що: створюється потенціал для більш швидкого і ефективного проникнення деструктивного інформаційного контенту в інфокомунікаційних простір; створюється потенціал для збільшення охоплення аудиторії підлітків для проведення деструктивного інформаційно-психологічного впливу.

Тоді в умовах наявності безлічі дестабілізуючих внутрішньодержавних чинників, недостатньої контрольованості такого простору як Інтернет і двох дисбалансів, а саме: на рівні інформаційної культури підлітка; на рівні використання джерел комунікаційних каналів виникають суттєві втрати ІП безпеки підлітків.

6. Обґрунтовано і розроблено концептуальну структура інформаційної технології забезпечення ІП безпеки підлітків щодо впливу інформаційних деструктивних трансформацій на їх підсвідомість і свідомість. На основі системного аналізу базових складових інформаційної технології забезпечення інформаційної безпеки підлітків обґрунтовується, що одним з ключових її технологічних етапів є складова, яка будується з використанням методів виявлення (детектування) наявності інформаційно-психологічних деструкцій в інформаційних ресурсах.

7. У той же час аналіз існуючих доступних підходів щодо забезпечення фільтрації деструктивних інформаційних модифікацій показав наступне.

7.1. Низька якість функціонування методів виявлення (детектування) наявності інформаційно-психологічних деструкцій в інформаційних ресурсах неминуче спричинить за собою зниження ефективності всієї інформаційної технології забезпечення інформаційно-психологічної безпеки підлітків.

7.2. Однак сфера розробки таких технологічних рішень знаходяться в критичному стані. Відповідні технології мають недостатній рівень розвитку, щоб бути адекватними існуючим інформаційно-технологічним можливостями протиборчої сторони щодо організації та проведення деструктивного ІП впливу.

Основні результати досліджень даного розділу опубліковані в таких працях [12, 13, 107, 108, 126].

РОЗДІЛ 2
РОЗРОБКА МОДЕЛІ ПРОЦЕСУ ВИЯВЛЕННЯ СУГЕСТИВНИХ ДЕСТРУКТИВНИХ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИХ ДІЙ

Викладається розробка моделі загроз ІП безпеки особистості в умовах інформаційного протиборства і демократизації соціуму. Обґрунтовується, що найбільш актуальними і значущими загрозами ІП безпеки особистості є сугестивні деструктивні ІП впливи на базі деструктивних інформаційних модифікацій в аудіоконтейнерах і електронних текстових ресурсах.

Обґрунтовано, що інформаційні технології, які відносяться до першого і другого класів представлені дуже широко, однак, не враховують сугестивну складову ІП впливу. Показано, що інформаційні технології, які дозволяють проведення більш глибинного аналізу інформаційних ресурсів, а саме враховують можливість виявлення сугестивного впливу на підсвідомість, характеризуються тим, що мають обмежену можливість щодо використання та проведення досліджень. Доводиться, що відсутність вітчизняних розробок в області інформаційних технологій забезпечення протидії сугестивним деструктивним ІП атакам на підсвідомість особистості створює критичний рівень загроз порушення національної безпеки держави. Стверджується, що існує необхідність в розробці комплексних методів виявлення сугестивних деструктивних ІП впливів на підсвідомість особистості в електронних текстових ресурсах з врахуванням сучасних технологічних аспектів створення інформаційних деструкцій протиборчою стороною.

2.1. Розробка моделі загроз інформаційно-психологічній безпеки з врахуванням прихованого інформаційного деструктивного впливу на підсвідомість підлітків

Для оцінки стану забезпечення інформаційної безпеки особистості (підлітків) і суспільства в інфокомунікаційному просторі в умовах ведення інформаційної боротьби (інформаційної протидії) необхідно виконати аналіз загроз, викликаних проведенням деструктивного ІП впливу з побудовою узагальненої моделі загроз інформаційній безпеці особистості (підлітка).

Під загрозою ***інформаційно-психологічної безпеки особистості*** (підлітка) в інфокомунікаційному (соціотехнічному) просторі розуміється множина $\Psi_{\text{зіб}}$ можливих порушень морально-психологічного стану підлітка, його внутрішніх установок [12, 13, 107, 108, 126]. ***Джерелом загроз*** (суб'єкт інформаційного протиборства) ІП безпеки є безліч $\Psi_{\text{дзіб}}$ носіїв загрози безпеки, дії яких можуть призвести до порушення здоров'я і нормального розвитку підлітків [12, 13, 107, 108, 126]. Суб'єктами інформаційного протиборства виступають спеціальні центри протидіє протиборчої сторони, спецслужби іноземних держав, терористичні організації, політизовані радикальні угруповання, кримінальні структури, транснаціональні корпорації та інші формальні й неформальні учасники сучасних міжнародно-правових відносин. Під ***вразливістю особистості (підлітків)*** розуміється множина $\Psi_{\text{вібо}}$ причин, що призводять до втрати ІП безпеки підлітків, і, як наслідок, до деградації їх морально-психологічного стану і здоров'я, тобто.

$$\Psi_{\text{вібо}} = \{\Psi_{\text{вібо/ву}}; \Psi_{\text{вібо/вп}}; \Psi_{\text{вібо/рп}}; \Psi_{\text{вібо/взв}}; \Psi_{\text{вібо/вс}}\}.$$

Уразливості можуть бути обумовлені причинами наступного характеру [12, 13, 42, 57, 64-66, 88, 107, 108, 126]:

1) рівнем внутрішніх установок (множина причин $\Psi_{\text{вібо/ву}}$), включаючи особливості менталітету, спадкові ознаки, генотип;

2) рівнем виховання підлітка (множина причин $\Psi_{\text{вібо/вп}}$);

3) рівнем розвитку підлітка (множина причин $\Psi_{\text{вібо}/\text{рп}}$), включаючи морально-психологічний, інтелектуальний, психіки та ін.;

4) рівнем сприйнятливості до зовнішніх впливу (множина причин $\Psi_{\text{вібо}/\text{взв}}$), в тому числі рівень критичного осмислення одержуваної інформації;

5) рівень взаємодії в соціумі (множина причин $\Psi_{\text{вібо}/\text{вс}}$).

У загальному випадку виділяються такі основні уразливості як: несформований і нестійкий до цього віку морально-психологічний стан підлітка; особливості менталітету і навколишнього соціального середовища, спадкові ознаки; недоліки у вихованні підлітка в сім'ї, в школі; слабка нервова система і нестійка психіка; слабкий фізичний розвиток; недостатній рівень критичного осмислення інформації; процеси, зумовлені кризою підліткового віку; недостатньо сформована інтелектуальна організованість; схильність до впливу ближньої і дальньої соціальної, соціотехнічного і інформаційного середовища. Атака (ІП вплив) це множина $\Psi_{\text{атк}/\text{іп}}$ дій з боку множини $\Psi_{\text{дзіб}}$ джерел загроз, що реалізує множину $\Psi_{\text{вібо}}$ вразливостей інформаційно-психологічної безпеки особистості. Відповідно безліч ІП атак (впливів) задається як:

$$\Psi_{\text{атк}/\text{іп}} \to \{\Psi_{\text{дзіб}}; \Psi_{\text{вібо}}\}.$$

Наслідки порушення ІП безпеки особистості це можлива множина $\Psi_{\text{зіб}}$ реалізацій загроз множиною $\Psi_{\text{дзіб}}$ джерел загроз через наявну множину $\Psi_{\text{вібо}}$ вразливостей, спрямованих на нанесення множини $\Psi_{\text{шк}}$ збитків як з позиції розвитку підлітків, так і з позиції їх ІП безпеки. Це записується таким виразом:

$$\Psi_{\text{зіб}}: \{\Psi_{\text{дзіб}}; \Psi_{\text{вібо}}\} \to \Psi_{\text{шк}}. \qquad (2.1)$$

Для оцінки і формування підходів підвищення протидії деструктивним ІП впливам потрібно провести аналіз безлічі можливих порушень ІП безпеки підлітків з обов'язковою ідентифікацією багатьох джерел загроз, множини $\Psi_{\text{дф}}$ дестабілізуючих факторів, що сприяють їх прояву і множини вразливостей [12, 13, 42, 57, 64-66, 88,

107, 108, 126]. Такий аналіз загроз ІП безпеки підлітків є одним з найважливіших етапів при оцінці реального стану забезпечення протидії деструктивним ІП атакам у відкритому інфокомунікаційному просторі в умовах проведення політики демократизації суспільства, свободи слова та інтеграції в світовий інформаційний простір. Його основою є розробка моделі загроз [12, 13, 42, 57, 64-66, 88, 107, 108, 126].

На підставі моделі загроз формується політика безпеки, ***тобто протидія деструктивним ІП атакам з урахуванням їх актуальності і значущості***. Для цього виконується моделювання та класифікація безлічі джерел загроз і безлічі їх проявів. Тут, як правило, використовується аналіз взаємодії наступного логічного ланцюжка: "безліч загроз в ІП просторі – безліч джерел загроз – безліч методів реалізації деструктивного ІП впливу – безліч вразливостей стану підлітків – безліч негативних наслідків для розвитку і здоров'я підлітків" (рис. 2.1). Вихідними даними для побудови моделі загроз і класифікації джерел загроз ІПБ особистості є [12, 13, 42, 57, 64-66, 88, 107, 108, 126]:

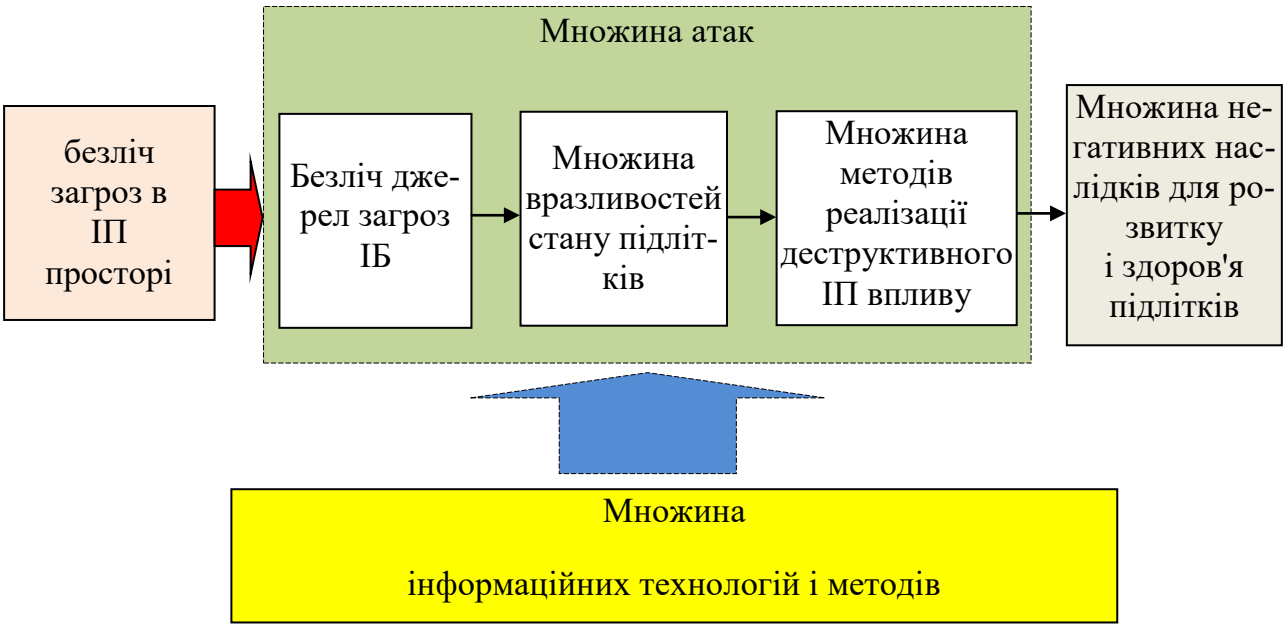


Рисунок 2.1 – Загальна модель реалізації загроз інформаційно-психологічної безпеки особистості

1) перспективна роль підліткового покоління в забезпеченні національної безпеки держави, створення умов для протидії в інформаційному протиборстві, досягненні стратегічних завдань розвитку держави і забезпечення стабільності в

суспільстві, в тому числі: в ближній перспективі рівень активності участі і організації рухів спротиву; в далекій перспективі ключова роль підліткового покоління в процесі прийняття рішень на різних рівнях системи державного управління і керівництва громадськими організаціями;

2) особливості психологічного, інформаційного, соціального, емоційного та інтелектуального стану розвитку підлітків;

3) структура і склад системи інформаційного обміну в соціумі, включаючи взаємодію в сім'ї, в школі, в дружньому середовищі, в соціальних групах;

4) особливості сприйняття інформаційних повідомлень з внутрішніх і зовнішніх інформаційних каналів в інформаційно-психологічному просторі;

5) об'єкти і суб'єкти доступу до інформаційного та ІП просторів підлітків, їх можливості і характеристики безпеки, можливості протиборчої сторони;

6) особливості інтересів і мотивацій підлітків в соціальній і соціотехнічній сферах;

7) зовнішні чинники впливів.

Структурна схема системи забезпечення інформаційно-психологічної безпеки підлітків у відкритому інфокомунікаційному просторі в умовах, коли з одного боку необхідно забезпечити концепцію демократизації суспільства, а з іншого боку, коли ведеться інформаційна війна, представлена на рис. 2.2. Як показано на рис. 2.2, прикладом зв'язки, представленої на рис. 2.1 для інформаційної безпеки підлітків може бути наступний варіант. Протиборча сторона (джерело загроз) - низька здатність підлітків щодо критичного аналізу інформації (вразливість обумовлена сприйнятливість до зовнішніх впливів) - дезінформація або деструктивний інформаційно-психологічний вплив на усвідомленому рівні сприйняття інформації підлітком (атака) - модифікація стану підлітка, його цільової мотивації і емоційних установок (результат, наслідки), в тому числі підтримка і участь в деструктивних рухах спротиву, формування антипатріотичних настроїв.

Проведений аналіз процесів деструктивних впливів соціальному і соціотехничному (інфокомунікаційному) просторах в умовах: з одного боку ведення інформаційної протидії, а з іншого боку проведення політики демократизації суспільства, його інформатизації, дозволяє зробити таку класифікацію загроз інформаційній безпеці підлітків, а саме (рис. 2.3):

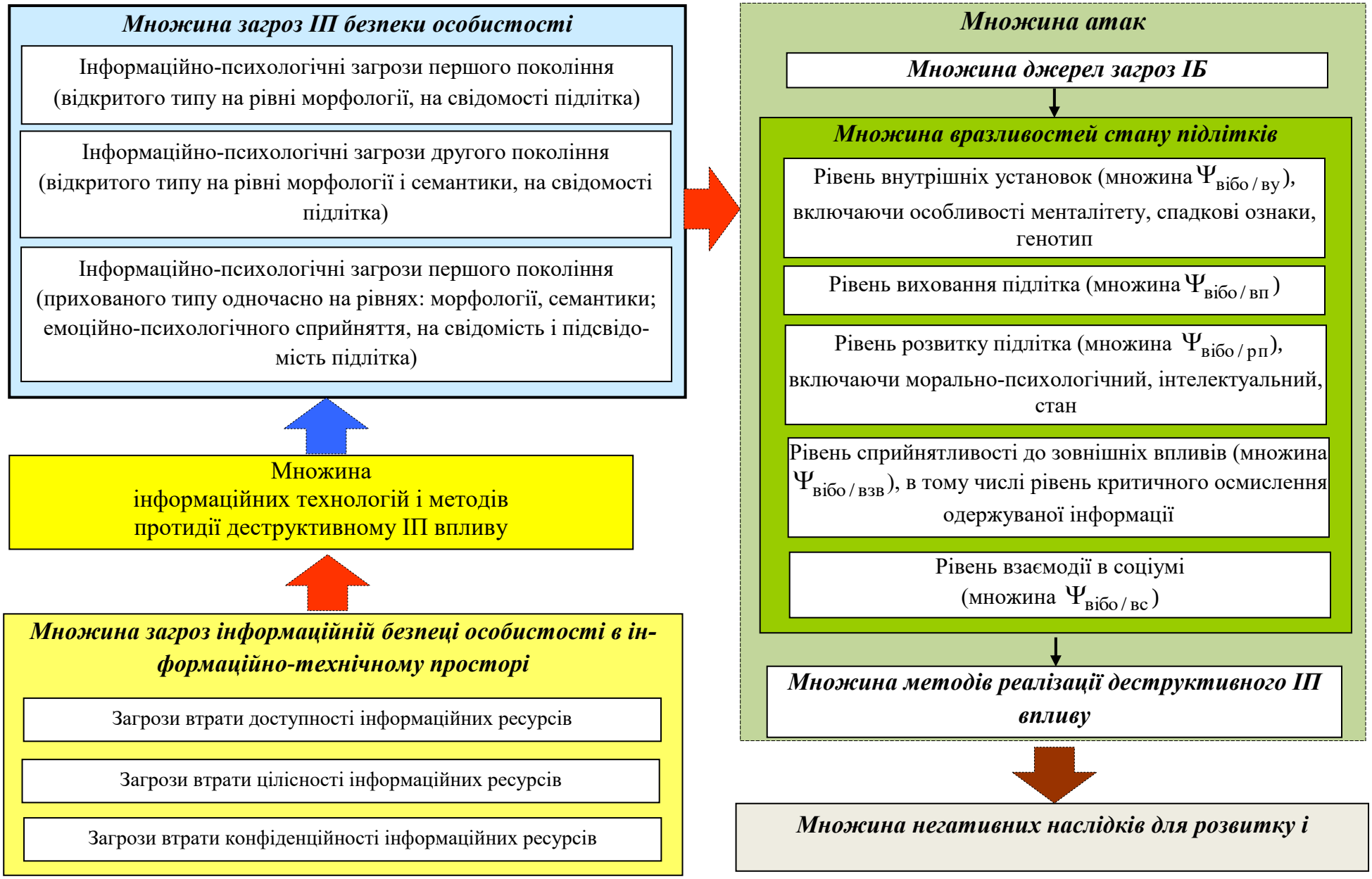


Рисунок. 2.2 – Структурна схема системи забезпечення інформаційно-психологічної безпеки підлітків у відкритому інфокомунікаційному просторі в умовах демократизації суспільства та інформаційної війни

Рисунок. 2.3 – Модель загроз інформаційно-психологічної безпеки особистості в інфокомунікаційному просторі

1. Безліч загроз в інформаційно-психологічному просторі. Тут в залежності від глибини використання інформаційних деструкцій розрізняють такі види загроз (деструктивних ІП атак):

1) до першого виду відносяться загрози (ІП загрози *першого покоління)*, які обумовлені відкритими ІП атаками на свідомість підлітків, які застосовують інформаційні деструкції на рівні морфологічного опису електронних текстових документів, тобто на рівні окремих слів;

2) інформаційно-психологічні загрози, які додатково використовують інформаційні деструкції на рівні семантичного опису інформаційних ресурсів (електронних текстових документів) створюють другий вид (загрози, які обумовлені відкритими ІП атаками *другого покоління* на свідомість підлітків);

3) третій вид ІП загроз це загрози які пов’язані з сугестивними (скритими) деструктивними ІП атаками на підсвідомість підлітків, з додатковим використанням інформаційних деструкцій текстових інформаційних ресурсів на рівні врахування психологічно-емоційної та внутрішньо-установочної складової особистості. Такі загрози відносяться до *третього покоління*.

2. Безліч загроз в ІТ просторі. Даний вид загроз пов'язаний з втратою інформаційної безпеки за такими категоріями як доступність, цілісність і конфіденційність. Розгляд таких загроз в єдиному ***мережоцентричному*** просторі щодо інформаційної безпеки підлітків (особистості) пов'язано з наявністю певного взаємозв'язку між загрозами в ІП та ІТ просторах. Наявність взаємозв'язку обумовлено наступними причинами:

- деструктивні модифікації можуть організовуватися на базі інформаційних потоків, які відповідають сервісам реального часу. Сервіси такого типу мають жорсткі вимоги по характеристикам доступності, своєчасності, цілісності отриманої інформації;

- дії, пов'язані із здійсненням протидії деструктивним ІП атакам супроводжуються необхідністю обчислювальних та інформаційних витрат, тобто формуються додаткові затримки на обробку інформаційних ресурсів (виникають ризики для втрати доступності інформації), можуть виникати загрози втрати цілісності в процесі обробки інформації;

- аналіз інформаційних ресурсів на наявність деструктивних трансформа-

ції може стосуватися інформаційних сегментів інфотелекомунікаційної системи, інформації з обмеженим доступом в інтересах особистості (персональні дані), соціуму і держави. Тут відповідно виникають загрози втрати конфіденційності інформаційних ресурсів. Такі загрози можна трактувати як загрозу втрати інформаційної безпеки особистості з позиції порушення категорій доступності та цілісності інформаційного ресурсу, тобто ***загрози в ІТ просторі, які виникають внаслідок протидії загрозам в ІП просторі,*** а саме: безліч загроз доступності, цілісності і конфіденційності.

Ефективність протидії деструктивному ІП впливу на особистість (підлітків) визначається тим, що:

І. З одного боку необхідно мінімізувати ступінь втрати доступності до інформаційних ресурсів (тобто потрібно забезпечити вільний доступ до відкритої інформації відповідно до прийнятої політики безпеки). Тут використовуються такі показники як: показники доступності або своєчасності отримання інформації; показники достовірності інформації; ступінь повноти інформації; ступінь актуальності інформації.

1. Категорія ***доступності до інформаційного ресурсу***. Доступність це гарантія отримання необхідної інформації або інформаційної послуги користувачем за певний час $t_{пот}$. При цьому фактор часу у визначенні доступності інформації в ряді випадків є дуже важливим і визначає ступінь актуальності отриманої інформації. Це обумовлено тим, що деякі види інформації та інформаційні послуги мають сенс тільки в певний проміжок часу $t_{пот}$ [64, 65]. У цьому випадку затримки відносно отримання інформації користувачами (підлітками), ***навіть*** такі, які обумовлені додатковими часовими витратами на проведення фільтрації інформаційного ресурсу на предмет наявності деструктивного ІП впливу, також є порушенням категорії інформаційної безпеки. З одного боку противник прагне заблокувати джерела або створити інші перешкоди для отримання користувачами своєчасної актуальної конструктивної інформації, що відображає інтереси суспільства і держави. Характеристикою такого процесу є часові затримки $t_{рбл/дж}$ на розблокування доступу до інформаційного ресурсу. З іншого боку для здійснення фільтрації інформаційних ресурсів, які містять

деструктивний ІП вплив, потрібно вносити додаткові затримки $t_{обр/ip}$ на реалізацію відповідної обробки.

2. Цілісність інформаційного ресурсу здатність зберігати вихідний семантичний зміст відеоінформації, в умовах: ведення інформаційного протиборства; існуючих характеристик процесів обробки, передачі, зберігання інформації в незалежності від територіальної прихильності її джерела і одержувача (підлітка) [64, 65]. З одного боку противник прагне порушити категорію цілісності інформаційного ресурсу, які відображають конструктивний підхід в інтересах суспільства і державної політики. Тут використовується показник ступеня внесених втрат цілісності інформації в результаті деструктивного ІТ впливу противника. З іншого боку процеси фільтрації деструктивного ІП впливу можуть супроводжуватись внесенням коригувань в передані інформаційні потоки. Цей процес також може супроводжуватись втратами цілісності інформації.

3. Конфіденційність інформаційного ресурсу. З одного боку противник прагне отримати несанкціонований доступ до інформаційних ресурсів для збору відомостей про об'єкти деструктивного ІП впливу. З іншого боку для виявлення деструктивного ІП впливу потрібно такий же доступ отримати для відповідних технологій протидії деструктивним впливам.

ІІ. З іншого боку потрібно забезпечити безпеку підлітків в інформаційно-психологічному просторі, тобто мінімізувати збиток від деструктивного ІП впливу, а саме мінімізувати ймовірність модифікації психологічного, морального, мотиваційного та інтелектуального стану особистості (підлітка).

В цьому випадку в процесі створення технологій протидії деструктивному ІП впливу потрібно враховувати наявність наступного протиріччя.

Протиріччя на рівні категорій інформаційної безпеки. Забезпечення однієї групи категорій може призвести до втрати рівня інших категорій інформаційної безпеки.

1. З одного боку потрібно блокувати інформаційний потік (динамічні і статичні інформаційні ресурси, аудіо дані і текстові дані) або організовувати додаткову їх обробку на предмет виявлення в його синтаксичному, морфологічному або семантичному представленні компонент деструктивного ІП впливу (атак). Це пов'язано з обмеженням доступності ІР, появою часових затримок на

його доставку та несвоєчасним отриманням інформації споживачами. Звідси виникає зниження рівня інформаційної безпеки за категоріями доступність і цілісність інформаційного ресурсу.

2. З іншого боку для організації необхідного рівня інформаційної безпеки особистості, соціуму і держави необхідно забезпечити необхідний рівень таких категорій як доступність, цілісність і конфіденційність. Такі вимоги обумовлені конституційним правом особистості на своєчасне отримання необхідної конструктивної інформації (демократичні свободи, свобода слова).

Отже, існує певна складність щодо встановлення жорсткого кордону між порушенням прав особистості на отримання інформації та порушенням інформаційної безпеки особистості щодо блокування деструктивного впливу.

Тому потрібно здійснювати розробку спеціального математичного апарату для створення і розвитку інформаційної технології забезпечення інформаційної безпеки підлітків, а саме забезпечення своєчасного виявлення та блокування деструктивного ІП впливу в умовах забезпечення заданого рівня доступності та цілісності отриманих інформаційних ресурсів.

Для узагальнення побудованої моделі загроз ІП безпеки підлітка будемо використовувати показник, що оцінюється як ймовірність локалізації загрози деструктивного ІП впливу при виконанні наступних вимог щодо:

- здійснення такої обробки з часовими витратами $t_{обр\sum}$, що не перевищують допустимий рівень $t_{пот\sum}$, $t_{обр\sum} \le t_{пот\sum}$;

- забезпечення необхідного рівня $t_{пот}$ категорії доступу користувача до ІР (відповідно до категорії інформаційної безпеки – доступність ІР), а саме $t_{ді} \le t_{пот}$;

- забезпечення необхідного рівня цілісність і повноти ІР (згідно категорії інформаційної безпеки – цілісність інформації), що задається умовою $P_ц \ge P_{ц/пот}$;

- зниження ймовірності ν_2 помилок першого та другого роду, тобто $\nu_1 \to 0$, $\nu_2 \to 0$.

В умовах:

- заданого рівня $P_{віпв/пот}$ виявлення інформаційних деструкцій, за потріб-

ний $t_{потр}$ час на виявлення деструктивних ІП атак з використанням необхідного $w_{потр}$ обсягу ІР для виявлення деструктивних трансформацій;

- заданого комплексу характеристик інфокомунікаційної системи, включаючи продуктивність $U_{обр}$ обчислювальної апаратури, характеристик пропускної здатності $U_{пск}$ мережі;

- наявності протиборчої сторони, що володіють можливістю проведення множини $\Psi_{атк/іт}$ інформаційно-технічних атак, спрямованих на втрату доступності ІР;

- наявність множини $\Psi_{атк/іп}$ інформаційно-психологічних атак, які призводять до необхідності використовувати технології протидії;

- маскування деструктивних ІП впливів, тобто використання технологій сугестивного деструктивного ІП впливу.

Все це можна описати наступною системою виразів:

$$P_{лок/іп} = F_{бл}(P_{віпв}; U_{обр}; U_{пск}; \nu_2; w_{потр}; t_{рбл/дж}; \Psi_{атк/іт}; \Psi_{атк/іп}) \to \max; \quad (2.2)$$

$$\Psi_{зіб}:\{\Psi_{дзіб}; \{\Psi_{вібо/ву}; \Psi_{вібо/вп}; \Psi_{вібо/рп}; \Psi_{вібо/взв}; \Psi_{вібо/вс}\}\} \to \Psi_{шк} \to \min; \quad (2.3)$$

$$\begin{cases} P_ц \geq P_{ц/пот}; \\ P_д \geq P_{д/пот}; \end{cases} \quad \begin{cases} t_{обр\sum} \leq t_{пот\sum}; \\ t_{ді} \leq t_{пот}; \end{cases} \quad \begin{cases} \nu_1 \to 0; \\ \nu_2 \to 0; \end{cases} \quad \begin{cases} t(w_{min})_{обр} \leq t_{потр}; \\ w_{min} \leq w_{потр}. \end{cases} \quad (2.4)$$

Тут: $F_{бл}(P_{віпв}; U_{обр}; U_{пск}; \nu_2; w_{потр}; t_{рбл/дж}; \Psi_{атк/іт}; \Psi_{атк/іп})$ - функціонал, що описує залежність величини $P_{лок/іп}$ ІР, $P_ц \geq P_{ц/пот}$; необхідної достовірності інформаційного ресурсу $P_д \geq P_{д/пот}$; $t_{обр\sum} \leq t_{пот\sum}$; $t_{ді} \leq t_{пот}$; $t_{ді}$ - реальний час доступу користувача до інформаційного ресурсу.

Відповідно сумарні часові $t_{обр\sum}$ витрати на весь цикл функціонування ІТІБП, оцінюються за формулою:

$$t_{обр\sum} = t_{пі} + t_{дст} + t_{обр/іп} + t_{ан/пр} + t_{рбл/дж},$$

де $t_{пі}$ - час на пошук джерела; $t_{дст}$ - час на доступ до інформаційних ресурсів; $t_{обр/іп}$ - час обробки на виявлення та ідентифікацію на предмет наявності де-

структивного ІП впливу; $t_{ан/пр}$ - час на прийняття рішення; $t_{лок/ip}$ - час на власне процес блокування джерела деструктивної інформації.

Розгляд загроз ІП безпеки підлітків в представленої моделі загроз дозволяє в умовах демократизації суспільства, його інформатизації та інтегрування в світовий інформаційний простір визначити найбільш актуальні загрози, визначити актуальні уразливості в процесі інформаційного забезпечення підлітків, оцінити взаємозв'язок множин ІП загроз, джерел загроз та вразливостей стану підлітків.

Проведемо визначення найбільш актуальних і значущих загроз втрати ІП безпеки підлітків. Деструктивні ІП впливу діляться на дві групи, а саме: відкритий і прихований ІП вплив.

Відкритий деструктивний ІП - такий вплив, коли об'єкт цілком усвідомлює цілі впливу, засоби, які використовує суб'єкт, особливості процесу впливу. ***Прихований*** (сугестивний) деструктивний ІП вплив (маніпуляція) це такий вплив, коли жоден з перерахованих аспектів об'єктом не усвідомлюється.

Найбільш складними з позиції: виявлення та організації протидії; нанесення шкоди є сугестивні деструктивні ІП впливи. Це обумовлено тим, що:

1) сугестивні ІП атаки на відміну від відкритих атак впливають на підсвідомість особистості. У зв'язку з чим, збиток від дії таких атак більш значний і досягається за більш короткі часові терміни з залученням меншої кількості інформаційних контейнерів;

2) сугестивні ІП атаки по своїй суті є прихованими і можуть маскуватися під конструктивні інформаційні ресурси. Необхідно враховувати, що в інформації, що є за своїм змістом конструктивною може виявитися деструктивною за своєю дією на підсвідомість (сугестивного канал). Також інформація, яка є "цікавою" може призвести до неусвідомлюваних психобіологічніх негараздів, стимулюючі девіантну поведінку особини та руйнуючі позитивні соціальні тенденції в суспільстві. Це є причиною виникнення складнощів виявлення таких інформаційних деструкцій;

3) виявлення прихованих деструктивних ІП впливів вимагає набагато більших витрат часового ресурсу на їх виявлення і блокування. Це обумовлено тим, що такі атаки додатково залучають більшу глибину аналізу тестової інформації до рівня врахування психологічно-емоційної та внутрішньо-установочної

складової особистості. Така обставина призводить до втрати доступності інформаційного контейнера, тобто порушується інформаційна безпека в ІТ просторі.

Отже, сугестивні деструктивні ІП атаки є найбільш перспективними, та складають базу для інформаційних операцій третього покоління. Такі ІП впливи є найбільш актуальними та значущими серед різних типів деструктивних ІП атак (рис. 2.4).

Класифікація основних прихованих деструктивних ІП впливів представлена на рис. 2.5. На рис. 2.5 сугестивні типи деструктивних ІП впливів в інфокомунікаційному просторі представлені у вигляді виділеної зони червоного кольору. Такі впливу поділяються залежно від інформаційних контейнерів, на базі яких здійснюються інформаційні деструкції (модифікації). При цьому одними з ключових ІП атак, які здійснюються в сучасному інформаційно-комунікаційному просторі, тут є наступні:

а) аудіосуггестія, приховані вставки в аудіопотоки;

б) сугестія текстів.

Це пояснюється найбільшим опрацюванням відповідних ІТ засобів і методів у протиборчої сторони щодо організації деструктивних впливів на ІП та інформаційно-емоційному рівнях. Тому потрібно провести дослідження існуючих інформаційних технологій і методів протидії різним ІП атакам. Тут потрібно враховувати умови (обмеження) інформаційної протидії, а саме забезпечення вимог (категорій інформаційної безпеки підлітків в ІТ просторі) щодо доступності, цілісності інформаційних ресурсів особистості, соціуму і держави. Іншими словами потрібно забезпечить умови мережецентричності безпеки підлітка в інформаційному просторі.

Значить по викладеному матеріалу можна зробити такі висновки:

- розроблена модель загроз ІП безпеки особистості в умовах інформаційного протиборства і демократизації соціуму, коли потрібно забезпечити баланс безпеки особистості одночасно в ІП та ІТ просторах (умова мережецентричності безпеки підлітка в інформаційному просторі);

- обґрунтовано, що найбільш актуальними і значущими загрозами ІП безпеки особистості з позиції: виявлення та організації протидії; нанесення шкоди є сугестивні деструктивні ІП впливи;

Рисунок 2.4 – Структурна схема обґрунтування актуальності і значущості сугестивних інформаційно-психологічних загроз

Рисунок 2.5 – Основні форми прихованих шкідливих впливів на інформаційно-психологічний стан людини

- показано, що одними з ключових ІП атак, які здійснюються в сучасному інформаційно-комунікаційному просторі, є деструктивні інформаційні модифікації в аудіоконтейнерах і електронних текстових ресурсах, а саме: аудіосуггестія, приховані вставки в аудіопотоки.

2.2. Обґрунтування проблемних недоліків існуючих інформаційних технологій та методів аналізу інформаційних ресурсів щодо наявності деструкцій

Аналіз публікацій з проблем забезпечення інформаційної безпеки свідчить, що на даний час достатньо добре досліджено [2-7, 22-34, 36, 38-40, 42, 45-69, 73-79, 88, 92-106, 112-122, 124, 127-129]:

– джерела та причини інформаційних загроз;

– компоненти, форми інформаційної боротьби;

– методи та засоби інформаційної боротьби;

– види реалізації інформаційно-психологічних впливів.

Більшість наукових праць зосереджені на проблемах забезпечення інформаційної безпеки у таких геополітичному та технологічному аспектах. Разом з тим, самі інформаційні технології та засоби ведення ІП протиборства або мають обмеження на відкрите використання, або досліджені на недостатньому рівні.

Головний інтерес тут стосується ключового компонента інформаційних технологій забезпечення ІП безпеки особистості, а саме методів аналізу та виявлення (детектування) інформаційних деструкцій в електронних документах. Отже необхідно розглянути ті інструменти ІТ, що використовуються для моніторингу засобів масової інформації. Таких технологій на даний час розроблено близько сотні. Але основні їх функціональні можливості, як правило, стосуються: організації зберігання середніх або великих обсягів інформації; забезпечення простих пошукових можливостей та / або тематичні рубрикатори.

При цьому не підтримується жодного механізму якісного аналізу ІР.

Всі існуючі інформаційні технології та методу в залежності від глибини аналізу текстової інформації можна розглядати за трьома класами, а саме:

1. До першого класу відносяться технології та методи, які забезпечують аналіз IP за ключовими словами. Відповідно такі методи дозволяють з одного боку створювати, а з іншого боку виявляти інформаційні атаки ***першого покоління***.

2. Інформаційні технології та методи, які додатково дозволяють аналізувати семантичний контент електронних ТІР створюють другий клас. Відповідно такі технологічні рішення забезпечують умови для здійснення та виявлення ІП атак ***другого покоління***. Саме такі ІП атаки здійснюють вплив на свідомість особистості.

3. Третій клас інформаційних технологій та методів формують такі технологічні рішення, які додатково дозволяють збільшити глибину аналізу текстової інформації до рівня врахування психологічно-емоційної та внутрішньо-установочної складової особистості. Такі інформаційно-технологічні рішення створюють ***потенційні*** можливості з одного боку для проведення, а з іншого – для детектування сугестивних ІП впливів на підсвідомість особистості. Саме такі ІП операції є найбільш значущими з позиції нанесення шкоди та найбільш непомітними для смислового аналізу. Отже такі впливи відносяться до атак ***третього покоління*** – найбільш перспективних та складних ІП атак.

Функціональні характеристики доступних технологічних рішень обробки, аналізу текстової інформації для створення умов протидії ІП атакам першого та другого поколінь представлено в табл. 2.1. Найбільш відомою з них є інформаційна технологія, що базується на комплексному смисловому аналізаторі електронного тексту ***Text Analyst*** [70, 90]. В створі задоволення потребам ІП операцій така технологія відноситься до *другого покоління*.

Аналізатор тексту Text Analyst – інтелектуальне програмне забезпечення для аналізу змісту електронних текстів, смислового пошуку інформації та формування електронних архівів [70, 90]. Програма є російською розробкою наукового центру “МикроСистемы”.

Процедури обробки інформації в системі включають:

1. Попередній аналіз текстової інформації (виділення в тексті понять, які входять в базові словники).

Таблиця 2.1

Огляд програмних реалізацій технологій обробки електронної текстової інформації

Назва системи	Основне призначення
Астарта	Інструмент автоматизації аналітичних досліджень. Експертний рубрикатор, призначений для збору, зберігання і семантичного аналізу текстових матеріалів. Під аналізом тут розуміється автоматичне створення рубрик і угруповання, а також інтелектуальна вибірка інформації по заданій темі
Галактика–Zoom	Програмний комплекс призначений для аналітичної обробки текстових неструктурованих документів. Здійснює швидкий пошук і контент-аналіз відібраної інформації. Побудований за принципом роботи з тематичним рубрикатором
Медиалогия	Інформаційно-аналітична система здійснює моніторинг понад 24 000 об'єктів, фіксуючи статистичну та аналітичну інформацію з тисячі джерел (центральна і регіональна паперова преса, інформаційні агентства, транскрипти та оригінали телерадіопередач, Інтернет-джерела). На обробці повідомлень задіяно кілька сотень кваліфікованих операторів, безупинно переглядають до десяти тисяч повідомлень на добу. Система дозволяє класифікувати публікації за значимістю, визначати ставлення ЗМІ до об'єктів, аналізувати характеристики PR–кампаній, встановлювати відображені в ЗМІ зв'язку між об'єктами і т. д
Hummingbird	Інформація автоматично рубрикується, а потім піддається OLAP–аналізу. Є засоби, за допомогою яких користувачі можуть самі створювати нові або настроювати наявні дерева рубрик. Вибірка документів проводиться за допомогою, як контекстного пошуку, так і OLAP–аналізу
TextAnalyst	Інструмент для аналізу змісту текстів, смислового пошуку інформації, формування електронних архівів. Здатна будувати семантичні дерева, але не за об'єктами, а за окремими статтями, в результаті чого створюється смисловий портрет кожного тексту на основі кількості згадувань і близькості зустрічання різних значущих, на думку програми, слів. Є модуль, що генерує реферат текстового документу

2. Статистичний аналіз тексту – визначення частот зустрічальності в тексті слів і словосполучень (важливість поняття оцінюється за частотою його використання в тексті).

3. За результатами частотного аналізу формування семантичної мережі для аналізованого тексту, що відбиває зв'язки між поняттями і об'єднуючою їх в єдину смислову картину (перед побудовою семантичної мережі встановлюється поріг значимості для понять і зв'язків між ними).

4. На основі семантичної мережі побудова тематичної структури тексту у вигляді дерева або лісу понять (кожній темі відповідає своє дерево понять).

5. Автоматичне реферування тексту на основі його тематичної структури.

6. Формування гіпертекстової розмітки;

5. Смисловий пошук інформації.

Основні функціональні принципи, що реалізовані в технологічному продукті Text Analyst включають до себе наступне. По-перше, принцип асоціативності, який полягає у використанні такої моделі представлення тексту, при якій його фрагменти вказують на місця їх зберігання. Якщо фрагменти збігаються, то вони вказують на одне і те ж місце, де записується частота їх зустрічальності. По-друге побудову структури понять, що представляє текст, відповідно до їх важливості і взаємозв'язків. По-третє формування тематичної структури тексту у вигляді багаторівневої ієрархії тем, і розкриваючих їх підтем.

Технологію Text Analyst розроблено з використанням об'єктно-орієнтованого підходу і COM–технології. На їх основі реалізовані два програмних об'єкта, а саме: лінгвістичний процесор і алгоритмічне ядро (рис. 2.6). На рис. 2.5 передбачені такі скорочення: ЛП – лінгвістичний процесор (модуль перетворення тексту); АЯ – алгоритмічне ядро (модуль аналізу тексту); DicEdit – редактор словників; 1 – інтерфейс обробки команд користувача; 2 – інтерфейс зберігання даних; 3 – інтерфейс між клієнтським додатком і АЯ; 4 – потік даних від ЛП до АЯ; 5 – потік даних від АЯ до ЛП.

Концепція Text Analyst передбачає наявність двох базових словників: для російської та англійської мов. Для них передбачені 4 підсловника: словник видаляємих слів; словник загальних слів; словник слів-уподобань користувача (предметних понять); словник слів-винятків з правил нормальної словозміни.

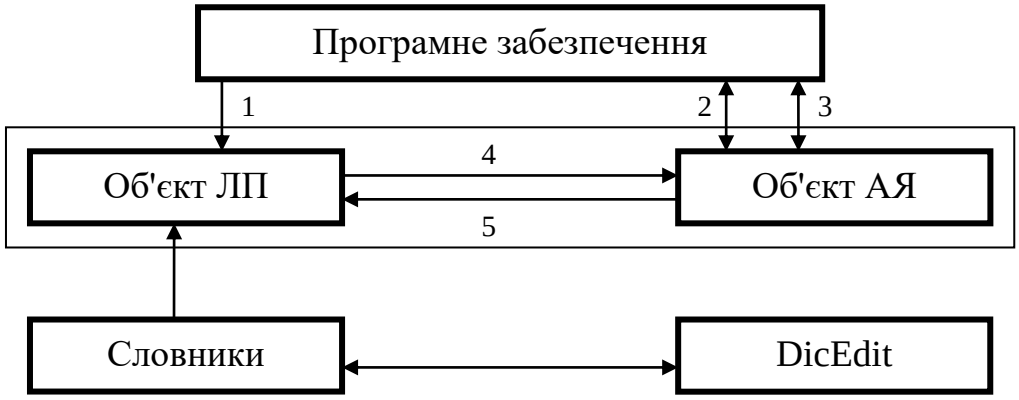


Рисунок 2.6 – Схема побудови Text Analyst

Додаток DicEdit дозволяє настроювати словники на програмне забезпечення аналізованих текстів чи створювати власні словники.

Основними функціями модуля ЛП є:

– виділення з тексту послідовності слів;

– виключення з цієї послідовності елементів словника видаляємих слів (він містить малозначущі і неінформативні слова);

– маркування слів атрибутами, визначаючими їх типи ;

– приведення словоформ до базової граматичної форми.

Таким чином, на вхід ЛП надходить рядок тексту. Відповідно на його виході формується послідовність слів, маркованих атрибутами, визначаючими їх типи. Словник ЛП встановлює набір слів, що видаляються з тексту, і атрибути слів у вихідний послідовності. Лінгвістичний процесор створює базу даних (БД), в яку заносить всю лінгвістичну інформацію про аналізований текст. Надалі робота відбувається з цією БД, а не з вихідним текстом, що значно спрощує обробку і збільшує її продуктивність.

На вхід модуля АЯ надходить послідовність слів з атрибутами, визначеними ЛП. Даний модуль виконує такі основні функції:

1) статистичний аналіз вхідних послідовностей слів і виділення понять, під якими в Text Analyst розуміються слова і словосполучення, зустрічальність яких у тексті не нижче встановленого порога;

2) визначення смислових зв'язків між поняттями;

3) завдання посилань на пропозиції, в які входять виділені поняття.

На виході АЯ формуються компоненти БД, що представляють зміст тексту. Основою цих компонентів служить семантична мережа, тобто безліч слів і словосполучень, пов'язаних між собою по граничному атрибуту (частоті). Побудована таким способом семантична мережа передає зміст текстів, значно скорочуючи при цьому обсяг вихідної інформації (за рахунок виключення несуттєвих деталей). Вона являє собою індекс аналізованого тексту, який може бути ефективно використаний для реалізації різних методів доступу до тексту, в тому числі асоціативного (смислового) пошуку.

Вершинами семантичної мережі є слова і словосполучення, що несуть у тексті основне смислове навантаження. Вони виділяються по частоті в тексті. Порогове значення цього параметра може задаватися користувачем. У формованої семантичної мережі кожне поняття, багаторазово згадане в тексті, представляється єдиним елементом, приведеним до базової граматичної форми. Зв'язки між вершинами відображають спільне використання понять в тексті. Крім того, вершина співвідноситься зі списком пропозицій, в яких вжито відповідне їй поняття. Таким чином, в "смисловому портреті" тексту інтегрується інформація, що відноситься до понять.

Кожне поняття, яке увійшло в семантичну мережу, представляє деяку тему тексту і характеризується числовий оцінкою – смисловим вагою. Ця ж оцінка приписується і зв'язків між поняттями. Значення смислового ваги лежить в інтервалі від 1 до 100 і відображає важливість поняття по відношенню до сенсу всього тексту. Чим воно більше, тим важливіше поняття. Поняття з максимальними значеннями (рівними або близькими до 100) є ключовими і являють найважливіші теми тексту.

Високе значення ваги зв'язку першого поняття з другим вказує на те, що більша частина інформації в тексті, що відноситься до першого поняття, відноситься і до другого. Проте зв'язок першого поняття з другим не завжди має ту ж вагу, що і зв'язок другого поняття з першим.

Користувач може настроювати засоби візуалізації семантичної мережі, встановлюючи порогові ваги відображуваних понять і зв'язків, а також спосіб їх сортування.

В області автоматизації побудови Text Analyst дозволяє автоматично перетворити мегабайтний масив текстової інформації в гіпертекст, виділивши істотні смислові взаємозв'язку між його фрагментами. Основою для формування гіпертексту служить семантична мережа. Її проекція на вихідні тексти трансформує їх у гіпертекст. У текстах виділяються кольором поняття семантичної мережі, що рекомендуються як гіперпосилань, які ведуть до фрагментів, що містить або ці поняття, або інші поняття, пов'язані за змістом з вихідними. В результаті виникає можливість циклічного руху по ланцюжку : обраний фрагмент тексту – поняття семантичної мережі – вибрана гіперпосилання – фрагмент тексту.

Однак, такі технологічні рішення не передбачають оцінку таких складових інформаційно-психологічних аспектів, як емоції, загрози, характер відносин між об'єктами та ін. Отже існуючі доступні інформаційні технології першого та другого класу не забезпечують якісний глибинний аналіз текстових інформаційних ресурсів.

З одного боку таке становище обумовлено тим, що сучасні теоретичні положення визнають явища існуючими лише тоді, коли вони або безпосередньо спостерігається, або відтворено проявляє себе в експериментах, або строго обчислюється. Причому в будь-якому випадку останнє слово залишається за практикою: потрібно, щоб явище спостерігаємо функціонувало або виявлялися б сліди його дії. Але, з іншого боку, там, де мова йде про психологічний стан особистості, все виглядає інакше.

Ця область науково-прикладних досліджень завіюється на недостатньому рівні. Наслідком чого є те, що не створено адекватних математичних інструментів для опису інформаційно-психологічних взаємозв’язків та їх впливу на моральне-психологічний стан особистості та зміни внутрішніх установок.

2.3. Обґрунтування підходу відносно детектування сугестивних інформаційно-психологічних деструкцій в електронних текстових ресурсах в умовах інформаційного протиборства

Психологічні явища найчастіше безпосередньо не спостерігаються, в експериментах, тобто: або проявляються, або ні; обчисленню піддаються погано; сліди їх функціонування невизначені або нерегулярні.

Особливо критичний стан спостерігається для спроб встановлення інформаційно-психологічних залежностей в області підсвідомості.

Отже, оскільки природна мова є одним з найсильніших засобів впливу на особистість, наприклад, психологічні теорії розглядають його як ефективний засіб програмування людей. Тому для ефективного ІП впливу на соціум та особистість важливі не тільки і не стільки логічність і аргументованість мови (синтаксичне, морфологічне та семантичне представлення текстової інформації), ***скільки емоційний і підсвідомий інформаційний вплив на слухача*** (особистість).

Саме такий тип деструктивних ІП атак складає найбільш перспективне ***третє покоління*** інформаційних операцій. Для нього характерно:

1) скритність (тому що не підлягає виявленню класичними технологіями аналізу тестової інформації);

2) низький рівень протидії та контролю (тому що його дія стосується саме підсвідомості особистості, що дуже складно контролювати).

В теж час, незважаючи на це, існують спроби створити методики, які в тій чи іншій мірі (обмеженій мірі) можуть визначити ІП вплив на підсвідомість особистості, шляхом аналізу інформації, яка людиною сприймається. Функціональні компоненти цих методик, які засновано на багаторазових експериментах, проведених з різними соціальними групами, не мають належного математичного обґрунтування. Однак, достатня кількість експериментів показує, що відповідні результати ІП впливу хоч і мають відхилення, але більшість випробовувань показують приблизно однакові результати. Отже саме ці середні показники залежностей ІП впливу і були закладені в методиках для аналізу ТІР.

В загальному випадку виявлення та створення ІП неусвідомленого (сугестивного) впливу на підсвідомість може використовуватись для:

1) безпосереднього деструктивного ІП впливу на особистість з боку протиборчої сторони;

2) забезпечення протидії шляхом нанесенні інформаційної атаки на противника в наших інтересах;

3) здійснення інформаційної пропаганди в інтересах ідейно-моральної політики держави та соціуму;

4) проведення конструктивних інформаційних впливів для оздоровлення морально-психологічного стану особистості (підлітка);

5) просунення комерційних інтересів, наприклад підготовка відповідних рекламних інформаційних блоків. Простим прикладом цього можна навести рекламу, мета якої не просто розповісти про новий продукт, як багато хто вважає, а змусити людину купити цей продукт. Дивлячись рекламу, у людини в підсвідомості може скластися думка про те, що товар йому дійсно потрібний або ж він віддасть йому перевагу при виборі серед інших. Такий вплив може бути закладено саме завдяки методикам неусвідомленого впливу на підсвідомість.

Представником третього класу інформаційних технологій є російська "***Психолінгвістична експертна система ВААЛ-2000***" [70-72]. Згідно відкритих публікацій [70-72] така технологія дозволяє в автоматизованому режимі проводити обробку великої кількості текстової інформації, виявити глибинні мотиви психолінгвістичного впливу слів і фраз на слухачів та забезпечити апарат для створення відповідних деструктивних ІП атак третього покоління. Треба відмити, що це технологічне рішення є закритим продуктом. Інформація стосовно її структурно-функціональних складових та тактико-технічних характеристик у відкритих публікаціях є обмеженою.

Дослідження побудови системи ВААЛ для аналізу сугестивних впливів на підсвідомість людини російськомовних текстів

Російська експертна система "ВААЛ" компанії "Тривола" призначена для психолінгвістичного аналізу текстів російською мовою з прогнозуванням

емоційних несвідомих реакцій аудиторії (слухачів, читачів) і, при необхідності, подальшим психологічним редагуванням тексту – ітераційним процесом його зміни в бажаному напрямку [71, 72].

Фактично система являє собою проблемно-орієнтований аналізатор текстів, реалізований у вигляді шаблону з макросами для текстового процесора MS Word з додатковими DLL – бібліотеками словників. Тому працює система тільки в сімействі операційних систем ОС Windows з встановленим програмним забезпеченням MS Word.

З відкритих джерел відомо, що в даний час система ВААЛ широко використовується в Російській Федерації у великих рекламних і PR-компаніях, консалтингових центрах, банках, видавництвах, вона з успіхом застосовується в передвиборних кампаніях [70-72]. Технологію ВААЛ також використовують в дослідницьких центрах психологи, психотерапевти, лінгвісти та практики нейролінгвістичного програмування.

Система володіє наступними можливостями:

- оцінювання неусвідомлюваного емоційного впливу фонетичної структури текстів та окремих слів на підсвідомість людини;

– генерування слів із заданими фоносемантичними характеристиками;

– завдання характеристики бажаного впливу і цілеспрямоване редагування текстів для досягнення зазначених характеристик;

– коригування тексту за обраними параметрами з використанням словника синонімів на 5 тис. синонімічних рядів з 25 тис. слів;

– настроювання на різні соціальні та професійні групи людей, які можуть бути виділені по використовуваної ними лексиці;

– оцінювання звуко-колірної характеристики текстів;

– введення додаткових нових фоносемантичних шкал користувачем, розширюючи систему в потрібному для нього напрямку;

– факторний аналіз даних з подальшою візуалізацією результатів;

– повноцінний контент-аналіз тексту за великим числом спеціально складених вбудованих і користувальницьких категорій;

– емоційно-лексичний аналіз текстів;

– контекстний контент-аналіз текстів;

– автоматична категоризація текстів.

В основі оцінки емоційного впливу фонетики слова і тексту лежить фоносемантичний аналіз і методи нейролінгвістичного програмування (визначення навантаження на основні сенсорних каналів сприйняття людини, мета-програми та ін.). Для оцінки фоносемантичного впливу слова або словосполучення в системі ВААЛ можна використовувати 24 біполярних шкали. Всім звукам російської мови за цими шкалами зіставлені оцінки. Спеціальні формули дозволяють на основі цих оцінок зіставити оцінки окремим словам, словосполученням, фразам і текстам. І хоча ці оцінки не усвідомлюються людьми, але, як показали експерименти, відбувається досить сильний вплив на підсвідомість.

Експертна система ВААЛ дозволяє проводити автоматизований аналіз тексту з декількох різних по суті, але додаткових до один одного за змістом, позицій. Користувач системи може сам визначити, які з можливих критеріїв варто використовувати для вирішення поставлених перед ним завдань. Безумовно, для ефективного використання того чи іншого блоку технології ВААЛ потрібна згода з вихідними припущеннями авторів і розуміння використовуваної термінології тільки в тому сенсі, в якому його використовують автори.

При реалізації проекту ВААЛ були використані наступні припущення :

1) вибір людиною лексичних та граматичних варіантів з можливих у його рідній мові залежить від його психологічних особливостей. Відповідно, психологічні особливості знаходять своє вираження в його усній і письмовій мові. Аналізуючи усну або письмову мову людини можна реконструювати його картину світу і здійснити атрибутування його картини світу і / або індивідуальності на основі тієї чи іншої системи класифікації;

2) у ситуації вільного вибору людина вибирає і / або краще сприймає тексти (усні чи письмові), відповідні його картині світу і схильний ігнорувати інші варіанти опису;

3) комунікативна ефективність тексту залежить від слабо- або неусвідомлюваних ефектів, створюваних окремими значущими для окремої людини або в культурі в цілому словами (різні форми лексичного символізму), нелінгвістичними характеристиками тексту (наприклад, фоно- та кольоро-ассоціації) і невербальними характеристиками процесу комунікації;

4) текст, включаючи його зміст і контекст, для автора і сприймаючого можуть значити більше, ніж може виявити будь-яка специфічна система опису тексту;

5) різні блоки аналізу текстів в системі ВААЛ є специфічними і незалежними один від одного системами класифікацій лексичних та граматичних форм. Спільна інтерпретація категорій з різних блоків аналізу авторами не передбачалося, але не відкидається, технічна можливість надана і залишається особистою прерогативою кожного легального користувача.

В системі ВААЛ-2000 користувач може сконструювати свої власні або скористатися наступними блоками критеріїв аналізу тексту: психіатричний аналіз; психоаналітичний аналіз; мотиваційний аналіз; емоційно-лексичний аналіз; діагностика мета-програм; фоно- та кольорово-семантичний аналіз.

Вибір блоків аналізу для вирішення конкретних завдань визначається згодою з теоретичними передумовами і методикою реалізації аналізу в ВААЛ, особистими перевагами, рівнем підготовки і завданнями дослідника.

Категорії «***Психіатричного аналізу***» атрибутують текст (як ціле) по відповідності текстам осіб з тією чи іншою акцентуацією. У технології ВААЛ реалізована діагностика паранояльний, демонстративної, депресивної, збудливої і гіпертермічної акцентуацій.

Категорії «***Психоаналітичного аналізу***» оцінюють вираженість в тексті слів, що відносяться до сексуальної символіки (за З.Фрейду), архетипів (за К.Юнгом) і вираженню агресивності.

Категорії «***Мотиваційного аналізу***» визначають вираженість в тексті предикатів мотивації у відповідності з традиційними категоріями мотиваційних властивостей (потреба, мотив, валентність, інструментальна діяльність) з

угрупованням по чотирьох групах мотивів: фізіологічні, досягнення, влади та афіляції.

Категорії «***Емоційно-лексичної оцінки***» дозволяють виявити емоційну насиченість і структуру оцінки за 15 емоційно – оціночними критеріями, виділеним і найбільш значущим в російській культурі.

Категорії «***Діагностики мета-програм***» включають в себе оцінку вираженості каналів репрезентації ; суб'єктивну організацію простору, часу і руху: категорії порівняння; логічних операцій; причинно-наслідковий і "свій-чужий" атрибуцію ; визначення "центру уваги".

Фоно- та ***кольорово-семантичний*** аналіз тексту дозволяє оцінити неусвідомлювані емоційні компоненти тексту і слова, згенерувати штучні слова з високою комунікативною ефективністю.

При необхідності користувач може створити власні лексичні та фонетичні категорії аналізу і використовувати їх окремо або спільно з категоріями, пропонованими концепцією ВААЛ.

Концептуально ВААЛ можна використовувати для забезпечення:

1) системи інформаційно-технологічної підтримки щодо створення деструктивних скритих інформаційно-психологічних атак;

2) протидії відповідним ІП атакам;

2) комерційних інтересів.

Для цього існує можливість, щодо:

– складання текстів виступів і документів з наперед заданими характеристиками впливу на потенційну аудиторію;

– проектування емоційної складової іміджу політичного діяча або організації та активного формування емоційного ставлення до них різних соціальних груп;

– створення емоційно забарвлених рекламних матеріалів і пошуку найбільш вдалих назв і торгових марок;

– неявний експрес-діагностики та психологічного тестування, психо- і гіпнотерапії;

– створення легких в засвоєнні навчальних матеріалів.

Можливе застосування системи в журналістиці, освіті, інформаційному протиборстві та інших областях діяльності людей, де словесний вплив на той чи інший сегмент соціуму є одним з визначальних факторів.

На сьогоднішній день істотним обмеженням системи є її висока вартість і жорстка прив'язка до стороннього програмного забезпечення. Також сама система є повністю закритою, що робить неможливим її подальший розвиток сторонніми розробниками або ж доповненням її необхідними мовними засобами для аналізу.

Отже з одного боку сугестивні деструктивні ІП атаки є найбільш актуальними та значимими з позиції швидкого та неконтрольованого нанесення шкоди, а з іншого боку інформаційні технології та методи щодо протидії такими впливам не мають належного чина науково-прикладних розробок. Це збільшую актуальність таких ІП впливів та рівень шкоди від їх застосування (рис. 2.7).

Таким чином, по зробленому дослідженню можна зробити такі висновки:

1. Інформаційні технології, які відносяться до першого і другого класів, та базуються на методах пошуку, аналізу, складання та формування текстів (інформації) представлені дуже широко. Однак, такі технології: з одного боку враховують лише аналіз текстової інформації за ключовими словами, або додатково за семантикою контенту; з іншого боку не враховується сугестивна складова ІП впливу, а саме психологічно-емоційні та внутрішньо-установочні характеристики особистості.

Тому такі технологічні рішення не забезпечують виявлення сугестивних (скритих) деструктивних ІП атак на підсвідомість особистості (підлітка), тобто вони в сучасній інформаційній війні не придатні для ведення інформаційно-психологічного протиборства та забезпечення національної безпеки держави.

2. Інформаційні технології, які дозволяють проведення більш глибинного аналізу інформаційних ресурсів, а саме враховують можливість виявлення сугестивного впливу на підсвідомість, характеризуються тим, що:

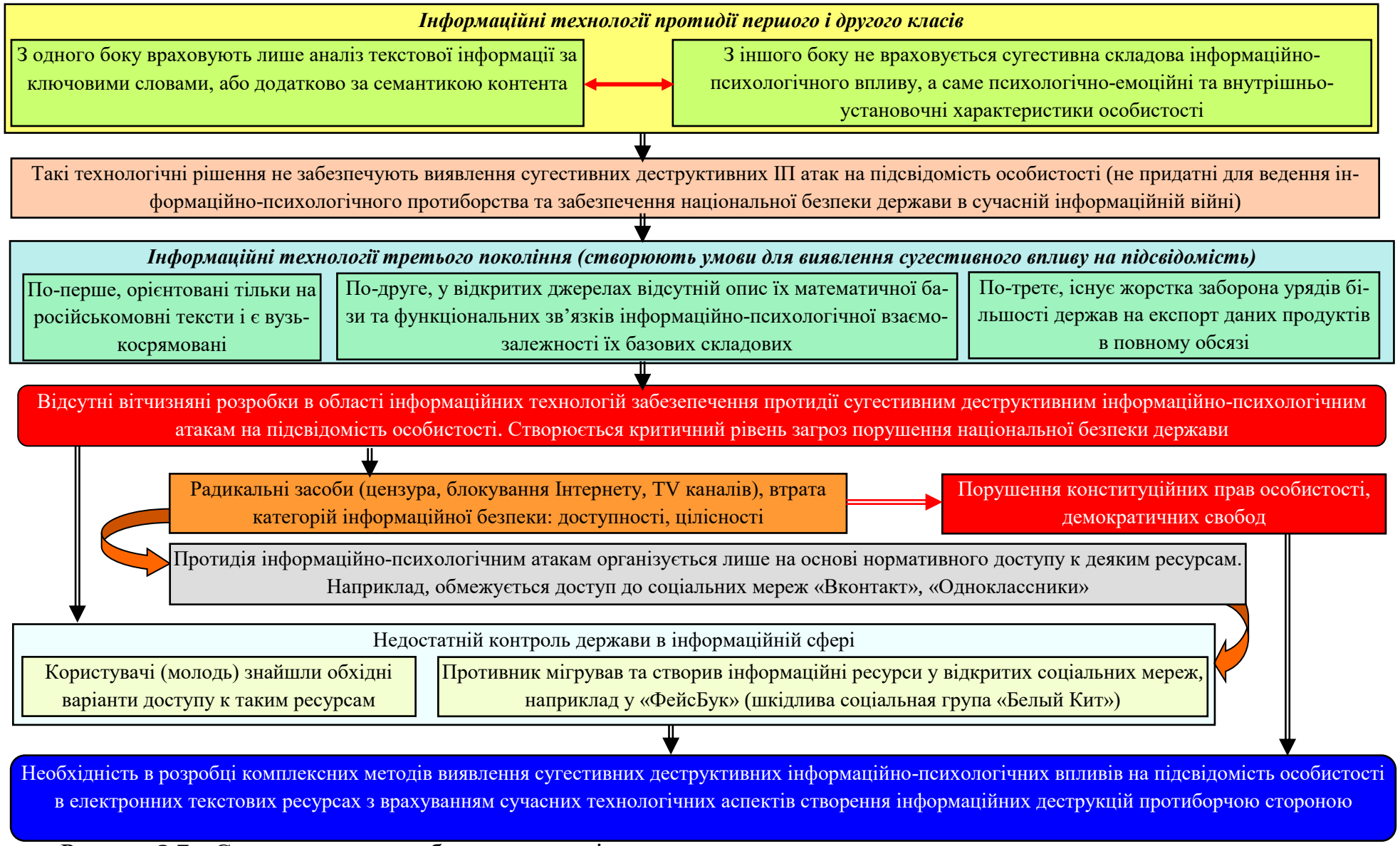


Рисунок 2.7 – Структурна схема обґрунтування підходу для створення комплексного методу виявлення сугестивних інформаційних деструкцій на підсвідомість підлітка

- по-перше, орієнтовані тільки на російськомовні тексти і є вузькоспрямовані;

- по-друге, у відкритих джерелах відсутній опис їх математичної бази та функціональні зв'язки ІП взаємозалежності їх базових скоадових;

- по-третє, існує жорстка заборона урядів більшості держав на експорт даних продуктів в повному обсязі.

3. Відсутність вітчизняних розробок в області інформаційних технологій забезпечення протидії сугестивним деструктивним інформаційно-психологічним атакам (ІП операціям третього покоління) на підсвідомість особистості (підлітків) створює критичний рівень загроз порушення національної безпеки держави.

Отже існує необхідність в розробці комплексних методів виявлення (детектування) сугестивних деструктивних інформаційно-психологічних впливів на підсвідомість особистості (підлітків) в електронних текстових ресурсах з врахуванням сучасних технологічних аспектів (особливостей) створення інформаційних деструкцій протиборчою стороною.

Висновки за другим розділом

1. Розроблено модель загроз ІП безпеки особистості в умовах інформаційного протиборства і демократизації соціуму, коли потрібно забезпечити баланс безпеки особистості одночасно в ІП та ІТ просторах (умова мережецентричності безпеки підлітка в інформаційному просторі). Обґрунтовано, що найбільш актуальними і значущими загрозами ІП безпеки особистості з позиції: виявлення та організації протидії; нанесення шкоди є сугестивні деструктивні ІП впливи. Показано, що одними з ключових ІП атак, які здійснюються в сучасному інформаційно-комунікаційному просторі, є деструктивні інформаційні модифікації в аудіоконтейнерах і електронних текстових ресурсах, а саме: аудіосуггестія, приховані вставки в аудіопотоки; сугестія текстів.

3. Інформаційні технології, які відносяться до першого і другого класів, та базуються на методах пошуку, аналізу, складання та формування текстів (інформації) представлені дуже широко. Однак, такі технологічні рішення не забезпечують виявлення сугестивних (скритих) деструктивних ІП атак на підсвідомість особистості (підлітка), тобто вони в сучасній інформаційній війні не придатні для ведення ІП протиборства та забезпечення національної безпеки держави.

4. Інформаційні технології, які дозволяють проведення більш глибинного аналізу ІР, а саме враховують можливість виявлення сугестивного впливу на підсвідомість, характеризуються тим, що: у відкритих джерелах відсутній опис їх математичної бази та функціональні зв'язки ІП взаємозалежності їх базових складових; існує жорстка заборона урядів більшості держав на експорт даних продуктів в повному обсязі.

5. Відсутність вітчизняних розробок в області інформаційних технологій забезпечення протидії сугестивним деструктивним ІП атакам (ІП операціям третього покоління) на підсвідомість особистості (підлітків) створює критичний рівень загроз порушення національної безпеки держави.

Отже існує необхідність в розробці комплексних методів виявлення (детектування) сугестивних деструктивних ІП впливів на підсвідомість особистості (підлітків) в електронних ТІР з врахуванням сучасних технологічних аспектів (особливостей) створення інформаційних деструкцій протиборчою стороною.

Наукова новизна

Вперше розроблена модель ІП безпеки особистості на основі мережецентричного підходу. Відмінні основи моделі полягають в тому, що: враховується третє покоління ІП атак - сугестивні деструктивні ІП впливу на підсвідомості; враховується наявність дисбалансу з категоріями інформаційної безпеки в ІТ просторі. Це дозволяє оцінити значимість і актуальність загроз ІП безпеки особистості в умовах інформаційного протиборства і демократизації соціуму.

Основні результати науково-прикладних досліджень другого розділу опубліковані та апробовані в таких наукових працях [9, 10, 111, 125].

РОЗДІЛ 3
ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ВИЯВЛЕННЯ СУГЕСТИВНОГО ДЕСТРУКТИВНОГО ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ВПЛИВУ НА ПІДСВІДОМІСТЬ ПІДЛІТКІВ

Викладається побудова інформаційної моделі аналізу ТІР на основі формування семантичного диференціала. На основі розробляється метод виділення значущих лінгвістичних біполярних ознак.

Розробляється метод ідентифікації інформаційно-психологічний вплив структурних компонент (слів) текстових інформаційних ресурсів на підсвідомість особистості на основі формування векторного семантичного диференціала.

Викладаються основні етапи побудови статичних підходів до статичного аналізу ІП впливу тексту на підсвідомість особистості на основі усереднення ВП впливу окремих слів на підсвідомість особистості. Створюється комплексний метод виявлення прихованого інформаційно-психологічного впливу в текстовому інформаційному ресурсі на підсвідомість особистості в багатовимірному фонетичному просторі з прив'язкою до векторних градаційних двополюсних шкал значущих біполярних лінгвістичних ознак на основі формування семантичного диференціала слів і обробкою їх по динамічній технології з накопиченням фрагментарної інформації. Тут базовими технологічними компонентами є: метод динамічного аналізу ТІР з накопиченням його фрагментів на основі формування одновимірного семантичного диференціала; метод динамічного аналізу ТІР з накопиченням його фрагментів на основі оцінки фонетичної значущості слова за однополярною значимою лінгвістичною ознакою

3.1. Створення інформаційної моделі аналізу текстових інформаційних ресурсів на основі формування семантичного диференціалу для виявлення прихованого впливу на підсвідомість особистості

Виявлення сугестивних інформаційних деструкцій в ТІР забезпечується на основі відповідного їх аналізу. При цьому такий аналіз потрібно здійснювати з врахуванням закономірностей звукового впливу ТІР на підсвідомість особистості. В цьому напрямку ключовим підходом є метод семантичного диференціалу [43, 44, 71, 72].

Семантичний диференціал – це технологія аналізу текстових структурних одиниць (елементів) S на основі встановлення кількісних оцінок (фонетичних значень) за сукупністю Θ характерних лінгвістичних біполярних ознак (область ознакового аспекту), що формуються на основі пар антонімів.

Залежно від рівня інтегрованості текстові структурні одиниці (елементи) розглядаються на трьох рівнях, а саме:

- рівень окремих слів S_{word} (текстовий структурний компонент першого порядку);

- рівень текстових фрагментів S_{frg} (текстовий структурний компонент другого порядку);

- рівень цілих текстових документів S_{doc} (текстовий структурний компонент третього порядку – ***текстовий інформаційний ресурс***).

Кількість Q_θ таких лінгвістичних біполярних (ЛБ) ознак вибирається експертним шляхом з урахуванням адаптації щодо предметної області. Відповідно сукупність Θ таких ЛБ ознак, $\Theta = \{\theta_i\}$, $i = \overline{1, Q_\theta}$, з урахуванням предметної області характеризує простір Ω підсвідомого звукового відчуття особистості.

Біполярність ознаки θ_i має на увазі під собою наявність пари антонімів, тобто $\theta_i = \{\alpha_i; \overline{\alpha}_i\}$, $i = \overline{1, Q_\theta}$ [35, 43, 44]. Відповідно формуються два полюси - антонімів характерних лінгвістичних ознак, а саме α_i - позитивний полюс i-го лінгвістичного ознаки з позиції сприйняття звуків на підсвідомість особистості. Від-

повідно $\overline{\alpha}_i$ - негативний полюс i-го лінгвістичного ознаки, формується як антонім щодо позитивного полюса α_i (рис. 3.1).

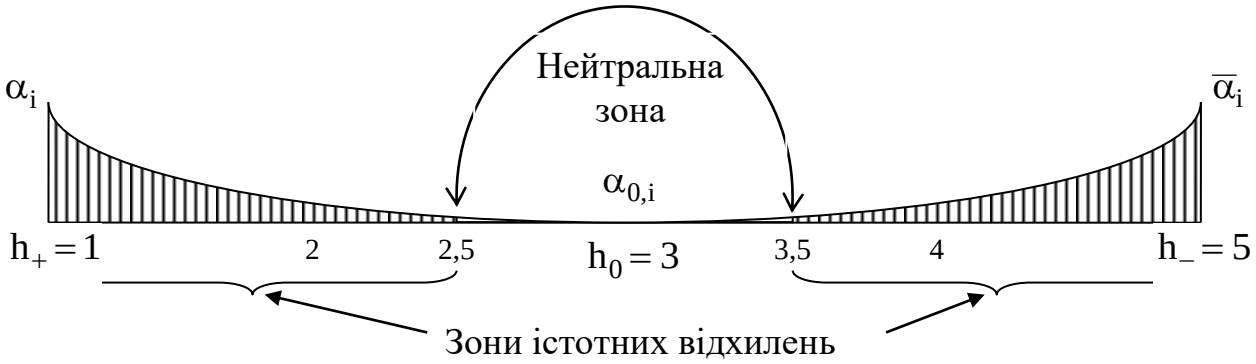


Рисунок 3.1 – Структурна схема лінгвістичної біполярної ознаки

У центрі шкали такого ознаки знаходиться нульовий (нейтральний) рівень $\alpha_{0,i}$, навколо якого утворюється нейтральна зона. Нейтральна зона використовується для виявлення незначущості впливу вибраної ознаки на підсвідомість особистості (підлітка) з урахуванням особливостей обраної предметної області. В табл. 3.1 наведено характерний приклад формування біполярних ознак для $Q_\theta = 25$. У цьому випадку формується 25 біполярних шкал для лінгвістичних біполярних ознак, за якими визначається семантичний диференціал.

Таблиця 3.1

Характерне формування 25 пар антонімів лінгвістичних біполярних ознак для розрахунку семантичного диференціалу

№ шкали, i	Ознаковий аспект, θ_i		№ шкали, i	Ознаковий аспект, θ_i	
	антонім 1	антонім 2		антонім 1	антонім 2
1	хороший	поганий	14	веселий	сумний
2	великий	маленький	15	безпечний	страшний
3	ніжний	грубий	16	величний	низинний
4	жіночий	мужній	17	яскравий	тьмяний
5	світлий	темний	18	округлий	незграбний
6	активний	пасивний	19	радісний	сумний
7	простий	складний	20	гучний	тихий
8	сильний	слабкий	21	довгий	короткий
9	гарячий	холодний	22	хоробрий	боягузливий
10	швидкий	повільний	23	добрий	злий
11	гарний	відштовхуючий	24	могутній	кволий
12	гладкий	шорсткий	25	рухомий	повільний
13	легкий	важкий			

Для отримання фонетичних значень $f_{i,\tau}$ букв s_τ (s_τ - τ-я буква алфавіту) текстових інформаційних ресурсів по ЛБ ознаками необхідно сформувати їх опис у вигляді звуко-букв b_τ (b_τ - τ-а звуко-буква). Це пояснюється тим, що самі літери при написанні не враховують всіх психологічно важливих особливостей звуків. ***Одна буква безпосередньо не може відобразити м'яку і тверду приголосну***. Навпаки, звуко-букви враховують особливості вимови.

У цьому випадку забезпечується облік вимови двох букв ***(поточної і наступної за нею)***. Відповідно варіації звучання всіляких двобуквених комбінацій утворюють алфавіт звуко-букв. Потужність такого алфавіту позначається як Q_b. Наприклад, для російськомовних текстів існує Q_b=45 звуко-букв b_τ, $\tau=\overline{1,45}$ в залежності від звучання букв алфавіту російської мови. Їх кількість більше потужності алфавіту, тобто $Q_s < Q_b$, за рахунок того, що деякі букви (голосні) по різному звучати перед деякими буквами (приголосними). В даному випадку враховується лінгвістичні особливості мови.

Кожній звуко-букві b_τ потрібно поставити кількісне значення $f_{i,\tau}$ відповідно до обраної шкали лінгвістичних біполярних ознак. Це дозволяє ідентифікувати рівень впливу кожної звуко-букви в просторі звукових відчуттів особистості. У цьому випадку кожна звуко-буква алфавіту детектується (розкладається) по Q_θ характерними біполярним ознаками

Таке детектування проводиться експертним шляхом. В цьому випадку виставляються експертні оцінки $f_{i,\tau}$ з урахуванням сприйняття кожної звуко-букви по градаціях шкал біполярного ознакового простору. Це задається таким співвідношенням:

$$\varphi_{sd}: b_\tau \xrightarrow{\theta_i = \{\alpha_i; \overline{\alpha}_i\}} f_{i,\tau}, \quad \tau=\overline{1,Q_b}, \; i=\overline{1,Q_\theta}. \qquad (3.1)$$

Тут φ_{sd} - функціонал встановлення кількісного відповідності кожної звуко-букви біполярній ознаці; $f_{i,\tau}$ - фонетичне значення τ-й звуко-букви по i-ій біполярній ознаці.

Фізичний сенс фонетичного значення. Величина $f_{i,\tau}$ позиціонує τ-у звуко-букву по шкалі i-і біполярної ознаки.

Величина $f_{i,\tau}$ кількісно відображає рівень позиціонування звуко-букви щодо позитивного і негативного її відчуття на підсвідомому рівні особистості (підлітка). Значить величина $f_{i,\tau}$ кількісним чином встановлює рівень і напрямок ІП впливу τ-й звуко-букви на підсвідомість підлітка по i-ій біполярній ознаці.

Весь процес можна назвати як ***ідентифікація звуко-букви в просторі ознак звукових відчуттів особистості на його підсвідомому рівні*** (в просторі звукового впливу на підсвідомість підлітка). Така ідентифікація проводиться шляхом позиціонування звуко-букви на шкалах біполярних ознак. Приклад таблиці формування фонетичних оцінок для 45 звуко-букв за Q_b ЛБ ознаками наведено в **Додатоку Б**.

В результаті ідентифікації всіх звуко-букв в просторі ознак їх звукового впливу на підсвідомість формується двовимірна матриця F_{sd}, тобто.

$$F_{sd} = \begin{vmatrix} f_{1,1} & \dots & f_{1,\tau} & \dots & f_{1,Q_b} \\ & & \dots & & \\ f_{i,1} & \dots & f_{i,\tau} & \dots & f_{i,Q_b} \\ & & \dots & & \\ f_{Q_\theta,1} & \dots & f_{Q_\theta,\tau} & \dots & f_{Q_\theta,Q_b} \end{vmatrix}$$

Простір звукових відчуттів (звукового впливу) є простором ознак. Причому кожна ознака є біполярною. Тому такий простір можна визначити як багатовимірний біполярний простір ознак.

Величина $f_{i,\tau}$ приймає значення з області $f_{i,\tau} \in [h_+ ; h_-]$.

Тут h_- - верхня межа для кількісної оцінки ступеня близькості i-ї звуко-букви щодо негативного полюса $\overline{\alpha}_i$ ознаки θ_i; h_+ - верхня межа для кількісної оцінки ступеня близькості i-й звуко-букви щодо позитивного полюса α_i ознаки θ_i.

Зріз (вектор) по кожному рядку F_i матриці F_{sd} визначає зміст (семантику) i-його біполярної ознаки за сукупністю звуко-букв, що записується таким виразом:

$$F_i = \{f_{i,1},...,f_{i,\tau},...,f_{i,Q_b}\}.$$

Вектор F_i визначає значимість i- біполярної ознаки за сукупністю звуко-букв для проведення оцінки впливу на підсвідомість особистості (підлітка) через його звукові відчуття. Чим більша кількість величин $f_{i,\tau}$, чиї значення наближаються до крайніх меж h_- і h_+ полюсів ознаки θ_i, тим вище значимість обраної біполярної ознаки для оцінки звукового впливу на підсвідомість особистості. Очевидно, що позиціювання значень $f_{i,\tau}$ поблизу нейтральної зони i-го біполярної ознаки вказує на його незначимість для визначення рівня звуку впливу на підсвідомість людини для даної предметної області.

Для кількісної оцінки ступеня значимості біполярної ознаки θ_i ***пропонується*** використовувати ***інформаційний підхід***. Тоді, чим більше ступінь $V(F_i)$ невизначеності (інформативності ознаки), тим вище його значимість для визначення рівня впливу звуко-букв на підсвідомість людини через звукове сприйняття. В даному випадку цікавить невизначеність без урахування знака впливу звуко-букв на підсвідомість людини (позитивне чи деструктивне). Тому для проведення такої оцінки пропонується використовувати величини $_{\Delta}f_{i,\tau}$, рівні абсолютним значенням відхилень відповідних фонетичних значень $f_{i,\tau}$ щодо нульового рівня h_0 градаційній шкали біполярних ознак θ_i, а саме:

$$_{\Delta}f_{i,\tau} = |h_0 - f_{i,\tau}|. \qquad (3.2)$$

В цьому випадку для i-ї біполярної ознаки утворюється послідовність $_{\Delta}F_i$ відліків (фонетичних значень), тобто:

$$_{\Delta}F_i = \{ _{\Delta}f_{i,1},..., _{\Delta}f_{i,\tau},..., _{\Delta}f_{i,Q_b}\}, \qquad (3.3)$$

довжина якої дорівнює Q_b.

Кожен такий відлік $_{\Delta}f_{i,\tau}$ в загальному випадку є дійсним числом, і буде обмежений зверху цілочисельною величиною $_{\Delta}f_{i,max}$, що задається наступною нерівністю:

$$0 \le {}_{\Delta}f_{i,\tau} < {}_{\Delta}f_{i,max}. \qquad (3.4)$$

У цьому співвідношенні величина $_{\Delta}f_{i,max}$ визначається за формулою:

$$_{\Delta}f_{i,max} = ((\max_{1\le\tau\le Q_b} {}_{\Delta}f_{i,\tau} - \min_{1\le\tau\le Q_b} {}_{\Delta}f_{i,\tau})/\delta_i) + 1,$$

де δ_i - крок дискретизації величин $_{\Delta}f_{i,\tau}$ для послідовності $_{\Delta}F_i$.

Тому ***послідовність*** $_{\Delta}F_i$ ***пропонується розглядати як число в матеріальному нерівноважному просторі ознак*** Ω. Звідки кількість $V(F_i)$ інформації (ступінь інформативності ознаки θ_i) буде визначатися як

$$V(F_i) = [\ell og_2 \prod_{\tau=1}^{Q_b}((\max_{1\le\tau\le Q_b} {}_{\Delta}f_{i,\tau} - \min_{1\le\tau\le Q_b} {}_{\Delta}f_{i,\tau})/\delta_i) + 1)] + 1. \qquad (3.5)$$

Чим більше величина $V(F_i)$, тим вище інформативність біполярної ознаки θ_i. І, навпаки, зниження величини $({}_{\Delta}f_{i,\tau} + 1)$ відповідає зменшенню ступеня невизначеності розподілу значень $_{\Delta}f_{i,\tau}$ для відповідної ознаки.

Визначення величин $V(F_i)$ для всіх ознак простору Ω, тобто. $i=\overline{1, Q_\theta}$ дозволяє виділити найбільш значущі біполярні ознаки для проведення оцінки ступеня ІП впливу звуко-букв на підсвідомість людини через його звукове сприйняття. Відсікання незначущих ознак проводиться з використанням порогового значення $V(F)_h$. Тоді, якщо виконується нерівність

$$V(F_i) < V(F)_h, \qquad (3.6)$$

то і-й ознака є незначимим. Навпаки, для умови $V(F_i) \geq V(F)_h$ біполярна і-а ознака буде значимою, тобто. $\theta_i \rightarrow \theta(h)_i$. Послідовність значущих ознак буде позначатися як $\Theta(h)_i = \{\theta(h)_1,...,\theta(h)_i,...,\theta(h)_{Q_h}\}$. В результаті такої селекції подальша обробка ТІР буде здійснюватися з використанням інформації тільки по значимим біполярним ознакам $\theta(h)_i$

Значить по викладеному матеріалу можна зробити висновок, побудована (***вперше***) інформаційна модель аналізу ТІР на основі формування семантичного диференціала (формування фонетичних оцінок з прив'язкою до двополюсної шкали лінгвістичних ознак). На основі чого були розроблені:

- метод виділення значущих лінгвістичних біполярних ознак на основі представлення фонетичних оцінок звуко-букв алфавіту в матеріальному нерівноважному позиційному просторі. Основна відмінність тут складається в тому, що векторний фонетичний простір лінгвістичної біполярної ознаки по всім звуко-буквах представляється в двополярному матеріальному нерівноважному позиційному базисі. Це дозволяє використовувати в процесі аналізу ТІР тільки значущі ЛБ ознаки, що в кінцевому підсумку скорочує часові затримки на обробку ТІР.

3.2. Розробка методу виявлення прихованого інформаційно-психологічного впливу в локальній компоненті текстового інформаційного ресурсу на підсвідомість особистості на основі семантичного диференціала

Для виявлення прихованого інформаційно-психологічного впливу в структурних компонентах ТІР ***пропонується*** використовувати технологію семантичного диференціала. В цьому випадку структурна компонента ТІР представляється в фонетичному просторі (просторі сприйняття звуків на рівні підсвідомості особистості) з урахуванням прив'язки до двополюсної (біполярної) шкали лінгвістичних ознак, тобто з урахуванням позиціонування щодо негативного і позитивного полюсів.

Фонетичний опис структурних компонент ТІР представляє собою семантику їх звукового сприйняття але тільки не на свідомому рівні, а на рівні підсвідомості особистості. Диференціал визначається наявністю прив'язки до двополюсної шкали лінгвістичних ознак.

У загальному випадку визначення спрямованості прихованого ІП впливу слова на підсвідомість особистості в фонетичному просторі з використанням технології семантичного диференціала пропонується організовувати на основі двох підходів, а саме:

1. Перший підхід базується на визначенні прихованого ІП впливу структурних компонент ТІР на основі фонетичних оцінок з прив'язкою до окремих лінгвістичних біполярних ознак (одномірний фонетичний простір по ЛБ ознаці). Відповідно кількість таких оцінок буде дорівнює кількості Q_h значимих ЛБ ознак.

2. Другий підхід полягає у визначенні інтегрованих оцінок фонетичного впливу структурних компонент ТІР на підсвідомість особистості за всіма ЛБ ознаками. Тут розглядається векторний простір звукового впливу на підсвідомість особистості.

Перевага першого підходу полягає в тому, що існує можливість визначити деструктивність прихованого ІП впливу слова (структурної компоненти ТІР першого порядку) по конкретним лінгвістичним ознаками, тобто досягається деталізація аналізу ТІР за словами на предмет виявлення інформаційних деструкцій. Таку інформаційну технологію аналізу ТІР допускається використовувати для створення експертних систем підтримки та прийняття рішень спеціальними психологічними і реабілітаційними центрами. Наприклад, така технологія може використовуватися для створення автоматизованих робочих місць дитячих психологів, як підтримка процесу оцінки морально-психологічного стану підлітків, оцінки наявності інформаційних деструкцій в ІР в автоматизованому режимі, створення спеціальних ТІР для коригувальних ІП впливів в напрямку нормалізації і гармонійності розвитку особистості.

У той же час такий підхід не забезпечує отримання інтегрованих оцінок. У свою чергу інтегровані оцінки дозволяють підвищити ефективність всього інформаційно-технологічного процесу інформаційно-психологічної протидії, а саме:

- по-перше скорочуються часові затримки на обробку великої сукупності фонетичних значень по кожній ЛБ ознаці, а також знижується обсяг пам'яті на зберігання результатів аналізу. Це створює умови для забезпечення таких категорій інформаційної безпеки особистості як доступність і цілісність ІР;

– по-друге інтегрована оцінка створює можливість для створення технологій інформаційно-психологічної корекції ТІР без їх блокування.

Другий підхід для аналізу ТІР допускає своє використання як складова етапу інформаційної технології забезпечення ІП безпеки підлітків в інфокомунікаційних просторі. Тут використовується перевага другого підходу, що складається в автоматичної обробки ТІР без участі особи приймаючої рішення. Тоді існує можливість використовувати такий підхід для:

– моніторингу Інтернет ресурсів;

– створення спеціальних мережевих фільтрів для виявлення прихованого деструктивного ІП впливу в автоматичному режимі.

Введемо структурну одиницю текстового повідомлення першого порядку $S(\ell;t)_u$, де $S(\ell;t)_u$ - u-е слово для t-го фрагмента ℓ-го документа (закінченого за змістом повідомлення). Величина $S(\ell;t)_u$ є лінгвістичної змінною, довжина $|S(\ell;t)_u|$ якої дорівнює кількості букв в слові, тобто.

$$S(\ell;t)_u = \{s(\ell;t)_{u,1},...,s(\ell;t)_{u,\tau},...,s(\ell;t)_{u,|S(\ell;t)_u|}\}, \quad (3.7)$$

де $s(\ell;t)_{u,\tau}$ - τ-а буква для слова $S(\ell;t)_u$, $\tau = \overline{1,|S(\ell;t)_u|}$.

Для оцінки такого сугестії все вихідне текстове слово $S(\ell;t)_u$ виражається через звуко-слово $B(\ell;t)_u$. Дане перетворення задається функціоналом φ_{vc}, званим також звуковим компілятором (voice compiling) текстового слова, тобто:

$$\varphi_{vc}: S(\ell;t)_u \to B(\ell;t)_u. \quad (3.8)$$

В результаті чого, формується лінгвістична змінна (звуко-слово) $B(\ell;t)_u$, що має довжину $|B(\ell;t)_u|$ звуко-букв., тобто

$$B(\ell;t)_u = \{b(\ell;t)_{u,1},...,b(\ell;t)_{u,\tau},...,b(\ell;t)_{u,|B(\ell;t)_u|}\}, \quad (3.9)$$

де $B(\ell;t)_u$ - u-е звуко-слово для t-го фрагмента ℓ-го документа (закінченого за змістом повідомлення); $b(\ell;t)_{u,\tau}$ - τ-я звуко-буква для звуко-слова $B(\ell;t)_u$, $\tau = \overline{1,|B(\ell;t)_u|}$.

Після чого здійснюється фонетичний аналіз кожної звуко-букви $b(\ell;t)_{u,\tau}$ окремо. Для всіх звуко-букв слова $B(\ell;t)_u$ формуються фонетичні значення $f(\ell;t;u)_{i,\tau}$. Тут використовується наступне функціональне перетворення:

$$\varphi_{sd}: b(\ell;t)_{u,\tau} \xrightarrow{\theta_i = \{\alpha_i;\ \overline{\alpha}_i\}} f(\ell;t;u)_{i,\tau},\ \tau=\overline{1,|B(\ell;t)_u|},\ i=\overline{1,Q_h}, \quad (3.10)$$

де $f(\ell;t;u)_{i,\tau}$ - фонетичне значення τ-ї звуко-букви по i-ій біполярній ознаці для u-го звуко-слова t-го фрагмента ℓ-го документа (закінченого за змістом повідомлення або текстового інформаційного ресурсу (TIP)); Q_h - кількість значущих ознак для досліджуваної предметної сфери з позиції значущості впливу на підсвідомість людини через його звукові відчуття.

Шкала відхилень семантичного диференціала по їх фонетичним значенням для лінгвістичного біполярного ознаки представлена на рис. 3.1. Центральне значення шкали h_0 дорівнює 3,0. Це нейтральне значення, яке не може виділити жоден ознаковий аспект. Так само нейтральною зоною вважається зона від 2,5 до 3,5. Значення в цих межах вважаються незначними коливаннями. Все що виходить за межі коливань, можна вважати відхиленням від норми відповідно в напрямку позитивного або негативного інформаційно-психологічного впливу. Саме зони істотного відхилення говорять нам про те, до якого ознакового аспекту можна віднести букву та все слово, як структурний компонент текстового інформаційного ресурсу. Оцінки є імовірнісними, тобто, підтверджені випадковим коливанням. При цьому самі ознакові аспекти не варто погоджувати

із значенням слова. Це обумовлено тим, що оцінка дається по змістовності звукової форми, а не за значенням слова.

Розглянемо перший підхід. Тут проводиться оцінка сугестивного впливу звуко-слова на підсвідомість особистості через його звукове сприйняття в одно-вимірному фонетичному просторі, тобто в фонетичному просторі з прив'язкою до шкалою окремих ЛБ ознак.

Визначити семантичну складову для слова на базі першого підходу можна ***двома основними способами***.

Першим і більш простим варіантом розрахунку є визначення середньої $F(\ell;t;u)_i$ значимості всіх звуко-букв в слові по i-ій лінгвістичній біполярній ознаці. Визначення величини $F(\ell;t;u)_i$ проводиться по формулі:

$$F(\ell;t;u)_i = \sum_{\tau=1}^{|B(\ell;t)_u|} f(\ell;t;u)_{i,\tau}, \qquad (3.11)$$

де $f(\ell;t;u)_{i,\tau}$ - фонетичне значення τ-й звуко-букви по i-му біполярному признаку для u-го звуко-слова t-го фрагмента ℓ-го документа (закінченого по змістом повідомлення або ТІР);

$|B(\ell;t)_u|$ - кількість звуко-букв в слові $B(\ell;t)_u$.

Фонетичне значення $f(\ell;t;u)_{i,\tau}$ звуко-букв це встановлена ймовірнісна величина, яка визначається та корегується експериментальним шляхом. Фонетичне значення $f(\ell;t;u)_{i,\tau}$ для кожної звуко-букви встановлюється окремо залежно від шкали ЛБ ознак, за якою здійснюється аналіз. У табл. 3.2 наведена частина фонетичних значень звуко-букв для трьох шкал ЛБ ознак.

Таблиця 3.2

Фрагмент фонетичного значення звуко-букв

Ознакова шкала для розрахунку семантичного диференціалу	Звуко-буква				
	А	Б	В	Г	Д
хороший – поганий	1,5	2,4	2,9	3,2	2,4
світлий – темний	2,2	3,2	3,0	3,3	3,2
красивий – відштовхуючий	2,0	2,6	3,0	2,8	2,4

Однак даний підхід визначення семантичної складової для слова за формулою (3.11) не дає точного уявлення про значущість слова, так як не всі звуко-букви в слові є рівноправними.

В цьому випадку пропонується враховувати наступні особливості.

По-перше. Психологи вважають, що для людини перший звук у слові має куди більше значення, ніж інші, за їх твердженням він в 4 рази помітніше. Так само не варто забувати про ударний звук, він так само виділяється в слові, хоча і не так як перший, тільки в 2 рази. Це говорить нам про те, що при розрахунку сумарної фонетичної складової всіх звуко-букв слова, вагу першого потрібно збільшити в 4 рази, а ударного в 2 рази.

По-друге. Крім розташування букв у слові, не менш важливу роль грає зустрічальність букв в словах. Тобто, є букви, які часто зустрічаються (наприклад, А, О, Т, Н), а є, які рідко зустрічаються (наприклад, Ф, Х). Пи цьому ті букви, що рідко зустрічаються є більш помітними в словах в процесі їх фонетичного представлення. Звідси випливає висновок, що при розрахунку фонетичної значимості слова потрібно брати до уваги зустрічальність букв в словах. Коефіцієнт зустрічальності, або частотність, визначається з урахуванням кількості разів зустрічаємості букви на тисячу звукобукв.

По-третє. Звукобукви ж у свою чергу ще поділяються на ударні і безударні.

З цього випливає що інформативність (фонетична помітність) звуко-букви знаходиться в зворотній залежності від її частотності (зустрічальності). Тобто найменш інформативна звуко-буква має максимальну частотність. Навпаки звуко-буква буде в стільки разів інформативніше, скільки разів її частотність менше максимальної для звуко-букв даного слова.

Тому, при розрахунку фонетичної складової звукового комплексу потрібно збільшити вагу середніх оцінок для: першої, ударної звуко-букви, та для всіх звуко-букв, крім звуко-букви з максимальною частотою. Вираз для визначення коефіцієнту $k(\ell;t;u)_{i,\tau}$ кожної звуко-букви $b(\ell;t)_{u,\tau}$ в звуко-слові $B(\ell;t)_u$ має наступний вигляд:

$$k(\ell;t;u)_{i,\tau} = P(\ell;t;u)_{i,\tau}^{(max)} / P_{\tau}, \qquad (3.12)$$

де $P(\ell;t;u)_{i,\tau}^{(max)}$ – це максимальна частотність звуко-букви $b(\ell;t)_{u,\tau}$ в даному слові $B(\ell;t)_u$; P_{τ} – це табличне значення частотності звукобукви (**Додаток Б**).

Відповідно для першої звуко-букви необхідно збільшити значення коефіцієнта $k(\ell;t;u)_{i,1}$ в 4 рази. Тоді вираз (3.12) запишеться як:

$$k(\ell;t;u)_{i,1} := 4k(\ell;t;u)_{i,1} = 4P(\ell;t;u)_{i,\tau}^{(max)} / P_{\tau}. \qquad (3.13)$$

Для ударної звуко-букви необхідно збільшити значення коефіцієнта в 2 рази, тобто вираз (3.12) прийме вигляд:

$$k(\ell;t;u)_{i,\tau}^{(уд)} = 2\,k(\ell;t;u)_{i,\tau} = 2P(\ell;t;u)_{i,\tau}^{(max)} / P_{\tau}. \qquad (3.14)$$

З урахуванням коефіцієнтів $k(\ell;t;u)_{i,\tau}$ кожної звуко-букви $b(\ell;t)_{u,\tau}$, оцінка фонетичної складової $F'(\ell;t;u)_i$ слова $B(\ell;t)_u$ *по* i*-ій лінгвістичній біполярній ознаці* проводиться за такою формулою:

$$F'(\ell;t;u)_i = \Big(\sum_{\tau=1}^{|B(\ell;t)_u|} k(\ell;t;u)_{i,\tau}\, f(\ell;t;u)_{i,\tau}\Big) / \sum_{\tau=1}^{|B(\ell;t)_u|} k_i, \qquad (3.15)$$

де $f(\ell;t;u)_{i,\tau}$ - фонетичне значення τ-й звуко-букви по i-ій біполярній ознаці для u-го звуко-слова t-го фрагмента ℓ-го документа (закінченого за змістом повідомлення або текстового інформаційного ресурсу (ТІР)); $|B(\ell;t)_u|$ - кількість звуко-букв в слові $B(\ell;t)_u$.

На рис. 3.2 приведена структурно-функціональна схема методу розрахунку одновимірного семантичного диференціала для звуко-слова $B(\ell;t)_u$.

Розрахунок семантичного диференціала для слова $S(\ell;t)_u$ пропонується проводити на основі наступних етапів (послідовності дій):

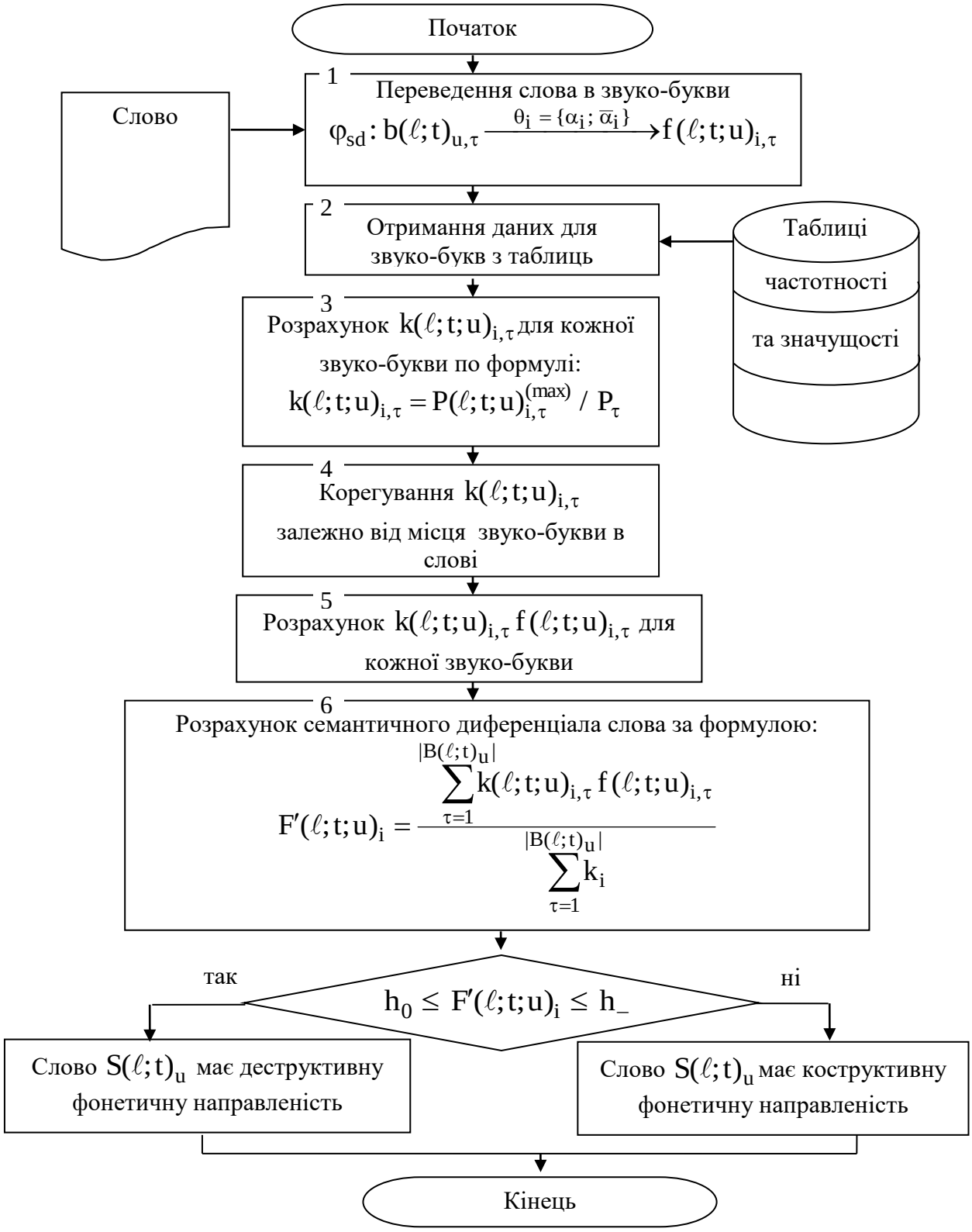


Рисунок 3.2 – Структурно-функціональна схема визначення одномірного семантичного диференціала слова за окремою ЛБ ознакою

1) мінімальної одиницею для розрахунків виступає слово $S(\ell;t)_u$. Необхідно враховувати, що важливі не тільки букви, а й місце їх розташування в

слові. Це дозволяє з набору букв отримати звуко-букви $b(\ell;t)_{u,\tau}$. Тому на першому (підготовчому) етапі аналізу проводиться переклад слова або послідовності букв в набір звуко-букв. Для цього використовується співвідношення (3.10) по значимим ЛБ ознаками;

2) на другому етапі для кожної звуко-букви вибираються табличні значення їх частотності і значущості виходячи з аналізованого простору ознак аспекту. Для цього використовуються дві таблиці. Перша таблиця містить інформацію P_τ про частотність звуко-букв, друга таблиця включає дані про значимість звуко-букв. З таблиці частотності завжди вибираються однакові значення незалежно від ознаки за яким здійснюється аналіз. Таблиця значущості має 25 різних наборів для кожної звуко-букви в залежності від простору ознак аспекту;

3) на третьому етапі розраховуються коефіцієнти $k(\ell;t;u)_{i,\tau}$ кожної звуко-букви $b(\ell;t)_{u,\tau}$ в звуко-слові $B(\ell;t)_u$ по формулі (3.12);

4) після чого отримані коефіцієнти коригуються в залежності від помітності букв в звуко-слові, а саме:

- за допомогою формул (3.13) для першої звуко-букви $b(\ell;t)_{u,1}$ звуко-слова;

- вираз (3.14) для ударної звуко-букви $b(\ell;t)_{u,удр}$. При цьому визначення ударних звуків у слові можна реалізувати за допомогою спеціально сформованих словників;

5) на п'ятому етапі спостерігається збільшення фонетичного значення для кожного звуко-букви $b(\ell;t)_{u,\tau}$ в залежності від коефіцієнта. Тоді кожне фонетичне значення отримане на другому етапі перемножуємо на відповідний коефіцієнт $k(\ell;t;u)_{i,\tau}$;

6) наступним етапом є розрахунок значення ***одновимірного семантичного диференціала*** - узагальненої фонетичної оцінки спрямованості та рівня ІП впливу структурної компоненти (слова) ТІР на підсвідомість особистості в одновимірному біполярному лінгвістичному просторі по всьому звуко-буквах. Для цього використовується співвідношення (3.15). Величина $F'(\ell;t;u)_i$ є

значенням одновимірного семантичного диференціала слова по значимого i-ій ЛБ ознаці.

7) завершальний етап використовується для встановлення спрямованості сугестивного ІП впливу конкретного слова текстового інформаційного ресурсу на підсвідомість особистості по i-ій Тут здійснюєься перевірка входження величини $F'(\ell;t;u)_i$ в інтервал негативною спрямованості шкали ЛБ ознаки. Якщо виконується нерівність $h_0 \le F'(\ell;t;u)_i \le h_-$, то слово $S(\ell;t)_u$ має деструктивну фонетичну направленість. Та, навпаки.

Розглянемо оцінку інтегрованого сугестивного впливу звуко-слова на підсвідомість особистості через його звукове сприйняття по всім біполярним лінгвістичним ознакам.

Для всіх звуко-букв слова $B(\ell;t)_u$ будується двовимірна матриця $F(\ell;t)_u$, яка є вибіркою з матриці F_{sd}, а саме:

$$F(\ell;t)_u = \begin{vmatrix} f(\ell;t;u)_{1,1} & \dots & f(\ell;t;u)_{1,\tau} & \dots & f(\ell;t;u)_{1,|B(\ell;t)_u|} \\ & & \dots & & \\ f(\ell;t;u)_{i,1} & \dots & f(\ell;t;u)_{i,\tau} & \dots & f(\ell;t;u)_{i,|B(\ell;t)_u|} \\ & & \dots & & \\ f(\ell;t;u)_{Q_h,1} & \dots & f(\ell;t;u)_{Q_h,\tau} & \dots & f(\ell;t;u)_{Q_h,|B(\ell;t)_u|} \end{vmatrix}, \qquad (3.16)$$

де $f(\ell;t;u)_{i,\tau}$ - фонетичне значення τ-ї звуко-букви по i-ій біполярній ознаці для u-го звуко-слова t-го фрагмента ℓ-го документа (закінченого за змістом повідомлення або ТІР); Q_h - кількість значущих ознак для досліджуваної предметної сфери з позиції значущості впливу на підсвідомість особистості через його звукові відчуття.

При цьому потрібно враховувати, що на різних позиціях можуть перебувати однакові звуко-букви, тобто.

$$b(\ell;t)_{u,\gamma} \equiv b(\ell;t)_{u,\chi}, \quad \gamma \ne \chi. \qquad (3.17)$$

Величини $f(\ell;t;u)_{i,\tau}$ є оцінками фонетичного значення відповідних звуко-букв без урахування спрямованості їх звукового впливу на підсвідомість підлітка. Тому для врахування такого впливу матриця $F(\ell;t)_u$ перекладається в матрицю ${}_\Delta F(\ell;t)_u$ відносних відхилень фонетичних величин ${}_\Delta f(\ell;t;u)_{i,\tau}$, відносно нульового рівня h_0 градаційній шкали лінгвістичної біполярної ознаки θ_i. Для цього використовується така формула ${}_\Delta f(\ell;t;u)_{i,\tau} = |h_0 - f(\ell;t;u)_{i,\tau}|$. З урахуванням знака ϕ такого відхилення, отримаємо наступне співвідношення для подання звуко-букви $b(\ell;t)_{u,\tau}$:

$$b(\ell;t)_{u,\tau} = \{{}_\Delta f(\ell;t;u)^{(\phi)}_{i,\tau};\ \phi(\ell;t;u)_{i,\tau}\}, \tag{3.18}$$

де $\phi(\ell;t;u)_{i,\tau}$ - знак відхилення фонетичного значення звуко-букви від нульового рівня h_0 градаційної шкали i-ї біполярної ознаки.

Цей вираз є ядром для формування функціоналу φ_{phc} реалізації фонетичного компілятора (phonetic compiler) звуко-букви, тобто:

$$\varphi_{phc}: b(\ell;t)_{u,\tau} \to \{{}_\Delta f(\ell;t;u)^{(\phi)}_{i,\tau};\ \phi(\ell;t;u)_{i,\tau}\}. \tag{3.19}$$

В результаті застосування функціоналу φ_{phc} до всіх звуко-букв звуко-слова $B(\ell;t)_u$, отримаємо

$$\varphi_{phc}: F(\ell;t)_u \to \{{}_\Delta F(\ell;t)_u;\ \Phi\} \tag{3.20}$$

або

$$F(\ell;t)_u \to \begin{vmatrix} {}_\Delta f(\ell;t;u)^{(\phi)}_{i,1} & \dots & {}_\Delta f(\ell;t;u)^{(\phi)}_{1,\tau} & \dots & {}_\Delta f(\ell;t;u)^{(\phi)}_{1,|B(\ell;t)_u|} \\ & & \dots & & \\ {}_\Delta f(\ell;t;u)^{(\phi)}_{i,1} & \dots & {}_\Delta f(\ell;t;u)^{(\phi)}_{i,\tau} & \dots & {}_\Delta f(\ell;t;u)^{(\phi)}_{i,|B(\ell;t)_u|} \\ & & \dots & & \\ {}_\Delta f(\ell;t;u)^{(\phi)}_{Q_h,1} & \dots & {}_\Delta f(\ell;t;u)^{(\phi)}_{Q_h,\tau} & \dots & {}_\Delta f(\ell;t;u)^{(\phi)}_{Q_h,|B(\ell;t)_u|} \end{vmatrix} \bigcup$$

$$\bigcup \begin{vmatrix} \phi(\ell;t;u)_{1,1} & \dots & \phi(\ell;t;u)_{1,\tau} & \dots & \phi(\ell;t;u)_{1,|B(\ell;t)_u|} \\ & \dots & & & \\ \phi(\ell;t;u)_{i,1} & \dots & \phi(\ell;t;u)_{i,\tau} & \dots & \phi(\ell;t;u)_{i,|B(\ell;t)_u|} \\ & \dots & & & \\ \phi(\ell;t;u)_{Q_h,1} & \dots & \phi(\ell;t;u)_{Q_h,\tau} & \dots & \phi(\ell;t;u)_{Q_h,|B(\ell;t)_u|} \end{vmatrix}.$$

Тут Ф - матриця знаків відхилень фонетичних значень від рівня h_0. Величина $\phi(\ell;t;u)_{i,\tau}$ вказує на спрямованість впливу фонетичного значення звуко-букви на підсвідомість особистості, а саме:

$$\phi(\ell;t;u)_{i,\tau} = \begin{cases} +, & \to h_+ \le f(\ell;t;u)_{i,\tau} \le h_0 - {}_\Delta h_0 - 1; \\ 0, & \to f(\ell;t;u)_{i,\tau} = h_0 \pm {}_\Delta h_0; \\ -, & \to h_0 + {}_\Delta h_0 + 1 \le f(\ell;t;u)_{i,\tau} \le h_-. \end{cases} \qquad (3.21)$$

Тут ${}_\Delta h_0$ - околицях нульового рівня біполярного ознаки, для якого зберігається нейтральний вплив звуко-букви на підсвідомість людини.

Надалі позитивна спрямованість буде відповідати рівності $\phi(\ell;t;u)_{i,\tau} = 1$, навпаки негативна $\phi(\ell;t;u)_{i,\tau} = -1$. Нейтральний вплив звуко-букви відповідає значенню $\phi(\ell;t;u)_{i,\tau} = 0$. Звуко-букви, фонетичні відхилення яких мають нейтральне значення, тобто $\phi(\ell;t;u)_{i,\tau} = 0$, виключаються з подальшої обробки. Тоді значення $\phi(\ell;t;u)_{i,\tau}$ буде здаватися такою знаковою функцією

$$\phi(\ell;t;u)_{i,\tau} = \operatorname{sign}(h_0 - f(\ell;t;u)_{i,\tau}). \qquad (3.22)$$

З урахуванням співвідношення (3.22), вираз (3.19) прийме наступний вигляд:

$$\varphi_{phc}: b(\ell;t)_{u,\tau} \to \{|h_0 - f(\ell;t;u)_{i,\tau}|;\ \operatorname{sign}(h_0 - f(\ell;t;u)_{i,\tau})\}. \qquad (3.23)$$

В результаті таких перетворень створюється можливість для побудови двох підматриць ${}_\Delta F(\ell;t)_u^+$ і ${}_\Delta F(\ell;t)_u^-$, містять в собі інформацію про відносні відхилен-

ня фонетичних величин ${}_{\Delta}f(\ell;t;u)_{i,\tau}^{(+)}$ и ${}_{\Delta}f(\ell;t;u)_{i,\tau}^{(-)}$, відповідно характеризуються позитивною (конструктивною) і негативною (деструктивною) спрямованістю впливу на підсвідомість особистості.

Підматриця ${}_{\Delta}F(\ell;t)_{u}^{+}$ і ${}_{\Delta}F(\ell;t)_{u}^{-}$ представляються такими співвідношеннями:

$$
{}_{\Delta}F(\ell;t)_{u}^{(\phi)}=\begin{vmatrix}
{}_{\Delta}f(\ell;t;u)_{1,1}^{(\phi)} & \ldots{}_{\Delta}f(\ell;t;u)_{1,\tau}^{(\phi)} & \ldots{}_{\Delta}f(\ell;t;u)_{1,|B(\ell;t;u)_{h}^{(\phi)}|}^{(\phi)} \\
\ldots & \ldots & \ldots \\
{}_{\Delta}f(\ell;t;u)_{i,1}^{(\phi)} & \ldots{}_{\Delta}f(\ell;t;u)_{i,\tau}^{(\phi)} & \ldots{}_{\Delta}f(\ell;t;u)_{i,|B(\ell;t;u)_{h}^{(\phi)}|}^{(\phi)} \\
\ldots & \ldots & \ldots \\
{}_{\Delta}f(\ell;t;u)_{Q(\ell;t;u)_{h}^{(\phi)},1}^{(\phi)} & \ldots{}_{\Delta}f(\ell;t;u)_{Q(\ell;t;u)_{h}^{(\phi)},\tau}^{(\phi)} & \ldots{}_{\Delta}f(\ell;t;u)_{Q(\ell;t;u)_{h}^{(+)},|B(\ell;t;u)_{h}^{(\phi)}|}^{(\phi)}
\end{vmatrix}.
$$

Тут ϕ - знак відповідно характеризується позитивною ϕ="+" і негативною ϕ="–" спрямованістю впливу на підсвідомість особистості.

У цих підматрицях прийняті наступні позначення:

- $Q(\ell;t;u)_{h}^{(+)}$ и $Q(\ell;t;u)_{h}^{(-)}$ - кількість інформативних ЛБ ознак, за якими фонетичні значення визначаються відповідно як з позитивної і негативної спрямованості впливу на підсвідомість підлітка;

- $|B(\ell;t;u)_{h}^{(+)}|$ и $|B(\ell;t;u)_{h}^{(-)}|$ - кількість звуко-букв в u-му звуко-слові, для фонетичних значень яких по інформативним ознаками формується відповідно позитивний і негативний напрямок впливу на підсвідомість підлітка.

У загальному випадку підматриці ${}_{\Delta}F(\ell;t)_{u}^{+}$ і ${}_{\Delta}F(\ell;t)_{u}^{-}$ інтерпретуються як числа в двовимірному ***матеріальному нерівноважному позиційному просторі*** з урахуванням спрямованості відхилень від нульових рівнів градаційної шкали лінгвістичних біполярних ознак. Тоді відповідна інтегрована кількість $V(Q(\ell;t;u)_{h}^{(+)};|B(\ell;t;u)_{h}^{(+)}|)$ та $V(Q(\ell;t;u)_{h}^{(-)};|B(\ell;t;u)_{h}^{(-)}|)$ інформації по всіх значимих ЛБ ознаками по всім звуко-буквах в слові, буде визначатися за допомогою таких формул:

$$V(Q(\ell;t;u)_h^{(\phi)};|B(\ell;t;u)_h^{(\phi)}|)=[\sum_{\tau=1}^{|B(\ell;t;u)_h^{(\phi)}|}\ell og_2\prod_{i=1}^{Q(\ell;t;u)_h^{(\phi)}}({}_\Delta f(\ell;t;u;\max)_{i,\tau}^{(\phi)})]+1; \quad (3.24)$$

Тут величина ${}_\Delta f(\ell;t;u;\max)_{i,\tau}^{(\phi)}$ визначається як мінімальне значення з двох цілочисельних значень ${}_\Delta f(\ell;t;u)_{i,\max}^{(\phi)}$ и ${}_\Delta f(\ell;t;u)_{\tau,\max}^{(\phi)}$, а саме:

$${}_\Delta f(\ell;t;u;\max)_{i,\tau}^{(\phi)}=\min\{{}_\Delta f(\ell;t;u)_{i,\max}^{(\phi)};\ {}_\Delta f(\ell;t;u)_{\tau,\max}^{(\phi)}\}; \quad (3.25)$$

$${}_\Delta f(\ell;t;u)_{i,\max}^{(\phi)}=(\max_{1\le\tau\le|B(\ell;t;u)_h^{(\phi)}|}{}_\Delta f(\ell;t;u)_{i,\tau}^{(\phi)}-\min_{1\le\tau\le|B(\ell;t;u)_h^{(\phi)}|}{}_\Delta f(\ell;t;u)_{i,\tau}^{(\phi)})/\delta_i^{(\phi)})+1;$$

$${}_\Delta f(\ell;t;u)_{\tau,\max}^{(\phi)}=(\max_{1\le i\le Q(\ell;t;u)_h^{(\phi)}}{}_\Delta f(\ell;t;u)_{i,\tau}^{(\phi)}-\min_{1\le i\le Q(\ell;t;u)_h^{(\phi)}}{}_\Delta f(\ell;t;u)_{i,\tau}^{(\phi)})/\delta_\tau^{(\phi)})+1.$$

Тоді, чим більші величини $V(Q(\ell;t;u)_h^{(+)};|B(\ell;t;u)_h^{(+)}|)$ и $V(Q(\ell;t;u)_h^{(-)};|B(\ell;t;u)_h^{(-)}|)$, тим вище інформативність u-го звуко-слова в напрямку надання відповідно позитивного ϕ="+" або негативного ϕ="–" впливу.

Інтегровані оцінки, отримані за допомогою формул (3.24) и (3.25) дозволяють:

1) використовувати одночасно інформацію про фонетичні відхилення по всім значимим ознаками простору Ω_h і всіх виділених звуко-буквах в звуко-слові для виявлення рівня відповідного впливу на підсвідомість особистості через його звукові відчуття;

2) встановити інтегровану спрямованість ІП впливу всього звуко-слова.

Для встановлення рівня значущості ІП впливу звуко-слова на підсвідомість особистості вводяться порогові рівні, а саме: $V(\ell;t;u)_h^+$ и $V(\ell;t;u)_h^-$. Тоді значимість звуко-слова визначається по наступних співвідношеннях::

$$V(Q(\ell;t;u)_h^{(+)};|B(\ell;t;u)_h^{(+)}|)>V(\ell;t;u)_h^+;\ \ V(Q(\ell;t;u)_h^{(-)};|B(\ell;t;u)_h^{(-)}|)>V(\ell;t;u)_h^-. \quad (3.26)$$

Якщо нерівності (3.26) виконуються, то u-е звуко-слово є значущим за рівнем свого ІП впливу на підсвідомість особистості відповідно в позитивної або негативної спрямованості.

Встановлення значущості напрямку впливу звуко-слова на підсвідомість людини з урахуванням всіх ознак простору організовується шляхом порівняння величин $V(Q(\ell;t;u)_h^{(+)};|B(\ell;t;u)_h^{(+)}|)$ и $V(Q(\ell;t;u)_h^{(-)};|B(\ell;t;u)_h^{(-)}|)$. В цьому випадку, якщо виконується нерівність

$$V(Q(\ell;t;u)_h^{(+)};|B(\ell;t;u)_h^{(+)}|) < V(Q(\ell;t;u)_h^{(-)};|B(\ell;t;u)_h^{(-)}|), \qquad (3.27)$$

то u-е звуко-слово інтегровано надає деструктивний вплив на підсвідомість особистості через його звукове сприйняття.

У разі виконання наступного співвідношення:

$$V(Q(\ell;t;u)_h^{(+)};|B(\ell;t;u)_h^{(+)}|) \approx V(Q(\ell;t;u)_h^{(-)};|B(\ell;t;u)_h^{(-)}|), \qquad (3.28)$$

приймається рішення про недостатність інформації для встановлення спрямованості впливу конкретного звуко-слова. В цьому випадку проводиться оцінка за іншими звуко-словами в текстовому інформаційному ресурсі або його окремих фрагментах (використовується динамічна схема); задіюється інший метод оцінки сугестії на підсвідомість особистості.

Структурно-функціональна схема методу виявлення сугестивного ІП впливу структурної компоненти (слова) ТІР на підсвідомості особистості на основі векторного семантичного диференціала представлена на рис. 3.3.

Під ***векторним семантичним диференціалом*** $\{V(Q(\ell;t;u)_h^{(\phi)};|B(\ell;t;u)_h^{(\phi)}|);\phi\}$ розуміється узагальнена фонетична оцінка рівня $V(Q(\ell;t;u)_h^{(\phi)};|B(\ell;t;u)_h^{(\phi)}|)$ і спрямованості ϕ сугестивного ІП впливу структурної компоненти (слова) ТІР на підсвідомість особистості в векторному біполярному лінгвістичному просторі.

За викладеного матеріалу можна зробити наступні висновки:

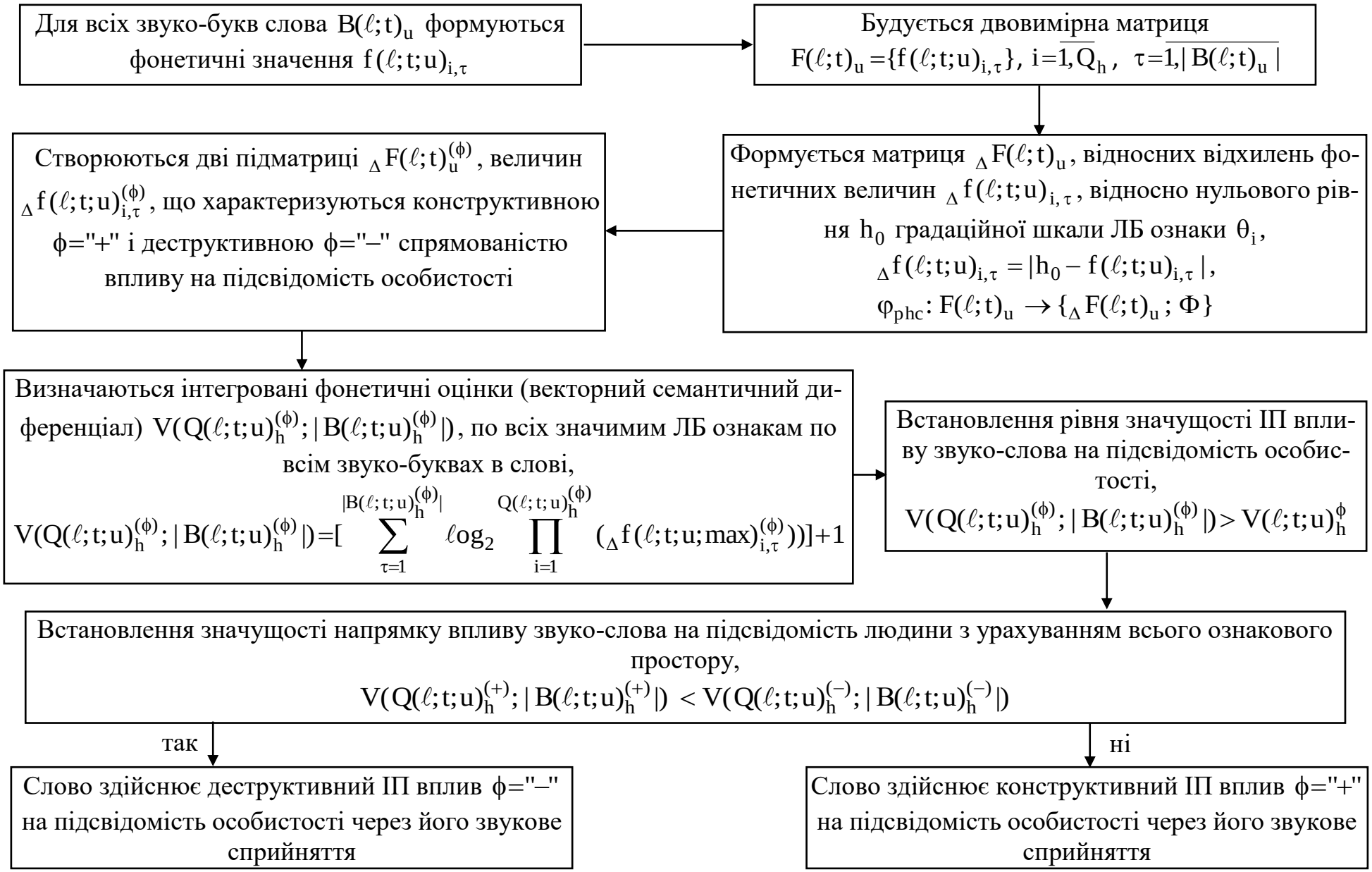


Рисунок 3.3 – Структурно-функціональна схема методу виявлення сугестивного ІП впливу структурної компоненти (слова) ТІР на підсвідомості особистості на основі векторного семантичного диференціала

1. Створений (*вдосконалений*) метод побудови одновимірного семантичного диференціала для оцінки рівня і напряму ІП впливу структурних компонент ТІР в фонетичному просторі з урахуванням прив'язки до градаційних двополюсних шкал окремих значущих ЛБ ознак. Відмінний аспект полягає у використанні для побудови фонетичного простору тільки значущих біполярних лінгвістичних ознак..

2. Розроблений (*вперше*) метод ідентифікації інформаційно-психологічний вплив структурних компонент (слів) текстових інформаційних ресурсів на підсвідомість особистості на основі формування векторного семантичного диференціала. Метод базується на таких етапах:

– встановленні векторної фонетичної оцінки рівня і спрямованості ІП впливу звуко-букв по всім біполярним лінгвістичним ознакам;

- здійснення векторної фонетичної ідентифікації рівня і напряму ІП впливу структурної компоненти (слова) ТІР на підсвідомість особистості за всіма звуко-буквами в значнимому двополюсному лінгвістичному біполярному просторі, який представлений як матерільний нерівноважний базис;

- визначення векторного семантичного диференціала на основі ідентифікації інтегрованих фонетичних оцінок за всіма біполярним поступовим шкалами значущих лінгвістичних ознак з урахуванням детектування двобічного ІП впливу (конструктивний і деструктивний) в двовимірному матеріальному нерівноважному просторі.

3. Побудований (*отримав подальший розвиток*) комплексний метод виявлення прихованого ІП впливу в локальній компоненті ТІР на підсвідомість особистості в багатовимірному фонетичному просторі з прив'язкою до векторних градаційних двополюсних шкал біполярних лінгвістичних ознак на основі формування семантичного диференціала.

У той же час метод аналізу ТІР на основі формування семантичного диференціала має суб'єктивний розмах з урахуванням біполярності лінгвістичного простору, тобто фонетичні оцінки можуть «тяжіти» до різнополярних характеристик. Це розмиває кінцевий результат оцінки ІП впливу слова

(структурної компоненти TIP) на підсвідомість особистості, і може створити невизначеність. Тому *пропонується* додатково враховувати фонетичний аналіз семантичної складової слова, що враховує тільки однополярні характеристики. Тут додатково *пропонується* розглянути закономірність в фонетичному поданні звуко-слів, що складається у врахуванні частоти відхилення фонетичних значень звуко-букв щодо нормативного рівня частоти появи звуко-букв в текстах.

3.3. Розробка концептуального ядра для оцінки спрямованості сугестивного ІП впливу складових текстових інформаційних ресурсів в фонетичному просторі

Метод фонетичного аналізу семантичної складової слова за однополярними лінгвистичними шкалами.

В даному методі оцінка проводиться за 20 однополярними шкалами на відміну від семантичного диференціала з 25 біполярними шкалами лінгвистичних ознак. Перелік таких ознак наведено в табл. 3.3. Обрані ознаки краще підходять для аналізу будь якого тексту.

Таблиця 3.3

Перелік 20 ознак для однополярного фонетичного аналізу

№ ознаки	Ознака для аналізу	№ ознаки	Ознака для аналізу	№ ознаки	Ознака для аналізу	№ ознаки	Ознака для аналізу
1	прекрасний	6	сумний	11	тужливий	16	піднесений
2	бадьорий	7	яскравий	12	радісний	17	повільний
3	світлий	8	темний	13	стрімкий	18	тихий
4	ніжний	9	сильний	14	похмурий	19	суворий
5	мінорний	10	страхітливий	15	важкий	20	зловісний

Метод аналізу базується на врахуванні психозвукової *закономірності*, яка полягає в тому, що людина звикла в розмовній мові до якоїсь частотності звуків і як встановили психологи, ми *визначаємо* цю частотність досить правильно. Відповідно, будь яке значне відхилення від цієї частотності має бути відмічено

підсвідомістю особистості. Визначивши, які звуко-букви переважають в тексті, та надавши їм деякі ознакові описи, можна судити про те який психоемоційний вплив спричинить той чи інший ТІР на підлітка.

При автоматичному аналізі тексту с використанням ПЕОМ, неможливо дати їй зрозуміти значення окремих слів мови. Це обумовлено тим, що машина оперує цифрами. Тому для розумінням звуко-букв у слові здійснюється оцінка їх значимості за допомогою ознакових шкал однополярних лінгвістичних ознак. При цьому формується кодове значення для кожної звуко-букви на певній шкалі однополярних лінгвістичних ознак. Але визначення позиції звуко-букви на шкалі це лише середнє значення яке було виведено шляхом багаторазових аналізів, що неповною мірою вказую на напрямок ІП впливу. Навпаки відхилення значущості від середнього значення дозволяє провести оцінку звуко-слова відносно його виразності або схильності до тої чи іншої ознаки. Тому для оцінки потрібно використовувати таблицю відхилень значущості звуків. Ці значення можна отримати шляхом вирахування позиції звуку з табл. 3.4 від середнього значення шкали $h_0 = 0{,}3$, а саме:

$$_{\Delta}\mathrm{d}(\ell;\mathrm{t};\mathrm{u})_{\mathrm{i},\tau} = \mathrm{h}_0 - \mathrm{d}(\ell;\mathrm{t};\mathrm{u})_{\mathrm{i},\tau} = 3 - \mathrm{d}(\ell;\mathrm{t};\mathrm{u})_{\mathrm{i},\tau}, \qquad (3.29)$$

де $\mathrm{d}(\ell;\mathrm{t};\mathrm{u})_{\mathrm{i},\tau}$ – значення відхілення значимості τ-ої звуко-букви, визначеної на основі таблиці.

Таблиця 3.4

Фрагмент таблиці відхилення фонетичних оцінок звуко-букв

Шкала	Буква				
	А	Б	В	Г	Д
хороший – поганий	+1,5	+0,6	+0,1	–0,8	+0,6
світлий – темний	+0,8	–0,8	0,0	–0.7	–0,8
красивий – відштовхуючий	+1,0	+0,4	0,0	+0,2	+0,6

Наприклад для букви А за шкалою "яскравий – тьмяний" це буде $3.0-2.0=+1.0$. Це означає що відхилення йде ближче до ознаки "яскравий". Негативне ж значення, означатиме, що відхилення відбувається в бік ознаки "тьмяний".

Розрахунок фонетичної складової $F''(\ell;t;u)_i$ для слова $S(\ell;t)_u$ заснований на наступних етапах (рис. 3.4):

1) Перший підготовчий етап полягає в перекладі слова $S(\ell;t)_u$ або ж послідовності букв $s(\ell;t)_{u,\tau}$ в набор $B(\ell;t)_u$ звуко-букв $b(\ell;t)_{u,\tau}$. На відміну від семантичного диференціала послідовність звуко-букв не важлива;

2) На другому етапі для кожної звуко-букви $b(\ell;t)_{u,\tau}$ вибираються табличні значення їх частотності і значущості відповідно до аналізованих ознаковим аспектом. Для цього використовуються дві таблиці. ***Перша*** таблиця містить інформацію про частотність $f'(\ell;t;u)_{i,\tau}^{(норм)}$ звуко-букв $b(\ell;t)_{u,\tau}$, з якої завжди вибираються однакові значення незалежно від однополярної лінгвістичної ознаки за яким проводиться аналіз. ***Друга*** таблиця включає в себе відхилення $d(\ell;t;u)_{i,\tau}$ значущості звуко-букв від норми. Тут утворюється 20 різних наборів для кожної звуко-букви в залежності від однополярної лінгвістичної ознаки;

3) На третьому етапі проводиться визначення частоти $f'(\ell;t;u)_{i,\tau}$ входження кожної звуко-букви $b(\ell;t)_{u,\tau}$ в слово $B(\ell;t)_u$ на основі:

- підрахунку загальної кількості $|B(\ell;t)_u|$ звуко-букв в аналізованому слові і кількості $q(\ell;t)_{u,\tau}$ кожної звуко-букви в слові;
- операції ділення кількості $q(\ell;t)_{u,\tau}$ входження τ-ї звуко-букви в слово на загальну кількість $|B(\ell;t)_u|$ звуко-букв в слові, тобто:

$$f'(\ell;t;u)_{i,\tau} = q(\ell;t)_{u,\tau} / |B(\ell;t)_u|,$$

де $|B(\ell;t)_u|$ – кількість звуко-букв $b(\ell;t)_{u,\tau}$ в слові $B(\ell;t)_u$; $q(\ell;t)_{u,\tau}$ - частотність τ-ї звуко-букви в слові;

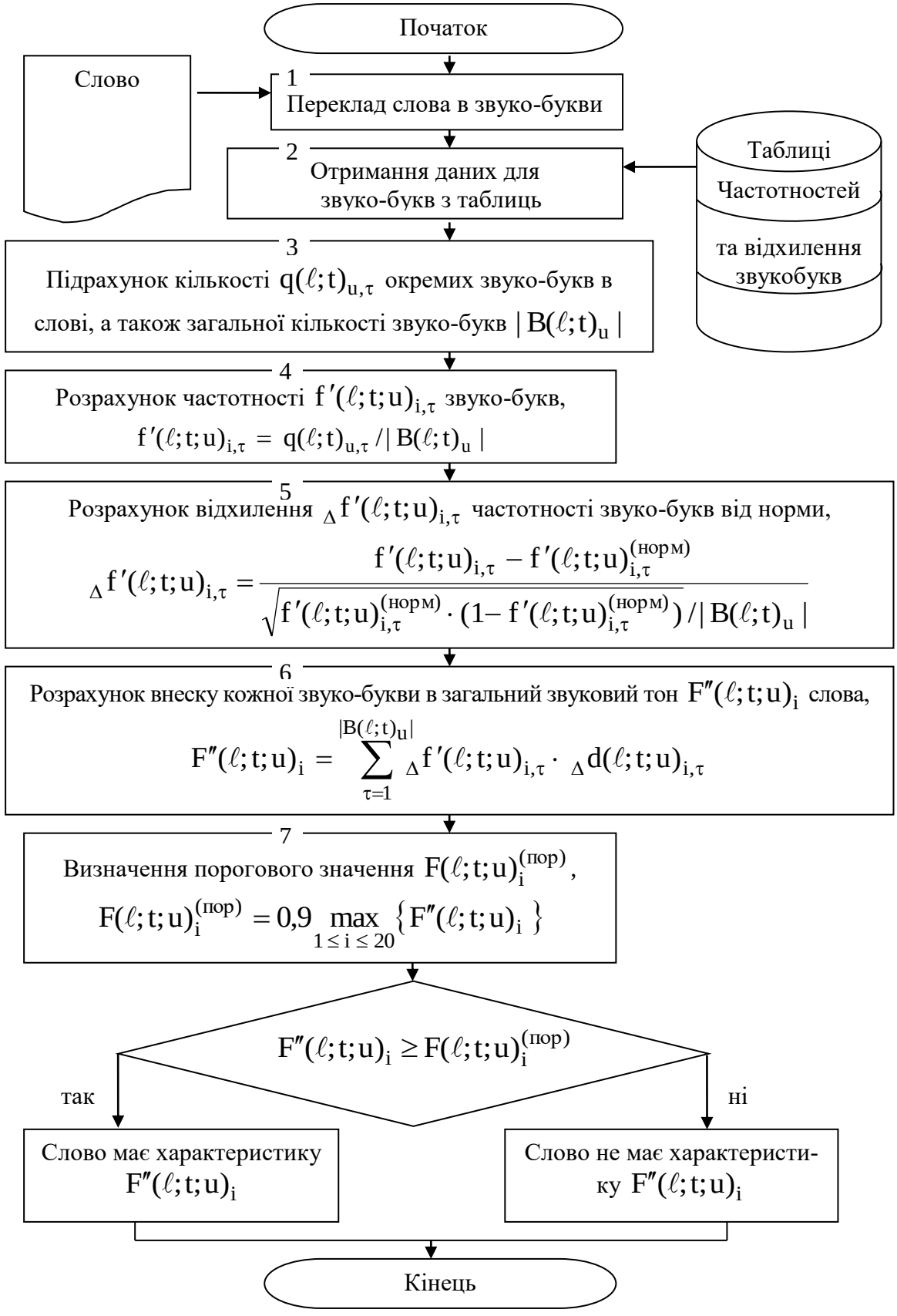


Рисунок 3.4 – Структурно-функціональна схема оцінки фонетичної значущості слова за однополярною лінгвістичною ознакою

4) наступним етапом є визначення відхилення ${}_{\Delta}f'(\ell;t;u)_{i,\tau}$ частотності $f'(\ell;t;u)_{i,\tau}$ звуко-букв $b(\ell;t)_{u,\tau}$ від норми $f'(\ell;t;u)_{i,\tau}^{(норм)}$. При цьому номінальна частотність $f'(\ell;t;u)_{i,\tau}^{(норм)}$ показує скільки разів повинна зустрітися конкретна звуко-буква в звичайному тексті. Однак, як правило, якщо взяти кілька різних текстів, то частотність не буде точно збігатися з табличним значенням. З цього випливає, що номінальна частотність схильна до коливань. Межі коливань визначаються з теорії ймовірностей. За одиницю, при вимірюванні розмаху коливань приймають величину σ. Приймається, що ***допустимі*** коливання будь-якої випадково величини не перевищуватимуть $\pm 2\sigma$. Поки величина коливається в цих межах, можна вважати, що вона як би "прив'язана" до середньої точки коливання і далеко від цієї точки не відхилиться. В іншому випадку, якщо коливання перевищать $\pm 2\sigma$, то вони ***аномальні***. Тому для визначення відхилення ${}_{\Delta}f'(\ell;t;u)_{i,\tau}$ частотності звуко-букв від норми буде застосовуватися формула:

$$ {}_{\Delta}f'(\ell;t;u)_{i,\tau} = \frac{f'(\ell;t;u)_{i,\tau} - f'(\ell;t;u)_{i,\tau}^{(норм)}}{\sqrt{f'(\ell;t;u)_{i,\tau}^{(норм)} \cdot (1 - f'(\ell;t;u)_{i,\tau}^{(норм)}) / |B(\ell;t)_u|}}, \qquad (3.30) $$

де $f'(\ell;t;u)_{i,\tau}$ – частота τ-ої звуко-букви в аналізованому слові $B(\ell;t)_u$; $f'(\ell;t;u)_{i,\tau}^{(норм)}$ – номінальна частота τ-ої звуко-букви в мові;

5) Даний етап полягає у визначенні фонетичної значущості $F''(\ell;t;u)_i$ для u-го слова $S(\ell;t)_u$ є підсумовування значень вкладів ${}_{\Delta}f'(\ell;t;u)_{i,\tau} \cdot {}_{\Delta}d(\ell;t;u)_{i,\tau}$ кожної звуко-букви в загальний звуковий тон слова. Внесок звуко-букви це множення величини відхилення ${}_{\Delta}f'(\ell;t;u)_{i,\tau}$ частотності від норми на величину ${}_{\Delta}f'(\ell;t;u)_{i,\tau}$ відхилення значущості від нейтральної точки, але тільки тих звуко-букв, чиї відхилення суттєві від норми. Це задається таким співвідношенням

$$ F''(\ell;t;u)_i = \sum_{\tau=1}^{|B(\ell;t)_u|} {}_{\Delta}f'(\ell;t;u)_{i,\tau} \cdot {}_{\Delta}d(\ell;t;u)_{i,\tau} = \sum_{i=1}^{|B(\ell;t)_u|} {}_{\Delta}f'(\ell;t;u)_{i,\tau} \cdot (h_0 - d(\ell;t;u)_{i,\tau}) = $$

$$= \sum_{\tau=1}^{|B(\ell;t)_u|} \frac{f'(\ell;t;u)_{i,\tau} - f'(\ell;t;u)_{i,\tau}^{(норм)}}{\sqrt{f'(\ell;t;u)_{i,\tau}^{(норм)} \cdot (1 - f'(\ell;t;u)_{i,\tau}^{(норм)}) / |B(\ell;t)_u|}} \cdot (3 - d(\ell;t;u)_{i,\tau}).$$

6) На завершальному етапі організовується оцінка характерності слова (структурної компоненти TIP) з позиції градаційної однополярної шкали лінгвістичних ознак. Таку оцінку пропонується здійснювати шляхом порівняння величини $F''(\ell;t;u)_i$ з пороговим рівнем $F(\ell;t;u)_i^{(пор)}$. Відповідно порогове значення пропонується знаходити з використанням такої формули

$$F(\ell;t;u)_i^{(пор)} = 0{,}9 \max_{1 \le i \le 20} \{F''(\ell;t;u)_i\}.$$

Значить по викладеному можна стверджувати, наступне.

Розроблено метод фонетичного аналізу семантичної складової слова, що враховує однополярність фонетичного впливу букв на підсвідомість особистості. Відмінні риси полягають в тому що ***пропонується*** статичний ідентифікатор для прийняття рішення щодо наявності деструктивного впливу слова на підсвідомість особистості по кожній конкретній однополярній ознаці на основі визначення відхилення частотності звуко-букв в слові від норми, тобто як часто конкретний набір звуків (звуко-слово) озвучується в тексті і його відхилення по частоті звучання від нормативно установленого рівня (**Додаток Б**). Це дозволяє знизити ймовірність помилок першого і другого роду в процесі оцінки деструктивності або конструктивності інформаційно-психологічного впливу окремих слів на підсвідомість особистості. Спільне (консолідоване) функціонування двох методів основаних на фонетичних оцінках звуко-букв, полягає в таких етапах: перший тип аналізу (семантичний диференціал) - визначається рівень позитивності або негативності слова по ЛБ ознаками. Другий тип аналізу - визначає конкретний якісний аспект за яким слово буде негативним або позитивним.

3.4. Підходи до оцінки текстів на основі методів тестування для виявлення сугестивних впливів

Підходи до статичного аналізу тексту для виявлення сугестивних впливів.

Аналіз окремих структурних компонент (слів) дозволяє як узагальнення здійснювати аналіз усього цілком текстового інформаційного ресурсу. Потрібно визначити яким чином їх слід застосувати до того набору слів, з яких складається текст. Методи виявлення сугестії як правило орієнтовані на аналіз слів, що дає розуміння яким чином воно сприймається людиною. Отже перший, (найочевидніший) підхід полягає в аналізі кожного слова $S(\ell;t)_u$ окремо і визначення середнього значення для всіх слів, тобто для всього ТІР S_{doc}. Тут недоліком є те, що аналізується кожне окреме слово, а кінцевий результат не пов'язаний з рядом стоячими словами. А це говорить про те, що будь-який текст, складений з цього набору слів, буде мати однакову оцінку. У той же час, використовуючи одні й ті ж слова, можна скласти текст абсолютно по різному і з різним посланням.

З цього випливає висновок, що необхідно якимось чином зафіксувати слова тексту в тому порядку, в якому їх розташував автор і ніяк інакше. Це дасть унікальну оцінку саме для такого упорядкованого набору слів.

Тому другій підхід пропонується будувати на основі перетворення набору окремих слів в єдиний, нерозривний рядок. Після чого проводиться аналіз усього отриманого рядка як єдиного слова.

Таким чином, *пропонується* два різних підходи до аналізу текстів. Кожен з них має свої плюси і мінуси. Тому варто розглядати обидва варіанти. При цьому аналіз, під час якого аналізується весь текст цілком будемо називати *статичним*.

Розглянемо підхід до статичного аналізу тексту по словам. Структурно-функціональна схема представлена на рис. 3.5. В цьому випадку застосовуються наступні етапи:

1) аналізований текст S_{doc} розбивається на окремі слова $S(\ell;t)_u$;

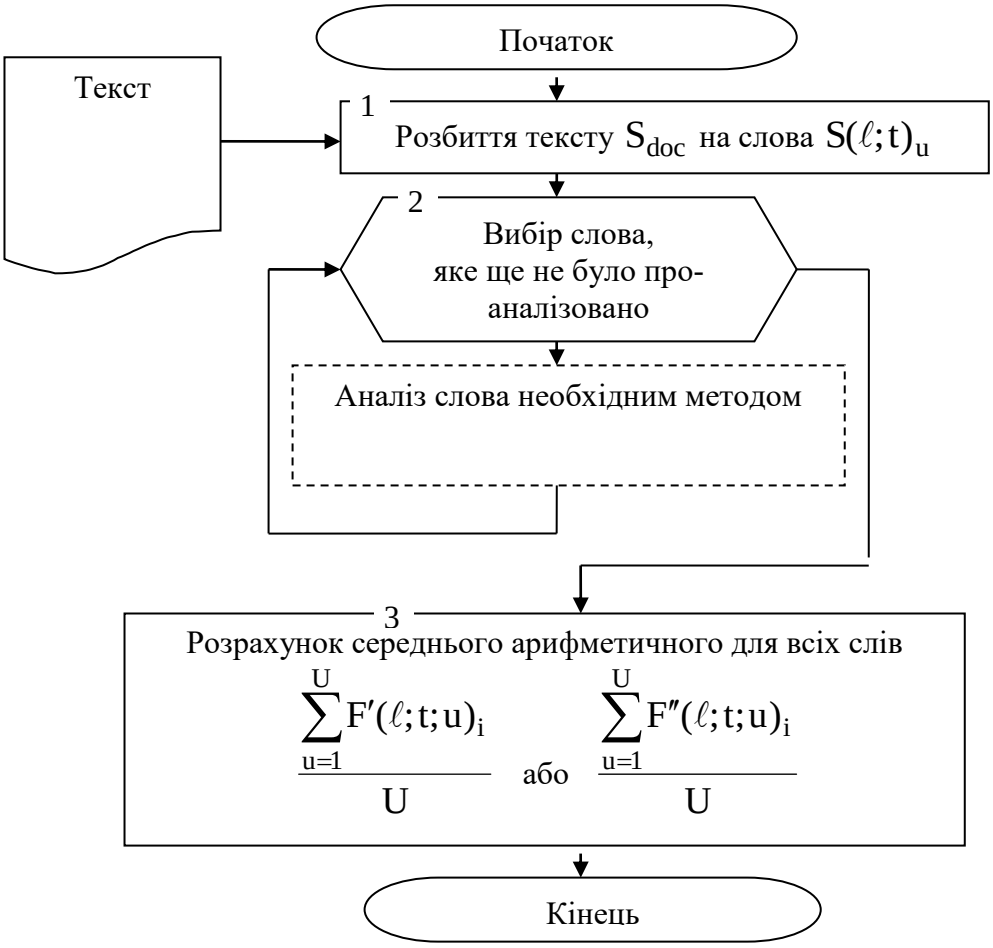


Рисунок 3.5 – Структурно-функціональна схема аналізу статичним методом за словами для усього тексту

2) кожне слово $S(\ell;t)_u$ окремо аналізується одним з методів виявлення сугестивного ІП впливу (семантичний диференціал, фонетичні оцінки по частотності звуко-букв);

3) після отримання всіх відповідних оцінок по кожному слову виводиться середня оцінка для всіх результатів шляхом обчислення середнього арифметичного.

Далі розглянемо підхід, при якому аналіз тексту S_{doc} проводиться як єдине ціле. Отже в цьому випадку застосовуються такі етапи:

1) весь аналізований текст перекладається в один нерозривний рядок $B(\ell;t)_U$, як дуже довге слово шляхом відкидання пробілів, розділових знаків, переведення чисел в текстову форму написання, тобто:

$$B(\ell;t)_U = \{B(\ell;t)_1, ..., B(\ell;t)_u, ..., B(\ell;t)_U\}.$$

В цьому випадку пов'язується кінець одного слова з початком наступного;

2) отриманий рядок $B(\ell;t)_U$ аналізується необхідним методом (семантичний диференціал, фонетичних оцінок по частотностям), за аналогією з аналізом окремих слів. Це дасть унікальну оцінку для такої послідовності слів в текстовому документі.

На рис. 3.6 наведено структурно-функціональна схема для статичного аналізу тексту рядком.

Рисунок 3.6 – Структурно-функціональна схема для статичного аналізу тексту єдиним рядком

Значить по підсумком викладеного матеріалу можна зробити висновок, що:

– розроблено підхід до статичного аналізу ІП впливу тексту на підсвідомість особистості на основі усереднення ВП впливу окремих слів на підсвідомість особистості. Даний підхід розглядає текст як набір окремих слів, кожне з яких несе свій вплив на підсвідомість в тій чи іншій мірі. При цьому таке ІП вплив може бути значущим для ІП впливу всього тексту на підсвідомість особистості.

– створений підхід, який розглядає текст як єдине ціле, тобто значення впливу окремого слова не суттєва. Сам текст розглядається як одне велике ціле слово.

Це дозволяє зробити оцінку деструктивного або конструктивного впливу всього текстового інформаційного ресурсу на підсвідомість особистості.

Підходи до динамічного аналізу тексту для виявлення сугестивних впливів.

Статичний аналіз всього тексту дає нам уявлення того, який ІП вплив він матиме на особистість при повному його прочитанні. При цьому отримується усереднені оцінки для всіх частин цього тексту. Отже не можна сказати, що кожна з частин тексту окремо має таку ж оцінку ІП впливу, як і весь текст цілком. Однак інформаційна деструкція у тексті може бути побудована таким чином, що кожна частина ТІР, має свій відмінний ІП вплив на підсвідомість особистості. Це стає важливим фактом в тому випадку, коли людина читає або чує тільки окрему частину тексту. У такому випадку статичний аналіз всього тексту буде не інформативний. Це обумовлено тим, що всього один абзац може чинити значний деструктивний ІП вплив, в той час як більша частина тексту буде нейтральною (або конструктивною), що зрештою змаже результати аналізу. Тому для підвищення ефективності виявлення сугестивних інформаційних деструкцій у разі їх додаткового маскування в конструктивному або нейтральному ТІР ***пропонується*** створювати динамічний аналіз.

Динамічний аналіз під собою має на увазі розбиття тексту на частини і аналіз кожної з цих частин окремо. Таким чином, можна простежити динаміку зміни сугестивного ІП впливу на підлітків від початку і до кінця тексту або ж оцінити тільки конкретну його ділянку. Такий аналіз так само може показати, які частини тексту має сенс урізати, а які залишити при необхідності скорочення тексту. Таким підходом можуть користуватися рекламні компанії, скорочуючи ефірний час реклами, але, не урізуючи її необхідного впливу на підсвідомість.

Як правило, більшість текстів складається з абзаців S_{frg}, як проміжної текстової одиниці між фразою і главою. Це служить в свою чергу для угруповання однорідних одиниць викладу. Тому можна зробити висновок, що динаміку краще простежувати за абзацами. В цьому випадку абзац виражає деяку спільну думку.

На рис. 3.7 наведено структурно-функціональна схема загального підходу до аналізу тексту динамічним методом. Відповідно послідовність технологічних дій задається такими компонентами:

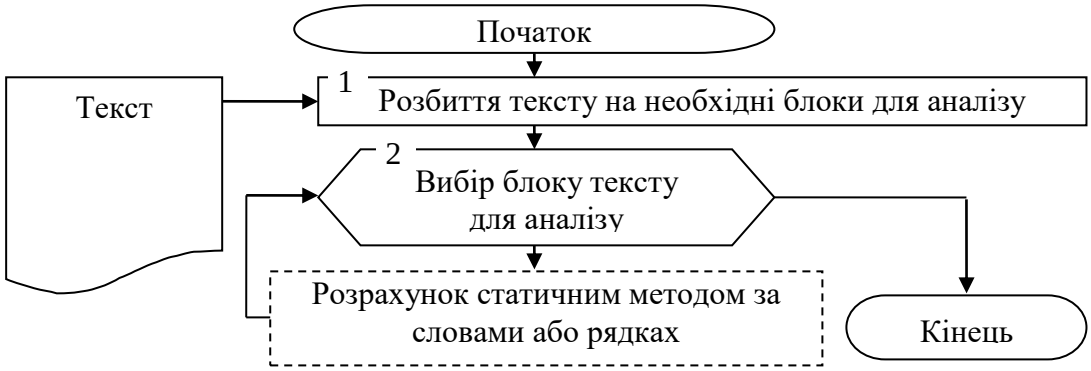


Рисунок 3.7. – Структурно-функціональна схема загального підходу до аналізу тексту динамічним методом

1) оригінальний текст розбивається на блоки S_{frg} тексту, які потрібно проаналізувати. Зручніше і найдоцільніше розбивати за абзацами;

2) далі визначається блок тексту, який потрібно проаналізувати;

3) застосовується один з двох статичних методів аналізу (підхід аналізу за словами або рядком) для вибраної частини TIP;

4) при необхідності обирається інший початковий фрагмент TIP, тобто динамічний процес повертається до другого етапу. Таким чином, на основі динамічного методу можна дати уявлення про те яким сугестивним впливом володіє кожна частина текстового інформаційного ресурсу.

Отже запропоновано підхід для динамічного аналізу впливу текстових інформаційних ресурсів на підсвідомість людини, який дозволяє оцінити сугестивний деструктивний ІП вплив на підсвідомість особистості не цілого тексту, а провести оцінку ІП впливу на підсвідомість людини окремих його фрагментів. Це важливо тому, що окремі фрагменти можуть оказати більше деструктивного впливу на підсвідомість ніж весь текст в цілому. Отже це дозволяє виявити приховані інформаційні деструкції у разі застосування протиборчою стороною додаткових маскувань під конструктивний або нейтральний текстовий інформаційний ресурс. Тобто тут проводиться оцінка наявності деструктивного ІП впливу в межах локальних чутливих зон текстового інформаційного ресурсу.

3.5. Методи динамічного аналізу текстів для виявлення сугестивної спрямованості

Обґрунтування підходів динамічного аналізу текстів за накопичувальною схемою для виявлення сугестивних впливів.

Як показує статистика [37, 91, 64, 65], близько половини підлітків не до кінця сприймають весь аудіо інформаційний ресурс (AIP) та TIP. Причиною цьому може бути: відсутність часу; відсутність зацікавленості; відсутність деяких емоцій, які очікувались під час сприйняття. При цьому сприймаючи текстову та аудіо інформацію від початку, особистість не сприймає кожен уривок або абзац як незв'язаний уривок, а як би накопичує ту інформацію, яку отримала зараз, з тією, яка була абзацом раніше. Тому можна зробити висновок, що в міру освоєння, кожна наступна отримана інформація, доповнюватиме вже наявну. Це значить те, що при аналізі подальшої частини AIP та TIP, необхідно так само враховувати і попередні його частини, так як кожний наступний відрізок буде доповнювати загальну картину ІП впливу на підсвідомість особистості. Для виявлення прихованих інформаційних деструкцій в AIP та TIP з врахуванням особливостей сприйняття інформації підлітками пропонується використовувати динамічний метод аналіз з накопиченням фрагментів (рис. 3.8).

Підхід до динамічного аналізу тексту за накопичувальною схемою передбачає наступні основні етапи:

1) початковий текст S_{doc} розбивається на блоки S_{frg} тексту. Це дозволить рухаючись послідовно по блокам, аналізувати накопичену інформацію, так само як би це робив підліток сприймаючи AIP і TIP. Тут в якості блоків пропонується використовувати цілі абзаци;

2) здійснюється аналіз блоків за динамічною накопичувальною схемою. При цьому кожний послідуючий блок уточняє попередні оцінки щодо рівня та наявності сугестивного деструктивного ІП впливу на підсвідомість особистості;

3) на кожному кроці накопичування блок застосовується один з двох статичних методів аналізу;

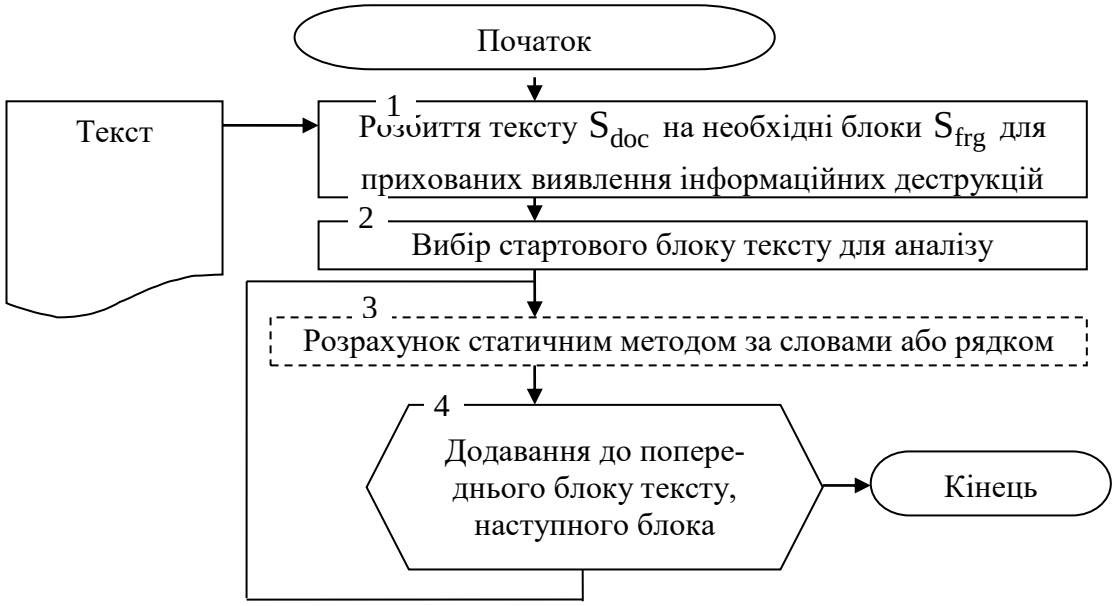


Рисунок 3.8 – Структурно-функціональна схема динамічного методу виявлення прихованих інформаційних деструкцій в AIP та TIP накопиченням фрагментів

4) для визначення, який сугестивний вплив справить наступна ділянка IP з уже накопиченими попередніми, необхідно до накопичених блоків тексту, додати наступний і повернутися до пункту 3 методу, зробивши повторний аналіз із знов накопиченої інформацією.

Метод аналізу текстів на основі семантичного диференціала накопичувальним підсумком. На основі даної технології, можна скласти наступний метод для семантичного диференціала за динамічною накопичувальною схемою за блоками S_{frg} TIP (рис. 3.9). Метод базується на таких технологічних етапах:

1) оригінальний текстовий інформаційний ресурс S_{doc} розбивається на блоки S_{frg} для накопичення;

2) далі визначається перший блок $S(\ell;t)$ тексту з якого буде проводитися накопичення;

3) наступним етапом є аналіз накопиченого тексту методом одновимірного семантичного диференціала за словами. Для цього визначається семантичний диференціал $F'(\ell;t;u)_i$ для кожного слова $S(\ell;t)_u$ з накопиченого TIP. В цьому випадку використовуються вирази (3.12) – (3.15) за конкретною градаційною шкалою ЛБ ознаки;

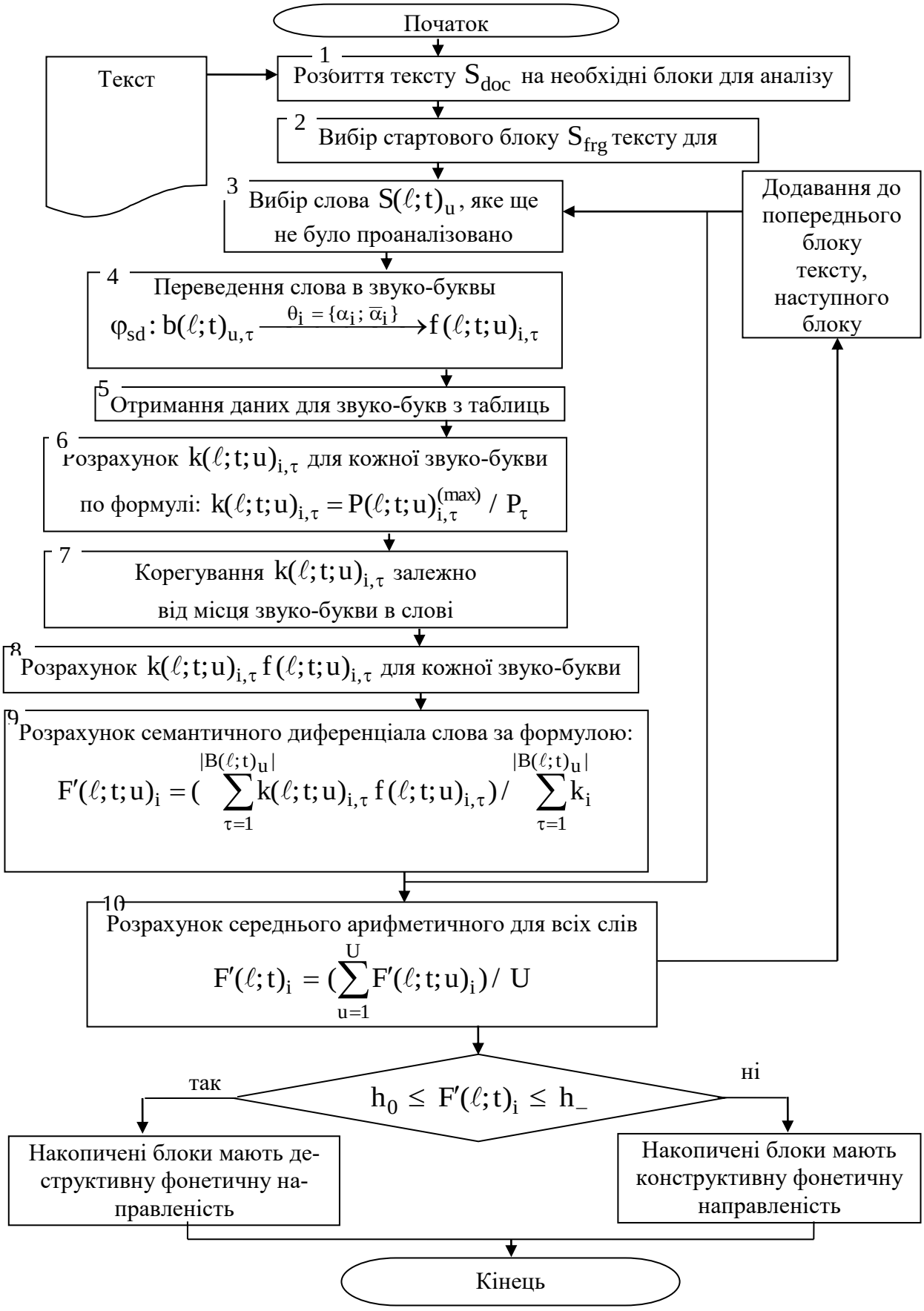


Рисунок 3.9 – Структурно-функціональна схема методу визначення семантичного диференціала за окремою ЛБ ознакою за динамічною накопичувальною схемою по блокам TIP

4) оцінюється середнє значення $F'(\ell;t)_i$ семантичного диференціалу для всіх слів, $F'(\ell;t)_i = (\sum_{u=1}^{U} F'(\ell;t;u)_i)/U$. Результатом буде значення семантичного диференціалу $F'(\ell;t)_i$ накопиченого тексту;

5) при необхідності додається ще один блок ТІР до вже накопиченого і аналіз проводиться повторно.

Метод фонетичного аналізу ТІР на базі визначення семантичної складової в однополярній градаційній шкалі лінгвістичної ознаки за динамічною накопичувальною схемою. На рис. 3.10 наведено метод фонетичного аналізу семантичної складової в однополярній шкалі лінгвістичної ознаки за динамічною накопичувальною схемою за блоками ТІР, який передбачає наступні етапи:

1) текстовий інформаційний ресурс S_{doc} розбивається на блоки S_{frg} для здійснення динамічного накопичення;

2) далі визначається перший блок ТІР, з якого буде проводитись накопичення;

3) наступним етапом є аналіз накопиченого тексту методом фонетичного аналізу семантичної складової за словами з прив'язкою до однополярної градаційної шкали лінгвістичної ознаки. Для цього визначається фонетичне значення $F''(\ell;t;u)_i$ для кожного слова $S(\ell;t)_u$ з накопиченого тексту. Такий технологічний етап базується на наступних співвідношеннях (3.29) – (3.30).

4) після аналізу всіх слів $S(\ell;t)_u$ накопиченого тексту, проводиться визначення середнього значення $F''(\ell;t)_i$ для всіх слів. Результатом буде фонетичне значення $F''(\ell;t)_i$ накопиченого тексту;

5) при необхідності додається ще один блок ТІР до вже накопиченого і аналіз проводиться повторно.

Запропоновано підхід та методи для проведення динамічного аналізу ТІР для виявлення сугестивного деструктивного ІП впливу ТІР на підсвідомість особистості за накопичуваною схемою. Тут проводиться оцінка динаміки зміни сугестивного навантаження ІП впливу в тексті на підсвідомість людини. Підхід засновано на розбивці ТІР на локальні фрагменти, оцінка яких проводиться з урахуванням оцінки впливу попереднього фрагменту на підсвідомість особистості.

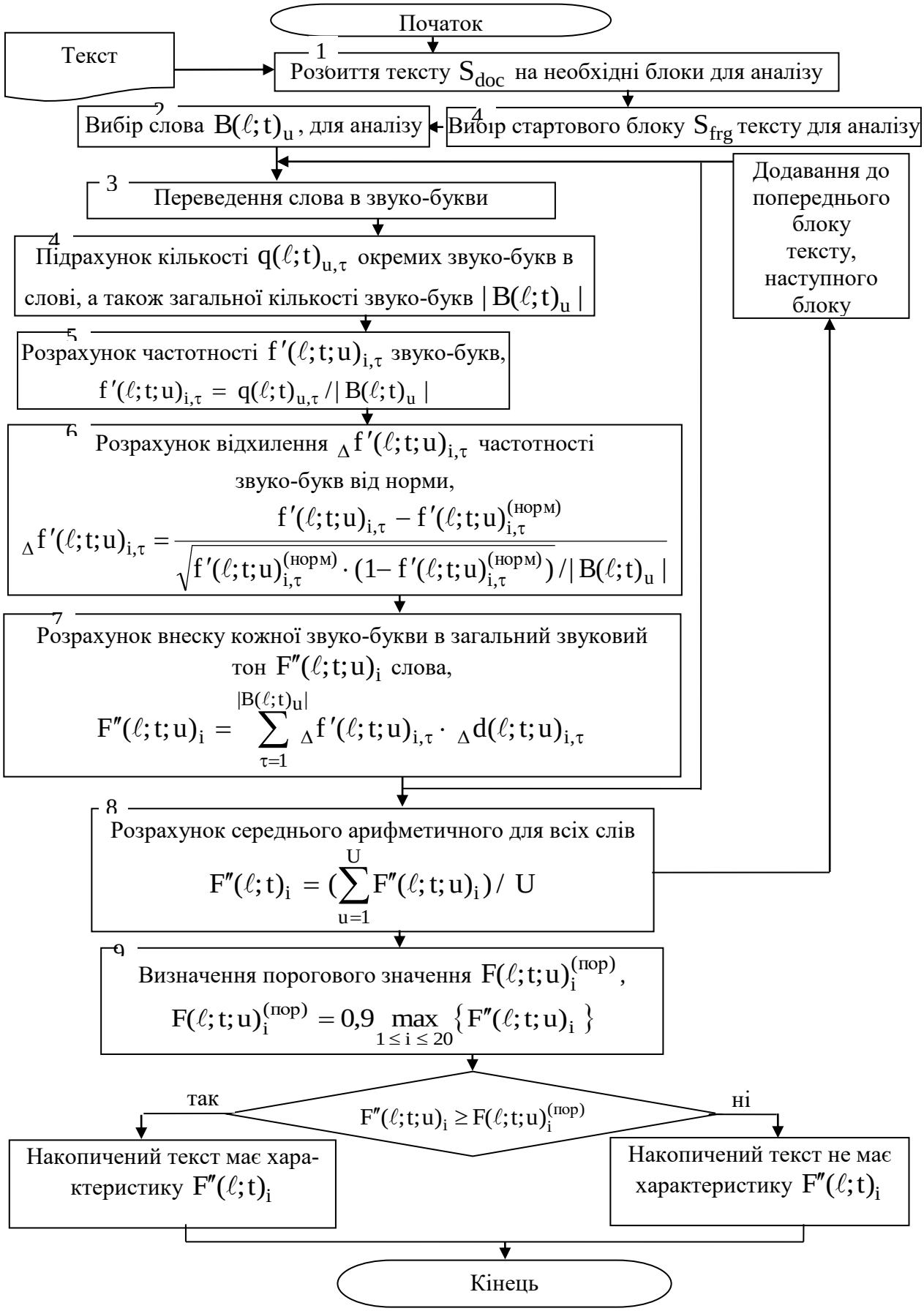


Рисунок 3.10. Структурно-функціональна схема методу оцінки фонетичної значущості за однополярною лінгвістичною ознакою за динамічною накопичувальною схемою по блокам TIP

Відмінність запропонованого підходу є те, що мається можливість оцінити в які моменти текстове інформаційне повідомлення змінювало свою сугестивну спрямованість та автор цього повідомлення бажав придати тесту визначену деструктивну сугестивну спрямованість.

Це дозволяє отримати більш виважені оцінки для визначення прихованої ІП спрямованості текстових інформаційних ресурсів. Забезпечити виявлення деструктивного сугестивного ІП впливу у разі коли протиборча сторона застосовує технології маскування інформаційних деструкцій по всьому тестовому ресурсу, який в загалі має конструктивну направленість. При роботі з підлітками даний підхід та методи на його основі дозволяють визначити зміні в їх поведінки (висловлювання) на підсвідомому рівні.

Висновки за третім розділом

1. Побудована (***вперше***) інформаційна модель аналізу ТІР на основі формування семантичного диференціала (формування фонетичних оцінок з прив'язкою до двополюсної шкали лінгвістичних ознак). На основі чого було розроблени метод виділення значущих лінгвістичних біполярних ознак на основі подання фонетичних оцінок звуко-букв алфавіту в матеріальному нерівноважному позиційному просторі. Основна відмінність тут полягає в тому, що векторний фонетичний простір лінгвістичної біполярної ознаки по всім звуко-буквах представляється в двополярному матеріальному нерівноважному позиційному базисі. Це дозволяє використовувати в процесі аналізу ТІР тільки значущі ЛБ ознаки, що в кінцевому підсумку скорочує часові затримки на обробку ТІР.

2. У загальному випадку визначення спрямованості прихованого інформаційно-психологічного впливу слова на підсвідомість особистості в фонетичному просторі з використанням технології семантичного диференціала ***пропонується*** організовувати на основі двох підходів.

2.1. Перший підхід базується на визначенні прихованого ІП впливу структурних компонент ТІР на основі фонетичних оцінок з прив'язкою до окремих лінгвістичних біполярних ознак (одномірний фонетичний простір по ЛБ ознаці). Відповідно кількість таких оцінок буде дорівнює кількості Q_h значущих ЛБ ознак.

2.2. Другий підхід полягає у визначенні інтегрованих оцінок фонетичного впливу структурних компонент ТІР на підсвідомість особистості за всіма ЛБ ознаками. Тут розглядається векторний простір звукового впливу на підсвідомість особистості.

3. Створений (*вдосконалений*) метод побудови одновимірного семантичного диференціала для оцінки рівня і напряму ІП впливу структурних компонент ТІР в фонетичному просторі з урахуванням прив'язки до градаційних двополюсних шкал окремих значущих ЛБ ознак. Відмінний аспект полягає у використанні для побудови фонетичного простору тільки значущих біполярних лінгвістичних ознак.

4. Розроблений (*вперше*) метод ідентифікації інформаційно-психологічний вплив структурних компонент (слів) текстових інформаційних ресурсів на підсвідомість особистості на основі формування векторного семантичного диференціала. Метод базується на таких еатпах:

- встановленні векторної фонетичної оцінки рівня і спрямованості ІП впливу звуко-букв по всім біполярним лінгвістичним ознакам;

- здійснення векторної фонетичної ідентифікації рівня і напряму ІП впливу структурної компоненти (слова) ТІР на підсвідомість особистості за всіма звуко-буквами в значимоиу двополюсному лінгвістичному біполярному просторі, яку представляють як матеріальний нерівноважний базис;

- визначення векторного семантичного диференціала на основі ідентифікації інтегрованих фонетичних оцінок за всіма біполярними градаційними шкалами значущих лінгвістичних ознак з урахуванням детектування двобічності ІП впливу (конструктивний і деструктивний) в двовимірному матеріальному нерівноважному просторі.

5. Розроблено статичні підходи до статичного аналізу ІП впливу тексту на підсвідомість особистості на основі усереднення ВП впливу окремих слів на підсвідомість особистості. Перший підхід розглядає текст як набір окремих слів, кожне з яких несе свій вплив на підсвідомість в тій чи іншій мірі. Другий підхід розглядає текст як одне велике ціле слово. Це дозволяє зробити оцінку деструктивного або конструктивного впливу Всього текстового інформаційного ресурсу на підсвідомість особистості.

6. Створено комплексний метод виявлення прихованого інформаційно-психологічного впливу в текстовому інформаційному ресурсі на підсвідомість особистості в багатовимірному фонетичному просторі з прив'язкою до векторних градаційних двополюсних шкал значущих біполярних лінгвістичних ознак на основі формування семантичного диференціала слів і обробкою їх по динамічній технології з накопиченням фрагментарної інформації.

Спільне (консолідоване) функціонування двох методів заснованих на фонетичних оцінках звуко-букв, полягає в таких етапах: перший тип аналізу (семантичний диференціал) - визначається рівень позитивності або негативності слова по ЛБ ознаками; другий тип аналізу - визначає конкретний якісний аспект за яким слово буде негативним або позитивним.

Тут базовими технологічними компонентами є:

6.1. Метод динамічного аналізу ТІР з накопиченням його фрагментів на основі формування одновимірного семантичного диференціала.

6.2. Метод динамічного аналізу ТІР з накопиченням його фрагментів на основі оцінки фонетичної значущості слова за однополярною значимою лінгвістичною ознакою. Відмінні риси полягають в тому що пропонується статичний ідентифікатор для прийняття рішення щодо наявності деструктивного впливу слова на підсвідомість особистості по кожній конкретній однополярній ознаці *на основі визначення відхилення частотності звуко-букв в слові від норми, тобто як часто конкретний набір звуків (звуко-слово) озвучується в тексті і його відхилення по частоті звучання від нормативно заставленого рівня.*

Основні відмінності комплексного методу динамічного аналізу впливу текстових інформаційних ресурсів на підсвідомість людини полягають в наступному:

- дозволяє оцінити сугестивний деструктивний ІП вплив на підсвідомість особистості не цілого тексту, а провести оцінку ІП впливу на підсвідомість людини окремих його фрагментів, тобто мається можливість оцінити в які моменти текстове інформаційне повідомлення змінювало свою сугестивну спрямованість;

- виявлення сугестивного деструктивного ІП впливу текстових інформаційних ресурсів на підсвідомість особистості здійснюється за технологією динамічного накопичування окремих фрагментів;

- для формування багатовимірного фонетичного простору задіються тільки значимі лінгвістичні ознаки.

Це дозволяє

1) підвищити ефективність виявлення сугестивних інформаційних деструкцій в АІР та ТІР в тому числі з врахуванням: можливості з боку протиборчої сторони їх додаткового маскування в конструктивному або нейтральному ТІР; особливостей сприйняття інформації підлітками;

2) знизити ймовірність помилок першого і другого роду в процесі оцінки деструктивності або конструктивності інформаційно-психологічного впливу окремих слів на підсвідомість особистості.

3) при роботі з підлітками визначити зміни в їх поведінки (висловлювання) на підсвідомому рівні.

Основні науково-прикладні результати даного розділу опубліковано та апробовано в наступних наукових працях [1, 8, 11, 14, 15, 16-19, 21, 85-87, 109, 110].

РАЗДЕЛ 4
ОЦІНКА ЕФЕКТИВНОСТІ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ ВИЯВЛЕННЯ СУГЕСТИВНОГО ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ВПЛИВУ НА ПІДСВІДОМІСТЬ ОСОБИСТОСТІ В ТЕКСТОВИХ ІНФОРМАЦІЙНИХ РЕСУРСАХ

Викладаються результати експериментальних досліджень з виявлення конструктивних та деструктивних сугестивних інформаційно-психологічних впливів в текстових інформаційних ресурсах на підсвідомість особистості. На основі чого обґрунтовано адекватність створених методів виявлення сугестивних деструктивних ІП впливів на основі формування одновимірного та векторного семантичного диференціалу багатовимірному фонетичному просторі з прив’язкою до значимих лінгвістичних ознак.

Показано, що за рахунок автоматизації, розроблених в дисертаційній роботі технології та методів, значно зменшується час для виявлення сугестивного ІП впливу на підсвідомість людини.

Викладено методику проведення експериментальних досліджень відносно проведення практичних досліджень щодо ймовірності виявлення сугестивних інформаційно-психологічних впливів на підсвідомість особистості в ТІР. Стверджено ефективність розроблених в дисертації методів в порівнянні з відомими аналогами.

4.1. Оцінка результатів процесу виявлення інформаційних деструкцій в текстових ресурсах на підсвідомість особистості

На основі методів семантичного диференціала, фонетичної складової, було розроблено автоматизоване програмне забезпечення, яке дозволяє здійснити аналіз за кожним методом трьома способами: статичним, динамічним і накопичувальним (**Додаток В**). Для аналізу роботи методів і програми, в якості тестових ТІР були обрані два вірші з заведемо характерним сугестивним ІП впливом, які збігаються з їх семантичною спрямованістю, а саме: "Зимнее утро" О.С. Пушкіна і "Нате!" В.В. Маяковського. Ці вірші були обрані, так як вони мають протилежні ознаки для сприйняття людиною.

Позитивним віршем виступає "Зимнее утро" О.С. Пушкіна. У ньому поет з любов'ю і в фарбах малює картини рідної природи. Тому вірш має світлі і яскраві фарби, викликає теплі почуття у читача. Негативним або ж темним виступає вірш "Нате!" В.В. Маяковського. У ньому виражено неприйняття існуючої дійсності, що характерно для ранньої лірики Маяковського. Поет нещадно, люто критикує існуючий світопорядок, створюючи яскраві сатірістичны образи самовдоволених, байдужих людей.

На рис. 4.1 і рис. 4.2 представлені результати роботи програми у вигляді діаграми результуючих значень за характеристиками однополярних лінгвістичних ознакових аспектів фонетичного аналізу вірша О.С. Пушкіна "Зимнее утро" та вірша В.В. Маяковського "Нате!". З аналізу даних на цих рисунках з врахуванням їх порівняння з семантичним навантаженням, можна заключити наступне. Перше що впадає до уваги, це абсолютно протилежні напрямки спрямування ІП впливу. Оскільки вірші були спеціально обрані з позитивним і негативним підтекстом (сугестивним інформаційно-психологічним впливом на підсвідомість особистості), то такого результату і слід було очікувати.

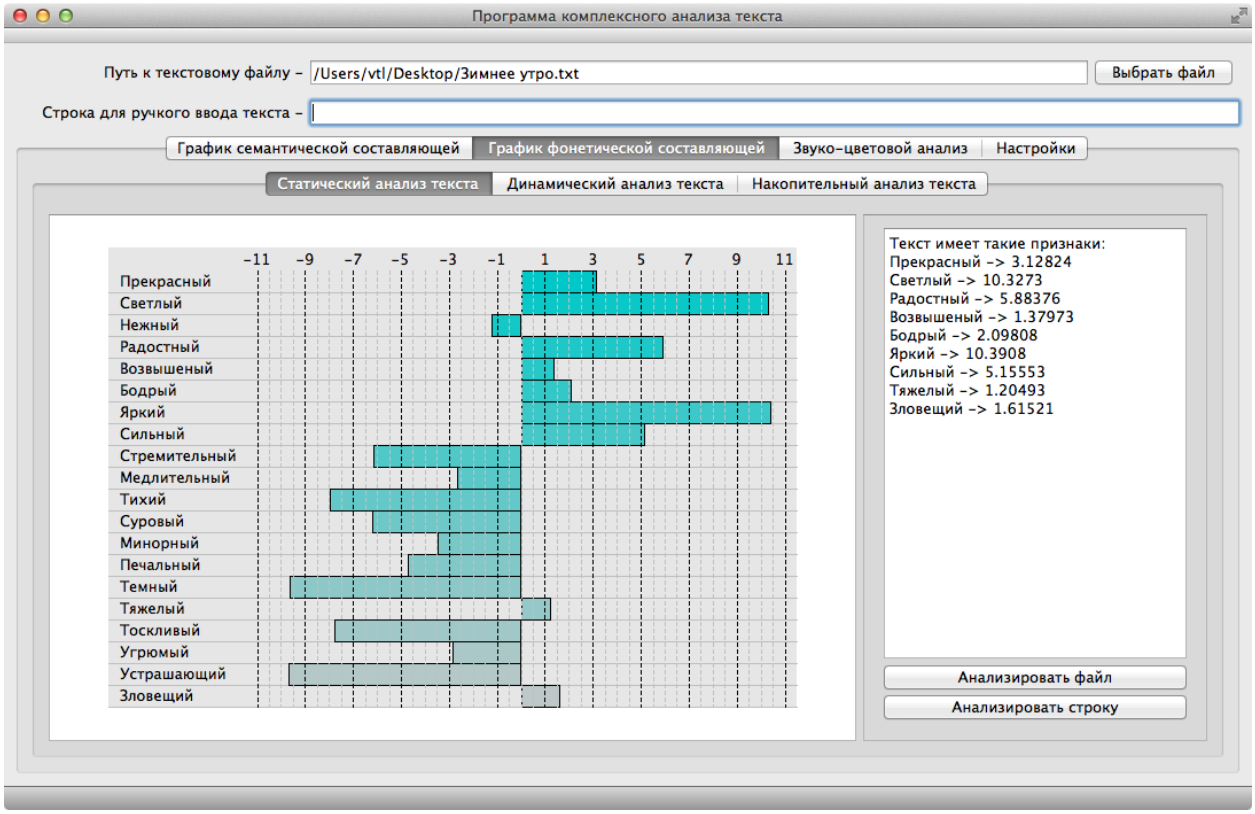


Рисунок 4.1 – Повний аналіз вірша “Зимнее утро” О.С. Пушкіна за лінгвістичними ознаками

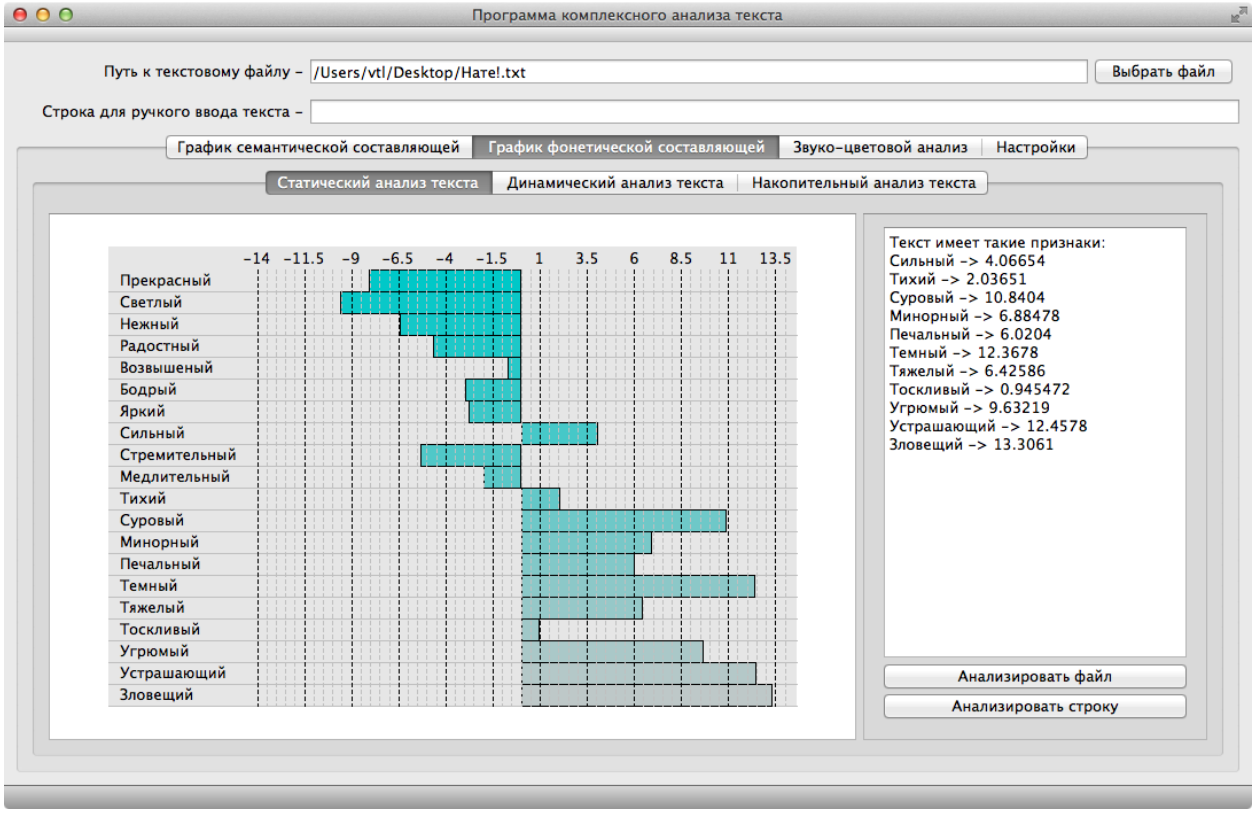


Рисунок 4.2 – Повний аналіз вірша “Нате!” В.В. Маяковского

Розглянемо обидва результати детальніше. Оскільки граничне значення від якого починається зона істотного відхилень становить 0,5, то з результатів аналізу видно, що для вірша "Зимнее утро" такі відхилення мають шкали таких лінгвістичних ознак, як: прекрасний, світлий, радісний, піднесений, бадьорий, яскравий, сильний. Але оскільки всі вони мають різні значення впливу, то для характеристики вірша виберемо найпомітніші. Таких шкал лінгвістичних ознак дві, а саме: світлий з коефіцієнтом 10,3 і яскравий з коефіцієнтом 10,4. Ці показники майже в 2 рази перевершують всі інші. Тому, виходячи з їх аналізу, можемо дати характеристику (відносно інформаційно-психологічного сприйняття на рівні підсвідомості) вірша "Зимнее утро" як світле і яскраве. І це буде досить вірний опис, так як вірш дійсно має "світле" і "яскраве" сприйняття, коли його читаєш.

Далі розглянемо результат аналізу другого вірша "Нате!" В.В. Маяковського. Як видно з діаграми, однополярних лінгвістичних ознак "яскравий" і "світлий" воно явно не має. А переважаючими лінгвістичними ознаками виступають: сильний, тихий, суворий, мінорний, сумний, темний, важкий, тужливий, похмурий, страхітливий і зловісний. З усіх ознак варто виділити: суворий – 10,8, темний – 12,4, похмурий – 9,6, страхітливий – 12,5, зловісний – 13,3, так як вони мають найвищі показники. Виходячи з цих показників, вірш можна описати як "зловісне", "темне" або ж "страхітливе". Це говорить нам про те, що воно має негативний ІП характер і сприймається особистістю як щось неприємне і темне. Ці показники так само досить точно описують характер твору, так як вірш, дійсно володіє негативними фарбами і багато в чому залишає неприємне відчуття від сприйняття.

Маючи оцінки подання загального характеру віршів, варто проаналізувати кожне з них за допомогою *методу динамічного аналізу текстових інформаційних ресурсів за окремими фрагментами*. Так як ми знаємо, що один вірш має "світле" забарвлення, а друге "темне", то варто простежити чи переважає цей окрас в усьому вірші рівними частинами, або ж це якась частина, яка має настільки

істотний вплив. Для цього варто виконати динамічний аналіз по кожному рядку вірша і простежити зміну коефіцієнтів тільки значимих шкал лінгвістичних ознак.

Простежимо за однією шкалою для кожного вірша, яка має найбільше відхилення. Для вірша “Зимнее утро” це буде шкала "яскравий", а для вірша "Нате!", Це буде шкала "зловісний ". На рис. 4.3 і рис. 4.4 наведені діаграми, складені після аналізу обох віршів методом динамічного аналізу фрагментів ТІР. Кожен стовпець діаграми представляє значення для одного рядка вірша з урахуванням назви. Як видно з діаграм, найбільш вагома ознака для віршів, не завжди має високий коефіцієнт на окремих рядках, а в деяких випадках, навіть відсутня. Але загальні значення семантичного диференціалу за цієї однополярною лінгвістичною ознакою по сприйняттю всього вірша, нададуть найбільший ІП вплив, ніж інші. За допомогою такого методу аналізу, можна визначити ті ділянки текстового ресурсу, для яких характеристика семантичного диференціалу лінгвістичної ознаки виходить за необхідну зону. Але розглянувши гістограму динамічного аналізу можна помітити, що для вірша “Зимнее утро”, властива зайва хвилеобразність значень. Але за загальними підсумками аналізу, значення все одно залишається найвищим і найбільш помітним. Цю властивість вірш набуває шляхом накопичення значень всіх його рядків. Простежити за накопичувальним значенням можна шляхом аналізу вірша накопичувальним методом.

На рис. 4.5 наведена діаграма зміни найбільш вагомого признакового аспекту "яскравий" для вірша О.С. Пушкіна “Зимнее утро” по всіх блоках за ***динамічною технологією з накопичуванням***. За блок було прийнято кожен рядок вірша разом з назвою. Звідки, можна простежити, що від самого початку і до кінця вірш поступово збільшує значення семантичного диференціалу за значимою лінгвістичною ознакою "яскравий" для всього тону вірша. При цьому перші три рядки вже відразу ж характеризують текст ознакою "яскравий". Потім на рядках 4,5,10 і 11 ознака стає не характерною. Починаючи з 16–го рядка і до кінця вірша ознака "яскравий" є визначальною для даного віршу.

Так само для вірша "Нате!" В.В. Маяковського на рис. 4.6 приведена гістограма фонетичного значення накопичувальним підсумком за ознаковим аспектом

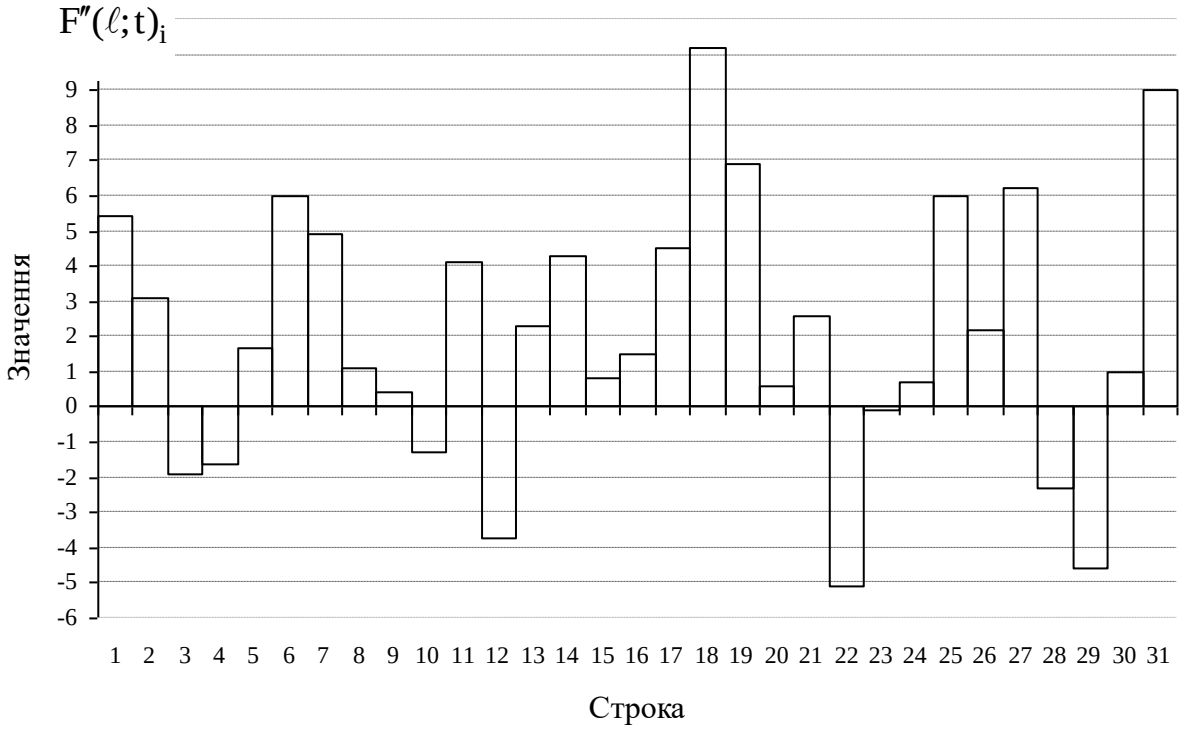


Рисунок 4.3 – Діаграма динамічної зміни лінгвістичної ознаки "яскравий" у вірші “Зимнее утро” О.С. Пушкіна

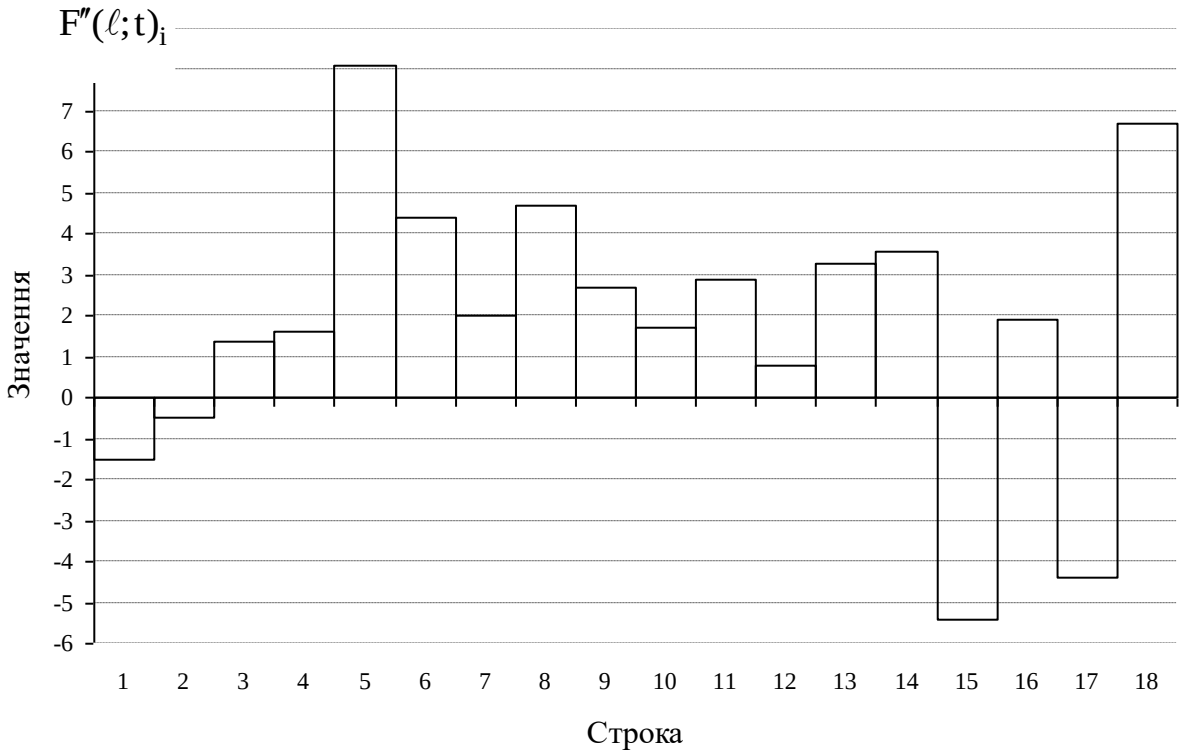


Рисунок 4.4 – Діаграма динамічної зміни лінгвістичної ознаки "зловісний" у вірші “Нате!” В.В. Маяковского

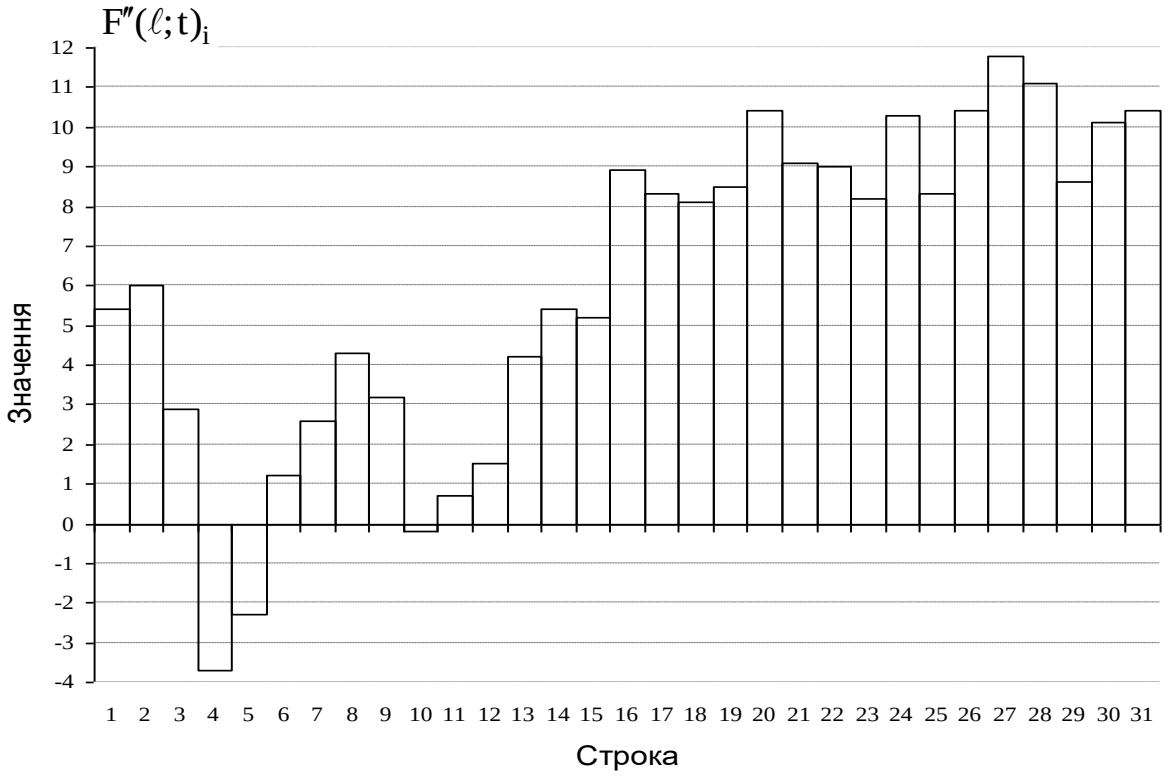


Рисунок 4.5 – Діаграма зміни ознакового аспекту "яскравий" за динамічною технологією з накопичуванням фрагментів

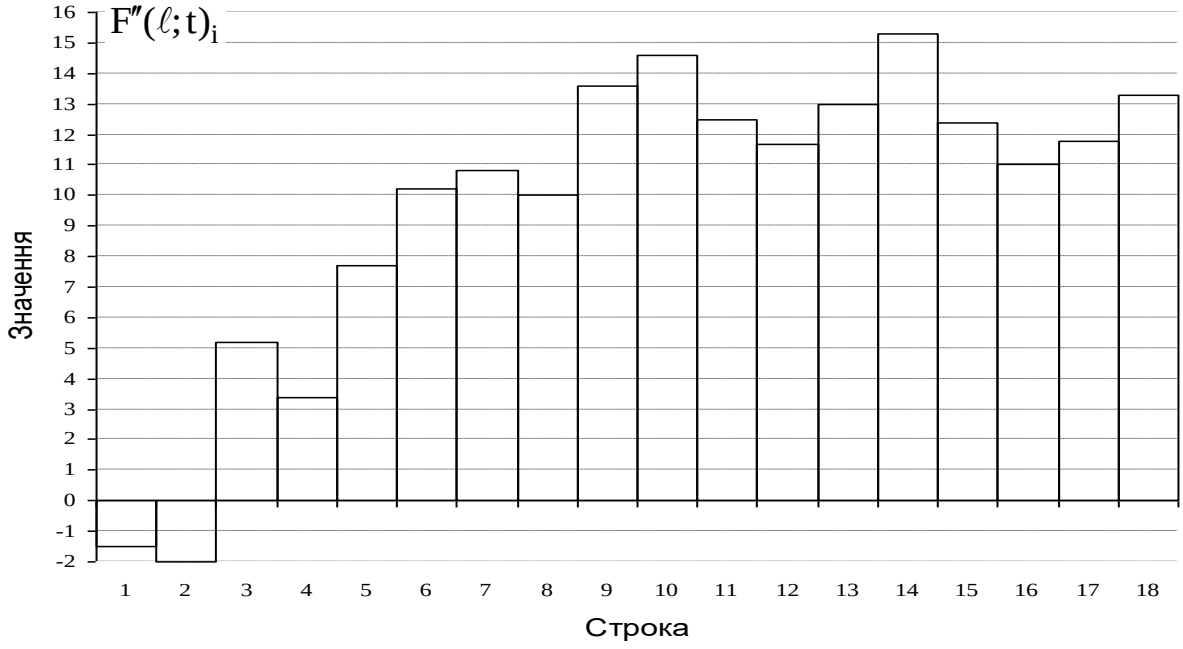


Рисунок 4.6 – Діаграма зміни ознакового аспекту "зловісний" накопичувальним підсумком

"зловісний". З аналізу діаграми на рис. 4.6 можна заключити, що практично протягом усього віршу простежується переважання значення семантичного диференціалу за лінгвістичною ознакою "зловісний". Перші два рядки вірша не мають характерної ознаки, а от починаючи з третього рядка, ознаковий аспект стає значним і, починаючи з дев'ятою строчки, є визначальним для вірша.

Отже можна зробити наступний узагальнюючий висновок.

1. Проведено аналіз тестових ресурсів з явно вираженою спрямованістю ІП впливу, а саме О.С. Пушкіна “Зимнее утро” та В.В. Маяковского “Нате!”. Результати аналізу показали наступне. Вірш "Зимнее утро" має відхилення в шкалах: прекрасний, світлий, радісний, піднесений, бадьорий, яскравий, сильний. При цьому властивостями, що характеризують спрямованість віршу є: світлий з коефіцієнтом 10,3, яскравий з коефіцієнтом 10,4. Вірш " Нате!" має відхилення в шкалах: сильний, тихий, суворий, мінорний, сумний, темний, важкий, тужливий, похмурий, страхітливий і зловісний. При цьому властивостями, що характеризують спрямованість віршу є: суворий – 10,8, темний – 12,4, похмурий – 9,6, страхітливий – 12,5, зловісний – 13,3.

2. Динамічний аналіз віршів показав наступні результати. Для вірша “Зимнее утро” властива зайва хвилеобразність значень. Але за загальними підсумками аналізу, значення все одно залишається найвищим і найбільш помітним. Цю властивість вірш набуває шляхом накопичення значень всіх його рядків. При тому, що на основі динамічного аналізу віршу накопичувальним підсумком видно, що вже перші три рядки відразу ж характеризують текст ознакою "яскравий". Потім на рядках 4,5,10 і 11 ознака стає не характерною. Починаючи з 16–го рядка і до кінця вірша (31-го рядка) ознака "яскравий" є визначальною для нього. Так само для вірша "Нате!" В.В. Маяковського на основі динамічного аналізу видно, що практично протягом усього вірша простежується переважання ознаки "зловісний".

4.2. Оцінка результатів експериментальних досліджень з виявлення сугестивних інформаційно-психологічних впливів на підсвідомість особистості на основі методу визначення семантичного диференціалу за динамічною технологією з накопичуванням фрагментів текстового ресурсу

Результати експерименту щодо визначення спрямованості текстового інформаційного ресурсу відносно інформаційно-психологічного впливу на підсвідомість особистості.

Для тестування розроблених методів була відібрана тестова група підлітків у кількості 30 чоловік та група експертів-викладачів у кількості 10 чоловік. Обом групам для аналізу були надані різні тексти для визначення їх сугестивної ІП спрямованості на підсвідомість особистості. Тобто, було запропоновано визначити із перелічених лінгвістичних ознак ті, що відповідають спрямованості віршу на думку тестуємих. Результати експерименту для віршів О.С. Пушкіна “Зимнее утро” та В.В. Маяковского “Нате!” щодо визначення їх фонетичних значень на основі методу визначення семантичного діференціалу за методом динамічного аналізу накопичувальним підсумком (МДАНП) для фрагментів текстового ресурсу представлені в табл. 4.1 та 4.2 відповідно. З аналізу результатів, представлених в табл. 4.1 та 4.2 можна зробити наступні висновки.

1. Результати експерименту щодо фонетичної складової збіглися, а саме:

1) для віршу О.С. Пушкіна “Зимнее утро” ті, хто тестувався, та програма на основі розробленого методу МДАНП визначили всі позитивні лінгвістичні ознакові шкали, а саме: прекрасний, світлий, радісний, піднесений, бадьорий, яскравий, сильний. Але найпомітнішими є дві шкали – світлий (тестова група – 100 % опитуваних, експериментальна група – 100 % опитуваних, розроблена технологія – 99,42 % від максимального результату) та яскравий (тестова група – 96,67 % опитуваних, експериментальна група – 100 % опитуваних, розроблена технологія –максимальний результат). Відхиленням в тестової групі склала ознака “стрімкий” (16,67 % проти 0 % для розробленої технології), що також можна віднести до позитивної шкали, та ознака “піднесений” (30 % проти 13,28 % для розробленої

Таблиця 4.1

Результати експерименту, щодо визначення спрямованості віршу О.С. Пушкіна “Зимнее утро”

№ ознаки	Ознака для аналізу	Оцінка		
		тестової групи	експертної групи	розробленим методом
1	прекрасний	11	3	3,13
2	бадьорий	7	3	2,10
3	світлий	30	10	10,33
4	ніжний	2	0	0
5	мінорний	0	0	0
6	сумний	0	0	0
7	яскравий	29	10	10,39
8	темний	0	0	0
9	сильний	12	4	5,15
10	суровий	0	0	0
11	тужливий	0	0	0
12	радісний	21	6	5,88
13	стрімкий	5	0	0
14	похмурий	0	0	0
15	важкий	0	0	0
16	піднесений	9	3	1,38
17	повільний	0	0	0
18	тихий	0	0	0
19	страхітливий	0	0	0
20	зловісний	0	0	0

Таблиця 4.2

Результати експерименту, щодо визначення спрямованості віршу В.В. Маяковского “Нате!”

№ ознаки	Ознака для аналізу	Оцінка		
		тестової групи	експертної групи	розробленим методом
1	прекрасний	0	0	0
2	бадьорий	0	0	0
3	світлий	0	0	0
4	ніжний	0	0	0
5	мінорний	2	3	6,88
6	сумний	11	4	6,02
7	яскравий	0	0	0
8	темний	27	9	12,37
9	сильний	19	5	4,07
10	суровий	5	2	0
11	тужливий	7	1	0,95
12	радісний	1	0	0
13	стрімкий	3	0	0
14	похмурий	24	7	9,63
15	важкий	17	6	6,43
16	піднесений	0	0	0
17	повільний	0	0	0
18	тихий	0	1	2,04
19	страхітливий	29	9	10,84
20	зловісний	29	10	13,31

технології). Але ці відхилення, скоріш, пов'язані з особливостями психіки підлітків, та не впливають на загальний результат експерименту. Тобто, за всіма результатами перевірки вірш О.С. Пушкіна "Зимнее утро" має позитивну спрямованість на підсвідомість особистості;

2) для віршу В.В. Маяковского "Нате!" тестуємі, та програма на основі розроблених методів визначили всі негативні лінгвістичні ознакові шкали, а саме: сильний, тихий, суворий, мінорний, сумний, темний, важкий, тужливий, похмурий, страхітливий, зловісний. Найпомітнішими є п'ять шкал – суворий (тестова група – 96,67 % опитуваних, експериментальна група – 90 % опитуваних, розроблена технологія – 81,44 % від максимального результату), темний (тестова група – 90 % опитуваних, експериментальна група – 90 % опитуваних, розроблена технологія – 92,94 % від максимального результату), похмурий (тестова група – 80 % опитуваних, експериментальна група – 70 % опитуваних, розроблена технологія – 72,35 % від максимального результату), страхітливий (тестова група – 96,67 % опитуваних, експериментальна група – 90 % опитуваних, розроблена технологія – 81,44 % від максимального результату), зловісний (тестова група – 96,67 % опитуваних, експериментальна група – 100 % опитуваних, розроблена технологія – максимальний результат). Значним відхиленням для тестовій групи склала лінгвістична ознака "сильний" (63,33 % проти 30,57 % для розробленої технології). Це пов'язано з особливостями психіки підлітків, та не впливає на загальний результат експерименту. Тобто, за всіма результатами перевірки вірш В.В. Маяковского "Нате!" має негативну спрямованість на підсвідомість людини.

2. Аналіз семантичної спрямованості віршів відповідає їх фонетичному значенню (табл. 4.3). Обідві групи тестуємих підтвердили факт відповідності семантичної та фонетичної спрямованості віршу (100 % тестової групи та 100 % експертної групи).

При чому, ті, хто тестувався, свої відповіді щодо фонетичного значення віршу визначали з урахуванням семантичної спрямованості (73,33 % тестової групи та 30 % експертної групи). В теж час розроблена технологія МДАНП враховувала

лише вплив на підсвідомість особистості без врахування семантичної спрямованості текстового ресурсу.

Таблиця 4.3

Збіг результатів семантичного та фонетичного значення віршів

Автор та назва віршу	Питання			
	Відповідність семантичної та фонетичної спрямованості?		Визначення фонетичної спрямованості з урахуванням семантичної спрямованості?	
	тестова група	експертна група	тестова група	експертна група
О.С. Пушкіна “Зимнее утро”	30	10	22	3
В.В. Маяковского “Нате!”	30	10	22	3

4.3. Порівняльна оцінка ефективності процесів виявлення сугестивних інформаційно-психологічних впливів на підсвідомість для текстових інформаційних ресурсів

В результаті досліджень було проведено 10 експериментів, в результаті яких тестуємим було запропоновано по 100 різних коротких текстових інформаційних повідомлень для виявлення сугестивного ІП впливу на підсвідомість особистості. Респондентам було необхідно лише виявити наявність сугестивних ІП впливу на підсвідомість в ТІР без визначення типу спрямованості.

Ефективність E виявлення сугестивних ІП впливу в ТІР експертною або тестовою групами розраховується за формулою:

$$E = \frac{\sum_{i=1}^{d} \beta_i}{d}, \qquad (4.1)$$

де β_i – ваговий коефіцієнт, що обчислюються, як питома кількість тих, хто тестується, що обрала i-й текстовий ресурс, як той що містить сугестивний ІП впливу на підсвідомість, а саме

$$\beta_i = \frac{a_i}{m}, \tag{4.2}$$

де a_i – кількість тестуємих, які обрали i-ій текстовий ресурс, як такий, що містить сугестивний ІП впливу на підсвідомість; m – загальна кількість тестуємих, яка приймала участь в експерименті; d – загальна кількість коротких текстових інформаційних повідомлень що пропонувалася для виявлення сугестивного ІП впливу на підсвідомість особистості в результаті експерименту.

Ефективність $E_м$ виявлення сугестивних ІП впливу в ТІР за допомогою ***методів МДАНП з визначенням семантичного діференціалу у векторному фонетичному просторі***, розраховується за формулою:

$$E_м = d_{ІПВ} / d, \tag{4.3}$$

де $d_{ІПВ}$ – кількість коротких текстових інформаційних повідомлень в яких за допомогою розроблених методів, виявлено сугестивний ІП впливу на підсвідомість особистості в результаті експерименту.

Результати оцінки ефективності виявлення сугестивних ІП впливу в ТІР представлені на рис. 4.7 та в табл. 4.4. З аналізу даних експериментів можна зробити наступні висновки:

– за допомогою розроблених методів було виявлено сугестивних ІП впливу на підсвідомість людини в ТІР на 3 % більше ніж експертною групою та на 21 % більше ніж тестовою групою. Експертна група виявила ІП впливу в ТІР на 18 % більше ніж тестова група. Даний результат пов'язаний з тим, що тестова група складається з підлітків, які не можуть чітко уявити сам неприхований вплив, який може суттєво відобразитися на їх психологічному стані. Результати між експертною групою та розроблених методів в середньому збігаються, але за допомогою розроблених методів процес виявлення є більш ефективним;

– з початку проведення досліджень розбіг результатів тестової групи від розроблених методів складав 30 % в першому експерименті. Але на при кінці досліджень результат звузився до різниці на 10 %. Це пов’язано з тим, що підлітки, які підвергалися тестуванню, в результаті спілкування між собою та дорослими поча-

ли більш уважно відноситися до прочитаного. Тому, в повсякденному житті, коли підлітки не уважно відносяться по прочитаного, результати негативного ІП впливу на їх підсвідомість будуть суттєвими.

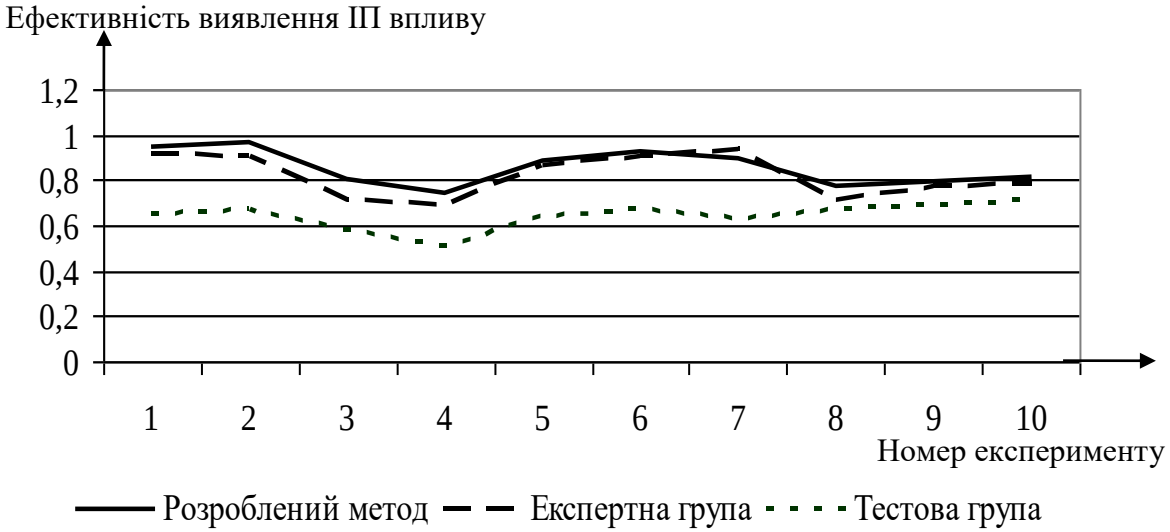


Рисунок 4.7 – Результати експериментального виявлення ІП впливу в ТІР

Таблиця 4.4

Результати експериментального виявлення ІП впливу в ТІР

Метод виявлення ІП впливу	Номер експерименту										Усереднене значення
	1	2	3	4	5	6	7	8	9	10	
Розроблені методи	0,95	0,97	0,8	0,74	0,88	0,93	0,89	0,77	0,79	0,81	0,85
Експертна група	0,92	0,91	0,71	0,69	0,86	0,9	0,94	0,71	0,77	0,78	0,82
Тестова група	0,65	0,67	0,58	0,51	0,64	0,67	0,63	0,67	0,69	0,71	0,64

У якості показника приросту ефективності $E_{ІПВ}$ виявлення сугестивних ІП впливів в ТІР на підсвідомість особистості за рахунок реалізації розроблених методів доцільно використовувати зважений показник, який має вид:

$$E_{ІПВ} = (E_м - E)/(1 - E), \tag{4.4}$$

де $E_м$ – ефективність виявлення сугестивних ІП впливів в ТІР за допомогою розроблених методів; E – ефективність виявлення сугестивних ІП впливів в ТІР експертною або тестовою групами.

Тоді формула (4.4) з врахуванням виразів (4.1) – (4.3) прийме вигляд:

$$E_{ІПВ} = \frac{E_м - E}{1 - E} = \frac{\frac{d_{ІПВ}}{d} - \frac{\sum_{i=1}^{d} \frac{a_i}{m}}{d}}{1 - \frac{\sum_{i=1}^{d} \frac{a_i}{m}}{d}} = \frac{d_{ІПВ} - \sum_{i=1}^{d} \frac{a_i}{m}}{d - \sum_{i=1}^{d} \frac{a_i}{m}} = \frac{m \cdot d_{ІПВ} - \sum_{i=1}^{d} a_i}{m \cdot d - \sum_{i=1}^{d} a_i}. \quad (4.5)$$

Сутність виразів (4.4) та (4.5) відображається в залежності, що отримана за допомогою системи Mathcad [123] та наведена на рис. 4.8.

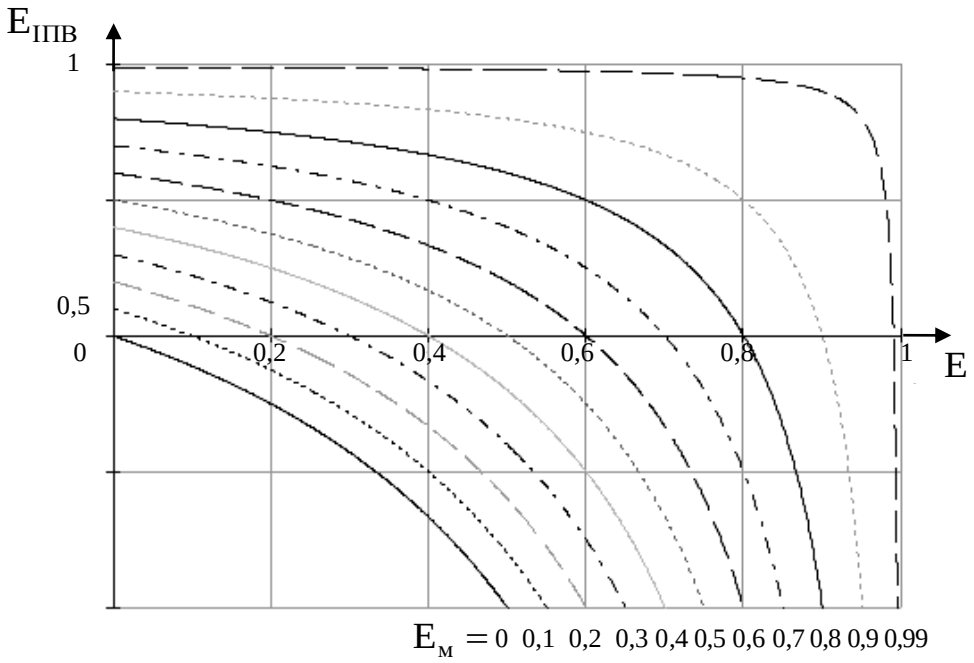


Рисунок 4.8 – Графік зміни показника ефективності $E_{ІПВ}$ в залежності від досягнутих результатів

Усереднені значення зваженого показника $E_{ІПВ}$, що отримані в результаті експериментів, наведені на рис. 4.9, 4.10 та в табл. 4.5.

З аналізу даних можна зробити висновок, що приріст ефективності щодо виявлення сугестивного ІП впливу на підсвідомість особистості в ТІР досягається за рахунок використання запропонованих в дисертації методів та складає у середньому до 16 % в порівнянні з експертною групою та у середньому до 59 % в порівнянні з тестовою групою.

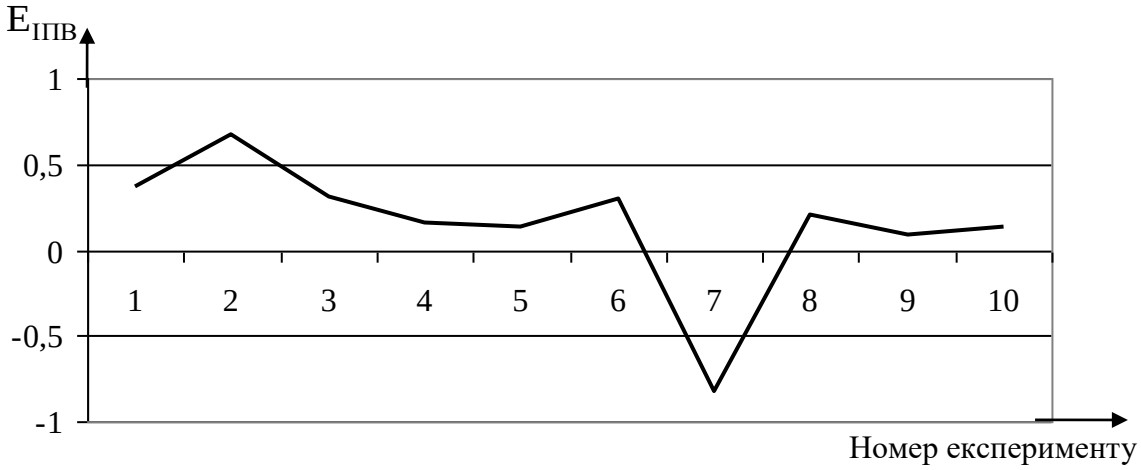


Рисунок 4.9 – Усереднені значення зваженого показника $E_{ІПВ}$ для розробленого методу в порівнянні з експертною групою

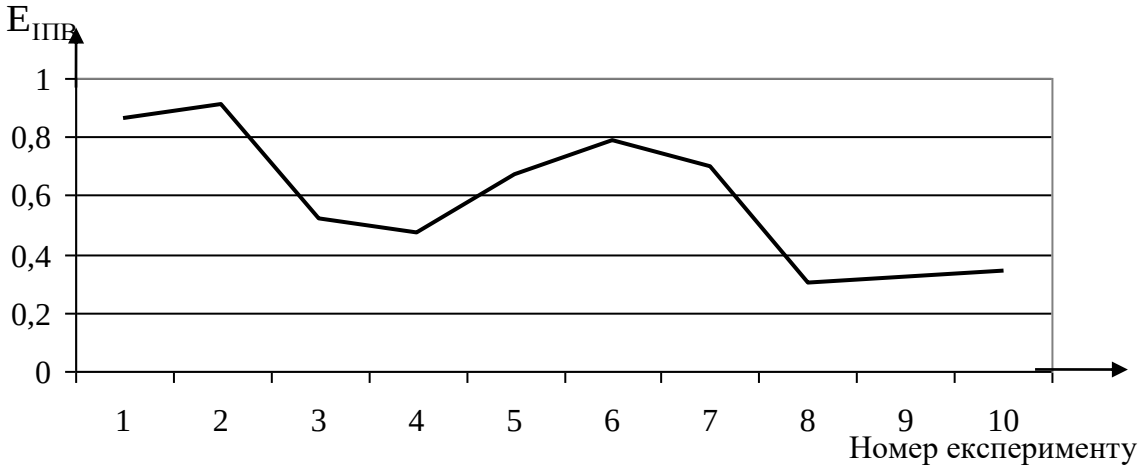


Рисунок 4.10 – Усереднені значення зваженого показника $E_{ІПВ}$ для розробленого методу в порівнянні з тестовою групою

Таблиця 4.5

Усереднені значення зваженого показника $E_{ІПВ}$

Показник приросту ефективності в порівнянні з	Номер експерименту										Усереднене значення
	1	2	3	4	5	6	7	8	9	10	
Експертною групою	0,37	0,67	0,31	0,16	0,14	0,3	-0,83	0,21	0,09	0,14	0,16
Тестовою групою	0,86	0,91	0,52	0,47	0,67	0,79	0,7	0,3	0,32	0,34	0,59

Обидві групи тестуємих підтвердили факт, що надавали свої відповіді відносно визначення наявності сугестивного ІП впливу на підсвідомість в ТІР з врахуванням семантичної спрямованості (табл. 4.6). Так в тестовій групі кількість таких осіб склала 96,67 %, а в експертній групі – 80 %. При тому, що розроблена технологія враховувала лише ІП вплив на підсвідомість особистості без врахування семантичної спрямованості тексту.

Таблиця 4.6

Відсоток осіб, що визначали фонетичну спрямованість ТІР з урахуванням їх семантичної спрямованості

Параметр	Тестова група	Експертна група
Кількість осіб	29	8
Відсоток	96,67	80

Усереднений час виявлення сугестивного ІП впливу на підсвідомість особистості в ТІР, який був затрачений тестовою, експертною групами та програмним засобом, що реалізує розроблені методи, наведено на рис. 4.11. Слід зазначити, що програмний засіб, який реалізує розроблені методи, не був оптимізованим по швидкості виконання та підключав в своїй роботі текстовий редактор Microsoft Word для використання його словників, на що витрачалося багато часу. Навпаки, оптимізований програмний засіб може значно знизити час, який витрачається на виявлення сугестивного ІП впливу на підсвідомість особистості.

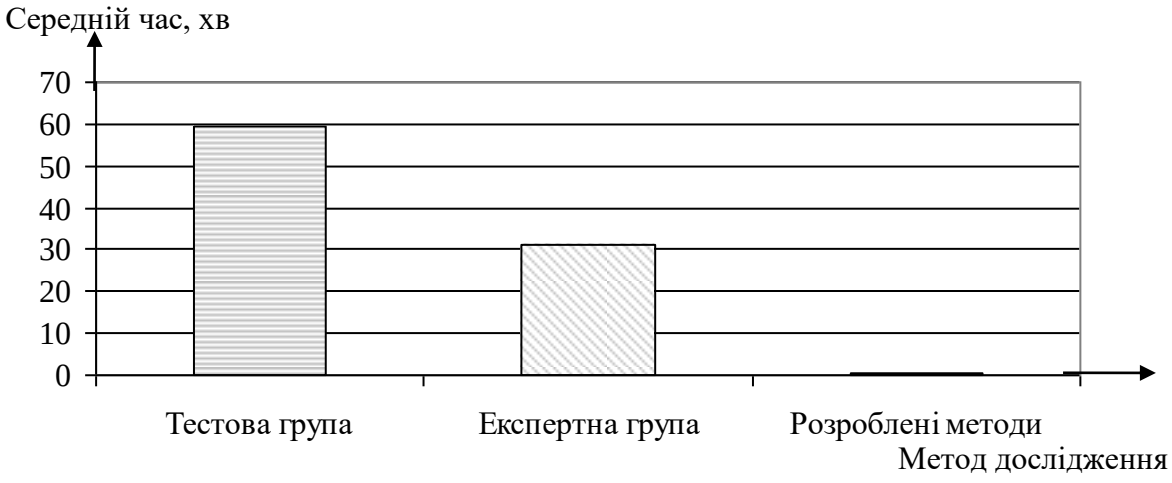


Рисунок 4.11 – Усереднений час виявлення сугестивного ІП впливу на підсвідомість людини в результаті експериментів

З аналізу даних на рис. 4.11 можна зробити висновок, що виявлення сугестивного ІП впливу на підсвідомість особистості найменше часу займає за допомогою автоматизації запропонованих методів. Процес виявлення, навіть без оптимізації програмного коду, швидше майже в 90 разів в порівнянні з експертами та майже в 170 разів в порівнянні з тими, на кого здійснюється ІП впливу. При чому, респонденти визначали лише наявність сугестивного ІП впливу на підсвідомість в ТІР, а за допомогою програмного засобу, що реалізує розроблені методи, визначався ще й тип спрямованості такого ІП впливу.

4.4. Оцінка ефективності виявлення деструктивних сугестивних інформаційно-психологічних впливів на підсвідомість особистості на основі методу векторного семантичного диференціалу в автоматичному режимі в інфокомунікаційному просторі

З метою практичного дослідження ймовірності виявлення сугестивних ІП впливів на підсвідомість особистості в повідомленнях був проведений експеримент з аналізу ТІР мережі Інтернет конструктивної та деструктивної спрямованості російського та українського походження. До експерименту було залучено 10 експертів, які є практикуючим викладачами-психологами для попереднього аналізу текстів з метою оцінки їх сугестивного навантаження на підсвідомість людини. Тексти перевірялися на наявність конструктивного або деструктивного сугестивного ІП впливу на підсвідомість особистості: програмним забезпеченням, розробленим на основі методу визначення векторного семантичного диференціалу; програмним забезпеченням щодо виявлення ІП впливу на основі ключових слів. Результати проведення експерименту наведені на рис. 4.12 та 4.13.

З аналізу даних, представлених на рис. 4.12 та 4.13, можна зробити наступні висновки:

– ймовірність виявлення сугестивних ІП впливів в ТІР на підсвідомість людини на основі розроблених підходів збігається з оцінками, отриманими групою

експертів, відхилення складає не більше 2 %. Ефективність виявлення сугестивних ІП впливів на підсвідомість особистості в ТІР складає від 98 до 100 %;

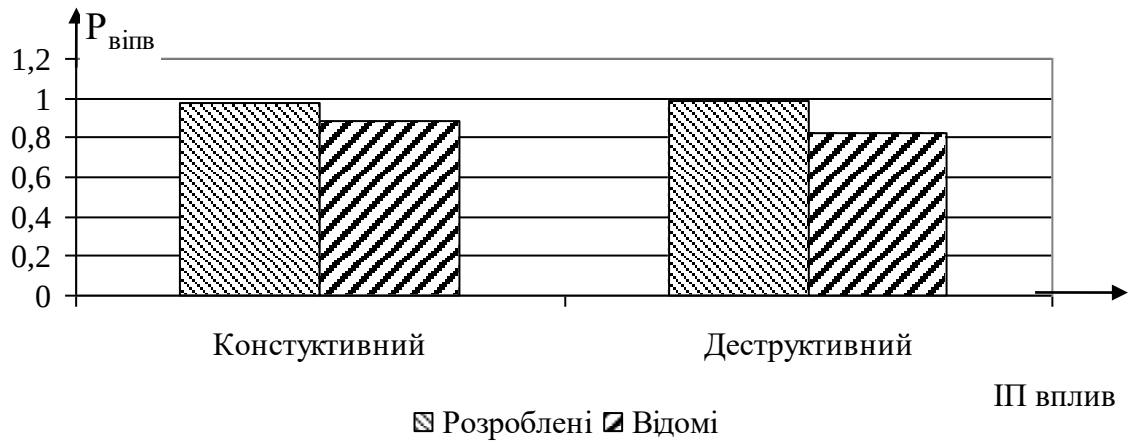


Рисунок 4.12 – Ймовірність виявлення сугестивних ІП впливів на підсвідомість особистості в ТІР російського контенту мережі Інтернет

Рисунок 4.13 – Ймовірність виявлення сугестивних ІП впливів на підсвідомість особистості в ТІР українського контенту мережі Інтернет

– в порівнянні з відомими методами оцінки ІП впливу на підсвідомість людини на основі ключових слів, розроблені в дисертаційної роботі технологія та методи виявили від 10 до 17 % більше ТІР, що носять конструктивний або деструктивний ІП вплив на підсвідомість людини. Це пов’язано в першу чергу з тим, що важко створити словники ключових “позитивно-негативних” слів, якиб могли читко описати вплив тих або інших слів на підсвідомість особистості. При тому що одні й тіж слова для різних груп людей можуть нести різну спрямованість.

Висновки за четвертим розділом

1. Технологія та методи, що розроблені в дисертаційної роботі, були реалізовані в програмному продукті з виявлення сугестивних ІП впливів в ТІР на підсвідомість людини. З використанням розробленого програмного забезпечення було проведено експериментальне дослідження з виявлення конструктивних та деструктивних сугестивних ІП впливів в ТІР на підсвідомість особистості. В експериментальному дослідженні було залучено дві групи: до складу експертної групи залучено 10 чоловік зі складу викладачів-психологів, що працюють в загальноосвітніх навчальних закладах; до складу текстової групи залучено 30 підлітків.

2. Проведено аналіз тестових віршів з явно вираженою спрямованістю, а саме О.С. Пушкіна “Зимнее утро” та В.В. Маяковского “Нате!”. Результати аналізу показали наступні результати. Вірш "Зимнее утро" має відхилення в шкалах: прекрасний, світлий, радісний, піднесений, бадьорий, яскравий, сильний. При цьому властивостями, що характеризують спрямованість віршу є: світлий з коефіцієнтом 10,3, яскравий з коефіцієнтом 10,4. Вірш " Нате!" має відхилення в шкалах: сильний, тихий, суворий, мінорний, сумний, темний, важкий, тужливий, похмурий, страхітливий і зловісний. При цьому властивостями, що характеризують спрямованість віршу є: суворий – 10,8, темний – 12,4, похмурий – 9,6, страхітливий – 12,5, зловісний – 13,3.

3. Динамічний аналіз віршів показав наступні результати. Для вірша “Зимнее утро” властива зайва хвилеобразність значень. Але за загальними підсумками аналізу, значення все одно залишається найвищим і найбільш помітним. Цю властивість вірш набуває шляхом накопичення значень всіх його рядків. При тому, що на основі динамічного аналізу віршу накопичувальним підсумком видно, що вже перші три рядки вже відразу ж характеризують текст ознакою "яскравий". Потім на рядках 4,5,10 і 11 ознака стає не характерною для вірша. Починаючи з 16–го рядка і до кінця вірша (31-го рядка) ознака "яскравий" є визначальною для нього. Так само для вірша "Нате!" В.В. Маяковського на основі динамічного аналізу видно, що практично протягом усього вірша

простежується переважання ознаки "зловісний". Перші два рядки вірша не мають характерної ознаки, а от починаючи з третього рядка, ознаковий аспект стає значним і, починаючи з дев'ятою строчки, є визначальним для вірша.

4. Експериментальні дослідження результатів аналізу віршів за допомогою програмних засобів на основі технології та методів, розроблених в дисертаційній роботі, в порівнянні з визначенням спрямованості сугестивного впливу експертною та тестовою групою показав, що

– результати експерименту щодо фонетичної складової збіглися. Так:

1) для віршу О.С. Пушкіна “Зимнее утро” найпомітнішими є дві ознаки – світлий (тестова група – 100 % опитуваних, експериментальна група – 100 % опитуваних, розроблена технологія – 99,42 % від максимального результату) та яскравий (тестова група – 96,67 % опитуваних, експериментальна група – 100 % опитуваних, розроблена технологія –максимальний результат);

2) для віршу В.В. Маяковского “Нате!” найпомітнішими є п’ять ознак – суворий (тестова група – 96,67 %, експериментальна група – 90 % опитуваних, розроблена технологія – 81,44 % від максимального результату), темний (тестова та експериментальна групи – по 90 % опитуваних, розроблена технологія – 92,94 % від максимального результату), похмурий (тестова група – 80 %, експериментальна група – 70 % опитуваних, розроблена технологія – 72,35 % від максимального результату), страхітливий (тестова група – 96,67 %, експериментальна група – 90 % опитуваних, розроблена технологія – 81,44 % від максимального результату), зловісний (тестова група – 96,67 %, експериментальна група – 100 % опитуваних, розроблена технологія –максимальний результат);

– аналіз семантичної спрямованості віршів відповідає їх фонетичну значенню. Обе групи тих, хто тестувалися, підтвердь факт відповідності семантичної та фонетичної спрямованості віршу (100 % тестової та експертної групи). При чому, ті, хто тестувався, свої відповіді щодо фонетичного значення віршу визначали з урахуванням семантичної спрямованості (73,33 % тестової групи та 30 % експертної групи), а розроблена технологія враховувала лише вплив на підсвідомість людини без врахування семантичної спрямованості тексту.

5. Проведено комплексне дослідження на основі 10 експериментів з виявлення сугестивного ІП впливу на підсвідомість особистості в 100 різних коротких текстових інформаційних повідомлень в кожному експерименті. Експеримент показав, що за допомогою методів, що розроблені в дисертаційної роботі, було виявлено сугестивних ІП впливу на підсвідомість людини в ТІР на 3 % більше ніж експертною групою та на 21 % більше ніж тестовою групою. Приріст ефективності виявлення сугестивного ІП впливу на підсвідомість особистості в ТІР досягається за рахунок використання запропонованих в дисертації методів та складає у середньому до 16 % в порівнянні з експертною групою та у середньому до 59 % в порівнянні з тестовою групою.

6. За рахунок автоматизації, розроблених в дисертаційної роботі технології та методів, значно зменшується час для виявлення сугестивного ІП впливу на підсвідомість людини. Так, процес виявлення, навіть без оптимізації програмного коду, швидший майже в 90 разів в порівнянні з роботою експертів та майже в 170 разів в порівнянні з аналізом тими, на кого здійснюється ІП впливу. При чому, респонденти здатні за зазначений час визначити лише наявність сугестивного ІП впливу на підсвідомість в ТІР, в той час, як за допомогою програмного засобу, що реалізує розроблені в дисертаційній роботі методи, мається можливість визначити ще й тип спрямованості такого ІП впливу.

7. Проведені практичні дослідження ймовірності виявлення сугестивних ІП впливів на підсвідомість особистості в ТІР. На основі аналізу результатів досліджень отримані наступні висновки:

– ефективність виявлення сугестивних ІП впливів на підсвідомість людини в ТІР складає від 98 до 100 %;

– розроблені в дисертаційної роботі технологія та методи виявили від 10 до 17 % більше ТІР з ІП впливом на підсвідомість особистості в порівнянні з відомими методами аналізу на основі ключових слів.

Основні науково-прикладні та експериментальні результати досліджень четвертого розділу опубліковано та апробовано в наступних наукових працях [1, 14, 16-18, 86, 87].

ВИСНОВКИ

У дисертаційній роботі вирішено науково-прикладне завдання, яке полягає в підвищенні інформаційної безпеки підлітків відносно деструктивних інформаційно-психологічних дій в інфокомунікаційному просторі. Розроблено метод ідентифікації ІП впливів структурних компонент ТІР на підсвідомість особи на основі формування векторного семантичного диференціала. Удосконалено інформаційну технологію забезпечення ІП безпеки підлітків на основі комплексного методу виявлення прихованого ІП впливу в ТІР на підсвідомість особи в багатовимірному фонетичному просторі з прив'язкою до векторних градаційних шкал значущих лінгвістичних ознак з формуванням семантичного диференціалу слів і обробкою їх за динамічною технологією з накопиченням фрагментарної інформації.

В умовах проведення гібридної та інформаційної війн з врахуванням наявності безлічі внутрідержавних дестабілізуючих чинників ключовий ефект в забезпеченні інформаційної переваги досягається у разі проведення інформаційно-психологічних атак. При цьому найуразливішими об'єктами деструктивної інформаційно-психологічної дії є підлітки. У разі атак на підлітків і молодь найбільш ефективними каналами комунікаційної дії є Інтернет і телебачення до 48% від загальної маси. Відповідна затребуваність в цих джерелах інформації для підлітків і молоді досягає 70%, а відповідна ступінь довіри – до 60 %. Тоді в умовах наявності множини дестабілізуючих внутрідержавних чинників, недостатньої контрольованості Інтернет-простору і дисбалансів на рівні: інформаційної культури підлітка; на рівні використання джерел комунікаційних каналів - виникають істотні втрати інформаційно-психологічної безпеки підлітків.

Отже пропонується удосконалити інформаційну технологію забезпечення протидії загрозам ІП безпеки підлітків. Як показує аналіз базових складових таких інформаційних технологій одним з ключових її технологічних етапів є методи виявлення (детектування) наявності ІП деструкцій в інформаційних ресурсах. Саме недоліки в процесі виявлення інформаційно-психологічних деструкцій в інформа-

ційних ресурсах неминуче спричиняє зниження ефективності всієї інформаційної технології забезпечення ІП безпеки підлітків. Проте сфера розробки технологічних рішень в напрямку виявлення ІП впливів знаходяться в критичному стані. Відповідні технології мають недостатній рівень розвитку, щоб бути адекватними існуючим інформаційно-технологічним можливостям протиборчої сторони щодо організації і проведення деструктивної дії ІП. З урахуванням чого, ***мета досліджень*** полягає в розробці методів виявлення деструктивної інформаційно-психологічної дії в інфокомунікаційному просторі для інформаційних технологій забезпечення безпеки підлітків.

Основними науковими результатами є.

1. Розроблено модель загроз ІП безпеки особистості в умовах інформаційного протиборства і демократизації соціуму, коли потрібно забезпечити баланс безпеки особистості одночасно в інформаційно-психологічному та інформаційно-технічному просторах (умова мережецентричності безпеки підлітка в інформаційному просторі). Обґрунтовано, що найбільш актуальними і значущими загрозами ІП безпеки особистості з позиції: виявлення та організації протидії; нанесення шкоди є сугестивны деструктивні ІП впливи. Показано, що одними з ключових ІП атак, які здійснюються в сучасному інформаційно-комунікаційному просторі, є деструктивні інформаційні модифікації в аудіоконтейнерах і електронних текстових ресурсах, а саме: аудіосуггестія, приховані вставки в аудіопотоки; сугестія текстів.

2. Побудовано інформаційна модель аналізу ТІР на основі формування семантичного диференціала. На основі чого було розроблений метод виділення значущих лінгвістичних біполярних ознак на основі представлення фонетичних оцінок звуко-букв алфавіту в речовому нерівноважному позиційному просторі. Основна відмінність тут полягає в тому, що векторний фонетичний простір лінгвістичної біполярної ознаки по всіх звуко-буквам представляється в раціональному нерівноважному позиційному базисі.

3. Розроблено метод ідентифікації інформаційно-психологічного впливу структурних компонент (слів) текстових інформаційних ресурсів на підсвідомість

особи на основі формування векторного семантичного диференціалу. Метод базується на визначенні векторного семантичного диференціалу на основі індентіфікациі інтегрованих фонетичних оцінок по всіх біполярних градаційних шкалах значущих лінгвістичних ознак з врахуванням детектування двунаправленності ІП атак (конструктивні та деструктивні) в двовимірному нерівноважному просторі.

4. Створено комплексний метод виявлення прихованого інформаційно-психологічного впливу в текстовому інформаційному ресурсі на підсвідомість особи в багатовимірному фонетичному просторі з прив'язкою до векторних градаційних двополюсних шкал значущих біполярних лінгвістичних ознак на основі формування семантичного диференціалу слів і обробкою їх за динамічною технологією з накопиченням фрагментарної інформації.

Основними практичними результатами дослідження є наступні:

1. Проведено комплексне дослідження на основі 10 експериментів з виявлення сугестивного інформаційно-психологічного впливу на підсвідомість особистості в 100 різних коротких текстових інформаційних повідомлень в кожному експерименті. Експеримент показав, що за допомогою методів, що розроблені в дисертаційної роботі, було виявлено сугестивних ІП впливів на підсвідомість особистості в ТІР на 3 % більше ніж експертною групою та на 21 % більше ніж тестовою групою. Приріст ефективності виявлення сугестивного ІП впливу на підсвідомість особистості в ТІР досягається за рахунок використання запропонованих в дисертації методів та складає у середньому до 16 % в порівнянні з експертною групою та у середньому до 59 % в порівнянні з тестовою групою.

2. За рахунок автоматизації, розроблених в дисертаційної роботі технології та методів, значно зменшується час для виявлення сугестивного ІП впливу на підсвідомість людини. Так, процес виявлення, навіть без оптимізації програмного коду, швидший майже в 90 разів в порівнянні з роботою експертів та майже в 170 разів в порівнянні з аналізом тими, на кого здійснюється ІП впливу. При чому, респонденти здатні за зазначений час визначити лише наявність сугестивного ІП впливу на підсвідомість в ТІР, в той час, як за допомогою програмного засобу, що

реалізує розроблені в дисертаційній роботі методи, мається можливість визначити ще й тип спрямованості такого ІП впливу.

3. Проведені практичні дослідження ймовірності виявлення суггестивних інформаційно-психологічних впливів на підсідомість особистості в ТІР. На основі аналіза результатів досліджень отримані наступні висновки:

– ефективність виявлення сугестивних ІП впливів на підсвідомість людини в ТІР складає від 98 до 100 %;

– розроблені в дисертаційної роботі технологія та методи виявили від 10 до 17 % більше ТІР з ІП впливои на підсвідомість особистості в порівнянні з відомими методами аналізу на основі ключових слів.

Результати дисертаційної роботи доцільно використати:

- у системах автоматичного виявлення сугестивних ІП впливів на підсвідомість підлітків в процесі моніторингу інфокомунікаційного простору та Інтернет ресурсів для детектування прихованих інформаційних деструкцій в інформаційних ресурсах;

- в експертних системах підтримки та прийняття рішень на автоматизованому робочому місці експертів з інформаційної безпеки та психологів для попередження, виявлення та корегування сугестивних ІП впливів на підлітків;

- в інформаційних технологіях забезпечення ІП безпеки особистості, соціуму та держави;

- в процесі вивчення дисциплін з теорії інформаційних війн, інформаційної безпеки в інфокомунікаційних системах, сучасних інформаційних технологій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Алімпієв А.М., Бараннік В.В., Белікова Т.В., Сідченко С.О. Теоретичні основи створення технологій протидії прихованим інформаційним атакам в сучасній гібридній війні. *Системи обробки інформації*. Харьков: ХНУПС. 2017. № 4(150). С. 113 – 121.

2. Анин Б. Защита компьютерной информации. СПб.: БХВ-Петербург. 2000. 384 с.

3. Аудиовизуальные системы связи и вещания: новые технологии третьего тысячелетия, задачи и проблемы внедрения в Украине / О. В. Гофайзен, А. И. Лях-ов и др. *Труды Украинского научно-исследовательского института радио и телевидения.* Одесса, 2000. № 3. С. 3 – 40.

4. Баранник В. В., Стасев Ю. В., Корольова Н. А. Структурно-комбинаторное представление данных в автоматизированных система управления: монография / под ред. В. В. Баранника; Харьков. ун-т. Возд. Сил. Харьков, 2009. 252 с.

5. Баранник В.В., Власов А.В. Модель загроз безпеки відеоінформаційного ресурсу систем відеоконференцзв'язку. *Наукоємні технології*. 2014. № 3 (19). С. 299 – 304.

6. Баранник В.В., Власов А.В. Обоснование значимых (актуальных) угроз безопасности видеоинформационного ресурса систем видеоконференцсвязи профильных систем управления. *Информационно – управляющие системы на железнодорожном транспорте*. 2014. № 3. С. 23 – 27.

7. Баранник В.В., Рябуха Ю.Н. Концептуальный метод повышения безопасности дистанционного видеоинформационного ресурса в системе аэромониторинга кризисных ситуаций на основе интеллектуальной обработки видеокадров. *Радиоэлектронные компьютерные системы*. 2015. № 3. С. 82 – 89.

8. Баранник В.В., Беликова Т.В., Довбенко О.В. Методи виявлення прихованих ої інформаційно-психологічних дій в інформаційному просторі. *Наукоємні*

технології. 2018. №3. С. 24 – 30.

9. Бараннік В.В., Белікова Т.В., Капко М.О., Гуржій І.А. Комплексний метод Автоматичного фоносемантичного аналізу текстової інформації на основі оцінки вагомих семантичних одиниць в умовах інформаційного протиборства. *Кібербезпека. освіта, наука, техніка*. 2019. №1(1). С. 13 – 22.

10. Баранник В.В., Сапрыкина Т.В., Сидченко С.А. Методология построения стойких к несанкционированной дешифровки изображений на базе систем компактного представления. *Проблеми інформатики та моделювання*: матеріали 15 Міжн. наук.-практ. конф. (Харків - Одеса, 14 - 18 вересня 2015 р.). Харків-Одеса, НТУ «ХПІ», 2015. С. 56.

11. Бараннік В.В., Белікова Т.В., Тупиця І.М. Кластеризація даних вхідного сигналу для підвищення захисту інформаційного ресурсу. *Захист інформації і безпека інформаційних систем*: матеріали V Міжн. наук.-практ. конф., (Львів, 2 - 03 червня 2016 р.). Львів: нац. ун-т "Львівська політехніка", 2016. С. 23 – 25.

12. Баранник В.В., Беликова Т.В. Метод анализа информационных ресурсов с выевлением семантики контента. *Актуальні питання забезпечення кібернетичної безпеки та захисту інформації*: матеріали III Міжн. наук.-практ. конф., (Закарпатська область Міжгірський район село Верхнє Студене, 22-25 лютого 2017 р.). Навчально-науковий інститут права та безпеки підприємництва Європейського університету, 2017. С. 28 – 31.

13. Баранник В.В., Беликова Т.В., Подлесный С.А., Хаханова А.В. Способ повышения целостности и доступности видеоконтента в условиях проведения кибернетических атак. *АВІА-2017*: матеріали XIII Міжн. наук.-техн. конф., (Київ, 19-21 квітня, 2017 р). Київ: НАУ, 2017. С. 40 – 43.

14. Баранник В. В., Белікова Т. В., Довбенко О. В., Сідченко С. О. Виявлення прихованих інформаційних впливів в інформаційно-комунікаційному просторі. *Проблеми кібербезпеки інформаційно-комунікаційних систем (PCSITS)*: матеріали I наук.-практ. конф., (Київ 5–6 квітня. 2018 р.). Київ: нац. ун-т імені Тараса Шевченка, 2018. С. 223 – 226.

15. Бараннік В.В., Белікова Т.В., Довбенко О.В. Методи виявлення прихо-

ваних інформаційно-психологічних дій в інформаційному просторі. *Перспективні напрямки захисту інформації*: матеріали IV Наук. практ. конф., (Одеса, 2 - 6 вересня 2018 р.). Одесса: ОНАЗ, 2018. С. 10 – 11.

16. Бараннік В.В., Белікова Т.В., Довбенко О.В., Сідченко С.О., Слободянюк О.В. Методика автоматизованого виявлення прихованих інформаційно-психологічних впливів. *Фізико-технологічні проблеми передавання, оброблення та зберігання інформації в інфокомунікаційних системах*: матеріали VII Міжн. наук.-практ. конф., (Чернівці, 8 - 10 листопада 2018 р.). Чернівці: Чернівецький нац. ун-т імені Юрія Федьковича, 2018. С. 20 – 21.

17. Бєлікова Т.В., Баранник В.В. Методика автоматичного підвищення суггестивної спрямованості семантичної складової тексту. *Фізико-технологічні проблеми передавання, оброблення та зберігання інформації в інфокомунікаційних системах*: матеріали V Міжн. наук.-практ. конф., (Чернівці, 3-5 листопада 2016 р.). Чернівці: Чернівецький нац. ун-т імені Юрія Федьковича, 2016. С. 45 – 48.

18. Беликова Т.В., Баранник В.В. Методы выявления суггестивных воздействий на подсознание человека в текстовых сообщениях в условиях информационно-психологического противоборства. Наукоемкие технологии в инфокоммуникациях: обработка информации, кибербезопасность, информационная борьба: коллективная монография / под редакцией В.М.Безрука. – Х.: ТОВ Вид. «Лідер», 2017. – С. 435 – 455.

19. Беликова Т.В. Методы выявления деструктивных суггестивных информационно-психологических операций в информационно-социальном пространстве. *Радиоэлектроника и информатика*. 2017. №2. С. 45 – 50.

20. Бєлікова Т.В., Баранник В.В. Методика автоматичного підвищення суггестивної спрямованості семантичної складової тексту. *Фізико-технологічні проблеми передавання, оброблення та зберігання інформації в інфокомунікаційних системах*: матеріали V Міжн. наук.-практ. конф., (Чернівці, 3-5 листопада 2016 р.). Чернівці: Чернівецький нац. ун-т імені Юрія Федьковича, 2016. С. 45 – 48.

21. Беликова Т.В. Методы противодействия скрытной информационно-психологическим атакам на социум в инфокомуникационном пространстве. *Об-*

робка сигналів і негаусівських процесів», присвяченій пам'яті професора Кунченка Ю.П.: матеріали VI Міжн. наук.-практ. конф., (Черкаси, 24 - 26 травня 2017 р.). Черкаси: ЧДТУ, 2017. С. 23 – 24.

22. Бєлов Є. Б., Лось В. П., Мещеряков Р. В., Шелупанов О. О. Основы информационной безопасности : учебное пособие для вузов. М. : Горячая линия – Телеком. 2006. 544 с.

23. Біла книга-2018. Збройні Сили України. К.: Військо України, 2019. 172 с.

24. Бобров А. Информационная война: от листовки до твиттера. *Зарубежное военное обозрение*. 2013. №1. С. 20 – 27.

25. Богданович В. Ю. Моделювання стратегії, орієнтованої на зміну режиму у вибраній країні-мішені через її занурення в хаос, на основі методу функціонально значимих проміжних станів. *Сучасний захист інформації*. 2015. № 2. С. 44 – 53.

26. Богданович В. Ю., Романченко І. С., Свида І. Ю. Теоретичні основи забезпечення національної безпеки України в умовах позаблоковості : монографія. Львів: АСВ. 2011. 414 с.

27. Богуш В.М., Юдин О.К. Інформаційна безпека держави. К.: МК-Прес. 2005. 432 с.

28. Буров Є., Пасічник В. Комп'ютерні мережі: підручник / ред. Пасічник В. 2-ге вид., оновл. і доп. Львів: Бак, 2003. 584 с.

29. Бурячок В.Л., Корченко О.Г., Хорошко В.О. Стратегія оцінювання рівня захищеності держави від ризику стороннього кібернетичного впливу. *Захист інформації*. 2013. Том 15, №1. С. 5 – 14.

30. Бурячок В.Л., Гулак Г.М., Хорошко В.О. Завдання, форми та способи ведення воєн у кібернетичному просторі. *Наука і оборона*. 2011. № 3. С. 35 – 42.

31. Бурячок В.Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби : підручник. К.: ДУТ. 2015.

32. Бурячок В.Л. Метод визначення найбільш значимих загроз із «генеральної сукупності загроз інформаційним ресурсам на підставі їх якісних і кількісних показ-

ників». *Сучасний захист інформації*. К.: ДУТ. 2015. № 3. С. 18 – 70.

33. Бурячок В.Л. Метод побудови класифікатора кібератак на державні інформаційні ресурси. *Технологический аудит и резервы производства*. 2015. №1/2(21). С. 38 – 43.

34. ВикипедиЯ: Манипуляция массовым сознанием [Электронный ресурс]. Режим доступа: http://ru.wikipedia.org/wiki/Манипуляция_массовым_сознанием.

35. Вентцель Е. С. Теория вероятностей и ее инженерные приложения: учебн. пособ. Москва, 1988. 480 с.

36. Галицкий А.В. Защита информации в сети – анализ технологий и синтез решений. М.: ДМК Пресс. 2005. 616 с.

37. Герасимов Б.М., Сергеев О.Ю., Субач И.Ю. Извлечение информационных фраз из первичных электронных документов в информационно–поисковых системах. *Управляющие системы и машины*. 2006. №1. С. 26 – 29.

38. Горбулін В. П. "Гібридна війна" як ключовий інструмент російської геостратегії реваншу. *Стратегічні пріоритети*. 2014. № 4(33). С. 5 – 12.

39. Горбулін В. П., Биченок М. М., Копка П. М. Актуальні проблеми системного забезпечення інформаційної безпеки України. *Форми та методи забезпечення інформаційної безпеки держави*: матеріали міжнар. наук.-практ. конф. – К.: Національна академія СБ України, 2008.– С. 79 – 85.

40. Гриняев С. Н. Интеллектуальное противодействие информационному оружию. М.: СИНТЕГ. 1999. 232 с.

41. Давыдов Д. Развитие сил информационных операций США до 2020 года. *Зарубежное военное обозрение*. 2014. №4. С. 3 – 10.

42. Деркаченко Я. Інформаційно-психологічні операції як сучасний інструмент геополітики. *Глобальна організація союзницького лідерства*. 2016 [Електронний ресурс]. Режим доступу : http://goal-int.org/informacijno-psixologichni-operacii-yak-suchasnij-instrument-geopolitiki/.

43. Журавлев А.П. Фонетическое значение. Л.: ЛГУ. 1974.

44. Журавлев А.П. Звук и смысл. М. 1981.

45. Ільяшов О.А., Бурячок В.Л. До питання захисту інформаційно-

телекомунікаційної сфери від стороннього кібернетичного впливу. *Наука и оборона*. 2010. №4. С.35 – 41.

46. Комов С. А. Информационная борьба в современной войне: вопросы теории. *Военная мысль*. 1996. № 3. С. 77 – 80.

47. Дудихин В.В., Дудихина О.В. Конкурентная разведка в Интернет. М.: ООО «Издательство АСТ»: Издательство «НТ Пресс». 2004. 229 с.

48. Клименко С. Теория и практика ведения “гибридных войн”. *Зарубежное военное обозрение*. 2015. № 5. С. 109 – 112.

49. Конституція України. Тлумачення від 15.05.2014 [Электронный ресурс]. Режим доступа: http://zakon2.rada.gov.ua/laws/show/254%D0%BA/96–%D0%B2%D1%80.

50. Концепція національної безпеки України: Постанова Верховної Ради України від 16 січня 1997 № 3/97-ВР. 1997. №10. С.85.

51. Концепция реформирования и развития Вооруженных Сил Украины на период до 2017 года. Рішення Ради національної безпеки і оборони України від 29 грудня 2012 року.

52. Кривуца В. Г., Беркман Л. Н., Толюпа С. В. Інфокомунікаційні мережі нового покоління: монографія / под ред. В. Г. Кривуца. Держ. ун-т. інформ. комунікац. технол. Київ: ДУІКТ, 2012. 286 с.

53. Крук Б.И., Попантонопуло В.Н., Шувалов В.П. Телекоммуникационные системы и сети. Том 1, 2, 3. М.: Горячая линия-Телеком, 2003. 647 с.

54. Лидовский В. В. Теория информации. Москва: Компания Спутник+, 2004. 111 с.

55. Литвиненко О.В. Спеціальні інформаційні операції та пропагандистські кампанії : монографія. К. : ВКФ “Сатсанга”. 2000. 222 с.

56. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції : навчальний посібник. К. : КНТ. 2006. 206 с. (Серія: Національна і міжнародна безпека).

57. Манойло А. В., Петренко А. І., Фролов Д. Б. Государственная информационная политика в условиях информационно–психологической войны.

М. : Горячая линия – Телеком. 2003. 541 с.

58. Марущак А.І. Щодо поняття "інформаційні ресурси держави". *Інформаційна безпека людини, суспільства, держави*. 2009. №1 (1). С. 11 – 15.

59. Международный стандарт ISO/IEC 15408-1-99 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель».

60. Миронець І.В., Рудницький В.М., Бабенко В.Г. Методологія підвищення оперативності доступу до конфіденційних інформаційних ресурсів. *Системи обробки інформації*. Харків: ХУПС. 2010. Вип. 5(86). С. 15 – 19.

61. Мороз Ю., Твердохліб Ю. Інформаційно-психологічні операції в умовах гібридної війни. *Вісник Львівського університету*. 2016. Вип. 38. С. 97 – 105.

62.Оксіюк О.Г. Модель оптимізації семантичної мережі. *Системи управління, навігації та зв'язку*. 2015. № 1(33). С. 143 – 145.

63.Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов. 3-е изд. Санкт-Петербург: Питер, 2006. 958 с.

64. Пєвцов Г.В., Залкін С.В., Сідченко С.О., Хударковський К.І. Інформаційна безпека у воєнній сфері: проблеми, методологія, система забезпечення: монографія. Харків : Цифрова друкарня № 1. 2013. 272 с.

65. Пєвцов Г.В., Гордієнко А.М., Залкін С.В., Сідченко С.О., Феклістов А.О., Хударковський К.І. Інформаційно-психологічна боротьба у воєнній сфері : монографія. Х. : Вид. Рожко С.Г. 2017. 276 с.

66. Почепцов Г. Г. Информационно–психологическая война. М. : СИНТЕГ. 2000. 180 с.

67. Почепцов Г. Г., Чукут С. А. Інформаційна політика : навч. посіб. К. : Знання. 2006. 663 с. (Вища освіта XXI століття).

68. Про інформацію: Закон України від 02.10.1995 №2658-XII-ВР. 1992. №48. С. 651.

69. Про Концепцію Національної програми інформатизації: Закон України від 04.02.1998 №75/98-ВР. 1998. №27-28. С. 182.

70. Программы анализа и лингвистической обработки текстов [Электрон-

ный ресурс]. Режим доступа: http://www.rvb.ru/soft/catalogue/index.html.

71. Психолингвистическая экспертная система Ваал [Электронный ресурс]. Режим доступа: http://www.vaal.ru.

72. Психолингвистическая экспертная система ВААЛ–2000. Руководство пользователя. 71 с.

73. Рекомендации по стандартизации «Информационные технологии. Основные термины и определения в области технической защиты информации» (Р 50.1.053-2005).

74. Расторгуев С. П. Информационная война. М. : Радио и связь, 1999. С. 221.

75. Руснак І. С., Телелим В. М. Розвиток форм і способів ведення інформаційної боротьби на сучасному етапі. *Наука і оборона*. 2000. № 2. С. 18 – 23.

76. Руснак І. С., Попов М. О., Лук'янець А. Г. До забезпечення воєнної безпеки в умовах загрози інформаційної війни. *Наука і оборона*. 1999. № 2. С. 37 – 43.

77. Рябуха Ю.Н. Метод идентификации степени информативности семантического содержания сегмента видеокадра. *Системи управління, навігації та зв'язку*. 2015. № 1(33). С. 52 – 56.

78. Рябуха Ю.Н., Баранник В.В., Бекиров А.Е., Комолов Д.И. Пути повышения информационной безопасности ресурсов в системах специального назначения. *Інформаційні технології та комп'ютерна інженерія*: четверта міжнародна науково-практична конференція, (Вінниця, 28 - 30 травня 2014 р.). Вінниця: Вінницький національний технічний університет. 2014. С. 151.

79. Рыбаков Ф.И., Руднев Е.А., Петухов В.А. Автоматическое индексирование на естественном языке. М.: Энергия. 1980. 160 с.

80. Сайт ресурсу новин 112 [Електронний ресурс]. Режим доступу : 112.ua.

81. Сайт телеканалу 1+1 [Електронний ресурс]. Режим доступу : 1plus1.ua.

82. Сайт телеканалу 5 [Електронний ресурс]. Режим доступу : www.medialogia.ru.

83. Сайт BINTEL.COM.UA. Незалежний аналітичний центр геополітичних

досліджень “Борисфен Інтел”. [Електронний ресурс]. Режим доступу : http://bintel.com.ua/uk/article/gibrid-war/.

84. Сайт RBC.UA "РБК-Україна" [Електронний ресурс]. Режим доступу : www.rbc.ua.

85. Сапрыкина Т.В., Сидченко С.А., Школяренко В.А. Информационная технология тестирования семантической составляющей для выявления суггестивного воздействия методом фонетического анализа накопительным итогом. *Автоматизированные системы управления и приборы автоматики*. 2013. № 165. С. 111 – 117.

86. Сапрыкина Т.В., Сидченко С.А., Школяренко В.А. Метод составления текста с заданной суггестивной направленностью контекста. *Системи обробки інформації*. Х.: ХУПС. 2014. № 4(120). С. 96 – 101.

87. Сапрыкина Т.В., Школяренко В.А. Информационная технология выявления суггестивных воздействий на подсознание человека. *Інформаційні технології: наука, техніка, технологія, освіта, здоров’я* (МикроКАД): матеріали XXII Міжн. наук.-практ. конф., тези доп., (Харків, 21-23 травня 2014 р.). Харків, НТУ «ХПІ»., 2014. С. 71.

88. Сидченко С.А., Хударковский К.И., Петров В.Л. Система анализа воздействия информации на подсознание человека в условиях информационно–психологического противоборства. *Теорія та методика навчання математики, фізики, інформатики*: збірник наукових праць. Кривий Ріг: Видавничий відділ НМетАУ, 2005. Т.3: Теорія та методика навчання інформатики. С. 303 – 314.

89. Сідченко С.О., Залкін С.В., В.В. Бєлімов Методика комплексного аналізу документу. *Системи обробки інформації*. 2007. Вип. 9 (67). С. 109 – 113.

90. Система автоматического анализа текста TextAnalyst [Электронный ресурс]. Режим доступа: www.analyst.ru.

91. Скороходько Е.Ф. Лінгвістичні основи автоматизації інформаційного пошуку. К.: Вища школа, 1970. 242 с.

92. Стасев Ю.В., Баранник В.В., Смірнов О.А. Захист інформації в автоматизованих системах управління / навч. посібник. Х.: ХУПС. 2015. 264 с.

93. Семко В. В., Бурячок В. Л., Толюпа С. В., Складанний П. М. Модель управління захистом інформації в інформаційно-телекомунікаційній системі. *Радіоелектроніка та телекомунікації:* 2015. С. 151 – 155.

94. Стрихалюк Б. М., Демидов І. В., Романчук В. І., Бешлей М. І. Дослідження статистичних параметрів та характеристик інформаційних потоків в гетерогенних мережах. *Наукові записки УНДІЗ*. 2014. №6(34). С. 82 – 92.

95. Сэлтон Г.А. Автоматическая обработка, хранение и поиск информации. М.: Сов. радио. 1973. 560 с.

96. Толубко В. Б. Інформаційна боротьба (концептуальні, теоретичні, технологічні аспекти) : монографія. К. : НАОУ. 2003. 315 с.

97. Толубко В.Б., Жук С.Я., Косевцов В.О. Концептуальні основи інформаційної безпеки України. *Наука і оборона*. 2004. № 2. С. 19 – 25.

98. Фролов В.С. Структурно логічна схема Єдиної автоматизованої системи управління Збройних Сил України. *Наука и оборона*. 2012. №1. С.15 – 24.

99. Цивільний кодекс України. *Офіційний вісник України.* 2003. № 11.ч. 3, ст. 307.

100. Шостак І. В., Сілін С. О. Підхід до створення віртуальної мережі між IoT-пристроями, що поєднані трансляцією мережевих адресів. *Системи управління, навігації та зв'язку*. 2017. Вип. 3(43). С. 114 – 116.

101. Указ Президента України №47/2017 Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України».

102. Улічев О. С., Мелешко Є. В. Програмне моделювання поширення інформаційно-психологічних впливів у віртуальних соціальних мережах. *Сучасні інформаційні системи*. 2018. Т. 2. № 2. С. 35 –39.

103. Юдін О.К. Інформаційна безпека. Нормативно-правове забезпечення: підручник. – К. : НАУ, 2011. – 640с.

104. Юдін О.К., Бучик С.С. Концептуальний аналіз уразливості державних інформаційних ресурсів. *Наукоємні технології*. 2013. № 3 (19). С. 299 – 304.

105. Air Force Doctrine Documents 2-5 "Information Operations". Air Force

Doctrine Center. 2005. 61 p. Available at: apps.dtic.mil/dtic/tr/fulltext/u2/b311353.pdf (accessed 11 January 2005).

106. Angerman, W.S. Coming full circle with Boyd`s OODA loop ideas: an analysis of innovation diffusion and evolution. Air Force Institute of Technology. 2004. 141 p. Available at: apps.dtic.mil/dtic/tr/fulltext/u2/a425228.pdf.

107. Barannik V., Belikova T., Podlesny S., Suprun O. The Alignment Method of Code Structures for Enhancing the Information's Reliability in the Infocommunication Networks. *The Experience of Designing and Application of CAD Systems in Microelectronics CADSM'2017*: The 14th International Conference, (Polyana-Svalyava (Zakarpattya), Ukraine, 21-25 February 2017). 2017. P. 29 – 31.

108. Barannik V., Belikova T, Komolov D., Krivonos V., Tarnopolov R. Estimate of the capacity of the closed video channel for the method based on the selection of relevant structural units. *International Symposium «IEEE East-West Design & Test*», (Batumi, 2016). Batumi: 2016. P. 325 – 328.

109. Belikova T.V. The Technology Of Suggestive Information-Psychological Operations Masking In The Infocommunication Space. *Science-Based Technologies.* 2017. № 3. P. 21 – 26.

110. Belikova T., Barannik V., Karpinskyi V. Development of technology analys for the content semantics, *Engineer of XXI Century - We Design the Future,* Bielsko-Biała, Poland: ATH, 2016. P.65 – 72.

111. Belikova T., Dovbenko O., Lekakh A., Dodukh O. Method of Increasing the Capacity of Information Threat Detection Filters in Modern Information and Communication Systems *Advanced Information and Communication Technologies, AICT 2019*: 3nd IEEE International Conference, Proceedings, (Lviv 2019). Lviv, 2019. P. 188 - 192.

112. Brehmer, B. (2005), "The dynamic OODA loop: Amalgamating Boyd's OODA loop and cybernetic approaches to command and control", 10th International Command and Control Research and Technology Symposium, 15 p., available at: www.dodccrp.org/events/10th_ICCRTS/CD/papers/365.pdf (accessed 17-21 June 2005).

113. Expending Joint Vision 2010 “Concept for Future Joint Operations Expending Joint Vision 2010”. Ft.Monroe: Office of Primary Responsibility. 1997. 96 p. Available at: www.iwar.org.uk/rma/resources/jv2010/concepts-jv-2010.pdf (accessed May 1997).

114. Field Manual (FM) 100-6 “Information Operations”. Washington, DC: Headquarters, Department of the Army. 1996. 162 p. Available at: www.bits.de/NRANEU/others/amd-us-archive/fm100-6%2896%29.pdf (accessed 27 August, 1996).

115. Field Manual (FM) 3-0 “Operations”. Washington, DC: Headquarters, Department of the Army. 2017. 366 p. Available at: fas.org/irp/doddir/army/fm3-0.pdf (accessed October 2017).

116. Field Manual (FM) 3-13 (FM 100-6) “Information Operations: Doctrine, Tactics, Techniques, and Procedures”. Washington, DC: Headquarters, Department of the Army. 2003. 314 p. Available at: www.iwar.org.uk/iwar/resources/doctrine/fm-3-13.pdf (accessed 28 November 2003).

117. Joint Publication 3-13 “Information Operations”. Joint Chiefs of Staff. 2014. 87 p. Available at: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf. (accessed 27 November 2012 incorporating Change 20 November 2014).

118. Joint Publication 3-13.1 “Electronic Warfare”. Joint Chiefs of Staff, Berlin Information-center for Transatlantic Security. 2012. 144 p. Available at: http://www.bits.de/NRANEU/others/jp-doctrine/JP3_13.1(12).pdf (accessed 8 February 2012).

119. Joint Publication 3-13.2 “Military Information Support Operations”. Joint Chiefs of Staff, Berlin Information-center for Transatlantic Security. 2011. 108 p. Available at: http://www.bits.de/NRANEU/others/jp-doctrine/JP3-13.2C1(11).pdf (accessed 7 January 2010 incorporating change 20 December 2011).

120. Joint Publication 3-13.3 “Operational Security”. Joint Chiefs of Staff, Berlin Information-center for Transatlantic Security. 2012. 75 p. Available at: http://www.bits.de/NRANEU/others/jp-doctrine/JP3-13-3(12).pdf (accessed 4 January 2012).

121. Joint Publication 3-13.4 “Military Deception”. Joint Chiefs of Staff, Berlin Information-center for Transatlantic Security. 2012. 81 p. Available at: http://www.bits.de/NRANEU/others/jp-doctrine/jp3_13_4(12).pdf (accessed 26 January 2012).

122. Lazarsfeld, Paul & Merton, Robert. Mass Communication, Popular Taste and Organized Social Action. New York. 2004.

123. MATLAB 6.0. Финансовые, инженерные и научные расчеты в среде Windows. Москва: Информ.-изд. дом «Филинъ». 1997. 712 с.

124. Perrin, Chad. The CIA Triad and Engineering Principles for Information Technology Security. Retrieved 31 May 2012.

125. Saprykina T.V., Sidchenko S.A. Method of complex information and psycho-logical document analysis. *Science-Based Technologies*. 2014. № 1(21). P. 79 – 83.

126. Saprykina T., Komolov Dm., Vlasov A., Sidchenko S. Assessment of Video Information Resource Security of Videoconferencing in Public Administration. *International Symposium «IEEE East-West Design & Test»*, (Kiev, Ukraine, September 26–29, 2014). Kiev: 2014. P. 329-331.

127. Strategy for Operations in the Information Environment. U.S. Department of Defense. 2016. 20 p. Available at: https://dod.defense.gov/Portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf (accessed 13 June 2016).

128. Strykhalyuk B., Kahalo I., Brych M., Beshley M., Seliuchenko M. Implementation of wireless heterogeneous network based on LTE core virtualization for military communication systems. *Systems of Arms and Military Equipment*. 2014. No. 4. P. 125-132.

129. Shostak I., Komolov D. The security and reliability improving of video information in departmental structures infocommunication systems. *Radioelectronics & Informatics*. 2016. No. 163. P. 32-35.

Додаток А

Список публікацій здобувача за темою дисертації та відомості про апробацію результатів дисертації

Список публікацій, в яких опубліковані основні наукові результати дисертації:

1. Беликова Т.В., Баранник В.В. Методы выявления суггестивных воздействий на подсознание человека в текстовых сообщениях в условиях информационно-психологического противоборства. Наукоемкие технологии в инфокоммуникациях: обработка информации, кибербезопасность, информационная борьба: коллективная монография / под редакцией В.М.Безрука. – Х.: ТОВ Вид. «Лідер», 2017. – С. 435 – 455.

2. Сапрыкина Т.В., Сидченко С.А., Школяренко В.А. Информационная технология тестирования семантической составляющей для выявления суггестивного воздействия методом фонетического анализа накопительным итогом. *Автоматизированные системы управления и приборы автоматики*. 2013. № 165. С. 111 – 117.

3. Saprykina T.V., Sidchenko S.A. Method of complex information and psychological document analysis. *Science-Based Technologies*. 2014. № 1(21). P. 79 – 83.

4. Сапрыкина Т.В., Сидченко С.А., Школяренко В.А. Метод составления текста с заданной суггестивной направленностью контекста. *Системи обробки інформації*. Х.: ХУПС. 2014. № 4(120). С. 96 – 101.

5. Беликова Т.В. Методы выявления деструктивных суггестивных информационно-психологических операций в информационно-социальном пространстве. *Радиоэлектроника и информатика*. 2017. №2. С. 45 – 50.

6. Belikova T.V. The Technology Of Suggestive Information-Psychological Operations Masking In The Infocommunication Space. *Science-Based Technologies*. 2017. № 3. P. 21 – 26.

7. Алімпієв А.М., Бараннік В.В., Белікова Т.В., Сідченко С.О. Теоретичні основи створення технологій протидії прихованим інформаційним атакам в сучасній гібридній війні. *Системи обробки інформації*. Харьков: ХНУПС. 2017. № 4(150). С. 113 – 121.

8. Баранник В.В., Беликова Т.В., Довбенко О.В. Методи виявлення прихованих ої інформаційно-психологічних дій в інформаційному просторі. *Наукоємні технології*. 2018. №3. С. 24 – 30.

9. Бараннік В.В., Белікова Т.В., Капко М.О., Гуржій І.А. Комплексний метод автоматичного фоносемантичного аналізу текстової інформації на основі оцінки вагомих семантичних одиниць в умовах інформаційного протиборства. *Кібербезпека. освіта, наука, техніка*. 2019. №1(1). С. 13 – 22.

Список публікацій, які засвідчують апробацію матеріалів дисертації:

1. Сапрыкина Т.В., Школяренко В.А. Информационная технология выявления суггестивных воздействий на подсознание человека. *Інформаційні технології: наука, техніка, технологія, освіта, здоров'я* (МикроКАД): матеріали XXII Міжн. наук.-практ. конф., тези доп., (Харків, 21-23 травня 2014 р.). Харків, НТУ «ХПІ»., 2014. С. 71.

2. Saprykina T., Komolov Dm., Vlasov A., Sidchenko S. Assessment of Video Information Resource Security of Videoconferencing in Public Administration. *International Symposium «IEEE East-West Design & Test»*, (Kiev, Ukraine, September 26–29, 2014). Kiev: 2014. P. 329 – 331.

3. Баранник В.В., Сидченко С.А., Сапрыкина Т.В. Методология построения стойких к несанкционированной дешифровки изображений на базе систем компактного представления. *Проблеми інформатики та моделювання*: матеріали 15 Міжн. наук.-практ. конф. (Харків - Одеса, 14 - 18 вересня 2015 р.). Харків-Одеса, НТУ «ХПІ», 2015. С. 56.

4. Бараннік В.В., Белікова Т.В., Тупиця І.М. Кластеризація даних вхідного сигналу для підвищення захисту інформаційного ресурсу. *Захист інформації і безпека інформаційних систем*: матеріали V Міжн. наук.-практ. конф., (Львів, 2 - 03 червня 2016 р.). Львів: нац. ун-т "Львівська політехніка", 2016. С. 23 – 25.

5. Barannik V., Belikova T, Komolov D., Krivonos V., Tarnopolov R. Estimate of the capacity of the closed video channel for the method based on the selection of

relevant structural units. *International Symposium «IEEE East-West Design & Test»*, (Batumi, 2016). Batumi: 2016. P. 325 – 328.

6. Бєлікова Т.В., Баранник В.В. Методика автоматичного підвищення суггестивної спрямованості семантичної складової тексту. *Фізико-технологічні проблеми передавання, оброблення та зберігання інформації в інфокомунікаційних системах*: матеріали V Міжн. наук.-практ. конф., (Чернівці, 3-5 листопада 2016 р.). Чернівці: Чернівецький нац. ун-т імені Юрія Федьковича, 2016. С. 45 – 48.

7. Belikova T., Barannik V., Karpinskyi V. Development of technology analys for the content semantics, *Engineer of XXI Century - We Design the Future*, Bielsko-Biała, Poland: ATH, 2016. P.65 – 72.

8. Barannik V., Belikova T., Podlesny S., Suprun O. The Alignment Method of Code Structures for Enhancing the Information's Reliability in the Infocommunication Networks. *The Experience of Designing and Application of CAD Systems in Microelectronics CADSM'2017*: The 14th International Conference, (Polyana-Svalyava (Zakarpattya), Ukraine, 21-25 February 2017). 2017. P. 29 – 31.

9. Баранник В.В., Беликова Т.В Метод анализа информационных ресурсов с выевлением семантики контента. *Актуальні питання забезпечення кібернетичної безпеки та захисту інформації*: матеріали III Міжн. наук.-практ. конф., (Закарпатська область Міжгірський район село Верхнє Студене, 22-25 лютого 2017 р.). Навчально-науковий інститут права та безпеки підприємництва Європейського університету, 2017. С. 28 – 31.

10. Беликова Т.В. Методы противодействия скрытной информационно-психологическим атакам на социум в инфокомуникационном пространстве. *Обробка сигналів і негаусівських процесів», присвяченій пам'яті професора Кунченка Ю.П.*: матеріали VI Міжн. наук.-практ. конф., (Черкаси, 24 - 26 травня 2017 р.). Черкаси: ЧДТУ, 2017. С. 23-24.

11. Баранник В.В., Беликова Т.В., Подлесный С.А., Хаханова А.В. Способ повышения целостности и доступности видеоконтента в условиях проведения кибернетических атак. *ABIA-2017*: матеріали XIII Міжн. наук.-техн. конф., (Київ, 19 - 21 квітня, 2017 р). Київ: НАУ, 2017. С. 40 – 43.

12. Баранник В. В., Белікова Т. В., Довбенко О. В., Сідченко С. О. Виявлення прихованих інформаційних впливів в інформаційно-комунікаційному просторі. *Проблеми кібербезпеки інформаційно-комунікаційних систем (PCSITS)*: матеріали І наук.-практ. конф., (Київ 5–6 квітня. 2018 р.). Київ: нац. ун-т імені Тараса Шевченка, 2018. С. 223 - 226.

13. Бараннік В.В., Белікова Т.В., Довбенко О.В. Методи виявлення прихованих інформаційно-психологічних дій в інформаційному просторі. *Перспективні напрямки захисту інформації*: матеріали IV Наук. практ. конф., (Одеса, 2 - 6 вересня 2018 р.). Одесса: ОНАЗ, 2018. С. 10 - 11.

14. Бараннік В.В., Белікова Т.В., Довбенко О.В., Сідченко С.О., Слободянюк О.В. Методика автоматизованого виявлення прихованих інформаційно-психологічних впливів. *Фізико-технологічні проблеми передавання, оброблення та зберігання інформації в інфокомунікаційних системах*: матеріали VII Міжн. наук.-практ. конф., (Чернівці, 8 - 10 листопада 2018 р.). Чернівці: Чернівецький нац. ун-т імені Юрія Федьковича, 2018. С. 20 – 21.

15. Belikova T., Dovbenko O., Lekakh A., Dodukh O. Method of Increasing the Capacity of Information Threat Detection Filters in Modern Information and Communication Systems. *on Advanced Information and Communication Technologies, AICT 2019*: 3nd IEEE International Conference, Proceedings, (Lviv, July 2019). Lviv, 2019. P. 188 - 192.

Апробація результатів дисертації була проведена на:

– XXII Міжнародній науково-практичній конференції, ″Інформаційні технології: наука, техніка, технологія, освіта, здоров’я (МикроКАД)″, (Харків, 21 - 23 травня 2014 р.), участь з доповіддю;

– International Symposium ″IEEE East-West Design & Test″, (Kiev, Ukraine, September 26 - 29, 2014), тези та її доповідь подано дистанційно;

– 15 Міжнародній науково-практичній конференції, ″Проблеми інформатики та моделювання: матеріали″, (Харків - Одеса, 14 - 18 вересня 2015 р.), участь з доповіддю;

– V Міжнародній науково-практичній конференції, ″Захист інформації і безпека інформаційних систем″, (Львів, 2 - 03 червня 2016 р.), участь з доповіддю;

– International Symposium ″IEEE East-West Design & Test″, (Batumi, 2016), тези та її доповідь подано дистанційно;

– V-а Міжнародна науково-практична конференція, "Фізико-технологічні проблеми передавання, оброблення та зберігання інформації в інфокомунікаційних системах", (Чернівці, 3-5 листопада 2016 р.), участь з доповіддю;

– Engineer of XXI Century - We Design the Future, Bielsko-Biała, Poland: ATH, 2016, тези та її доповідь подано дистанційно;

– 14th International Conference, "The Experience of Designing and Application of CAD Systems in Microelectronics CADSM’2017", (21-25 February 2017 Polyana-Svalyava (Zakarpattya), Ukraine), тези та її доповідь подано дистанційно;

– III Міжнародній науково-практичній конференції, "Актуальні питання забезпечення кібернетичної безпеки та захисту інформації", (Закарпатська область Міжгірський район село Верхнє Студене, 22-25 лютого 2017 р), участь з доповіддю;

– VI Міжнародній науково-практичній конференції, «Обробка сигналів і негаусівських процесів», присвяченій пам’яті професора Кунченка Ю.П. ″, (Черкаси, 24 - 26 травня 2017 р.), участь з доповіддю;

– XIII Міжнародній науково-технічній конференції, "АВІА-2017", (Київ, 19-21 квітня, 2017 р.), участь з доповіддю;

– I науково-технічній конференції "Проблеми кібербезпеки інформаційно-комунікаційних систем (PCSITS)", (Київ 5–6 квітня 2018 р.);

– IV Науково-практичній конференції "Перспективні напрямки захисту інформації", (Одеса, 2 - 6 вересня 2018 р.), участь з доповіддю;

– VII Міжнародній науково-практичній конференції "Фізико-технологічні проблеми передавання, оброблення та зберігання інформації в інфокомунікаційних системах", (Чернівці, 8 - 10 листопада 2018 р.), участь з доповіддю;

– 3rd IEEE International Conference, "on Advanced Information and Communication Technologies (AICT 2019)", (Lviv, July, 2019), участь з доповіддю.

Додаток Б

Табличні значення, що використовуються в технології виявлення сугестивного інформаційно-психологічного впливу

Таблиця Б.1

Символічні значення руських звуків у 25 ознакових шкалах

Ознаковий аспект		Звукобуква																						
антонім 1	антонім 2	в	с	а	д’	ж	ь,ъ	ю	р’	ш	г	и,й	п’	р	г’	ё	з	с’	в’	ц	э	м	б’	х’
хороший	поганий	2,9	3,6	1,5	2,8	3,7	2,9	1,8	2,6	4,0	3,2	1,7	3,6	2,9	3,6	2,3	3,1	3,8	3,4	4,0	2,0	2,5	3,0	4,3
великий	маленький	2,1	3,5	1,8	3,9	2,4	3,8	3,1	3,4	3,2	2,6	3,2	4,6	2,1	3,9	2,9	2,9	4,3	3,1	3,7	1,8	2,5	3,1	4,1
ніжний	грубий	3,6	3,2	2,8	2,6	4,0	3,1	1,9	3,2	3,2	3,8	1,8	2,4	4,6	2,6	2,4	3,5	2,0	2,4	3,2	3,4	3,2	2,6	2,5
жіночий	мужній	3,9	3,1	3,7	2,5	3,2	3,2	1,6	2,9	2,8	4,2	1,9	2,2	4,7	2,8	2,2	3,5	2,0	2,6	3,3	3,6	3,5	2,8	2,2
світлий	темний	3,0	2,5	2,2	2,2	3,8	2,6	2,3	2,9	4,3	3,3	2,0	3,3	3,8	2,9	2,5	2,5	2,4	2,8	3,5	2,5	3,3	2,6	3,5
активний	пасивний	2,4	3,2	2,1	2,0	3,0	2,2	3,4	2,1	3,6	2,8	2,9	3,6	2,0	2,9	3,4	2,8	3,5	3,2	3,4	3,6	4,0	3,0	4,4
простий	складний	2,4	3,0	1,4	3,6	4,0	3,9	2,6	3,7	3,1	2,6	1,8	3,5	3,1	3,5	1,8	3,0	3,8	3,7	3,4	2,2	3,1	3,4	3,8
сильний	слабкий	1,9	3,1	2,6	3,2	2,5	3,2	3,8	3,0	3,4	2,2	3,3	4,4	1,3	3,0	2,8	2,2	4,2	3,1	3,8	2,3	3,2	3,5	4,6
гарячий	холодний	2,4	3,3	3,2	2,3	2,3	2,6	2,8	2,7	2,8	3,6	3,2	2,6	4,0	2,4	2,9	3,6	3,1	2,5	3,6	3,6	3,8	2,9	2,4
швидкий	повільний	2,4	3,0	3,4	2,2	3,4	1,8	3,6	2,4	3,1	2,2	3,6	2,4	2,7	2,4	3,7	2,7	3,1	3,0	2,3	3,7	3,7	2,2	3,5
гарний	відштовхуючий	3,0	3,9	2,0	2,7	4,0	2,8	1,6	3,6	3,5	2,8	2,0	3,6	3,0	2,9	2,1	3,2	3,2	3,1	3,1	2,1	3,5	3,6	4,1
гладкий	шорсткий	3,5	3,6	1,6	3,0	4,5	3,4	2,4	4,0	4,1	3,6	2,0	3,5	4,0	3,2	2,5	4,0	3,5	3,0	3,9	2,2	2,8	3,2	3,8
легкий	важкий	3,3	2,4	2,3	2,8	4,0	2,5	2,1	3,3	3,4	3,0	2,0	2,9	4,1	2,9	2,6	3,2	2,1	2,6	3,1	2,7	3,8	2,5	3,1
веселий	сумний	2,5	2,9	2,7	2,1	2,7	2,6	2,5	2,4	3,6	2,9	2,5	3,4	2,6	2,5	2,7	2,4	3,1	2,7	3,7	3,0	3,6	2,1	3,4
безпечний	страшний	3,3	3,2	2,6	2,8	4,3	2,4	2,0	3,4	4,2	3,2	2,1	2,4	4,6	2,3	2,1	3,6	2,8	2,6	3,3	2,2	2,4	2,3	3,8
величний	низинний	1,8	3,6	2,0	3,5	3,6	3,0	2,8	2,8	4,0	2,8	3,0	4,0	1,7	3,8	2,7	2,8	4,2	2,8	3,8	2,1	3,0	3,2	4,5
яскравий	тьмяний	2,7	3,8	2,0	2,2	2,9	2,4	2,5	1,8	4,5	2,5	2,6	4,4	2,1	2,3	2,5	2,5	3,8	2,7	3,6	2,5	3,6	2,3	4,3
округлий	незграбний	2,9	3,1	1,4	3,2	3,4	3,2	2,0	4,0	3,5	4,0	2,2	3,5	4,0	3,6	2,5	3,5	3,0	3,0	3,9	2,0	3,1	3,0	3,2
радісний	сумний	2,3	3,5	1,9	2,3	3,5	2,9	2,5	1,9	3,8	3,0	2,3	4,0	2,7	2,7	2,6	2,5	3,6	2,6	3,5	2,6	3,9	2,8	4,0
гучний	тихий	2,2	3,8	1,9	2,7	2,9	2,7	3,2	2,1	4,7	3,3	3,3	4,8	1,8	2,9	2,5	2,5	4,3	3,0	4,3	2,2	3,1	2,9	4,7
довгий	короткий	3,8	3,7	1,8	4,3	3,0	4,1	2,6	3,5	3,3	3,9	2,5	4,6	2,5	3,9	2,2	2,9	3,6	3,9	4,0	2,2	3,3	3,9	4,0
хоробрий	боягузливий	2,5	4,0	1,8	2,6	1,9	3,2	2,8	2,5	3,3	2,8	2,9	4,1	1,4	3,4	2,4	2,9	4,5	3,6	3,7	2,2	3,3	3,2	4,4
добрий	злий	2,8	3,9	2,0	1,4	4,1	3,3	2,2	3,3	3,4	3,8	2,4	2,2	4,0	3,0	2,2	3,7	3,1	2,7	3,6	2,6	2,7	2,7	3,1
могутній	кволий	1,8	3,5	1,8	3,4	2,3	3,0	3,4	2,5	2,6	2,4	3,9	4,3	1,5	3,3	2,6	2,9	4,3	3,1	3,6	2,6	2,2	3,4	4,5
рухомий	повільний	2,6	3,5	2,9	2,3	3,2	1,9	3,2	2,1	3,5	2,2	3,4	2,5	2,0	2,6	3,3	3,1	3,0	2,7	2,5	3,5	4,1	2,3	3,7

Продовження табл. Б.1

Ознаковий аспект		Звукобуква																						
антонім 1	антонім 2	к	т’	я	н’	п	ф	н	д	л’	ы	ф’	м’	з’	б	у	к’	х	л	т	е	ч	щ	о
хороший	поганий	3,0	3,3	1,8	2,9	3,5	4,0	2,4	2,4	1,8	3,6	4,2	3,1	3,4	2,4	3,0	3,7	4,1	2,1	3,0	1,9	3,0	3,5	1,6
великий	маленький	3,3	4,1	2,1	3,2	3,4	2,8	2,1	2,0	3,7	1,7	4,3	3,7	3,6	2,1	2,2	4,2	3,4	2,2	3,1	2,8	3,9	3,8	1,3
ніжний	грубий	3,6	2,2	2,7	2,0	3,4	3,5	3,6	4,4	2,0	3,8	2,4	2,1	2,4	4,2	3,0	2,4	3,6	3,3	3,6	2,2	3,4	2,7	3,2
жіночий	мужній	3,5	2,4	3,6	2,3	3,6	3,3	4,0	4,5	1,8	3,8	2,2	2,0	2,6	4,3	3,8	2,5	3,6	3,5	3,1	2,9	2,7	2,5	3,7
світлий	темний	3,6	3,6	1,9	2,8	4,0	4,0	3,1	3,2	2,0	3,8	3,7	2,6	2,4	3,2	3,6	3,2	4,1	3,1	4,0	1,9	3,3	3,8	2,2
активний	пасивний	2,8	3,2	2,6	3,2	3,4	4,1	2,8	2,4	2,8	4,0	4,0	3,1	2,8	2,0	3,2	3,0	3,8	2,5	3,2	2,4	3,0	4,0	2,2
простий	складний	3,4	3,7	1,8	3,4	2,8	3,3	2,6	2,6	3,4	3,1	3,9	3,6	3,5	3,0	1,7	3,5	3,1	3,3	3,2	1,9	3,4	4,0	1,2
сильний	слабкий	3,7	4,2	1,7	3,4	4,0	3,6	2,4	1,9	3,4	2,5	4,3	3,5	2,8	2,1	2,8	4,5	3,4	2,2	3,4	2,1	3,8	4,2	1,7
гарячий	холодний	3,4	2,3	3,0	2,3	3,0	3,2	3,4	3,6	2,7	4,0	2,4	2,9	3,0	3,7	3,6	2,2	3,4	3,6	2,8	3,0	1,8	1,8	3,7
швидкий	повільний	2,0	2,5	3,2	3,4	1,9	3,4	3,9	2,4	3,0	4,4	3,7	3,4	3,1	1,9	4,3	1,9	3,7	3,5	2,0	3,8	2,0	3,8	3,6
гарний	відштовхуючий	3,4	2,9	1,9	2,4	3,5	3,9	2,6	2,4	1,9	3,7	3,4	3,3	3,2	2,6	2,9	3,4	3,9	2,3	3,2	1,7	3,0	3,7	1,9
гладкий	шорсткий	4,2	3,8	2,2	2,8	4,0	4,1	2,8	3,4	2,2	2,5	3,8	2,6	3,8	3,2	1,8	3,9	4,2	2,6	3,8	2,4	4,6	4,4	1,5
легкий	важкий	3,0	2,9	2,1	2,6	3,0	3,7	3,6	3,3	2,7	3,5	2,8	3,2	2,9	2,6	2,3	2,6	3,3	3,2	3,2	2,4	3,3	3,4	2,5
веселий	сумний	3,4	3,3	2,5	3,0	3,9	3,8	3,1	2,9	2,1	3,7	3,2	2,7	2,4	2,9	4,0	2,5	3,4	3,0	3,6	2,5	2,9	3,4	2,9
безпечний	страшний	3,8	3,2	2,1	2,2	3,8	4,4	2,8	2,8	1,7	3,5	3,2	2,2	2,9	3,2	3,6	3,0	4,1	2,5	3,4	2,2	3,4	4,3	2,8
величний	низинний	3,3	3,4	2,1	3,2	3,6	3,4	2,3	2,4	3,0	3,1	4,5	3,2	3,4	2,1	3,6	4,0	4,0	2,0	3,2	2,6	3,6	4,4	1,6
яскравий	тьмяний	4,0	3,9	1,6	3,0	4,1	4,4	2,7	2,1	2,3	3,6	4,3	3,2	2,2	2,0	3,7	3,8	4,1	2,4	3,8	3,6	3,3	3,9	1,8
округлий	незграбний	4,4	3,5	2,0	3,0	3,8	3,6	3,1	3,5	2,1	2,9	3,2	2,8	3,3	3,4	2,6	3,8	3,9	3,1	4,1	2,2	3,8	3,6	1,4
радісний	сумний	3,8	3,8	1,8	2,8	3,7	4,3	2,9	2,5	2,1	3,6	4,1	2,8	2,8	2,5	3,8	3,3	4,0	2,5	3,3	2,7	3,2	4,2	2,7
гучний	тихий	3,9	4,4	2,2	2,9	4,5	4,7	2,6	2,3	2,9	2,4	4,4	3,0	2,7	2,0	2,3	4,4	4,2	2,3	4,4	2,9	4,0	4,0	1,4
довгий	короткий	4,4	4,3	3,0	3,8	4,4	3,8	3,3	3,5	3,3	2,2	3,9	4,0	3,4	3,8	1,9	4,4	3,8	3,4	4,4	2,5	4,1	2,7	1,7
хоробрий	боягузливий	3,3	4,0	1,6	3,4	3,7	3,5	2,7	2,0	2,8	2,8	4,2	3,3	3,1	2,1	2,3	3,7	3,4	2,3	3,5	2,2	3,5	4,1	1,8
добрий	злий	3,2	2,7	2,4	2,1	3,3	3,8	3,4	3,1	1,9	2,7	3,2	1,9	3,1	3,3	3,3	3,0	3,5	3,3	3,4	2,7	3,3	3,3	2,7
могутній	кволий	3,8	4,2	2,0	3,6	3,5	3,8	2,4	2,2	3,6	2,5	3,9	3,7	3,4	1,6	2,9	4,0	3,4	2,1	3,3	2,3	3,6	4,0	1,7
рухомий	повільний	2,0	2,7	3,0	3,2	2,7	3,9	3,3	2,2	3,4	3,9	4,0	3,7	3,0	2,0	4,0	8,3	3,7	3,4	2,5	3,3	2,5	3,5	2,7

Таблиця Б.2

Лексикон для автоматичного аналізу фонетичного значення тексту

Ознаковий аспект	Звукобуква																						
	в	с	д	р	г	п	з	м	б	х	к	т	н	ф	л	в’	с’	д’	р’	г’	п’	з’	м’
прекрасний	+0,13	-0,60	+0,60	+0,13	-0,17	-0,50	-0,10	+0,50	+0,56	-1,08	-0,05	+0,04	+0,61	-1,05	+0,90	-0,36	-0,83	+0,22	+0,38	-0,60	-0,63	-0,45	-0,15
світлий	-0,05	+0,70	-0,20	-0,75	-0,30	-0,80	-0,06	-0,20	-0,20	-1,04	-0,54	-1,00	-0,09	-0,90	-0,17	+0,38	+0,95	+0,75	+0,09	+0,08	-0,30	+0,70	+0,40
ніжний	-0,29	+0,58	-0,29	-1,13	-0,04	-0,04	-0,17	-0,75	+0,42	-0,33	+0,00	-0,17	-0,58	-0,71	-0,21	+0,42	+0,92	+0,21	-0,33	+0,12	+0,08	+0,09	-0,21
радісний	+0,69	-0,54	+0,54	+0,31	-0,15	-0,69	+0,54	-0,92	+0,46	-1,00	-0,85	-0,31	+0,08	-1,31	+0,46	+0,46	-0,85	+0,69	+1,07	+0,23	-1,00	+0,15	+0,23
піднесений	+1,15	-0,55	+0,60	+1,30	+0,15	-0,55	+0,15	+0,00	+0,90	-1,00	-0,30	-0,25	+0,70	-0,40	+1,00	+0,15	-1,15	-0,50	+0,25	-0,85	-1,00	-0,35	-0,20
бадьорий	+0,65	-0,15	+0,63	+1,00	+0,20	-0,45	+0,20	-1,00	+1,00	-0,80	+0,20	-0,25	+0,20	-1,00	+0,50	-0,20	-0,50	+1,05	+0,90	+0,10	-0,55	+0,25	-0,10
яскравий	+0,32	-0,76	+0,88	+0,88	+0,52	-1,12	+0,45	-0,64	+1,04	-1,12	-1,04	-0,84	+0,32	-1,44	+0,60	+0,32	-0,84	+0,84	+1,20	+0,68	-1,40	+0,76	-0,16
сильний	+1,07	-0,11	+1,07	+1,71	+0,78	-1,00	+0,78	-0,15	+0,89	-0,44	-0,74	-0,37	+0,63	-0,56	+0,81	-0,07	-1,22	-0,15	+0,04	+0,00	-1,37	+0,15	-0,48
стрімке	+0,58	+0,00	+0,60	+0,30	+0,81	+1,10	+0,27	-0,70	+1,08	-0,70	+1,00	+1,00	-0,92	-0,40	-0,50	+0,00	-0,10	+0,80	+0,60	+0,60	-0,60	-0,10	-0,40
повільний	-0,40	+0,50	-0,80	-1,00	-0,80	-0,30	+0,10	+1,10	-1,00	+0,70	-1,00	-0,50	+0,30	+0,90	+0,40	-0,30	+0,00	-0,70	-0,90	-0,40	-0,50	+0,00	+0,70
тихий	-0,80	+0,80	-0,70	-1,20	+0,30	+1,50	-0,50	+0,10	-1,00	+1,20	+0,90	+1,40	-0,40	+1,70	-0,70	+0,00	+1,30	-0,30	-0,90	-0,10	+1,80	-0,30	+0,00
суворий	+0,90	-0,10	+1,40	+1,90	+1,10	-0,40	+0,50	+0,60	+1,40	+0,30	+0,70	+0,20	+1,00	+0,10	+0,60	-0,40	-1,00	-0,90	-0,30	-0,50	-0,10	-0,70	-0,90
мінорний	-0,13	+0,60	-0,60	-0,13	+0,17	+0,50	+0,10	-0,50	-0,56	+1,08	+0,05	-0,04	-0,61	+1,05	-0,90	+0,36	+0,83	-0,22	-0,38	+0,60	+0,63	+0,45	+0,15
сумний	-0,69	+0,54	-0,54	-0,31	+0,15	+0,69	-0,40	+0,60	-0,46	+1,00	+0,70	+0,87	-0,08	+1,31	-0,46	-0,46	+0,55	-0,69	-1,07	-0,23	+1,00	-0,30	-0,23
темний	+0,45	-0,10	+0,64	+0,95	+0,30	+1,05	-0,25	+0,50	+0,30	+1,14	+0,90	+1,20	+0,09	+1,30	+0,17	+0,00	-0,25	-0,25	+0,19	-0,05	+0,30	-0,32	-0,40
важкий	+0,29	-0,58	+0,29	+1,13	+0,04	+0,04	+0,17	+0,75	-0,42	+0,33	+0,00	+0,17	+0,58	+0,71	+0,21	-0,42	-0,92	-0,21	+0,33	-0,12	-0,08	-0,09	+0,21
тужливий	-0,47	-0,10	-0,13	-0,40	-0,13	+0,90	-0,60	+0,60	-0,10	+0,37	+0,37	+0,60	+0,13	+0,76	+0,00	-0,30	+0,10	-0,90	-0,63	-0,50	+0,43	-0,60	-0,30
похмурий	+0,60	+0,00	+1,70	+1,40	+0,90	+0,40	+0,30	+0,20	+1,20	+0,40	+0,50	+0,60	+0,30	+0,50	+0,30	-0,70	-1,10	-0,30	+0,20	-0,60	-0,60	-0,70	-1,10
страхітливий	+0,31	+0,25	-0,17	+1,56	+0,21	+0,81	+0,58	-0,56	+0,23	+1,08	+0,83	+0,35	-0,25	+1,44	-0,54	-0,35	-0,17	-0,25	+0,42	-0,71	-0,50	-0,12	-0,81
зловісний	-0,21	+0,91	+0,09	+1,00	+0,79	+0,29	+0,66	-0,26	+0,28	+0,50	+0,16	+0,41	+0,45	+0,75	+0,29	-0,34	+0,12	-1,55	+0,28	+0,00	-0,84	+0,12	-1,13

Продовження табл. Б.2

Ознаковий аспект	Звукобуква																					
	б’	х’	к’	т’	н’	ф’	л’	а	ж	й	ш	ц	э	ы	у	ч	щ	о	е	ю	я	и
прекрасний	+0,01	-1,25	-0,67	-0,28	+0,06	-1,20	+1,25	+1,48	-0,72	+0,13	-1,01	-0,95	+1,00	-0,60	+0,00	+0,00	-0,52	+1,35	+1,10	+1,18	+1,16	+1,32
світлий	+0,40	+0,00	-0,15	-0,59	+0,20	+0,65	+1,10	+0,80	-0,80	+0,85	-1,20	-0,35	+0,25	-1,00	-0,52	-0,55	-0,73	+0,80	+1,09	+0,75	+1,00	+1,00
ніжний	+0,46	-0,08	+0,42	+0,08	+0,37	+0,25	+0,33	+0,71	-1,04	+0,54	-0,38	+0,13	+0,33	-0,50	+0,17	-0,33	-0,42	+0,46	+0,62	+0,52	+0,89	+1,00
радісний	+0,23	-1,00	-0,31	-0,77	+0,46	-0,08	+0,92	+0,80	-0,46	+0,08	-0,85	-0,46	+0,50	-0,62	-0,77	-0,23	-1,23	+0,31	+0,31	+0,54	+1,15	+0,46
піднесений	-0,15	-1,50	-0,95	-0,45	-0,25	-1,50	+0,00	+1,00	-0,60	+0,00	-1,00	-0,85	+0,90	-0,10	+0,60	-0,55	-1,40	+1,40	+0,40	+0,15	+0,90	+0,05
бадьорий	+0,00	-1,35	+0,05	-0,22	-0,23	-1,00	+0,25	+0,90	+0,00	+0,85	-0,60	-0,45	-0,55	-1,00	-0,15	+0,05	-1,05	+0,83	+0,60	-0,35	+0,35	+0,10
яскравий	+0,72	-1,32	-0,76	-0,92	+0,04	-1,28	+0,72	+0,96	+0,08	+0,64	-1,48	-0,60	+0,52	-0,64	-0,12	-0,32	-0,96	+1,24	+0,60	+0,48	+1,44	+0,40
сильний	-0,52	-1,56	-1,48	-1,22	-0,40	-1,32	-0,40	+0,44	+0,52	-0,19	-0,44	-0,78	+0,70	+0,52	+0,19	-0,81	-1,22	+1,26	+0,89	-0,85	+1,26	-0,26
стрімке	+0,80	-0,54	-1,10	+0,50	-0,40	-0,70	+0,00	-0,40	-0,40	+1,12	-0,10	-0,70	-0,70	-1,39	-1,30	+1,00	-0,85	-0,60	-0,80	-0,60	-0,20	-0,60
повільний	-0,70	+0,70	-0,70	-0,30	+0,20	+1,00	+0,40	-0,10	+0,20	-1,12	+0,50	-0,50	+0,50	-0,90	+1,00	-0,50	+0,50	+0,30	+0,30	+0,20	+0,00	+0,40
тихий	-0,10	+1,70	+1,40	+1,40	-0,10	+1,40	-0,10	-1,10	-0,10	-0,30	+1,70	+1,30	-0,80	-0,60	-0,70	+1,00	+1,00	-1,60	-0,10	+0,20	-0,80	+0,30
суворий	-0,10	-0,80	-0,70	-0,60	-0,50	-0,75	-1,40	+0,60	+0,50	+0,40	-0,10	+0,20	+0,25	+0,70	+0,90	-0,50	-0,40	+0,80	-0,20	-1,70	+0,70	-1,00
мінорний	-0,01	+1,27	+0,67	+0,28	-0,06	+1,20	-1,25	-1,48	+0,72	-0,13	+1,01	+0,95	-1,00	+0,45	-0,92	+0,00	+0,52	-1,35	-1,10	-1,18	-1,16	-1,32
сумний	-0,23	+1,00	+0,31	+0,77	-0,46	+1,08	-0,42	-1,10	+0,53	-0,20	+0,85	+0,46	-0,50	+0,72	+0,87	+0,23	+1,23	-0,81	-0,80	-0,54	-1,15	-0,70
темний	-0,20	+0,68	+0,15	+0,59	-0,20	+0,65	-1,00	-1,30	+1,10	-0,28	+1,45	+0,85	-0,73	+0,80	+0,52	+0,37	+0,91	-0,70	-1,32	-0,75	+1,45	-0,90
важкий	-0,46	+0,08	-0,42	-0,08	-0,37	-0,25	-0,33	-0,71	+1,04	-0,54	+0,38	+0,13	-0,33	+0,50	-0,67	+0,33	+0,42	-0,46	-0,62	-0,92	-0,89	-1,00
тужливий	-0,90	+0,40	-0,50	+0,33	+0,00	+0,20	-0,87	-0,23	-0,27	-0,43	+0,60	+0,70	-0,03	+0,80	+1,00	-0,10	+0,35	-0,10	-0,50	-0,50	-0,50	-0,23
похмурий	-0,60	-0,70	-0,60	-0,80	-1,10	-0,80	-1,00	-0,10	+1,30	-0,10	+0,10	+0,00	+0,00	+1,00	+0,00	+0,60	-0,30	+0,30	+0,70	-1,10	-0,30	-1,10
страхітливий	-0,71	+0,83	+0,04	+0,23	-0,85	+0,25	-1,29	-0,42	+1,27	-0,55	+1,17	+0,31	-0,81	+0,46	-0,60	+0,40	+1,29	-0,25	-0,81	-1,04	-0,87	-0,92
зловісний	-0,12	+0,12	+0,04	-0,34	-0,98	+0,16	-1,10	-0,96	+1,08	+0,28	+0,41	+0,58	-0,39	+0,50	+0,33	+0,28	+0,30	-0,30	-0,30	-0,85	-0,59	-0,63

Таблиця Б.3

Матриця нормальної (середньої) частотності звукобукв руського тексту)

Звуки	Нормальна (середня) частотність
в	0,028
с	0,032
д	0,020
р	0,024
г	0,012
п	0,020
з	0,013
м	0,025
б	0,013
х	0,008
к	0,030
т	0,055
н	0,040
ф	0,002
л	0,020
в’	0,011
с’	0,017
д’	0,017
р’	0,014
г’	0,003
п’	0,006
з’	0,002
м’	0,007
б’	0,005
х’	0,001
к’	0,003
т’	0,020
н’	0,024
ф’	0,001
л’	0,017
а	0,093
ж	0,008
й	0,015
ш	0,012
ц	0,004
э	0,005
ы	0,018
у	0,029
ч	0,020
щ	0,003
о	0,102
е	0,089
ю	0,006
я	0,024
и	0,056

Додаток В

Текст програми

A.2 DPMainWindow.cpp

```
#include "DPMainWindow.h"
#include "ui_DPMainWindow.h"
#include <iostream>

#include <string>
#include <wchar.h>
#include "stdio.h"
#include <QtDebug>
#include <map>
#include "qfiledialog.h"
#include <QGraphicsScene>
#include "math.h"

#include "Logic/DPPhoneticsTable/DPPhoneticsTable.h"
#include "Logic/DPSemanticTable/DPSemanticTable.h"
#include "View/PDPhoneticHistogram.h"
#include "Logic/DPTextParser/DPTextParser.h"
#include "Models/DPText/DPText.h"
#include "DPDebug.h"
#include "Logic/DPDatabaseManager/DPDatabaseManager.h"
#include "View/PDSemanticHistogram.h"
#include "Logic/DPColorAnalizer.h"
#include "Models/DPSemanticRow/DPSemanticRow.h"

using namespace std;

DPMainWindow::DPMainWindow(QWidget *parent) : QMainWindow(parent), ui(new Ui::DPMainWindow)
{
    ui->setupUi(this);

    cyrillicAlphabet = DPDatabaseManager::supportedAlphabetSet();
    separateSymbols = DPDatabaseManager::wordsSeparatedSymbolsSet();
    sentencesSeparatedSymbols = DPDatabaseManager::sentencesSeparatedSymbolsSet();

    analizeType = DPAnalizeTypeByWords;
    ui->radio_button_analizeTypeByWord->setChecked(true);
    currentParagraphForDynamicAnalize = 1;
    currentParagraphForPhoneticDynamicAnalize = 1;
    ui->dynamic_analyze_paragraph_text_field->setValidator(new QIntValidator(0, 999999, this));
    ui->accumulate_analyze_paragraph_text_field->setValidator(new QIntValidator(0, 999999, this));
    ui->dynamic_phonetic_paragraph_text_field->setValidator(new QIntValidator(0, 999999, this));
    ui->accumulate_phonetic_analyze_paragraph_text_field->setValidator(new QIntValidator(0, 999999, this));
    ui->color_dynamic_analize_text_field->setValidator(new QIntValidator(0, 999999, this));
    ui->color_accumulate_analize_text_field->setValidator(new QIntValidator(0, 999999, this));
}

DPMainWindow::~DPMainWindow()
{
    delete ui;
}

// Actions

void DPMainWindow::on_openFileButton_clicked()
```

```
{
    QString filePath = QFileDialog::getOpenFileName(this, tr("Open File"), "", tr("Files (*.*)"));

    ui->lineEdit->setText(filePath);
    this->parseFile();
}

void DPMainWindow::parseFile()
{
    QFile file(ui->lineEdit->text());
    bool fileOpened = file.open(QIODevice::ReadOnly | QIODevice::Text);

    if (fileOpened)
    {
        QTextStream stream(&file);
        QString fileContent = stream.readAll();
        fileContent = fileContent.toLower();
        textString = fileContent;

        DPTextParser *parser = new DPTextParser(cyrillicAlphabet, sentencesSeparatedSymbols, separateSymbols);
        text = parser->textFromString(fileContent);
        delete(parser);

        currentParagraphForDynamicAnalize = 1;
        ui->dynamic_analyze_paragraph_text_field->clear();
        ui->dynamic_textBrowser->clear();

        if (ui->dynamic_graphicsView->scene())
        {
            ui->dynamic_graphicsView->scene()->clear();
        }

        this->dynamic_analize_paragraphs_text_label_initialize();
    }
}

void DPMainWindow::printSemanticGraf(QList<float> values, QGraphicsView *graphicView)
{
    QGraphicsScene *scene = new QGraphicsScene(this);
    graphicView->setScene(scene);

    DPSemanticTable *phoneticsTable = new DPSemanticTable;

    PDSemanticHistogram *phoneticHistogram = new PDSemanticHistogram();
    phoneticHistogram->values = values;
    phoneticHistogram->rows = phoneticsTable->rows;
    scene->addItem(phoneticHistogram);

    delete phoneticsTable;
}

void DPMainWindow::printPhoneticGraf(QList<float> values, QGraphicsView *graphicView)
{
    QGraphicsScene *scene = new QGraphicsScene(this);
    graphicView->setScene(scene);

    DPPhoneticsTable *phoneticsTable = new DPPhoneticsTable;

    PDPhoneticHistogram *phoneticHistogram = new PDPhoneticHistogram();
    phoneticHistogram->values = values;
    phoneticHistogram->rows = phoneticsTable->rows;
    scene->addItem(phoneticHistogram);
```

```
    delete phoneticsTable;
}

// ======================== ДИФФЕРЕНЦИАЛ СТАТИЧЕСКИЙ АНАЛИЗ ========================

void DPMainWindow::on_static_text_analyze_button_clicked()
{
    QList<float> semanticTableValues;

    DPSemanticTable *semanticTable = new DPSemanticTable;

    foreach (DPSemanticRow row, semanticTable->rows)
    {
        float value = semanticTable->semanticValueForText(text, row, analizeType);
        semanticTableValues << value;
    }

    this->staticSemanticAnalizeViewer(semanticTableValues, semanticTable, ui->textBrowser_3, ui->graphicsView);

    delete semanticTable;
}

void DPMainWindow::on_static_string_analyze_button_clicked()
{
    QString string = ui->lineEdit_2->text().toLower();
    DPText textFromString = this->paseString(string);

    QList<float> semanticTableValues;

    DPSemanticTable *semanticTable = new DPSemanticTable;

    foreach (DPSemanticRow row, semanticTable->rows)
    {
        float value = semanticTable->semanticValueForText(textFromString, row, analizeType);
        semanticTableValues << value;
    }

    this->staticSemanticAnalizeViewer(semanticTableValues, semanticTable, ui->textBrowser_3, ui->graphicsView);

    delete semanticTable;
}

void DPMainWindow::staticSemanticAnalizeViewer(QList<float> semanticTableValues, DPSemanticTable
*semanticTable, QTextBrowser *textBrowser, QGraphicsView *graphicView)
{
    textBrowser->clear();

    QList<float> sortedValues = semanticTableValues;

    for (int x = 0; x < sortedValues.count(); ++x)
    {
        sortedValues[x] = fabs(sortedValues[x] - 3);
    }

    qSort(sortedValues);
    float koef = 0.5f;

    if (sortedValues.last() < 0.5f)
    {
        textBrowser->append("Текст не имеет существенных отклонений.\n");
        textBrowser->append("Наибольшие отклонение имеют шкалы:");
```

```
        koef = sortedValues[sortedValues.count() - 3];
    }
    else
    {
        textBrowser->append("Текст имеет отклонения по шкалам:");
    }

    int rowNumber = 0;

    foreach (DPSemanticRow row, semanticTable->rows)
    {
        float value = semanticTableValues[rowNumber];

        if (value < 3.0f - koef || value > 3.0f + koef)
        {
            float direction = 3.0f - value;

            if (direction < 0)
            {
                textBrowser->append(QString("%1 -> %2").arg(row.negativeSign, QString::number(direction)));
            }
            else
            {
                textBrowser->append(QString("%1 -> %2").arg(row.positiveSign, QString::number(direction)));
            }
        }

        ++rowNumber;
    }

    printSemanticGraf(semanticTableValues, graphicView);
}

// ========================= ДИФФЕРЕНЦИАЛ ДИНАМИЧЕСКИЙ АНАЛИЗ ========================

void DPMainWindow::on_dynamic_analyze_button_clicked()
{
    if (text.paragraphs.count() == 0)
    {
        ui->dynamic_analyze_paragraph_text_field->setText("");

        return;
    }

    if (ui->dynamic_analyze_paragraph_text_field->text().toInt() < 1)
    {
        ui->dynamic_analyze_paragraph_text_field->setText("1");

        return;
    }

    if (text.paragraphs.count() < ui->dynamic_analyze_paragraph_text_field->text().toInt())
    {
        ui->dynamic_analyze_paragraph_text_field->setText(QString::number(text.paragraphs.count()));

        return;
    }

    currentParagraphForDynamicAnalize = ui->dynamic_analyze_paragraph_text_field->text().toInt();

    this->dynamic_analize_paragraph();
```

```
}

void DPMainWindow::on_dynamic_next_button_clicked()
{
   ui->dynamic_analyze_paragraph_text_field->setText("");
   int nextParagraphNumber = currentParagraphForDynamicAnalize + 1;

   if (text.paragraphs.count() == 0)
   {
      return;
   }

   if (nextParagraphNumber < 1)
   {
      return;
   }

   if (text.paragraphs.count() < nextParagraphNumber)
   {
      return;
   }

   currentParagraphForDynamicAnalize = nextParagraphNumber;

   this->dynamic_analize_paragraph();
}

void DPMainWindow::on_dynamic_back_button_clicked()
{
   ui->dynamic_analyze_paragraph_text_field->setText("");
   int prevParagraphNumber = currentParagraphForDynamicAnalize - 1;

   if (text.paragraphs.count() == 0)
   {
      return;
   }

   if (prevParagraphNumber < 1)
   {
      return;
   }

   if (text.paragraphs.count() < prevParagraphNumber)
   {
      return;
   }

   currentParagraphForDynamicAnalize = prevParagraphNumber;

   this->dynamic_analize_paragraph();
}

void DPMainWindow::dynamic_analize_paragraphs_text_label_initialize()
{
   ui->dynamic_analyze_paragraph_number_label->setText("Выберите часть для анализа");
}

QString DPMainWindow::dynamic_analize_paragraphs_text_label(DPText text)
{
   return QString("Часть %1 из
%2").arg(QString::number(currentParagraphForDynamicAnalize)).arg(QString::number(text.paragraphs.count()));
}
```

```
void DPMainWindow::dynamic_analize_paragraph()
{
    QList<float> semanticTableValues;

    DPSemanticTable *semanticTable = new DPSemanticTable;

    foreach (DPSemanticRow row, semanticTable->rows)
    {
        float value = semanticTable->semanticValueForParagraph(text.paragraphs[currentParagraphForDynamicAnalize - 1],
row, analizeType);
        semanticTableValues << value;
    }

    this->staticSemanticAnalizeViewer(semanticTableValues, semanticTable, ui->dynamic_textBrowser, ui-
>dynamic_graphicsView);

    ui->dynamic_analyze_paragraph_number_label->setText(this->dynamic_analize_paragraphs_text_label(text));

    delete semanticTable;
}

// ======================== ДИФФЕРЕНЦИАЛ НАКОПИТЕЛЬНЫЙ АНАЛИЗ ======================

void DPMainWindow::on_accumulate_analyze_button_clicked()
{
    if (text.paragraphs.count() == 0)
    {
        ui->accumulate_analyze_paragraph_text_field->setText("");

        return;
    }

    if (ui->accumulate_analyze_paragraph_text_field->text().toInt() < 1)
    {
        ui->accumulate_analyze_paragraph_text_field->setText("1");

        return;
    }

    if (text.paragraphs.count() < ui->accumulate_analyze_paragraph_text_field->text().toInt())
    {
        ui->accumulate_analyze_paragraph_text_field->setText(QString::number(text.paragraphs.count()));

        return;
    }

    startParagraphForAccumulateAnalize = ui->accumulate_analyze_paragraph_text_field->text().toInt();
    currentParagraphForAccumulateAnalize = startParagraphForAccumulateAnalize;

    accumulateText = DPText();
    accumulateText.paragraphs << text.paragraphs[startParagraphForAccumulateAnalize - 1];

    this->accumulate_analize_paragraph();
}

void DPMainWindow::on_accumulate_next_button_clicked()
{
    ui->accumulate_analyze_paragraph_text_field->setText("");
    int nextParagraphNumber = currentParagraphForAccumulateAnalize + 1;

    if (startParagraphForAccumulateAnalize == 0)
```

```
    {
        return;
    }

    if (text.paragraphs.count() == 0)
    {
        return;
    }

    if (nextParagraphNumber < 1)
    {
        return;
    }

    if (text.paragraphs.count() < nextParagraphNumber)
    {
        return;
    }

    currentParagraphForAccumulateAnalize = nextParagraphNumber;

    accumulateText.paragraphs << text.paragraphs[currentParagraphForAccumulateAnalize - 1];

    this->accumulate_analize_paragraph();
}

void DPMainWindow::on_accumulate_back_button_clicked()
{
    ui->accumulate_analyze_paragraph_text_field->setText("");
    int prevParagraphNumber = currentParagraphForAccumulateAnalize - 1;

    if (startParagraphForAccumulateAnalize > prevParagraphNumber)
    {
        return;
    }

    if (text.paragraphs.count() == 0)
    {
        return;
    }

    if (prevParagraphNumber < 1)
    {
        return;
    }

    if (text.paragraphs.count() < prevParagraphNumber)
    {
        return;
    }

    currentParagraphForAccumulateAnalize = prevParagraphNumber;

    accumulateText.paragraphs.removeLast();

    this->accumulate_analize_paragraph();
}

void DPMainWindow::accumulate_analize_paragraph()
{
    QList<float> semanticTableValues;
```

```
    DPSemanticTable *semanticTable = new DPSemanticTable;

    foreach (DPSemanticRow row, semanticTable->rows)
    {
        float value = semanticTable->semanticValueForText(accumulateText, row, analizeType);
        semanticTableValues << value;
    }

    this->staticSemanticAnalizeViewer(semanticTableValues, semanticTable, ui->accumulate_textBrowser, ui-
>accumulate_graphicsView);

    ui->accumulate_analyze_paragraph_number_label->setText(this-
>accumulate_analize_paragraphs_text_label(accumulateText));

    delete semanticTable;
}

QString DPMainWindow::accumulate_analize_paragraphs_text_label(DPText text)
{
    return QString("Части с %1 по
%2").arg(QString::number(startParagraphForAccumulateAnalize)).arg(QString::number(text.paragraphs.count() +
(startParagraphForAccumulateAnalize - 1)));
}

// ====================================================================
// ====================================================================
// ====================================================================
// ====================================================================
// ====================================================================

DPText DPMainWindow::paseString(QString string)
{
    DPTextParser *parser = new DPTextParser(cyrillicAlphabet, sentencesSeparatedSymbols, separateSymbols);
    DPText resultText = parser->textFromString(string);
    delete(parser);

    return resultText;
}

// ======================== ФОНЕТИЧЕСКИЙ СТАТИЧЕСКИЙ АНАЛИЗ ========================

void DPMainWindow::on_static_phonetic_text_analyze_button_clicked()
{
    DPPhoneticsTable *phoneticsTable = new DPPhoneticsTable;
    QList<float> values;

    foreach (DPPhoneticsRow row, phoneticsTable->rows)
    {
        float value = phoneticsTable->phoneticValueForText(text, row, analizeType);
        values<<value;
    }

    this->phoneticAnalizeViewer(values, phoneticsTable, ui->static_phonetic_textBrowser, ui-
>static_phonetic_graphicsView);

    delete phoneticsTable;
}

void DPMainWindow::on_static_phonetic_string_analyze_button_clicked()
{
    QString string = ui->lineEdit_2->text().toLower();
    DPText textFromString = this->paseString(string);
```

```
    DPPhoneticsTable *phoneticsTable = new DPPhoneticsTable;
    QList<float> values;

    foreach (DPPhoneticsRow row, phoneticsTable->rows)
    {
        float value = phoneticsTable->phoneticValueForText(textFromString, row, analizeType);
        values<<value;
    }

    this->phoneticAnalizeViewer(values, phoneticsTable, ui->static_phonetic_textBrowser, ui-
>static_phonetic_graphicsView);

    delete phoneticsTable;
}

void DPMainWindow::phoneticAnalizeViewer(QList<float> phoneticTableValues, DPPhoneticsTable *phoneticTable,
QTextBrowser *textBrowser, QGraphicsView *graphicView)
{
    textBrowser->clear();

    QList<float> sortedValues = phoneticTableValues;
    qSort(sortedValues);

    if (sortedValues.last() < 0.0f)
    {
        textBrowser->append("Текст не имеет выраженых признаков.\n");
    }
    else
    {
        textBrowser->append("Текст имеет такие признаки:");
    }

    int rowNumber = 0;

    foreach (DPPhoneticsRow row, phoneticTable->rows)
    {
        float value = phoneticTableValues[rowNumber];

        if (value > 0.5f)
        {
            textBrowser->append(QString("%1 -> %2").arg(row.sign, QString::number(value)));
        }

        ++rowNumber;
    }

    printPhoneticGraf(phoneticTableValues, graphicView);
}

// ======================== ФОНЕТИЧЕСКИЙ ДИНАМИЧЕСКИЙ АНАЛИЗ ========================

void DPMainWindow::on_dynamic_phonetic_analyze_button_clicked()
{
    if (text.paragraphs.count() == 0)
    {
        ui->dynamic_phonetic_paragraph_text_field->setText("");

        return;
    }

    if (ui->dynamic_phonetic_paragraph_text_field->text().toInt() < 1)
```

```
    {
        ui->dynamic_phonetic_paragraph_text_field->setText("1");

        return;
    }

    if (text.paragraphs.count() < ui->dynamic_phonetic_paragraph_text_field->text().toInt())
    {
        ui->dynamic_phonetic_paragraph_text_field->setText(QString::number(text.paragraphs.count()));

        return;
    }

    currentParagraphForPhoneticDynamicAnalize = ui->dynamic_phonetic_paragraph_text_field->text().toInt();

    this->phoneticDynamicAnalizeParagraph();
}

void DPMainWindow::on_dynamic_phonetic_next_button_clicked()
{
    ui->dynamic_phonetic_paragraph_text_field->setText("");
    int nextParagraphNumber = currentParagraphForPhoneticDynamicAnalize + 1;

    if (text.paragraphs.count() == 0)
    {
        return;
    }

    if (nextParagraphNumber < 1)
    {
        return;
    }

    if (text.paragraphs.count() < nextParagraphNumber)
    {
        return;
    }

    currentParagraphForPhoneticDynamicAnalize = nextParagraphNumber;

    this->phoneticDynamicAnalizeParagraph();
}

void DPMainWindow::on_dynamic_phonetic_back_button_clicked()
{
    ui->dynamic_phonetic_paragraph_text_field->setText("");
    int prevParagraphNumber = currentParagraphForPhoneticDynamicAnalize - 1;

    if (text.paragraphs.count() == 0)
    {
        return;
    }

    if (prevParagraphNumber < 1)
    {
        return;
    }

    if (text.paragraphs.count() < prevParagraphNumber)
    {
        return;
    }
```

```
    currentParagraphForPhoneticDynamicAnalize = prevParagraphNumber;

    this->phoneticDynamicAnalizeParagraph();
}

void DPMainWindow::phoneticDynamicAnalizeParagraph()
{
    DPPhoneticsTable *phoneticsTable = new DPPhoneticsTable;
    QList<float> values;

    foreach (DPPhoneticsRow row, phoneticsTable->rows)
    {
        float value = phoneticsTable-
>phoneticValueForParagraph(text.paragraphs[currentParagraphForPhoneticDynamicAnalize - 1], row, analizeType);
        values<<value;
    }

    this->phoneticAnalizeViewer(values, phoneticsTable, ui->dynamic_phonetic_textBrowser, ui-
>dynamic_phonetic_graphicsView);

    ui->dynamic_phonetic_analyze_paragraph_number_label->setText(this-
>phoneticDynamicAnalizeParagraphsTextLabel(text));

    delete phoneticsTable;
}

QString DPMainWindow::phoneticDynamicAnalizeParagraphsTextLabel(DPText text)
{
    return QString("Часть %1 из
%2").arg(QString::number(currentParagraphForPhoneticDynamicAnalize)).arg(QString::number(text.paragraphs.count()));
}

// ======================== ФОНЕТИЧЕСКИЙ НАКОПИТЕЛЬНЫЙ АНАЛИЗ ======================

void DPMainWindow::on_accumulate_phonetic_analyze_button_clicked()
{
    if (text.paragraphs.count() == 0)
    {
        ui->accumulate_phonetic_analyze_paragraph_text_field->setText("");

        return;
    }

    if (ui->accumulate_phonetic_analyze_paragraph_text_field->text().toInt() < 1)
    {
        ui->accumulate_phonetic_analyze_paragraph_text_field->setText("1");

        return;
    }

    if (text.paragraphs.count() < ui->accumulate_phonetic_analyze_paragraph_text_field->text().toInt())
    {
        ui->accumulate_phonetic_analyze_paragraph_text_field->setText(QString::number(text.paragraphs.count()));

        return;
    }

    startParagraphForPhoneticAccumulateAnalize = ui->accumulate_phonetic_analyze_paragraph_text_field->text().toInt();
    currentParagraphForPhoneticAccumulateAnalize = startParagraphForPhoneticAccumulateAnalize;

    accumulatePhoneticText = DPText();
```

```
    accumulatePhoneticText.paragraphs << text.paragraphs[startParagraphForPhoneticAccumulateAnalize - 1];

    this->accumulatePhoneticAnalizeParagraph();
}

void DPMainWindow::on_accumulate_phonetic_next_button_clicked()
{
    ui->accumulate_phonetic_analyze_paragraph_text_field->setText("");
    int nextParagraphNumber = currentParagraphForPhoneticAccumulateAnalize + 1;

    if (startParagraphForPhoneticAccumulateAnalize == 0)
    {
        return;
    }

    if (text.paragraphs.count() == 0)
    {
        return;
    }

    if (nextParagraphNumber < 1)
    {
        return;
    }

    if (text.paragraphs.count() < nextParagraphNumber)
    {
        return;
    }

    currentParagraphForPhoneticAccumulateAnalize = nextParagraphNumber;

    accumulatePhoneticText.paragraphs << text.paragraphs[currentParagraphForPhoneticAccumulateAnalize - 1];

    this->accumulatePhoneticAnalizeParagraph();
}

void DPMainWindow::on_accumulate_phonetic_back_button_clicked()
{
    ui->accumulate_phonetic_analyze_paragraph_text_field->setText("");
    int prevParagraphNumber = currentParagraphForPhoneticAccumulateAnalize - 1;

    if (startParagraphForAccumulateAnalize > prevParagraphNumber)
    {
        return;
    }

    if (text.paragraphs.count() == 0)
    {
        return;
    }

    if (prevParagraphNumber < 1)
    {
        return;
    }

    if (text.paragraphs.count() < prevParagraphNumber)
    {
        return;
    }
```

```
    currentParagraphForPhoneticAccumulateAnalize = prevParagraphNumber;

    accumulatePhoneticText.paragraphs.removeLast();

    this->accumulatePhoneticAnalizeParagraph();
}

void DPMainWindow::accumulatePhoneticAnalizeParagraph()
{
    QList<float> phoneticTableValues;

    DPPhoneticsTable *phoneticTable = new DPPhoneticsTable;

    foreach (DPPhoneticsRow row, phoneticTable->rows)
    {
        float value = phoneticTable->phoneticValueForText(accumulatePhoneticText, row, analizeType);
        phoneticTableValues << value;
    }

    this->phoneticAnalizeViewer(phoneticTableValues, phoneticTable, ui->accumulate_phonetic_textBrowser, ui-
>accumulate_phonetic_graphicsView);

    ui->accumulate_phonetic_analyze_paragraph_number_label->setText(this-
>accumulatePhoneticAnalizeParagraphsTextLabel(accumulatePhoneticText));

    delete phoneticTable;
}

QString DPMainWindow::accumulatePhoneticAnalizeParagraphsTextLabel(DPText text)
{
    return QString("Части с %1 по
%2").arg(QString::number(startParagraphForPhoneticAccumulateAnalize)).arg(QString::number(text.paragraphs.count() +
(startParagraphForPhoneticAccumulateAnalize - 1)));
}

void DPMainWindow::on_radio_button_analizeTypeByWord_clicked()
{
    analizeType = DPAnalizeTypeByWords;
}

void DPMainWindow::on_radio_button_analizeTypeByString_clicked()
{
    analizeType = DPAnalizeTypeByStrings;
}
```

Додаток Д

Акти реалізації науково-прикладних результатів досліджень

ЗАТВЕРДЖУЮ
Заступник начальника управління зв'язку та телекомунікацій ГУНП в Харківській області
Єрмаков Д.С.
"13" березня 2018 р.

А К Т
впровадження результатів науково-прикладних досліджень
Белікової Тетяни Вячеславівни

Комісія у складі: голови начальника відділу організації відео та аудіосервісів управління зв'язку та телекомунікацій ГУНП в Харківській області, кандидата технічних наук Комолова Д.І. та членів комісії головного спеціаліста управління зв'язку та телекомунікацій ГУНП в Харківській області Свиридова О.О., старшого інженера управління зв'язку та телекомунікацій ГУНП в Харківській області Ставицького С.С. склала дійсний акт, який полягає в тому, що при виконанні дослідно-конструкторських робіт використані наступні результати науково-прикладних досліджень **Белікової Тетяни Вячеславівни**:

1. Побудовано інформаційна модель аналізу ТІР на основі формування семантичного диференціала. На основі чого було розроблений метод виділення значущих лінгвістичних біполярних ознак на основі представлення фонетичних оцінок звуко-букв алфавіту в речовому нерівноважному позиційному просторі. Основна відмінність тут полягає в тому, що векторний фонетичний простір лінгвістичної біполярної ознаки по всіх звуко-буквам представляється в раціональному нерівноважному позиційному базисі.

2. Створено комплексний метод виявлення прихованого інформаційно-психологічного впливу в текстовому інформаційному ресурсі на підсвідомість особи в багатовимірному фонетичному просторі з прив'язкою до векторних градаційних двополюсних шкал значущих біполярних лінгвістичних ознак на основі формування семантичного диференціалу слів і обробкою їх за динамічною технологією з накопиченням фрагментарної інформації.

Впровадження результатів досліджень **Белікової Тетяни Вячеславівни** в методики аналізу ризиків порушення інформаційної безпеки та в процесі моніторингу Інтернет ресурсів на предмет виявлення та локалізації деструктивного

та шкідливого контенту на основі програмно-апаратних реалізацій дозволило забезпечити:

1) значне зменшення часу для виявлення прихованого ІП впливу на підсвідомість особистості. Так, процес виявлення, навіть без оптимізації програмного коду, швидший майже в 90 разів в порівнянні з роботою експертів та майже в 170 разів в порівнянні з аналізом тими, на кого здійснюється ІПВ. При чому, респонденти здатні за зазначений час визначити лише наявність сугестивного ІПВ на підсвідомість в ТІР, в той час, як за допомогою програмного засобу, що реалізує розроблені в дисертаційній роботі методи, мається можливість визначити ще й тип спрямованості такого ІПВ;

2) ефективність виявлення сугестивних ІПВ на підсвідомість людини в ТІР складає від 98 до 100 %;

3) виявилення від 10 до 17 % більше ТІР з ІПВ на підсвідомість особистості в порівнянні з відомими методами аналізу на основі ключових слів.

Голова комісії
Начальник відділу організації
відео та аудіосервісів управління
зв'язку та телекомунікацій ГУНП в
Харківській області
кандидат технічних наук Д.І. Комолов

Члени комісії:
Головний спеціаліст управління
зв'язку та телекомунікацій ГУНП в
Харківській області О.О. Свиридов

Старший інженер управління
зв'язку та телекомунікацій ГУНП в
Харківській області С.С. Ставицький

Затверджую

ТВО заступника начальника Харківського національного університету Повітряних Сил імені Івана Кожедуба з навчальної роботи

полковник К.С. ВАСЮТА

«23» квітня 2018 р.

АКТ

науково-технічної комісії щодо впровадження наукових положень і результатів кандидатської дисертації Белікової Тетяни Вячеславівни

Науково-технічна комісія у складі: голова комісії начальник кафедри бойового застосування та експлуатації АСУ полковник, доктор технічних наук, професор Бараннік Володимир Вікторович, члени комісії: доцент кафедри бойового застосування та експлуатації АСУ підполковник, кандидат технічних наук Королюк Наталія Олександрівна, старший викладач кафедри бойового застосування та експлуатації АСУ підполковник, кандидат технічних наук, Ларін Володимир Валерійович, викладач кафедри бойового застосування та експлуатації АСУ майор, кандидат технічних наук Мусієнко Олександр Павлович, склала даний акт про те, що в навчальнму процесі під час підготовки навчальних занять і курсових проектів та під під час наукової й науково-технічної діяльності були використані та впроваджені наступні наукові положення та результати, що отримані Беліковою Т.В., а саме:

1. Метод виявлення дій суггестій на підсвідомість людини в текстових повідомленнях в умовах інформаційно-психологічного протиборства, а саме аналізу слів, статичного і динамічного аналізу текстових документів.

2. Комплекс методів розпізнавання фонетичного, синтаксичного і семантичного значень інформаційних ресурсів на підсвідомість людини. Метод базується на розрахунку семантичного диференціалу для слова, що пропонується проводити на основі наступних етапів: переведення слова або послідовності букв в набір звукобукв; для кожної звукобукви вибираються табличні значення їх частотності та значущості виходячи з аналізованого признакового аспекту; розраховуються коефіцієнти кожного звуку в слові, як відношення максимальної частотності звуку в даному слові до табличного

значення частотності звукобукви; отримані коефіцієнти коректуються залежно від помітності букв в слові для першого букви і для наголошеного звуку. При цьому, визначення наголошеного звуку в слові може бути реалізоване за допомогою спеціальних сформованих словників; проводиться збільшення фонетичної значущості для кожної звукобукви залежно від коефіцієнту, для чого кожне фонетичне значення перемножуємо на значення відповідного коефіцієнту; розрахунок значення семантичного диференціалу для слова, як співвідношення суми усіх збільшених фонетичних значень кожної звукобукви до суми значень їх коефіцієнтів.

Це забезпечує виявлення сугестивних деструктивних дій на соціум.

Розроблені в дисертації Белікової Т.В. методи дозволють оцінювати емоційний вплив окремих слів і фонетичної структури текстів на підсвідомість людини, а також задавати характеристики бажаного впливу і створювати (коректувати) текстові структури відповідної спрямованості.

Створені методи дозволяють в автоматичному режимі для статичних і динамічних інформаційних ресурсів оцінити: емоційний вплив окремих слів на підсвідомість людини; емоційний вплив фонетичної структури текстів на підсвідомість людини; рівень агресивності текстів на основі аналізу позитивного і негативного впливів окремих слів на змістовне значення тексту в цілому; звуко-кольорові характеристики текстів.

Отримані результати було реалізовані при проведені курсу (лекційних, групових, лабораторних занять, розробки курсових проектів) з наступних навчальних дисциплін «Інформаційні технологіх в АСУ спеціального призначення», «Інформаційна безпека в АСУ авіації та ППО», «Сучасні кібернетичні технології», «Основи кібербезпеки», «Основи обробки відеоінформаційних ресурсів в АСУ».

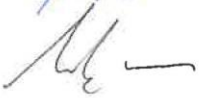
Голова комісії

Бараннік В.В.

Члени комісії:

Королюк Н.О.

Ларін В.В.



Мусієнко О.П.

ЗАТВЕРДЖУЮ

Ректор Національного університету

цивільного захисту України

д.н.держ.упр., професор

_____В. П. Садковий

"___" _____ 2018 року

АКТ

про впровадження результатів дисертаційного дослідження здобувача Черкаського державного технологічного університету Белікової Тетяни В'ячеславівни на здобуття наукового ступеня кандидата технічних наук.

Комісія у складі:

Голова комісії:

– проректор з навчальної та методичної роботи НУЦЗУ, к.псих.н., проф., О.О. Назаров.

Члени комісії:

– начальник навчально-науково-виробничого центру, д.н.держ.упр., проф. С.М. Домбровська:

– завідувач кафедри публічного адміністрування у сфері цивільного захисту д.н.держ.упр., проф. С.В. Майстро

цим Актом засвідчує, що результати дисертаційного дослідження здобувача Черкаського державного технологічного університету Белікової Тетяни В'ячеславівни, які стосуються розробки методів виявлення дій суггестій на підсвідомість людини в текстових повідомленнях в умовах інформаційно-психологічного протиборства, а саме аналізу слів, статичного і динамічного аналізу текстових документів, використовуються викладачами кафедри публічного адміністрування у сфері цивільного захисту НУЦЗУ при викладанні модулів дисциплін , які стосуються формуванню уявлень про державну безпеку, з підготовки фахівців з державного управління у сфері цивільного захисту: «Управління соціальним і гуманітарним розвитком», «Державне управління в економічній сфері», та «Державна політика: аналіз та механізми впровадження».

Голова комісії:
к.псих.н., проф. О.О. Назаров
Члени комісії:
д.н.держ.упр., проф. С.М. Домбровська:
д.н.держ.упр., проф. С.В. Майстро