Загальні питання

УДК 623.618:519.686 DOI: 10.30748/soivt.2019.60.16

В.В. Бараннік, С.О. Сідченко, Т.В. Белікова, Ю.О. Олійник

Харківський національний університет Повітряних Сил ім. І. Кожедуба, Харків

МЕТОД ВИЯВЛЕННЯ ДЕСТРУКТИВНО ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ВПЛИВУ НА ПІДСВІДОМІСТЬ ОСОБОВОГО СКЛАДУ ТА НАСЕЛЕННЯ УКРАЇНИ

У статті представлені результати аналізу методу виявлення деструктивних інформаційно-психологічних впливів в електронних ЗМІ на підсвідомість та свідомість особового складу збройних формувань сектору оборони та безпеки України та населення України. Визначено, що запропонований метод лінгвістичного процесору дає можливість для визначення в текстовому повідомленні головних слів, що характеризують текст, та визначити їх спрямованість щодо впливу на підсвідомість особистості. Проведені практичні дослідження показали працездатність даного методу для виявлення сугестивного деструктивного ІПВ на підсвідомість військовослужбовців сектору оборони безпеки України та населення України.

Ключові слова: *інформаційно-психологічний вплив, ЗМІ, лінгвістичний процесор, структура бази знань.*

Вступ

Постановка проблеми. В сучасному інформаційному просторі України постає ряд питань, де головною проблемою є виявлення та протидія негативним інформаційно-психологічним впливам противника, як однієї зі складових розпаленого збройно-інформаційного протистояння, тобто оборони [1–7]. Поява нових технологій надає особливу гостроту і витонченість сучасним конфліктам, у яких все частіше використовуються методи, засновані на комплексному застосуванні політичних, економічних, інформаційних та інших невоєнних заходів, реалізованих з опорою на військову силу.

Реалії сьогодення призвели до того, що інформацію населення отримує вже не зі шпальт друкованих газет та журналів, а за допомогою електронних засобів масової інформації та соціальних мереж.

Інтернет поступово “витісняє” традиційні ЗМІ у процесах формування масової свідомості, інформування суспільства про поточні події, діяльності публічної влади та її інститутів, відображення реакції суспільства на рішення та дії влади, поширення політичних, соціально-економічних, правових і культурних ідей і знань.

У зв’язку зі стрімким поширенням інформації виникає потреба аналізу її як складової яка безпосередньо впливає на масову свідомість.

Головною складовою інформаційного впливу шляхом інформаційного простору Інтернету служить свідомість людини і підсвідомість індивіда, тобто колективна свідомість, на яку безпосереднім чином здійснюється інформаційний вплив різними інформаційними ресурсами.

Виходячи з того, що для здійснення інформаційного впливу достатньо не лише створювати певну інформацію, а шляхом її повторення та розповсюдження в мережі Інтернет, необхідно здійснювати виявлення інформаційних потоків, для подальших аналізів безпосередньо складової текстової інформації.

Аналіз останніх досліджень і публікацій. У сучасній Доктрині інформаційної безпеки України від 25.03.2017 року узагальнюється практичний досвід війни та значно розширюється поняття сучасних загроз національним інтересам та національній безпеці України в інформаційній сфері, визначено завдання щодо протидії інформаційній агресії, включно із захистом громадян від негативного інформаційного (у тому числі психологічного) впливу супротивника [8–10].

Розрізняють різні форми ведення інформаційної боротьби [11–17]:

– інформаційна кампанія (носить переважно довготерміновий перманентний характер і залежить від цілей кампанії та поточної ситуації);

– інформаційна операція (від одного до декількох місяців);

– інформаційна акція (від декількох тижнів до декількох місяців);

– інформаційна атака (від декількох днів до тижня);

– інформаційний (інформаційно-психологічний) вплив (від декількох хвилин до декількох днів).

З аналізу публікацій інформаційного простору

(Інтернету, соціальних мереж, телебачення, тощо) можна запропонувати наступну класифікацію спрямованості інформаційних (інформаційно-психологічних) впливів (в подальшому будемо застосовувати ІПсВ) на особовий склад військових формувань сектору оборони та безпеки України та населення України:

– ІПсВ на державних, політичних, релігійних, бізнесових діячів і окремих громадян України;

– ІПсВ на особовий склад військових формувань сектору оборони та безпеки України;

– ІПсВ на населення України;

– ІПсВ на особовий склад військових формувань сектору оборони та безпеки України, що знаходяться на території проведення операцій об'єднаних сил;

– ІПсВ на населення України, що знаходяться на території проведення операцій об'єднаних сил;

– ІПсВ на населення, що знаходиться на тимчасово окупованих окремих регіонах Донецької та Луганських областей;

– ІПсВ на населення України, що знаходяться на тимчасово окупованих території АР Крим;

– ІПсВ на українську діаспору та громадян України, які тимчасово проживають за межами держави;

– ІПсВ з розповсюдження не достовірної та антиукраїнської пропаганди на міжнародному рівні керівництво та населення іноземних держав, які підтримують Україну;

– ІПсВ з розповсюдження не достовірної та антиукраїнської пропаганди на міжнародному рівні на керівництво та населення іноземних держав, які є прихильниками РФ.

З аналізу відкритих публікацій, на сьогоднішній день, можна визначити, що вітчизняний науковий доробок на тему інформаційних операцій, як і значна частина методологічної літератури з інформаційної безпеки, детально розглядає методи інформаційного наступу, однак темі протидії інформаційно-психологічним впливам приділено значно менше уваги.

Мета статті – розробка методу виявлення деструктивних інформаційно-психологічних впливів в електронних ЗМІ на підсвідомість та свідомість особового складу збройних формувань сектору оборони та безпеки України та населення України.

Виклад основного матеріалу

У зв'язку з постійним впливом зовнішніх інформаційних потоків, а саме за допомогою ЗМІ (соціальних мереж та Інтернету взагалі), відбувається постійний вплив на свідомість та підсвідомість людини.

Для вирішення задачі аналізу прихованого інформаційного впливу на підсвідомість особистості доцільно використовувати комплекс методів, які можуть бути поєднані в лінгвістичному процесорі, та до якого доцільно включити методи, які здійснюють:

– морфологічний, синтаксичний та семантичний аналіз, які можуть використовуватись для розбору речень і текстів та виявлення головних слів та сенсу текстового повідомлення;

– методів, що виявляють сугестивний вплив на підсвідомість особистості. До таких методів можна віднести методи фонетичного аналізу, аналізу на основі семантичного дефиренціалу, звукокольорового аналізу, тощо.

Розглянемо особливості математичних підходів до роботи елементів лінгвістичного процесору, за допомогою якого можна семантичну спрямованість тексту, визначити головні (ключові) слова та оцінити прихований інформаційно-психологічний вплив на підсвідомість особистості.

Морфологічний аналіз текстової інформації.

Від початку система не повинна мати ніяких даних ні про слово, ні про мову до якого воно відноситься.

Кінцева задача алгоритму зводиться до розділення слова на частини, і класифікація цих частин як елементів певної групи, що є множиною однакових за структурою частин.

Іншими словами, задача навчання алгоритму є групування однакових частин слова, за певними критеріями та параметрами.

Для дослідження взята українська мова, для слов'янської групи мов, нижче описаний метод вважається актуальним.

Щодо відмінностей між словами, то критерії, які є вагомими для морфологічної оцінки наступні:

– довжина (кількість букв);

– послідовність букв;

– місце в реченні.

Інформація на основі даних критеріїв поверхнева, тому необхідно розглянути внутрішнє влаштування слова. Слово α можна представити наступним чином:

$$\alpha = X + Y + Z + Q, \qquad (1)$$

де X – префікс;

Y – корінь;

Z – суфікс;

Q – закінчення.

Але це тільки одна з можливих комбінацій. Слова можуть мати і наступну будову:

$$\alpha = X + Y, \qquad (2)$$

$$\alpha = Y + Z, \qquad (3)$$

$$\alpha = Y + Q, \qquad (4)$$

$$\alpha = Y + Z + Q, \qquad (5)$$

$$\alpha = X + Y + Z, \qquad (6)$$

$$\alpha = X + Y + Q. \qquad (7)$$

Ключові для морфологічного аналізу відмінності в морфемах виражені в наступних критеріях:

– послідовність букв;

– положення в слові;

– довжина (кількість букв);

Положення морфеми в слові характеризується кількістю букв до морфеми від початку слова та від кінця. Звідси, положення частини слова відносно інших частин слова:

$$\alpha = X \succ Y \succ Z \succ Q\,, \qquad (8)$$

якщо відлік букв іде від кінця, і:

$$\alpha = X \prec Y \prec Z \prec Q\,, \qquad (9)$$

якщо відлік букв від початку.

Положення морфеми в слові характеризується кількістю букв до морфеми від початку слова та від кінця. Інформація на основі даних критеріїв поверхнева, тому необхідно розглянути внутрішнє влаштування слова.

Таким чином, метод що описаний вище дозволяє групувати за морфологічними ознаками слова, мов слов'янських груп. Далі, за допомогою експертів надається класифікація груп. Після чого створена база знань буде готова, до автоматичного морфологічного аналізу, з подальшим паралельним навчанням.

Один з можливих варіантів представлення семантичного уявлення – структура, що складається з "текстових фактів". Семантичний аналіз в межах одного речення називається локальним семантичним аналізом.

Синтаксичний та семантичний аналіз тексту. Семантичний аналіз – етап в послідовності дій алгоритму автоматичного розуміння текстів, що полягає у виділенні семантичних відносин, формуванні семантичного уявлення текстів.

Глибина семантичного аналізу може бути різною, а в реальних системах найчастіше будується тільки синтаксико-семантичне уявлення тексту або окремих пропозицій. Частіше в проаналізованих роботах семантичний аналіз здійснюється одночасно з синтаксичним за допомогою механізму розширених мереж переходів. В іншому поверхневому семантичному аналізу передує етап синтаксичного аналізу, на основі якого будуються семантичні вузли і відносини між ними. В основу проекту ЕТАП-3 покладена модель мови "Сенс ↔ Текст", розроблена І.А. Мельчук, де на етапі семантичного аналізу визначаються лексичні функції на основі Толково-комбінаторного словника [18].

На рис. 1 зображена схема, що показує внутрішню структуру та організацію бази знань з семантичними зв'язками. Головними вузлами системи є слова, що є об'єктами або суб'єктами, в досліджуваній структурі. Навколо цього слова накопичується інформація на відстані двох слів. В свою чергу кожен елемент структури, як об'єкт, чи суб'єкт, дія, характеристика накопичує інформацію про себе, таку, як:

– морфологічні характеристики, основна інформація про слово, на основі якої визначаються наступні етапи, вказуючи характер, вид слова та його зв'язки;

– інші слова, що вказують на те ж саме, що й досліджуване слово. Це як синоніми, так і слова, які по своїй суті говорять про один і той же об'єкт, характеристику, дію. Наприклад українську владу можна характеризувати наступними словами: Київ, Верховна Рада України, президент України, українські політики та ін.;

– роль в структурі, як речення, так і тексту в цілому.

Кожна характеристика та параметр, слово володіє числовим значенням, що вказує на кількість повторень ситуації. Саме цим числовим значенням виділяється істинність роботи системи.

З кожним новим реченням, система оволодіває більшим масивом інформації, яка в подальшому використовується для оперативного та більш достовірного виконання завдання.

Система шукає у власній базі знань потрібний випадок. Якщо знаходиться один і більше, приймається рішення керуючись числовим значенням повторень ситуації, та морфологічними характеристиками.

На вході текст, при послівному переборі якого відбувається, спочатку послівне генерування інформації, за допомогою функції, яка вбирає методи морфологічного аналізу. По закінченню речення, на його основі генерується наступна інформація, за допомогою функції, яка вбирає методи синтаксичного аналізу. По завершенню тексту, інформація генерується та узагальнюється за допомогою функції семантичного аналізу.

Проаналізовано метод ймовірнісного синтаксичного аналізу та адаптовано його для комплексного фоносемантичного аналізу на основі побудови семантичних зв'язків. Розроблений метод семантичного аналізу текстової інформації. Метод включає доморфологічний аналіз та ймовірнісний синтаксичний аналіз, має три рівні: слово, речення, текст, на яких будує семантичні зв'язки, пов'язуючи смислові одиниці та виділяючи головні.

Фонетичний аналіз тексту. Вплив інформації на підсвідомість людини пропонується оцінювати на основі фонетичного аналізу текстових інформаційних ресурсів [17; 19–22]. Фонетичний аналіз тексту зводиться до розрахунку оцінки слова за 20-ма однополярними шкалами. Сама ж методика аналізу базується на тому, що людина звикла в розмовній мові до якоїсь частотності звуків і як встановили психологи, ми визначаємо цю частотність досить правильно.

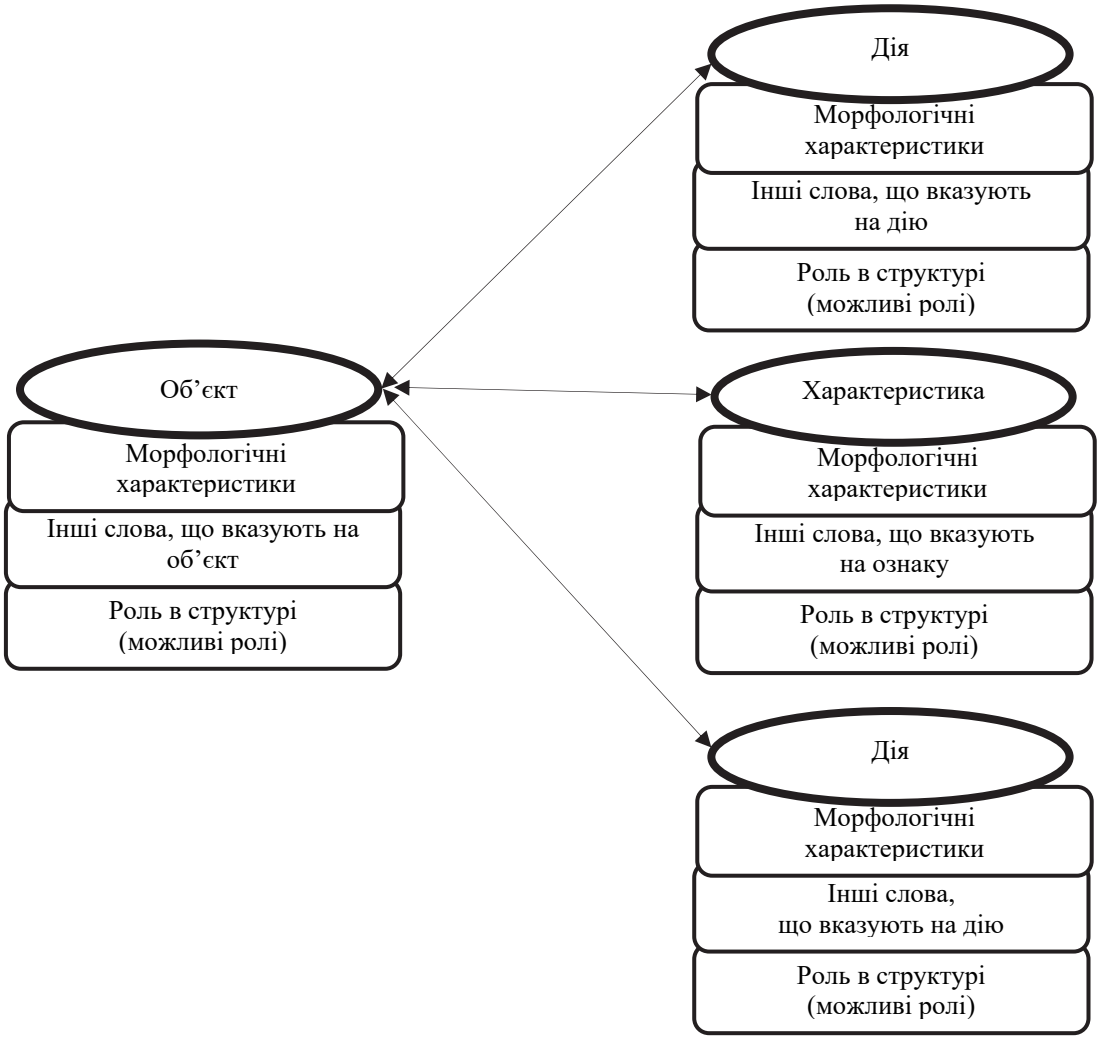

Рис. 1. Структура бази знань системи з семантичними зв'язками

Відповідно, будь-яке значне відхилення від цієї частотності має бути помічено підсвідомістю людини. Для аналізу роботи запропоновано на основі лінгвістичного процесору для виявлення сугестивної спрямованості інформаційних повідомлень на підсвідомість людини проведемо аналіз віршу Ліни Костенко "Крила".

Для аналізу сугестивної спрямованості тексту використовувався авторський колективний програмний засіб "Анализатор документов WordSD", який був орієнтований на аналіз лише російськомовних текстів. З метою аналізу українськомовних текстових документів в програмному засобі були адаптовані коефіцієнти для обрахунку фонетичних значень, які притаманні українській мові. Якщо прочитати вірш "Крила", то у читача складається приємні та піднесені враження , вирисовується яркий образ людини, яка має крила , та може подолати всі незгоди. Це вирисовується семантичної складової віршу та після прочитаного, читач залишається в гарному настрої. Запропонована технологія не здійснює оцінку семантичну складової текстів, текстів в явному вигляді, а лише здійснюється оцінка впливу текстової інформації на підсвідомість людини на основі звучання букв, слів та речень.

На рис. 2 наведено результати фонетичного аналізу віршу "Крила" за всіма 20-ти ознаковими фонетичними шкалами. З аналізу графіку видно, що крім ознак суворого та піднесеного тексту характерна ознака – яскравість, яка наближена до ознаки піднесеної.

До ознак, які можуть характеризувати вірш, наближаються ознаки сильний та прекрасний. Якщо проаналізувати результати, отримані читачами після читання віршу, які враховували семантичну складову та своє уявлення і почуття, та результати, що отримані на основі реалізації запропонованої технології, які враховують лише вплив на підсвідомість особистості без врахування семантичної складової, то можна зробити висновок, що результати збігаються. Це може говорити про те, що автор віршу Ліна Костенко намагалася підбором слів надати віршу відповідної окраси, та щоб у читача залишились враження, які він міг почути не лише в словах, а й душою, тобто на рівні підсвідомості.

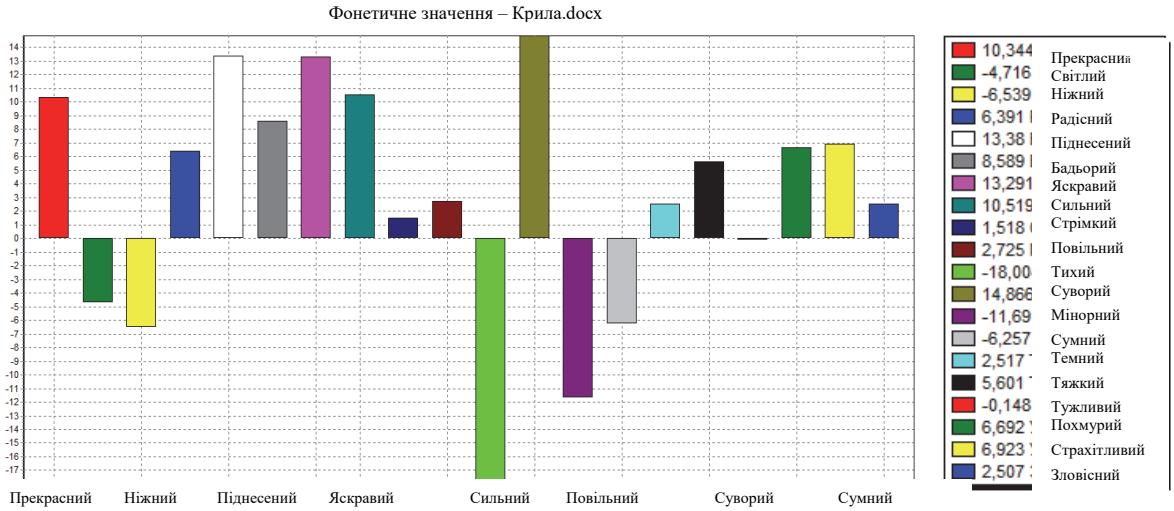

Рис. 2. Фонетична оцінка віршу “Крила” за 20-ю ознаковими шкалами

Висновки

Для вирішення задачі аналізу прихованого інформаційного впливу на підсвідомість особистості доцільно використовувати комплекс методів, які можуть бути поєднані в лінгвістичному процесорі, до якого доцільно включити методи, які здійснюють:

– морфологічний, синтаксичний та семантичний аналіз, які можуть використовуватись для розбору речень і текстів та виявлення головних слів та сенсу текстового повідомлення;

– методів, що виявляють сугестивний вплив на підсвідомість особистості.

До таких методів можна віднести методи фонетичного аналізу, аналізу на основі семантичного дефиренціалу, звукокольорового аналізу, тощо.

Для виявлення сугестивного впливу на підсвідомість особистості запропоновано використовувати метод фонетичного аналізу текстів, який був адаптований для україномовних текстів.

За допомогою запропонованого лінгвістичного процесору є можливість визначення в текстовому повідомленні головних слів, що характеризують текст, та визначити їх спрямованість щодо впливу на підсвідомість особистості.

Практичні дослідження показали працездатність запропонованого підходу для виявлення сугестивного деструктивного ІПсВ на підсвідомість військовослужбовців сектору оборони безпеки України та населення України.

Список літератури

1. Беликова Т.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 / Т.В. Беликова, В.В. Баранник. – Х.: Лідер. – 2017. – 455 с.

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

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

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

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

6. Теоретичні основи створення технологій протидії прихованим інформаційним атакам в сучасній гібридній війні / А.М. Алімпієв, В.В. Бараннік, Т.В. Белікова, С.О. Сідченко // Системи обробки інформації. – 2017. – № 4(150). – С. 113-121. https://doi.org/10.30748/soi.2017.150.24.

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

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

9. Method of Increasing the Capacity of Information Threat Detection Filters in Modern Information and Communication

Systems on Advanced Information and Communication Technologies / T. Belikova, O. Dovbenko, A. Lekakh, O. Dodukh // 3nd IEEE International Conference, Proceedings. – Lviv, July 2019. – P. 188-192.

10. Основы информационной безопасности / Є.Б. Бєлов, В.П. Лось, Р.В. Мещеряков, О.О. Шелупанов. – М.: Горячая линия-Телеком, 2006. – 544 с.

11. Біла книга – 2018. Збройні Сили України. – К.: Військо України, 2019. – 172 с.

12. Бобров А. Информационная война: от листовки до твиттера / А. Бобров // Зарубежное военное обозрение, 2013. – № 1. – С. 20-27.

13. Богданович В.Ю. Теоретичні основи забезпечення національної безпеки України в умовах позаблоковості: монографія / В.Ю. Богданович, І.С. Романченко, І.Ю. Свида. – Львів: АСВ, 2011. – 414 с.

14. Бурячок В.Л. Стратегія оцінювання рівня захищеності держави від ризику стороннього кібернетичного впливу / В.Л. Бурячок, О.Г. Корченко, В.О. Хорошко // Захист інформації. – 2013. – № 1(15). – С. 5-14.

15. Бурячок В.Л. Завдання, форми та способи ведення воєн у кібернетичному просторі / В.Л. Бурячок, Г.М. Гулак, В.О. Хорошко // Наука і оборона. – 2011. – № 3. – С. 35-42.

16. Бурячок В.Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби / В.Л. Бурячок. – К.: ДУТ. – 2015. – 228 с.

17. Герасимов Б.М. Извлечение информационных фраз из первичных электронных документов в информационно-поисковых системах / Б.М. Герасимов, О.Ю. Сергеев, И.Ю. Субач // Управляющие системы и машины. – 2006. – № 1. – С. 26-29.

18. Деркаченко Я. Інформаційно-психологічні операції як сучасний інструмент геополітики [Електронний ресурс] / Я. Деркаченко // Глобальна організація союзницького лідерства. – 2016. – Режим доступу: http://goal-int.org/informacijno-psixologichni-operacii-yak-suchasnij-instrument-geopolitiki/.

19. Ліпкан В.А. Інформаційна безпека України в умовах євроінтеграції / В.А. Ліпкан, Ю.Є. Максименко, В.М. Желіховський. – К.: КНТ, 2006. – 206 с.

20. Мороз Ю. Інформаційно-психологічні операції в умовах гібридної війни / Ю. Мороз, Ю. Твердохліб // Вісник Львівського університету. – 2016. – № 38. – С. 97-105.

21. Руснак І.С. Розвиток форм і способів ведення інформаційної боротьби на сучасному етапі / І.С. Руснак, В.М. Телелим // Наука і оборона. – 2000. – № 2. – С. 18 – 23.

22. Руснак І.С. До забезпечення воєнної безпеки в умовах загрози інформаційної війни / І.С. Руснак, М.О. Попов, А.Г. Лук'янець // Наука і оборона. – 1999. – № 2. – С. 37-43.

References

1. Belikova, T.V. and Barannik, V.V. (2017), "*Metody vyyavleniya suggestivnyh vozdejstvij na podsoznanie cheloveka v tekstovyh soobshcheniyah v usloviyah informacionno-psihologicheskogo protivoborstva. Naukoemkie tekhnologii v infokommunikaciyah: obrabotka informacii, kiberbezopasnost', informacionnaya bor'ba*" [*Methods for detecting suggestive effects on the subconscious of a person in text messages in conditions of information and psychological confrontation. High-tech technologies in infocommunications: information processing, cybersecurity, information fight*], Lider, Kharkiv, pp. 435-455.

2. Saprykina, T.V., Sidchenko, S.A. and Shkolarenko, V.A. (2013), "Informacionnaya tekhnologiya testirovaniya semanticheskoj sostavlyayushchej dlya vyyavleniya suggestivnogo vozdejstviya metodom foneticheskogo analiza nakopitel'nym itogom" [Information technology testing of semantic component for detection of suggestive influence by phonetic analysis by cumulative result], *Automated Control Systems and Automation Devices*, No. 165, pp. 111-117.

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

4. Belikova, T.V. (2017), [Methods for detecting destructive suggestive information-psychological operations in the information-social space], *Radio Electronics and Informatics*, No. 2, pp. 45-50.

5. Belikova, T.V. (2017), The Technology Of Suggestive Information-Psychological Operations Masking in the info-communication Space, *Science-Based Technologies*, No. 3, pp. 21-26.

6. Alimpiiev, A.M., Barannik, V.V., Belikova, T.V. and Sidchenko, S.O. (2017), "Teoretychni osnovy stvorennia tekhnolohii protydii prykhovanym informatsiinym atakam v suchasnii hibrydnii viini" [Theoretical foundations of the establishment of the technologies of co-operation to the hidden information attacks in the modern hybrid war], *Information Processing Systems*, No. 4(150), pp. 113-121. https://doi.org/10.30748/soi.2017.150.24.

7. Barannik, V.V., Belikova, T.V. and Dovbenko, O.V. (2018), "Metodi viyavlennya prihovanih informacijno-psihologichnih dij v informacijnomu prostori" [Methods for detecting hidden information-psychological actions in the information space], *Technology-intensive*, No. 3, pp. 24-30.

8. Barannik, VV, Belikova, T.V., Kapko, M.O. and Gurzhi, I.A. (2019), "Kompleksnij metod avtomatichnogo fonosemantichnogo analizu tekstovoy informaciy na osnovi ocinki vagomih semantichnih odinic' v umovah informacijnogo protiborstva" [A complex method of automatic phonosemantic analysis of textual information based on the evaluation of significant semantic units in conditions of information confrontation], *Kibersecurity, Education, Science, Technology*, No. 1(1), pp. 13-22.

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

10. Belov, E.B., Los, V.P., Mescheryakov, R.V. and Shelupanov, O.O. (2006), "*Osnovy informacionnoj bezopasnosti*" [*Fundamentals of information security*], Hotline Telecom, Moscow, 544 p.

11. (2019), "*Bila kniga – 2018, Zbrojni Sili Ukrayni*" [*White Book – 2018, Armed Forces of Ukraine*], Armed of Ukraine, Kyiv, 172 p.

12. Bobrov, A. (2013), "Informacionnaya vojna: ot listovki do tvittera" [Information warfare: from leaflets to twitter], *Foreign Military Observation*, No. 1, pp. 20-27.

13. Bogdanovich, V.Yu., Romanchenko, I.S. and Svida, I.Yu. (2011), "*Teoretichni osnovi zabezpechennya nacional'noj bezpeki Ukraini v umovah pozablokovosti*" [*Theoretical bases of national security of Ukraine under non-aligned conditions*], ACS, Lviv, 414 p.

14. Buryachok, V.L., Korchenko, O.G. and Khoroshko, V.A. (2013), "Strategiya ocinyuvannya rivnya zahishchenosti derzhavi vid riziku storonn'ogo kibernetichnogo vplivu" [A strategy for assessing the state's level of protection against the risk of cybernetic exposure], *Protection of Information*. No. 1(15), pp. 5-14.

15. Buryachok, V.L., Gulak, G.M. and Khoroshko, V. (2011), "Zavdannya, formi ta sposobi vedennya vojn u kibernetichnomu prostori" [Tasks, forms and ways of waging war in cyberspace], *Science and Defense*, No. 3, pp. 35-42.

16. Buryachok, V.L. (2015), "*Informacijnij ta kiberprostori: problemi bezpeki, metodi ta zasobi borot'bi*" [*Information and cyberspace: security issues, methods and means of combat*], DUT, Kyiv, 228 p.

17. Gerasimov, B.M., Sergeev, O.J. and Subach, I.Y. (2006), "Izvlechenie informacionnyh fraz iz pervichnyh elektronnyh dokumentov v informacionno-poiskovyh sistemah" [Extraction of information phrases from primary electronic documents in information retrieval systems], *Control Systems and Machines*, No. 1, pp. 26-29.

18. Derkachenko, J. (2016), "Informacijno-psihologichni operaciy yak suchasnij instrument geopolitiki" [Information-psychological operations as a modern tool of geopolitics], *Global Allied Leadership Organization*, available at: www.goal-int.org/information-psixologichni-operacii-yak-suchasnij-instrument-geopolitiki/.

19. Lipkan, V.A., Maksimenko, Yu. E., and Zhelikhovsky, V.M. (2006), "*Informacijna bezpeka Ukrayni v umovah yevrointegraciy*" [*Information security of Ukraine in the context of European integration*], KNT, Kyiv, 206 p.

20. Moroz, Y. and Tverdokhlib, Y. (2016), [Information-psychological operations in the conditions of hybrid war. Bulletin of the University of Lviv], *Science and Defense*, No. 38, pp. 97-105.

21. Rusnak, I.S. and Telelim, V.M. (2000), "Rozvitok form i sposobiv vedennya informacijnoy borot'bi na suchasnomu etapi" [Development of forms and ways of conducting information struggle at the present stage], *Science and Defense*, No. 2, pp. 18-23.

22. Rusnak, I.S., Popov, M.O. and Lukyanets, A.G. (1999), "Do zabezpechennya voennoj bezpeki v umovah zagrozi informacijnoj vijni" [Towards ensuring military security in the face of the threat of an information war], *Science and Defense*, No. 2, pp. 37-43.

Надійшла до редколегії 06.09.2019
Схвалена до друку 15.10.2019

Відомості про авторів:

Бараннік Володимир Вікторович
доктор технічних наук професор
начальник кафедри
Харківського національного університету
Повітряних Сил ім. І. Кожедуба,
Харків, Україна
https://orcid.org/0000-0002-2848-4524

Сідченко Сергій Олександрович
кандидат технічних наук
докторант Харківського національного
університету Повітряних Сил ім. І. Кожедуба,
Харків, Україна
https://orcid.org/0000-0002-1319-6263

Белікова Тетяна Вячеславівна
здобувач
Черкаського державного
технологічного університету,
Черкаси, Україна
https://orcid.org/ 0000-0001-8178-6903

Олійник Юлія Олександрівна
курсант
Харківського національного
університету Повітряних Сил ім. І. Кожедуба,
Харків, Україна
https://orcid.org/0000-0001-6119-1005

Information about the authors:

Volodymyr Barannik
Doctor of Technical Sciences Professor
Head of Department
of Ivan Kozhedub Kharkiv
National Air Force University,
Kharkiv, Ukraine
https://orcid.org/0000-0002-2848-4524

Serhii Sidchenko
Candidate of Technical Sciences
Doctoral Student of Ivan Kozhedub Kharkiv
National Air Force University,
Kharkiv, Ukraine
https://orcid.org/0000-0002-1319-6263

Tatyana Belikova
PhD student
of Cherkasy State
Technological University,
Cherkasy, Ukraine
https://orcid.org/ 0000-0001-8178-6903

Yulia Oliynuk
Cadet
of Kharkiv National
Air Force University Ivan Kozhedub,
Kharkiv, Ukraine
https://orcid.org/0000-0001-6119-1005

МЕТОДЫ ВЫЯВЛЕНИЯ ДЕСТРУКТИВНО ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОГО ВОЗДЕЙСТВИЯ НА ПОДСОЗНАНИЕ ЛИЧНОГО СОСТАВА И НАСЕЛЕНИЯ УКРАИНЫ

В.В. Баранник, С.А. Сидченко, Т.В. Беликова, Ю.О. Олейник

В статье представлены результаты анализа метода выявления деструктивных информационно-психологических воздействий в электронных СМИ на подсознание и сознание личного состава вооруженных формирований сектора обороны и безопасности Украины и населения Украины. Определено, что предлагаемый метод лингвистического процессора представляет собой возможность определения в текстовом сообщении главных слов, характеризующих текст, и определить их направленность относительно влияния на подсознание личности. Проведённые практические исследования показали работоспособность данного метода для выявления суггестивного деструктивного ИПВ на подсознание военнослужащих сектора обороны безопасности Украины и населения Украины.

Ключевые слова: *информационно-психологическое воздействие, СМИ, лингвистический процессор, структура базы знаний.*

METHODS FOR IDENTIFYING DESTRUCTIVE INFORMATION-PSYCHOLOGICAL IMPACTS ON UNDERSTANDING PERSONAL COMPOSITION AND POPULATION OF UKRAINE

V. Barannik, S. Sidchenko, T. Belikova, Yu. Oliynuk

The article presents the results of the analysis of the method of detecting destructive information and psychological influences in the electronic media on the subconscious and consciousness of the personnel of the armed forces of the defense and security sector of Ukraine and the population of Ukraine. To solve the problem of hidden information influence on the subconscious personality, it is proposed to use a set of methods that can be combined in a linguistic processor, which should include methods that perform: morphological, syntactic and semantic analysis that can be used to parse sentences and texts and identification of the main words and meaning of the text message; methods that have a suggestive effect on the subconscious personality. Such methods include methods of phonetic analysis, analysis based on semantic defiance, sound-color analysis, etc. To identify the suggestive influence on the subconscious personality, it is proposed to use a method of phonetic text analysis, which was adapted for Ukrainian-language texts. With the help of the proposed linguistic processor it is possible to identify in the text message the main words that characterize the text and to determine their orientation in influencing the subconscious personality. Practical studies have demonstrated the feasibility of the proposed approach for detecting suggestive destructive STIs on the subconscious of military personnel in the defense sector of Ukraine and the population of Ukraine.

Keywords: *information-psychological impact, media, linguistic processor, structure of the knowledge base.*