УДК 004:316.472.4
DOI: 10.31866/2617-796x.2.2018.155667

Войтович Олеся,
кандидат технічних наук, доцент,
Вінницький національний технічний університет,
Вінниця, Україна
nika.ostrovska21@gmail.com
https://orcid.org/0000-0001-8964-7000

Островська Вероніка,
магістр факультету інформаційних технологій
та комп'ютерної інженерії,
Вінницький національний технічний університет,
Вінниця, Україна
nika.ostrovska21@gmail.com
https://orcid.org/0000-0002-2374-1501

Закалов Ігор,
генеральний директор Main Academy,
Київ, Україна
zakalov@mainacad.com
https://orcid.org/0000-0001-8892-6120

ВИЯВЛЕННЯ НЕГАТИВНИХ ВПЛИВІВ У СОЦІАЛЬНИХ ІНТЕРНЕТ-СЕРВІСАХ

Беручи до уваги останні події в нашій країні, можна стверджувати, що мережа Інтернет поступово стала джерелом загроз інформаційній безпеці людини, суспільства, держави, оскільки поширення у глобальній мережі сумнівного та необ'єктивного контенту разом із технологіями інформаційно-психологічного впливу на свідомість індивідів може сприяти виникненню у суспільстві невдоволення діючою державною владою, міжнаціональних конфліктів, соціальної агресії тощо

Метою дослідження є огляд методів орієнтованих на підвищення достовірності виявлення негативних інформаційно-психологічних впливів у соціальних інтернет-сервісах шляхом здійснення автоматизованого аналізу текстового контенту.

Методи дослідження. В ході дослідження використовувалися методи теорії аналізу соціальних мереж (Social Network Analysis, SNA), методи обробки природної мови (Natural Language Processing, NLP), методи машинного навчання (Machine Learning), в тому числі глибокого навчання (Deep Learning).

Наукова новизна одержаних результатів полягає в тому, що в роботі вперше запропоновано метод застосування моделей глибокого навчання до задачі аналізу тональності текстових даних, який відрізняється від існуючих своєю структурою, що дозволяє підвищити точність виявлення інформаційно-психологічних впливів у контенті соціальних мереж.

Висновки. Результати дослідження можуть бути використані при подальшій розробці засобів автоматизованого виявлення негативних інформаційно-психологічних впливів.

Ключові слова: аналіз даних; нейронні мережі; машинне навчання; глибоке навчання; аналіз даних; інтернет; соціальні мережі; соціальні інтернет-сервіси.

Вступ. Розвиток інформаційно-комунікаційних технологій в умовах глобалізації призводить до того, що в сучасних міждержавних конфліктах все частіше застосовуються методи, що ґрунтуються на комплексному використанні політичних, економічних, інформаційних та інших невійськових заходів, реалізованих з опорою на військову силу. Це так звані «гібридні» методи, що дають змогу досягти політичних цілей конфлікту з мінімальним військово-силовим впливом на противника.

Одним із найяскравіших проявів інформаційно-психологічного впливу за допомогою інформаційно-психологічних операцій, є тролінг (англ. Trolling – «виспівування») – процес розміщення в Інтернеті провокаційних повідомлень з метою посилення соціальної напруги шляхом порушення правил етичних норм комунікації в мережі Інтернет (Кокарча, 2016).

Навіть простий користувач Інтернету здатний легко відслідкувати тролінг. Але набагато важче простежити чітку межу між випадковою і несвідомою маніпуляцією та свідомою і навмисною маніпуляцією. Великі об'єми інформації ускладнюють процес виявлення тролінгу вручну, адже на це необхідно багато часу та зусиль. Таким чином, актуальним у сфері наукових досліджень технологій маніпулятивного впливу на учасників спілкування у соціальних мережах є автоматизоване виявлення тролінгу.

Проаналізувавши роботи А. Манойла (2003), О. Литвиненка (2003), Г. Почепцова (2001), О. Поляруша (2008), С. Расторгуєва (1999) можна стверджувати, що нині ще немає однозначного тлумачення поняття інформаційно-психологічного впливу і його найпоширеніших форм. Деякі дослідження Д. Ланде (Ланде та Фурашев, 2009) присвячені пошукам алгоритмів автоматизованого оброблення матеріалів засобів масової інформації для виявлення інформаційних операцій, війн, однак без їхньої практичної реалізації. В свою чергу, запропоновані В. Панченко та В. Полевим (2011) в публікаціях підходи до виявлення інформаційно-психологічних впливів у віртуальних спільнотах носять описовий характер, автори не наводять методику їх реалізації.

Здійснений аналіз показав, що на сучасному етапі проблемі визначення інформаційно-психологічних впливів в соціальних мережах приділено неналежну увагу. Тому можна стверджувати, що розробка методу і засобу виявлення інформаційно-психологічних впливів є актуальною задачею.

Результати дослідження. Сучасні війни – це гібридні війни, у яких основним засобом досягнення політичних цілей є інформаційна зброя. Інформаційна складова гібридної війни реалізується у вигляді інформаційно-психологічного впливу – цілеспрямованого виробництва і розповсюдження спеціальної інформації, для безпосереднього впливу (позитивного або негативного) на функціонування і розвиток інформаційно-психологічного середовища суспільства, психіку і поведінку населення, керівництва держави, військових (Саєнко, 2015).

Інформаційно-психологічний вплив маніпулятивного характеру, здійснюваний в інтересах людини або груп людей по відношенню до інших, є специфічною формою управління, яка носить небезпечний характер у випадках, коли воно здійснюється таємно, приносить односторонні вигоди його організаторам. В якості найважливішого джерела небезпек такого роду, що діє постійно і все більш активно і потужно, виступають держави, які ведуть масові психологічні операції проти населення або окремих соціальних груп іншої країни, обраної в якості їх об'єкта впливу.

Основною метою інформаційно-психологічного впливу є зміна установок особистості. Інформаційно-психологічний вплив на емоційну сферу свідомості включає нецілеспрямоване сприйняття та запам’ятовування, характеризується низьким рівнем усвідомлення змісту впливу. Усе, що сьогодні у ході гібридної війни поширюється російськими засобами масової інформації на території України, зокрема у східних областях, є відкритим спотворенням картини дійсності. Механізм інформаційно-психологічного впливу заснований на маніпуляції свідомістю мас шляхом внесення у свідомість дезінформації.

Маніпулювання містить ряд компонентів: подачу часто грубо сфабрикованої інформації; навмисне приховування істинної інформації; забезпечення інформаційного перевантаження, що ускладнює людині можливість розібратися в дійсному стані справи. Таким чином, соціально-політична та безпекова ситуація в Україні загалом та в її окремих територіях штучно розхитується до небезпечного рівня.

Деструктивний інформаційно-психологічний вплив досягається шляхом проведення інформаційно-психологічних операцій. У своїй праці «Операции информационно-психологической войны» автори В. Вепрінцев, А. Манойло, А. Петренко та Д. Фролов (2005) визначають інформаційно-психологічну операцію як комплекс узгоджених та взаємопов’язаних заходів маніпулювання інформацією, що здійснюють за загальним планом з метою досягнення та утримання переваги через вплив на інформаційні процеси в системах противника.

Для досягнення поставлених цілей використовується майже повний спектр каналів комунікацій – традиційні та електронні засоби масової інформації. Найактивніше застосовуються телебачення, Інтернет і соціальні мережі. При цьому використовуються всі методи інформаційно-психологічної боротьби – від спотворення фактів до неприхованої брехні («фейку»).

В гібридних війнах соціальні мережі виступають в якості збройних засобів. З точки зору інформаційних загроз небезпечною є діяльність тролів, які є безпосередніми учасниками інтернет-спілкування та мають завдання щодо провокування та розповсюдження конфлікту, в тому числі шляхом приниження або образи почуттів інших співрозмовників.

Таким чином, соціальні інтернет-сервіси є ефективним засобом впливу на суспільні й політичні процеси у державі. Тому забезпечення виявлення

негативних інформаційно-психологічних впливів у соціальних інтернет-сервісах в умовах глобалізації інформаційного простору і гібридизації військових конфліктів залишається однією із нагальних проблем, які потребують свого вирішення.

Ринок ПЗ в Україні характеризується таким чином: 90% – ПЗ західних фірм, 10% – українські розробки. На українському ринку присутні більше ніж 200 фірм, які так чи інакше пов'язані з виробництвом програмних продуктів. Однак більш половини цих компаній займаються дистрибуцією програмних продуктів іноземних виробників.

За результатами даних моніторингу стану забезпечення органів державної влади програмним забезпеченням в органах державної влади використовується більше 1700 тис. примірників комп'ютерних програм.

За даними проведеного онлайн опитування обліку програмних продуктів, що використовуються в органах виконавчої влади було отримано відомості від 60 % від загальної кількості центральних органів виконавчої влади, що становить більше 1200 тис. примірників комп'ютерних програм. Для аналізу було використано дані від органів державної влади, які використовують більше 1100 тис. примірників комп'ютерних програм та від обласних державних адміністрацій – більше 60 тис. примірників.

До програмних засобів інформаційної безпеки, що використовуються в роботі органів державної влади належать Putty, Comodo, Symantec, Гриф. Тобто, можна зробити висновок, що органи державної влади не використовують програми для аналізу даних великого обсягу у задачах кібербезпеки. На вітчизняному ринку присутнє програмне забезпечення для аналізу даних великого обсягу, але воно призначене для формування звітів, в яких відображаються думки споживачів, клієнтів і конкурентів про різні бренди. Існуючі програми для аналізу тональності тексту не використовуються в задачах кібербезпеки.

Аналіз текстових даних із соціальних мереж в Інтернеті через величезний потік інформації не може здійснюватися вручну. Процес відбувається автоматизовано, з використанням спеціальних сервісів або програмного забезпечення – як платного, так і безкоштовного.

Технології обробки природної мови вже не можна назвати новими. Вже є вироблені методики синтаксичного і семантичного аналізу текстів, існують і модулі вирішення певних завдань в цій сфері. І, звичайно, провідні технологічні компанії, такі як IBM, Microsoft, Google, Apple, Facebook, Yandex та інші активно розвивають API-сервіси і застосовують natural language processing в своїх власних проектах. Однак, названі компанії є закордонними, вітчизняні компанії майже не розвивають дані технології (http://pa.stateandregions.zp.ua).

Повідомлення, що використовуються для здійснення інформаційно-психологічного впливу, містять обов'язкове емоційне забарвлення для інформування і стимулювання певних емоцій об'єкта з метою регулювання його

цілеспрямованої поведінки. Тому для виявлення інформаційно-психологічних впливів необхідно використовувати програми для аналізу емоційного забарвлення повідомлень. У таблиці 1 наведена порівняльна характеристика основних програм для аналізу тональності тексту.

Таблиця 1

Порівняльна характеристика програм для аналізу тональності тексту

Назва	**Метод**	**Мова**	**Ліцензія**	**Платформа**
Sentiment140	Машинне навчання	Англійська, іспанська	Комерційна	Веб-сервіс
TextBlob	Машинне навчання	Англійська	MIT	Python
Eureka Engine	Машинне навчання	Російська	Комерційна	Веб-сервіс
RCO	Правила	Російська	Комерційна	Windows
Russian SentimentAnalyzer	Правила	Російська	Комерційна	JSON API / Java & .NET SDK
DictaScope	Правила	Російська	Комерційна	FreeBSD, Windows
Pattern	Правила, регулярні вирази	Англійська, іспанська, німецька, французька	BSD	Python

Як видно з таблиці 1, більшість програмних засобів є комерційними. Також майже половина існуючих програмних рішень розроблена переважно для англійської та інших мов. Більшість з них націлені на відслідковування думок про товари, послуги, бренди і персон. А решта аналізують дані лише окремими реченнями. Тому необхідність дослідження за темою роботи визначається тим, що в світі поки що не існує доступних систем автоматичної оцінки тональності текстів російською мовою з метою виявлення в них інформаційно-психологічних впливів.

На сучасному етапі значну роль в процесах комунікації суспільства відіграють соціальні інтернет-сервіси, які забезпечують учасників віртуальних спільнот – індивідів, новітніми засобами взаємодії (Грищук та Данник, 2016). Соціальні інтернет-сервіси все активніше і масштабніше використовують у власних інтересах засоби інформаційно-психологічного впливу. Вони надають широкі можливості щодо впливу на формування громадської думки з багатьох актуальних питань, прийняття політичних, економічних і військових рішень, впливу на інформаційні ресурси противника і поширення спеціально підготовленої інформації (дезінформації) (Гриценко та Прокофьєва-Янчиленко, 2012). Внаслідок широкої популярності віртуальні спільноти стали ефективним засобом проведення інформаційних операцій проти людини, суспільства,

держави. Процеси в соціальних мережах викликають підвищений інтерес в науці, однак темпи теоретичних досліджень істотно відстають від темпів розвитку соціальних мереж.

Для виявлення ознак інформаційно-психологічних впливів використовуються методи, загальна назва яких – «аналіз емоційного забарвлення тексту». Термін «аналіз емоційного забарвлення тексту» використовується в роботі як переклад оригінального терміна «sentiment analysis», який часто так само перекладається, як «аналіз тональності тексту». Аналіз емоційного забарвлення тексту – завдання автоматичного аналізу думок і емоційно забарвленої лексики, що виражені в тексті.

Підходи, які застосовуються для аналізу тональності текстової інформації природною мовою, поділяють на дві основні групи: інженерно-лінгвістичні методи і методи на основі машинного навчання. Інженерно-лінгвістичні методи використовують спеціальні, попередньо підготовлені експертами-лінгвістами тональні словники і (або) лінгвістичні правила, на основі яких відбувається аналіз текстового фрагмента (Большакова, Воронцов, Ефремова, Клышинский, Лукашевич и Сапин, 2017.). Методи машинного навчання, список яких включає в себе (але не обмежується) метод Байєсової (наївної) класифікації, метод опорних векторів, метод k-найближчого сусіда, регресію. Також до даної групи відносяться і нейромережеві методи. Ця група методів використовує математичні моделі, що дозволяють автоматично визначити оптимальний набір параметрів для вирішення конкретної задачі, в даному випадку – визначення тональності. Варто відзначити наявність комбінованих (гібридних) методів, що включають в себе як інженерно-лінгвістичні елементи, так і машинне навчання.

Нині багато досліджень, що стосуються класифікації текстів і різного контенту, сходяться на думці, що лідерство належить технологіям, які мають в основі нейромережеві технології і машинне навчання (Ильвовский и Черняк, 2017). Ці методи здатні здійснювати автоматичну обробку текстів на природній мові, виявляючи зв'язки між словами і категорію, до якої вони можуть належати. Дані методи здатні знизити трудомісткість класифікації текстів та підвищити якість рішення багатьох завдань такого типу, зменшуючи кількість помилок в роботі і труднощі, що випливають з продуктивності систем. Розглядаючи нейромережеві методи машинного навчання, необхідно згадати, що кожен метод з даного класу в свою чергу теж має свої особливості.

У підході, що заснований на словниках, кожному окремому слову в словнику присвоюється значення тональності (шкали визначаються заздалегідь). Для отримання підсумкового значення тональності часто використовують простий спосіб: обчислюють середнє арифметичне або суму значень тональності всіх слів з документа. Більш складний спосіб – навчання класифікатора (наприклад, нейронної мережі). Перевагою є простота у застосуванні. Недоліки: метод не універсальний, для нової предметної області потрібно складання нового словника.

Підхід, заснований на правилах, полягає в застосуванні правил, які складаються експертами на основі аналізу предметної області. Приклад такого правила: якщо текст містить один або кілька позитивних прикметників з набору {«веселий», «смішний», «добрий»…} і не містить прикметників {«поганий», «нудний», «страшний»…}, то текст відноситься до позитивного класу тональності. Розглянемо ще один приклад: слово «сліпучий» в більшості випадків зустрічається як позитивна характеристика, але в реченні: «Сніг на сонці був настільки сліпучим, що я вже нічого навколо не бачив» – є негативною характеристикою, так як вживається в значенні «засліплював». Перевагою є те, що даний підхід може давати хороші результати при великому наборі правил. Недоліки: складання великого набору правил – дуже трудомісткий процес, дуже часто правила прив'язуються до певної тематичної області. Цей підхід не дуже підходить для аналізу мікроблогів через «зашумленість» даних, обумовленою наявністю помилок (https://www.hse.ru/data/2017).

Найбільш поширеним підходом є машинне навчання з учителем. Спочатку на заздалегідь розмічених текстах навчається машинний класифікатор, а потім отримана модель використовується при аналізі нових текстів. Короткий алгоритм (http://machinelearningmastery.com):

Недоліком є те, що необхідна розмічена колекція текстів (розмітка є вельми трудомістким процесом).

Машинне навчання без вчителя спрямоване на виявлення внутрішніх взаємозв'язків, залежностей, закономірностей, що існують між об'єктами. Для тренування алгоритму використовується навчальна вибірка, що складається з текстів, класи яких заздалегідь невідомі (або відомі, але ця інформація не використовується алгоритмом). Перевагою є те, що не потрібна розмічена колекція документів. Недоліком є низька точність, в порівнянні з навчанням з учителем.

Для класифікації текстів за допомогою машинного навчання з учителем існують кілька відомих алгоритмів:

- наївний класифікатор Байєса;
- метод k-найближчих сусідів;
- метод опорних векторів;
- метод логістичної регресії.

Для автоматичного визначення емоційного забарвлення контенту соціальних мереж можна окремо слід виділити штучні нейронні мережі.

Висновки. Дослідження методів автоматичного аналізу настроїв в соціальних мережах показало, що найбільш придатними для виявлення у текстах інформаційно-психологічних впливів є нейронні мережі, оскільки вони не потребують складання словників, обов’язкової попередньої лінгвістичної обробки текстів, можуть застосовуватися до різних типів даних та здатні здійснювати класифікацію за декількома категоріями, що дозволить виявляти різні типи інформаційно-психологічних впливів.

Також для поставленої задачі можна використовувати інженерно-лінгвістичні методи, метод опорних векторів, дерева прийняття рішень та наївний класифікатор Байєса. Недоліком методу опорних векторів є те, що він здійснює бінарну класифікацію, яка дозволить розподілити дані тільки за двома категоріями: дані без інформаційно-психологічних впливів та дані з інформаційно-психологічними впливами. Основний недолік наївного класифікатора Байєса – неможливість врахування залежності результату від комбінації слів. Спільним недоліком інженерно-лінгвістичних методів та наївного класифікатора Байєса є необхідність складання словників, що вимагає тісної співпраці з лінгвістами.

Однак, слід зазначити, що жоден із методів автоматичної класифікації тексту не може дати беззаперечних результатів. Помилки даних методів пояснюються наступними проблемами: орфографічними помилками у тексті, відсутністю зв'язків у тексті. Для підвищення якості роботи класифікаторів треба забезпечувати автоматичне виправлення орфографічних помилок, вдосконалювати словники і навчальні вибірки.

Список посилань

Большакова, Е.И., Воронцов, К.В., Ефремова, Н.Э., Клышинский, Э.С., Лукашевич, Н.В. и Сапин А.С., 2017. *Автоматическая обработка текстов и анализ даннях*. [online] Доступно: <https://www.hse.ru/data/ 2017/08/12/1174382135/NLP_and_DA.pdf> [Дата обращения 16 ноября 2018].

Вепринцев, В., Манойло, А., Петренко, А. и Фролов Д., 2005. *Операции информационно-психологической войны* [online] Доступно: <https://psyfactor.org/psyops/psyops4.htm> [Дата обращения 16 ноября 2018].

Горбулін, В.П., Додонов, О.Г. та Ланде, Д.В., 2009. *Інформаційні операції та безпека суспільства: загрози, протидія, моделювання.* Київ: Інтертехнологія.

Гриненко, І. та Прокофьєва-Янчиленко, Д., 2012. Вплив віртуальних спільнот на інформаційну безпеку: сучасний стан та тенденції розвитку. *Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні*, 1, с.18-23.

Грищук, Р.В. та Даника, Ю.Г., 2016. *Основи кібернетичної безпеки.* Житомир: Житомирський національний агроекологічний університет.

Ильвовский, Д. и Черняк, Е., 2017. *Глубинное обучение для автоматической обработки текстов.* [online] Доступно: <https://www.osp.ru/os/2017/02/13052221> [Дата обращения 16 ноября 2018].

Кокарча, Ю.А., 2016. Тролінг як засіб політичної маніпуляції в Інтернет-просторі. *Науковий часопис НПУ імені М. П. Драгоманова. Серія 22 : Політичні науки та методика викладання соціально-політичних дисциплін*, 20. [online] Доступно: <http://enpuir.npu.edu.ua/bitstream/ 123456789/17544/1/Kokarcha.pdf> [Дата звернення 16 листопада 2018].

Концепція Big Data в Україні: перспективи застосування в державних органах. [online] Доступно: <http://pa.stateandregions.zp.ua/archive/ 4_2017/19.pdf> [Дата звернення 16 листопада 2018].

Ланде, Д. та Фурашев, В., 2009. Інформаційні операції крізь призму системи моніторингу та інтеграції інтернет-ресурсів. *Правова інформатика,* 2 (22), с.49-57.
Литвиненко, О.В., 2003. *Інформаційні впливи та операції: Теоретико-аналітичні нариси.* Київ.
Манойло, А.В., 2003. *Государственная информационная политика в особых условиях.* Москва: МИФИ.
Панченко, В.М., 2009. Лінгвостатистичні ознаки маніпулювання суспільною свідомістю в засобах масової комунікації. *Сучасні інформаційні технології у сфері безпеки та оборони*, 1 (4), с.81-85.
Панченко, В.М. та Полевий, В.І., 2011. Методика виявлення ознак інформаційного впливу в засобах масової інформації. *Інформаційна безпека людини, суспільства, держави*, 3 (7), с.70-77.
Поляруш, О.О. та Тарасенко, О.Є., 2008. Парадигма інформаційних впливів в перехідних політичних системах. *Сучасні технології у сфері безпеки та оборони*, 3, с.81-85.
Почепцов, Г.Г., 2001. *Информационные войны*. Москва: Рефл-бук.
Расторгуев, С.П., 1999. *Информационная война*. Москва: Радио и связь.
Саєнко, О., 2015. Механізм інформаційно-психологічного впливу в умовах гібридної війни. *Вісник Національної академії Державної прикордонної служби України. Серія: Психологія,* [online] 1, Доступно: <http://nbuv.gov.ua/UJRN/Vnadpn_2015_1_11 > [Дата звернення 16 листопада 2018].
Brownlee, J., 2016. Supervised and Unsupervised Machine Learning Algorithms. In. *Machine Learning Mastery*. [online] Available at: <http://machinelearningmastery.com/supervised-and-unsupervised-machinelearning-algorithms> [Accessed 16 November 2018].

References

Bolshakova, E.I., Vorontcov, K.V., Efremova, N.E., Klyshinskii, E.S., Lukashevich, N.V. and Sapin A.S., 2017. *Avtomaticheskaya obrabotka tekstov i analiz dannyakh* [Automatic text processing and data analysis]. [online] Available at: <https://www.hse.ru/data/2017/ 08/12/1174382135/ NLP_and_DApdf> [Accessed 16 November 2018].
Brownlee, J., 2016. Supervised and Unsupervised Machine Learning Algorithms. In. *Machine Learning Mastery*. [online] Available at: <http://machinelearningmastery.com/supervised-and-unsupervised-machinelearning-algorithms> [Accessed 16 November 2018].
Gorbulin, V.P., Dodonov, O.G. and Lande, D.V., 2009. *Informatsiini operatsii ta bezpeka suspilstva: zahrozy, protydiia, modeliuvannia* [Informatsiyni operatsiya that bezpenka suspense: zaglozi, protidiya, modeluvannya]. Kyiv: Intertekhnolohiia.
Grinenko, I. and Prokofєva-Ianchilenko, D., 2012. Vplyv virtualnykh spilnot na informatsiinu bezpeku: suchasnyi stan ta tendentsii rozvytku [Inserting virtual spillots to information for safeguarding: a good deal that trend development]. *Pravove, normatyvne ta metrolohichne zabezpechennia system zakhystu informatsii v Ukraini*, 1, pp.18-23.
Grishchuk, R.V. and Danika, Iu.G., 2016. *Osnovy kibernetychnoi bezpeky* [Foundations of security networking]. Zhytomyr: Zhytomyrskyi natsionalnyi ahroekolohichnyi universytet.
Ilvovskij, D. and Cherniak, E., 2017. *Glubinnoe obuchenie dlya avtomaticheskoj obrabotki tekstov* [Deep learning for automatic text processing]. [online] Available at: <https://www.osp.ru/os/2017/02/ 13052221> [Accessed 16 November 2018].

Kokarcha, Yu.A., 2016. Trolinh yak zasib politychnoi manipuliatsii v Internet-prostori [Troling yak of the political mania in the Internet]. *Naukovyi chasopys NPU imeni M. P. Drahomanova. Seriia 22 : Politychni nauky ta metodyka vykladannia sotsialno-politychnykh dystsyplin,* [online] 20. Available at: <http://enpuir.npu.edu.ua/bitstream/123456789/17544/1/Kokarcha.pdf> [Accessed 16 November 2018].

Kontseptsiia Big Data v Ukraini: perspektyvy zastosuvannia v derzhavnykh orhanakh [Concepts of Big Data in Ukraine: perspectives in the state organs]. [online] Available at: <http://pa.stateandregions.zp.ua/archive/4_2017/19.pdf> [Accessed 16 November 2018].

Lande, D. and Furashev, V., 2009. Informatsiini operatsii kriz pryzmu systemy monitorynhu ta intehratsii internet-resursiv [Informatsiyni operations kriz prism of system monitoring and ıntegratsin internet resources]. *Pravova informatyka*, 2 (22), pp.49-57.

Lytvynenko, O.V., 2003. *Informatsiini vplyvy ta operatsii: Teoretyko-analitychni narysy* [Informatsiyni plyvili and operations: Theoretical and analytical naris]. Kyiv.

Manoilo, A.V., 2003. *Gosudarstvennaya informacionnaya politika v osobykh usloviyakh* [State information policy in special conditions]. Moscow: MIFI.

Panchenko, V.M. and Polevyi, V.I., 2011. Metodyka vyiavlennia oznak informatsiinoho vplyvu v zasobakh masovoi informatsii [The method of converting the information of information into the fields of mass information]. *Informatsiina bezpeka liudyny, suspilstva, derzhavy*, 3 (7), pp.70-77.

Panchenko, V.M., 2009. Linhvostatystychni oznaky manipuliuvannia suspilnoiu svidomistiu v zasobakh masovoi komunikatsii [Lingvostatisticheskii signs of manipulyannya suspension of sv_domomu in the masses of the commune]. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony,* 1 (4), pp.81-85.

Pocheptcov, G.G, 2001. *Informacionnye vojny* [Information Wars]. Moscow: Refl-buk.

Poliarush, O.O. and Tarasenko, O.Ie., 2008. Paradyhma informatsiinykh vplyviv v perekhidnykh politychnykh systemakh [The paradigm of informative in-force in the auxiliary political systems]. *Suchasni tekhnolohii u sferi bezpeky ta oborony*, 3, pp.81-85.

Rastorguev, S.P., 1999. *Informacionnaya vojna* [Information warfare]. Moscow: Radio i svyaz.

Saienko, O., 2015. Mekhanizm informatsiino-psykholohichnoho vplyvu v umovakh hibrydnoi viiny [Mechanism of information-psychological psychology in the minds of hybrid war]. *Visnyk Natsionalnoi akademii Derzhavnoi prykordonnoi sluzhby Ukrainy. Seriia: Psykholohiia,* [online] 1, Available at: <http://nbuv.gov.ua/UJRN/Vnadpn_2015_1_11> [Accessed 16 November 2018].

Veprincev, V., Manojlo, A., Petrenko, A. and Frolov, D., 2005. *Operacii informacionno-psikhologicheskoj vojny* [Operations of the information-psychological war]. [online] Available at: <https://psyfactor.org/psyops/ psyops4.htm> [Accessed 16 November 2018].

Стаття надійшла до редакції 16.11.2018

UDC 004:316.472.4

Voitovych Olesia,
PhD in Technical Sciences, Associate Professor,
Vinnytsia National Technical University,
Vinnytsia, Ukraine
nika.ostrovska21@gmail.com
https://orcid.org/0000-0001-8964-7000

Ostrovska Veronika,
Magistrate of Information Protection Department,
Vinnytsia National Technical University,
Vinnytsia, Ukraine
nika.ostrovska21@gmail.com
https://orcid.org/0000-0002-2374-1501

Zakalov Igor,
CEO Main Academy,
Kyiv, Ukraine
zakalov@mainacad.com
https://orcid.org/0000-0001-8892-6120

NEGATIVE INFLUENCES EXPOSURE IN SOCIAL INTERNET-SERVICES

Having regard to the last events in our country, it is possible to assert that network the Internet gradually became the source of threats to informative safety of man, society, state, as distribution in the global network of doubtful and biased content together with technologies of informatively-psychological influence on consciousness of individuals can assist an origin in society of dissatisfaction by operating state power, international conflicts, social aggression and others like that.

The purpose of the article is to review method oriented to increase authenticity exposure negative informatively-psychological influence in social internet-service by realization automated analysis text content.

Research methods. During research the methods of theory of social networks analysis (Social Network Analysis, SNA), methods of treatment of human language (Natural Language Processing, NLP), and methods of machine studies (Machine Learning), including deep studies (Deep Learning) have been used.

The scientific novelty of the got results consists in that in-process first the method of application of deep studies models offers to the analysis task of the key in text data, that differs from existing structure, which allows promoting exactness of informatively-psychological influences exposure in content of social networks.

Conclusions. Research results can be drawn on at further development of facilities in the automated negative informatively-psychological influences exposure.

Key words: analysis of data; neural networks; machine studies; deep studies; data analysis; internet; social networks; social internet-services.

УДК 004:316.472.4

Войтович Олеся,
кандидат технических наук, доцент,
Винницкий национальный технический университет,
Винница, Украина
nika.ostrovska21@gmail.com
https://orcid.org/0000-0001-8964-7000

Островская Вероника,
магистр факультета информационных технологий
и компьютерной инженерии,
Винницкий национальный технический университет,
Винница, Украина
nika.ostrovska21@gmail.com
https://orcid.org/0000-0002-2374-1501

Закалов Игорь,
Генеральный директор Main Academy,
Киев, Україна
zakalov@mainacad.com
https://orcid.org/0000-0001-8892-6120

ОПРЕДЕЛЕНИЕ НЕГАТИВНЫХ ВЛИЯНИЙ В СОЦИАЛЬНЫХ ИНТЕРНЕТ-СЕРВИСАХ

Принимая во внимание последние события в нашей стране, можно утверждать, что сеть Интернет постепенно стала источником угроз информационной безопасности человека, общества, государства, поскольку распространение в глобальной сети сомнительного и необъективного контента вместе с технологиями информационно-психологического влияния на сознание индивидов может способствовать возникновению в обществе недовольства действующей государственной властью, межнациональных конфликтов, социальной агрессии и тому подобное.

Целью исследования является обзор методов ориентированных на повышение достоверности выявления негативных информационно-психологических влияний в социальных интернет-сервисах путем осуществления автоматизированного анализа текстового контента.

Методы исследования. В ходе исследования использовались методы теории анализа социальных сетей (Social Network Analysis, SNA), методы обработки естественного языка (Natural Language Processing, NLP), методы машинного обучения (Machine Learning), в том числе глубокого обучения (Deep Learning).

Научная новизна полученных результатов заключается в том, что в работе впервые предложен метод применения моделей глубокого обучения к задаче анализа тональности текстовых данных, который отличается от существующих своей структурой, что позволяет повысить точность выявления информационно-психологических влияний в контенте социальных сетей.

Выводы. Результаты исследования могут быть использованы при дальнейшей разработке средств автоматизированного выявления негативных информационно-психологических влияний.

Ключевые слова: анализ данных; нейронные сети; машинное обучение; глубокое обучение; анализ данных; интернет; социальные сети; социальные интернет-сервисы.