

## РОЗРОБЛЕННЯ АЛГОРИТМУ ВИЯВЛЕННЯ ШКІДЛИВИХ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИХ МАНІПУЛЯЦІЙ В ОНЛАЙН-СПІЛЬНОТАХ ВНЗ

© Голуб З., 2017

**This paper is devoted to the detection of informational and psychological manipulation (IPM) in online communities. The algorithm for monitoring community with the aim to detect IPM in online communities of a higher education institution is developed. The algorithm constitutes of four stages, namely searching for thematically relevant communities, detecting IPM occurrences, determining possible ways of dissemination of manipulative information and providing recommendations for neutralization of IPM. Actions, tools and methods employed on each stage of the algorithm are discussed.**

**Key words: informational and psychological manipulation, online community, piecewise-linear aggregate.**

У статті запропоновано загальний алгоритм моніторингу онлайн-спільноти з метою виявлення інформаційно-психологічної маніпуляції (ІПМ) тематичного спрямування. Алгоритм передбачає пошук спільнот, в яких потенційно можуть бути ІПМ, виявлення ІПМ, визначення можливих шляхів поширення ІПМ та надання рекомендацій щодо нейтралізації ІПМ. Розглянуто дії, засоби і методи кожного з чотирьох етапів моніторингу онлайн-спільноти.

**Ключові слова: інформаційно-психологічна маніпуляція, онлайн-спільнота, кусково-лінійний агрегат.**

### Вступ

Стан внутрішніх та зовнішніх комунікацій є важливим для успішної діяльності вищого начального закладу (ВНЗ). У сучасному динамічному світі інформаційних технологій важливу роль у поширенні інформації відіграють онлайн-спільноти. Популярність цього інформаційного ресурсу спричинила їх використання як платформи для здійснення інформаційно-психологічних маніпуляцій (ІПМ). ІПМ полягає в такому: маніпулятор під час подачі інформації застосовує психологічні механізми впливу на підсвідомість реципієнта, як наслідок, реципієнт засвоює інформацію, яка є вигідною лише для замовника ІПМ.

ІПМ є завадою для успішної діяльності ВНЗ [1]. Небезпечна для ВНЗ маніпуляція може бути спрямована на суб'єктів не лише освітньої галузі, а саме: студентів, абітурієнтів, роботодавців, адміністративних кадрів та обслуговувальний персонал. ІПМ може мати різні цілі: дискредитація ВНЗ як освітнього закладу, зниження шансів випускників ВНЗ на ринку праці, наклепи на працівників. ІПМ часто є однією з причин таких глобальних і локальних проблем ВНЗ, як зменшення кількості абітурієнтів, конфлікти між працівниками і зниження успішності студентів.

За умови виявлення і протидії ІПМ за допомогою аналітичної оцінки інформаційного наповнення онлайн-спільнот необхідно великий штат експертів. Інакше робота цього відділу буде не ефективною: ІПМ будуть виявлені запізно або пропущені. Для усунення шкоди, завданої запізно виявленою ІПМ, потрібно використати набагато більше ресурсів, ніж для

нейтралізації ІМП під час її здійснення. Адже запобігти зміні поглядів на протилежні складніше, ніж переконати людину в протилежному.

Постає потреба в автоматизованих або частково автоматизованих засобах виявлення ІПМ в онлайн-спільнотах ВНЗ, які підвищили б ефективність роботи працівників відповідальних за інформаційний образ ВНЗ, і, таким чином, знизили ризик деструктивних змін у якості освіти, обслуговуванні та інших сферах функціонування підрозділів ВНЗ. Загальний алгоритм моніторингу онлайн-спільноти з метою виявлення ІПМ необхідний як основа для розроблення автоматизованих методів і засобів виявлення ІПМ.

### **Актуальність**

Виявлення ІПМ є актуальною проблемою сучасності, адже до атак за допомогою маніпулятивних повідомлень вразливі, як комерційні організації та державні установи, так і відомі особистості, бренди і медіа. Для вирішення цієї проблеми застосовують інструментарій комп'ютерних технологій, математики, лінгвістики, психології та соціології. Проводять дослідження, спрямовані на вирішення дотичних проблем, та розробляють засоби, за допомогою яких можна буде частково автоматизувати їх вирішення. До прикладу розроблені додатки до браузерів для виявлення посилань у Facebook, які переводять на ресурси з недостовірним контентом [2], для попередження про ненадійність веб-сайту як джерела інформації [3, 4], для виявлення викривленого представлення політичних поглядів на веб-сайтах [5], для перевірки фактів і цитат, розміщених на веб-сайтах [6,7], виділення елементів пропаганди на веб-сайтах [8]. Але ці всі додатки працюють завдяки наповненій вручну базі даних, крім того, одиниці з них підтримують кирилицю. Технічно складнішим продуктом є розроблений Google Perspective API для автоматизації роботи модератора [10]. Perspective використовує методи машинного навчання для виявлення повідомлень, які можуть негативно впливати на обговорення. Вважається, що це повідомлення, які мають інвективний характер. Perspective не інтернаціоналізовано, тому його не можна використовувати для модерації обговорень українською. Більше того, Perspective розроблено для боротьби з тролінгом, а тролінг є лише одним із видів ІПМ. Незважаючи на численні наукові дослідження, запропоновані рішення проблеми виявлення ІПМ в онлайн-спільнотах мають частковий чи локальний характер, а пропозиції загального алгоритму, який можна було б застосувати для виявлення ІПМ спрямованого на ВНЗ – відсутні.

### **Загальний опис алгоритму**

Алгоритм моніторингу онлайн-спільнот ґрунтується на формальних моделях спільноти і тактики маніпуляції [11,12]. Алгоритм поділено на чотири етапи: підготовки, виявлення, нейтралізації та завершальний (рис. 1).

Етап підготовки полягає у пошуку релевантних до тематики ВНЗ обговорень та сортування обговорень за наявністю передумов для здійснення ІПМ. Результатом цього етапу є черга обговорень, які необхідно проаналізувати на наявність ІПМ. Обговорення сортуються за найсприятливішими передумовами для здійснення маніпуляції в порядку спадання.

На етапі виявлення визначають уривки обговорення, з яких варто почати пошук ІПМ, та аналізують інформаційне наповнення з метою виявити прецеденти маніпуляції. Результатом цього етапу є опис прецеденту маніпуляції, а саме суб'єктів ІПМ, застосованої тактики та використаних прийомів.

На третьому етапі – нейтралізації – проводиться аналіз даних про суб'єкти ІПМ, з метою виявити угруповання маніпуляторів. Також аналізують зв'язки учасників обговорення, отриману інформацію використовують для визначення можливих шляхів поширення ІПМ.

На завершальному етапі на основі результатів попередніх етапів надаються поради щодо нейтралізації ІПМ, до черги додають нові обговорення, які необхідно проаналізувати на наявність ІПМ. На цьому етапі результати моніторингу заносять до бази даних виявлених прецедентів маніпуляції.

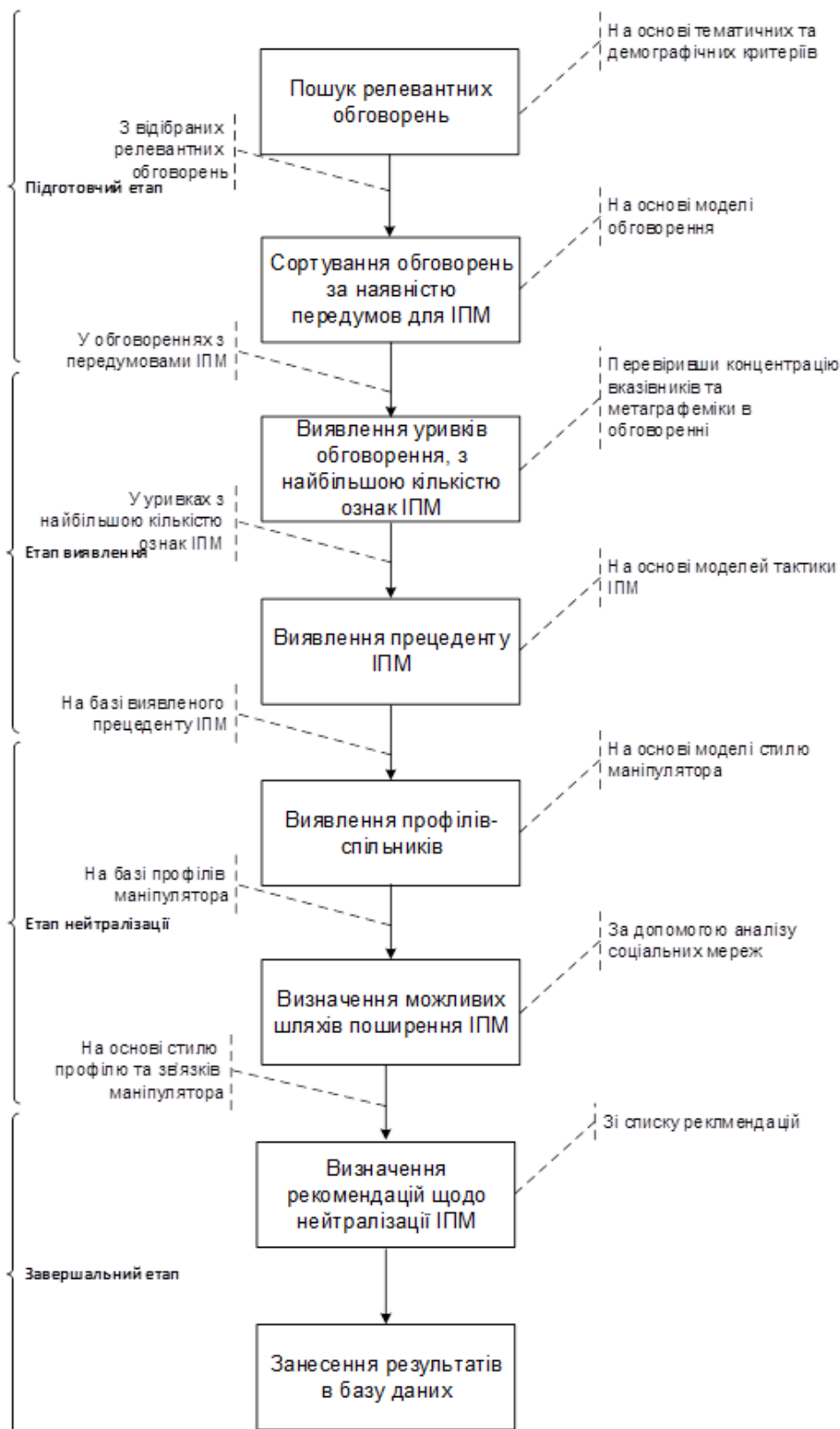


Рис. 1. Алгоритм моніторингу онлайн-спільноти з метою виявлення ІПМ

### Етап пошуку

На етапі підготовки, для пошуку релевантних онлайн-спільнот, використовуються глобальні пошукові системи (ГПС), засоби пошуку в Facebook, а також здійснюється пошук в базі даних виявлених прецедентів ІПМ. Для ефективного пошуку релевантних обговорень недостатньо

використовувати одну ГПС, оскільки внаслідок різних алгоритмів обходу, індексації, ранжування, результати пошуку будуть відмінними. В цьому дослідженні використовувались найпопулярніші ГПС, а саме: Google, Bing, Yahoo!Search та DuckDuckGo. Ці ГПС дають змогу використовувати оператори пошуку, які можуть відрізнитись, але їхній зміст збігається. На основі операторів пошуку Google розроблено алгоритм побудови параметризованого запиту для відбору релевантних дискусій [13]. Пошук обговорень, які відбуваються Facebook, здійснюється не тільки за допомогою ГПС, а проводиться засобами Facebook. Результати пошуку в Facebook залежать від профілю, з якого здійснюється пошук, оскільки Facebook спочатку обходитиме сторінки, які найсильніше пов'язані з цим профілем. Отже, використовуючи для пошуку різні ГПС та засоби Facebook, забезпечено достатній обсяг результатів.

Наступним етапом пошуку релевантних обговорень є перевірка результатів ГПС на основі тематичних та демографічних критеріїв.

Тематичні критерії розраховуються за допомогою аналізу заголовку та інформаційного наповнення обговорення. Заголовок обговорень аналізують на наявність ключових слів тематики, а також беруть до уваги їхнє розташування відносно одне-одного. Для аналізу інформаційного наповнення спільноти використовують модель Bag of Words (BOW) [14]. Релевантність обговорення визначають за відносною кількістю аспектів, пов'язаних із діяльністю ВНЗ, які трапляються в обговоренні.

Як критерії пошуку релевантних обговорень використовуються демографічні характеристики цільової аудиторії. Обрані такі характеристики: територіальне розташування, вік, професія. Для того, щоб використовувати демографічні критерії пошуку релевантних обговорень необхідно припустити: які ПІМ можуть бути спрямовані на ВНЗ у конкретній ситуації. Наприклад, влітку найімовірніше ПІМ пов'язані з вступом абітурієнтів до ВНЗ. Таким чином, можна окреслити і цільову аудиторію, на яку спрямована ПІМ. В цьому прикладі, це передусім будуть особи молодого віку, випускники середніх навчальних закладів, мешканці населеного пункту, де розташований ВНЗ.

Після пошуку обговорень необхідно створити чергу обговорень, які треба аналізувати на наявність ПІМ. Терміновість аналізу певного обговорення зумовлена трьома групами критеріїв: критерії популярності обговорення, підозрілості та вразливості (табл. 1). Критерії популярності розраховуються на основі формальної моделі обговорення [11]. Якщо в базі даних виявлених прецедентів маніпуляції наявна інформація про обговорення, то варто врахувати критерії підозрілості та вразливості. Кількість представників цільової аудиторії визначати недоцільно, оскільки вони вимагають великих затрат часу.

Таблиця 1

### Критерії сортування обговорень

Популярність	Підозрілість	Вразливість
Кількість учасників	Кількість підозрілих профілів	Кількість впливових профілів
Дата останнього допису	Кількість метаграфеміки	Кількість представників цільової аудиторії
Кількість дописів на день	Кількість емотиконів	

### Етап виявлення

Етап виявлення передбачає виконання двох ключових завдань: виділення уривків обговорення з найбільшою концентрацією ознак ПІМ та виявленні тактик ПІМ в обговоренні. Для виконання першого завдання необхідно виявити ознаки ПІМ. Виявлення ПІМ відбувається в уривках обговорення з великою концентрацією ознак ПІМ. Кількість ознак

ІПМ визначає послідовність аналізу уривків обговорення: спочатку аналізують уривки з найбільшою кількістю ознак ІПМ.

ІПМ часто супроводжуються нагнітанням емоцій, адже в емоційному стані людині складно об'єктивно сприймати інформацію. Тому, високий рівень емоційності обговорення свідчить про наявність ІПМ. Об'єкти маніпуляції можуть виражати свої емоції за допомогою емоційно забарвлених слів, емотиконів чи метаграфеміки. Відповідно, за концентрацією цих ознак визначаються уривки, які необхідно перевірити на ІПМ (рис. 2).

Пошук застосованих прийомів ІПМ потрібно починати з повідомлень, авторами яких є підозрілі профілі, або повідомлень, які містять вказівники ІПМ. Вказівник ІПМ – це лексичний, метаграфічний засобів чи посилання, яке часто використовують для реалізації прийому ІПМ. Також необхідно перевірити повідомлення, які провокують бурхливу активність в обговоренні. Це відображається великою кількістю реакцій, наприклад, коментарів та уподобань (рис. 2).

Для формалізації тактик ІПМ використано кусково-лінійний агрегат [11]. Ця модель універсальна, за її допомогою можна формалізувати тактики маніпуляції описані за допомогою транзакційного аналізу, інструментарію НЛП, а також характерні для онлайн-спільнот тактики ІПМ виявлені внаслідок експертного аналізу комунікації в онлайн-спільнотах.

Тактики ІПМ реалізуються внаслідок застосування прийомів ІПМ у визначеній послідовності. Тому виявленню ІПМ за допомогою кусково-лінійних агрегатів передую виявлення прийомів ІПМ у повідомленнях обговорення. З метою автоматизації виявлення прийомів, їх формалізовано за допомогою нотації Бекуса-Наура [11].

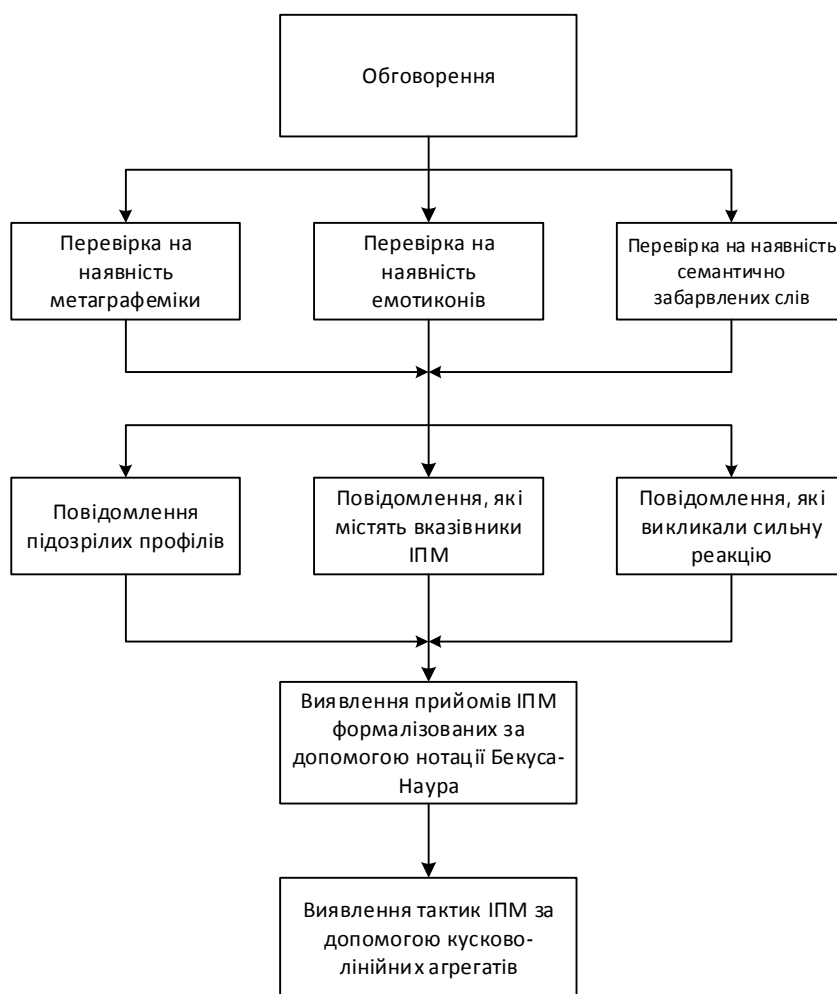


Рис. 2. Виявлення прецедентів ІПМ

### Етап нейтралізації

Маніпулятори переважно діють за допомогою групи профілів, імітуючи, таким чином, дискусію необхідного спрямування. З метою ефективної нейтралізації ПМ необхідно виявити всі профілі і запобігти їхній подальшій діяльності.

Виявленню профілів спілльників передують визначення характеристик профілів маніпуляторів. Виявлення профілів спілльників полягає у порівнянні профілів учасників обговорення з характеристиками профілю-маніпулятора. Якщо подібні поведінкові характеристики, характеристики стилю чи характеристики профілю, тоді виявлено профіль-спільник (рис. 3).

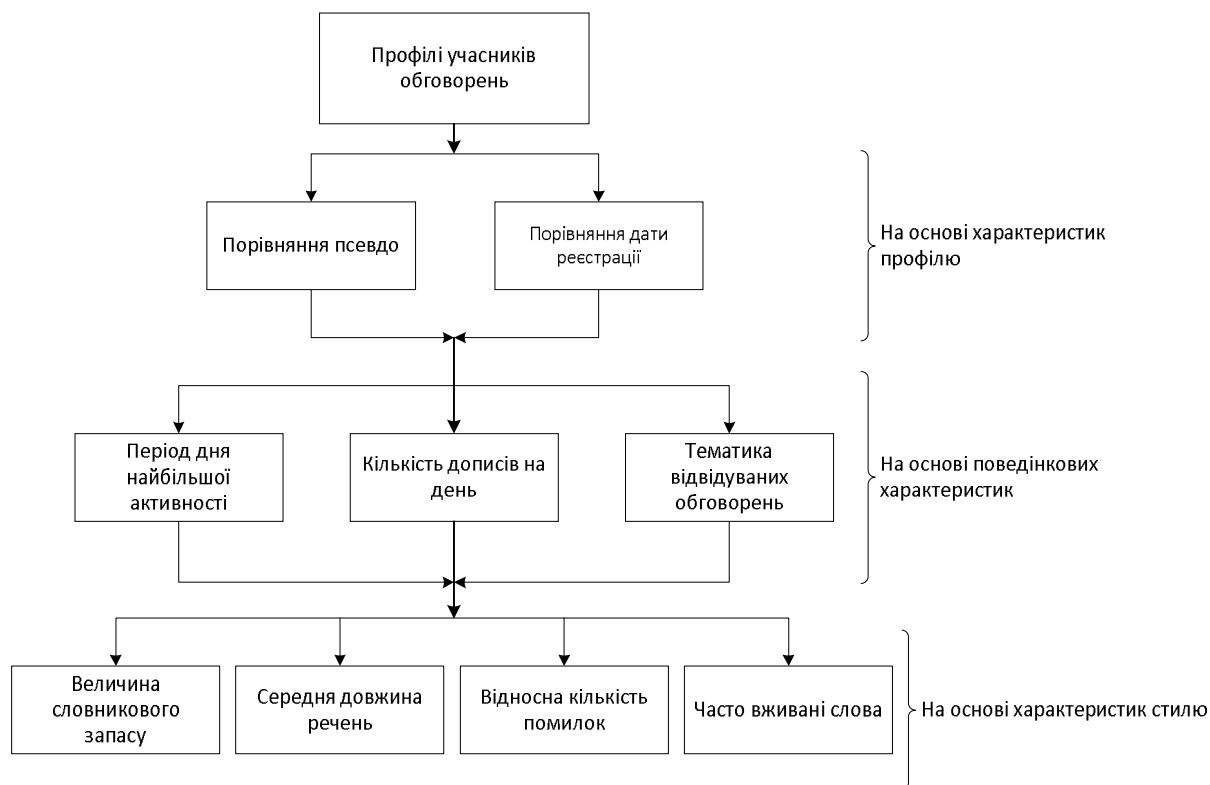


Рис. 3. Виявлення профілів-спілників

Кожен із маніпулятивних профілів має своїх друзів (серед них є і незловмисні учасники) і свою аудиторію. Побудувавши граф, який відображає мережу пов'язаних профілів та види зв'язків між ними, можна передбачити можливі шляхи поширення ПМ. Для зображення зв'язків між профілями використовується орієнтований граф, вершинами якого є профілі учасників, а ребрами – зв'язки між учасниками. Аналізуючи зв'язки графу, необхідно відповісти на питання: хто спілкується в одному обговоренні, цитує один одного, коментує ставить уподобання, стежить. Також потрібно вирахувати показники вершин, які визначають важливість кожної вершини для комунікації.

### Завершальний етап

На завершальному етапі на основі результатів попереднього етапу даються рекомендації щодо нейтралізації ПМ та заносять результати до бази даних виявлених прецедентів ПМ.

Інформацію з бази даних використовують на кожному з етапів алгоритму виявлення маніпуляції. Проміжні та кінцеві результати попередніх аналізів з метою виявлення ПМ використовують для пошуку релевантних спільнот, розрахування значень критеріїв підозрливості і вразливості обговорень. База даних містить інформацію про прийоми ПМ, характеристики

маніпулятивних профілів. Крім того, аналізуючи базу даних, можна відслідковувати тенденції маніпуляції, аналізувати помилки алгоритму. Отже, ця інформація використовуватиметься для підвищення ефективності виявлення маніпуляції.

### Висновки

Своєчасне виявлення ПІМ в онлайн-спільнотах ВНЗ є важливим і складним завданням. Важливим, оскільки ПІМ загрожує зовнішньому іміджу ВНЗ, як і внутрішньому стабільному функціонуванню ВНЗ. Процес виявлення ПІМ є часо- і трудозатратним, тому існує потреба в автоматизованому рішенні. Алгоритм виявлення ПІМ в онлайн-спільнотах ВНЗ передбачає пошук обговорень, виявлення прецедентів ПІМ, передбачення можливих шляхів поширення ПІМ, надання рекомендацій щодо нейтралізації та збереження результатів. На етапах алгоритму створюються пошукові запити, визначаються вихідні точки для аналізу обговорень, за допомогою кусково-лінійних агрегатів здійснюється виявлення прецедентів маніпуляції, використовуючи інструментарій аналізу соціальних мереж, визначаються можливі шляхи поширення ПІМ.

### Література

1. Korzh R. O. *Analysis of Integrity and Coverage Completeness of the Informational Image of a Higher Education Institution* / R. O. Korzh, A. M. Peleschyshyn, Z. D. Holub // In: *proceedings of the XIIIth International Conference. TCSET'2016, February 23–26, Lviv–Slavske, Ukraine*. – Lviv: Publishing House of Lviv Polytechnic, 2016. *Modern problems of radio engineering, telecommunications and computer science*. – P. 825–827.2. FiB | Devpost [Electronic resource]. – Access mode: <https://devpost.com/software/fib> (last access: 15.03.17). – Title from the screen. 3. B. S. Detector [Electronic resource]. – Access mode: <https://chrome.google.com/webstore/detail/bs-detector/dlcgkekjiopabcifhebmphmfndbjod> (last access: 15.03.17). – Title from the screen. 4. Fake News Alert [Electronic resource]. – Access mode: <https://chrome.google.com/webstore/detail/fake-news-alert/aickfmgkhocegpdbfnfnedpeionfkbh> (last access: 15.03.17). – Title from the screen. 5. Media Bias/Fact Check [Electronic resource]. – Access mode: <https://mediabiasfactcheck.com/> (last access: 15.03.17). – Title from the screen. 6. FactChecker [Electronic resource]. – Access mode: [https://www.washingtonpost.com/news/fact-checker/?utm\\_term=.e45d6c8b0350](https://www.washingtonpost.com/news/fact-checker/?utm_term=.e45d6c8b0350) (last access: 15.03.17). – Title from the screen. 7. PolitiFact [Electronic resource]. – Access mode: <http://www.politifact.com/> (last access: 15.03.17). – Title from the screen. 8. PropOrNot Propaganda Flagger [Electronic resource]. – Access mode: <https://chrome.google.com/webstore/detail/propornot-propaganda-flag/ogmjlmfjnmhcllijlbaomamgfaiflai> (last access: 15.03.17). – Title from the screen. 9. Phillips E. *Extracting Social Structure from DarkWeb Forums* / E. Phillips, J. R.C. Nurse, M. Goldsmith, S. Creese // *SOTICS 2015 : The Fifth International Conference on Social Media Technologies, Communication, and Informatics – 2015*. 10. *What if technology could help improve conversations online?* [Electronic resource]. – Access mode: <https://www.perspectiveapi.com/> (last access: 15.03.17). – Title from the screen. 11. A. Peleschyshyn, Z. Holub, "Development of the System for Detecting Manipulation in Online Discussions", *International Conference on Systems, Control and Information Technologies 2016*. Springer International Publishing, vol. 543, pp. 111-117, 2016. 12. A. Peleschyshyn, Z. Holub, and I. Holub. "Methods of real-time detecting manipulation in online communities." *Scientific and Technical Conference "Computer Sciences and Information Technologies (CSIT), 2016 XIth International. IEEE*, pp.15-17, 2016. 13. Тимовчак-Максимець О. Ю. *Методи використання розширених можливостей глобальних пошукових систем в задачі пошуку споживацького досвіду в онлайн середовищах* / О. Ю. Тимовчак-Максимець // *Вісн. Нац. ун-ту "Львів. політехніка"*. – 2011. – № 715. – С. 333–342. – Бібліогр.: 13 назв. – укр. 14. Zhang, Y., Jin, R., & Zhou, Z. H. *Understanding bag-of-words model: A statistical framework*. *International Journal of Machine Learning and Cybernetics*. – 2010. – 1(1–4), P. 43–52.

## **DEVELOPING THE ALGORITHM FOR DETECTING MALICIOUS INFORMATIONAL AND PSYCHOLOGICAL MANIPULATIONS IN ONLINE COMMUNITIES OF A HIGHER EDUCATION INSTITUTION**

© Holub Z., 2017

Detection of informational and psychologic manipulation (IPM) is of utmost importance for a higher education institution (HEI) in the light of the popularity of online communities. Condition of in-house and foreign communications is crucial for successful performance of a HEI. In the modern fast-paced world of informational technologies online communities play an important role in information dissemination. Popularity made this information resource a convenient platform for IPM. The term IPM determines the following activities: while presenting information, a manipulator employs psychological mechanisms of influence on the subconsciousness of a recipient, as a result the recipient adopts attitudes and viewpoints that are advantageous for a manipulator.

IPM poses a threat to successful performance of a HEI. IPM is dangerous for a HEI because it is aimed at influencing not only subjects of educational sphere, but administrative personnel, service staff, students, prospective students and employers. There are various goals of IPM: discrediting a HEI as an educational institution, decreasing chances of HEI graduates on the job market, slandering employees. IPM is often a reason of global and local problems of a HEI, for instance, decrease in the number of prospective students, low team morale at the departments, decrease of educational progress of students.

In order to detect and conduct a successful counteraction to IPM through the analytic assessment of online communities content, a many experts is required. Otherwise, results of IPM detection would be unsatisfactory: IPM occurrences would be missed or detected too late. Much more resources are required to eliminate damages caused by failure to detect IPM in time, than to neutralize IPM when it is in process. It is easier to prevent groundless attitudes shift than to persuade a person in an opposite idea.

Arises a demand for automatic or partly automatic tools for detecting IPM in online communities of a HEI. These tools are expected to improve efficiency of employees responsible for an informational image of a HEI. As a result, the risk of destructive changes in education quality and related services would decrease. A general algorithm for monitoring online communities with the aim to detect IPM is required for development of automated tools and methods for detecting IPM.

The algorithm for monitoring online communities of a HEI is based on online community and manipulation tactic formal models. The algorithm constitutes of four stages: preparatory, detection, neutralization and final.

At the preparatory stage, search for thematically relevant discussions is conducted and discussions are sorted taking into consideration preconditions for IPM of every discussion. The results of this stage is a queue of discussions that are to be analyzed for IPM occurrences. Discussion are sorted considering the amount of advantageous preconditions for IPM, in reverse order.

At the detection stage, a seed for IPM occurrences detection is determined. The seed constitutes of discussion pieces that have a great number of features of a discussion containing IPM. After that, applying piecewise-linear aggregates IPM tactic is detected. The outcome of the stage is a description of a detected IPM precedent, subjects of IPM and used IPM tools.

At the neutralization stage, IPM actors data is analyzed with the aim to detect groups of manipulators. Analysis of relations of discussion participants is conducted. Obtained information is used for implying possible ways of IPM spreading.



At the final stage, on the basis of previous stages results, recommendations for IPM neutralization are provided. Besides, new discussions are added to discussions queue. At this stage, interim and final results of the algorithm for IPM detection in online communities of a HEI are added to the database.

### References

1. Korzh R. O. *Analysis of Integrity and Coverage Completeness of the Informational Image of a Higher Education Institution*. / R.O. Korzh, A.M. Peleschyshyn, Z.D. Holub // In: *proceedings of the XIIIth International Conference. TCSET'2016, February 23–26, 2016, Lviv–Slavske, Ukraine*. Lviv, Publishing House of Lviv Polytechnic, 2016. *Modern problems of radio engineering, telecommunications and computer science*. pp. 825–827.
2. FiB Devpost [Electronic resource]. – Access mode: <https://devpost.com/software/fib> (last access: 15.03.17). – Title from the screen.
3. B. S. Detector [Electronic resource]. – Access mode: <https://chrome.google.com/webstore/detail/bs-detector/dlcgkekjiopopabcifhebpmhmfmdbjod> (last access: 15.03.17). – Title from the screen.
4. Fake News Alert [Electronic resource]. – Access mode: <https://chrome.google.com/webstore/detail/fake-news-alert/aickfmgkhocegpdbfnpfndpeionfkbh> (last access: 15.03.17). – Title from the screen.
5. Media Bias/Fact Check [Electronic resource]. – Access mode: <https://mediabiasfactcheck.com/> (last access: 15.03.17). – Title from the screen.
6. FactChecker [Electronic resource]. – Access mode: [https://www.washingtonpost.com/news/fact-checker/?utm\\_term=.e45d6c8b0350](https://www.washingtonpost.com/news/fact-checker/?utm_term=.e45d6c8b0350) (last access: 15.03.17). – Title from the screen.
7. PolitiFact [Electronic resource]. – Access mode: <http://www.politifact.com/> (last access: 15.03.17). – Title from the screen.
8. PropOrNot Propaganda Flagger [Electronic resource]. – Access mode: <https://chrome.google.com/webstore/detail/propornot-propaganda-flag/ogmjlmhfmhchlijlbaomamgfaiflai> (last access: 15.03.17). – Title from the screen.
9. Phillips E. *Extracting Social Structure from DarkWeb Forums* / E. Phillips, J. R.C. Nurse, M. Goldsmith, S. Creese // *SOTICS 2015 : The Fifth International Conference on Social Media Technologies, Communication, and Informatics – 2015*.
10. What if technology could help improve conversations online? [Electronic resource]. – Access mode: <https://www.perspectiveapi.com/> (last access: 15.03.17). – Title from the screen.
11. A. Peleschyshyn, Z. Holub. *Development of the System for Detecting Manipulation in Online Discussions*, *International Conference on Systems, Control and Information Technologies 2016*. Springer International Publishing, vol. 543, pp. 111–117, 2016.
12. A. Peleschyshyn, Z. Holub, and I. Holub. *Methods of real-time detecting manipulation in online communities*. *Scientific and Technical Conference “Computer Sciences and Information Technologies (CSIT)”*, 2016 XIth International. IEEE, pp. 15–17, 2016.
13. Tymovchak-Maksymets O. *Methods of using the advanced features of global search engines to find consumer experience in online media* / A. Y. Tymovchak Maksymets // *Visn. Nat. Univ “Lviv. Polytechnic”*. – 2011. – No. 715. – S. 333–342. – Ref. : 13 names. - thesis.
14. Zhang, Y., Jin, R., & Zhou, Z. H. *Understanding bag-of-words model: A statistical framework*. *International Journal of Machine Learning and Cybernetics* – 2010. – 1(1-4), 43–52.