DOI: https://doi.org/10.35681/1560-9189.2019.21.3.183717

УДК 004.942

А. М. Соболєв
Інститут спеціального зв'язку та захисту інформації
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»
вул. Верхньоключова, 4, 03056 Київ, Україна

Виявлення в глобальній мережі Інтернет інформаційних джерел, які розповсюджують недостовірну інформацію

Наведено метод, який базується на значеннях дисперсії і показника Херста в часових рядах, що утворюють масиви публікацій в інформаційних джерелах глобальної мережі Інтернет. Запропоновано алгоритм, який дозволяє виявляти інформаційні джерела з ознаками «фейків» або інформаційної операції в інформаційних ресурсах глобальної мережі.

***Ключові слова**: показник Херста, інформаційні агентства, рівень стабільності, інформаційні джерела, інформаційні операції.*

Вступ

У сучасних умовах одним із значущих сегментів у засобах масової інформації є сукупність джерел мережі Інтернет. Це обумовлено широким охопленням аудиторії, високою швидкістю поширення інформації і можливістю інтеграції в одному повідомленні контенту різного типу (текст, відео, фото, аудіо). Саме інформаційні ресурси глобальної мережі Інтернет являються джерелом інформації, на основі якого сучасна людина формує певний світогляд щодо способу та стилю життя, моделей поведінки, і отримує необхідну їй інформацію.

Результати соціологічних досліджень показали, що безперервно збільшується кількість користувачів мережею Інтернет. Найпопулярнішими пристроями доступу до мережі виявилися мобільні телефони та планшети. Це дозволило розширити спектр послуг, які надаються за допомогою глобальної мережі. Споживачі інформації усе частіше використовують запропоновані послуги з мережі Інтернет у повсякденному житті. Ця особливість використовується, в тому числі, і в маніпулятивних цілях під час ведення інформаційних війн чи атак для навіювання неправдивої інформації користувачам. У такому випадку використовують ненадійні інформаційні джерела глобальної мережі Інтернет для розповсюдження фейкових даних і запуску процесу розповсюдження цієї інформації на інших джерелах. Слід

відмітити, що комплекс узгоджених і взаємопов'язаних заходів з маніпулюванням інформацією, здійснюваних за загальним планом з метою досягнення та отримання переваги через вплив на інформаційні процеси в системах супротивника, називають інформаційною операцією (ІО).

Складність виявлення інформаційних джерел з ознаками «фейків» або ІО у ЗМІ глобальної мережі Інтернет обумовлена не тільки скритністю її проведення але й великою кількістю інформаційних джерел (ЗМІ) і їхніх публікацій. Кількість офіційно зареєстрованих і функціонуючих ЗМІ в мережі Інтернет постійно зростає (за останні 3 роки приблизно в 2 рази).

Аналіз останніх досліджень і публікацій

На даний час існує багато критеріїв щодо актуальності інформації у мережі Інтернет. Наприклад, кількість створеної інформації щодо події за одиницю часу, загальна кількість створеної інформації, яка стосується даної події, кількості переглядів даної події на ресурсі джерела ЗМІ та кількість згадувань у соціальних мережах.

Таким чином, для надання події ознак актуальності необхідно забезпечити опублікування інформації щодо даної події на ресурсах декількох джерел ЗМІ протягом невеликого проміжку часу. Також, доволі часто зустрічаються випадки, коли одне джерело публікує інформацію 2 чи 3 рази на своєму ресурсі для збільшення кількості опублікованої інформації щодо даної події.

Запропоновані в [1] методи виявлення інформаційних операцій засновані на семантичному підході до оцінки повідомлення ЗМІ. Ці методи мають велику точність виявлення інформаційних операцій, але використовуються вже після проведення інформаційних операцій за участі експертів. З огляду на експертне оцінювання, складно забезпечити високу оперативність і, отже, своєчасність виявлення інформаційних атак.

У роботах [2–4] критерієм виявлення інформаційних атак є відповідність динаміки інтенсивності тематичного інформаційного потоку деякому шаблону інформаційної атаки. При використанні даного підходу не виконується вимога щодо своєчасності, тому що для його застосування необхідно отримати динаміку інтенсивності тематичного інформаційного потоку протягом активної і пасивної фаз інформаційної атаки.

У [5–7] обґрунтовано необхідність оперативного та точного виявлення інформаційних операцій у ЗМІ. При цьому вирішення даного завдання є достатньо складним через великий обсяг повідомлень ЗМІ і відсутність алгоритму для виявлення інформаційних операцій. Однак у вищезазначених роботах не розглядається властивість своєчасності виявлення інформаційних атак і, зокрема, інформаційних операцій до моменту початку їхньої пасивної фази. При своєчасному виявленні інформаційної операції залишається час на вживання заходів протидії інформаційній атаці. Класичний підхід для виявлення інформаційних атак базується на оцінюванні кількості повідомлень негативної тональності щодо об'єкта спостереження в різні проміжки часу. Якщо їхня кількість більше порогового значення, робиться висновок щодо проведення інформаційної атаки [9]. Однак на даний час методи проведення інформаційних атак удосконалюються і можуть використову-

вати повідомлення нейтральної позитивної тональності. Отже, використання алгоритмів на основі негативної тональності повідомлень ЗМІ може призводити до похибки виявлення інформаційних операцій.

У роботах [8–10] надано визначення джерела з ознаками «фейків» (фейкові новини). Дана проблема являється глобальною у всьому світі та містить багато факторів, які і досі залишаються невідомими. Необхідний певний механізм, що дозволить виявляти такі джерела та забезпечити контроль за достовірністю інформації, яка розповсюджується інформаційними джерелами в глобальній мережі Інтернет

Виклад основного матеріалу

Виникає протиріччя між сучасним станом інформаційного простору глобальної мережі Інтернет і можливостями оперативного та достовірного виявлення ненадійних інформаційних джерел ЗМІ існуючими засобами протидії.

Необхідно забезпечити своєчасне виявлення інформаційних джерел з ознаками «фейків» чи ІО на етапі активної фази, щоб запобігти проведенню подальшої атаки та неконтрольованого розповсюдження інформації на етапі пасивної фази. Для цього потрібно провести дослідження критичності інформаційних джерел глобальної мережі Інтернет та виявити найбільш критичні, за якими необхідно проводити моніторинг на предмет «фейків».

Джерела інформації перш за все характеризуються рівнем стабільності. Прикладом стабільних джерел можуть служити великі інформаційні агентства, які регулярно викладають користувачам приблизно однакові обсяги інформації протягом тривалого часу, а нестабільні — малі журнали, багато з яких активно діють протягом декількох днів, а потім поступово зменшують темп створення інформації. Також трапляються випадки, коли малі журнали постійно підтримуються, щоб у необхідний період часу розпочати інформаційну атаку.

Нестабільні джерела відповідальні за хаотичність динамічної частини мережевого інформаційного простору та грають ключову роль, що відображають (і якоюсь мірою породжують) реальні закономірності мережевої динаміки, і це дозволяє визначати найбільш критичні інформаційні джерела.

Для визначення стабільності інформаційного джерела необхідно провести дослідження розподілу кількості публікацій упродовж певного періоду часу шляхом визначення коефіцієнта нормованого розмаху кількості опублікованої інформації джерелом [11].

Показник Херста (H) — пов’язаний з коефіцієнтом нормованого розмаху:

$$\frac{R}{S} = \left(\frac{N}{2}\right)^{H}, H \geq 1, \qquad (1)$$

де S — середньоквадратичне відхилення ряду спостережень за інформаційним джерелом; R — розмах кількості опублікованої інформації; N — дні, за які відбуваються спостереження.

Виходячи з (1), отримуємо наступний вираз для визначення показника Херста:

$$H = \frac{\ln(R/S)}{\ln(N/2)}. \qquad (2)$$

Показник Херста представляє собою міру персистентності — схильності процесу до трендів (на відміну від звичайного броунівського руху). Значення $H > 0,5$ означає, що спрямована в певний бік динаміка процесу в минулому, найімовірніше, спричинить продовження руху в тому ж напрямку. Якщо $H < 0,5$, то прогнозується, що процес змінить спрямованість. $H = 0,5$ означає невизначеність — броунівський рух [11].

Для вивчення фрактальних характеристик тематичних інформаційних потоків за певний період для часових рядів, які належать до цих повідомлень, вивчалося значення показника Херста за (2).

При розрахунку показника Херста фактично визначається показник тематичного інформаційного потоку як фрактальна розмірність. Тобто, дослідження тематичних інформаційних потоків підтверджують припущення щодо самоподібності й ітеративності процесів у веб-просторі. Передрук, цитування, прямі посилання породжують подібність, що виявляється в стійких статистичних розподілах і відомих емпіричних законах. Аналіз самоподібності інформаційних масивів може розглядатись як технологія для здійснення прогнозування [11].

Для дослідження інформаційних джерел як експериментальну базу вибрано сервіс контент-моніторингу новин InfoStream, який дозволяє отримати інформацію про всі періодичні видання глобальної мережі Інтернет поточного та архівного періоду. Початковими даними пошуку вибрано щоденні видання, так як джерела, що публікують інформацію раз на тиждень чи на місяць, являються недостатньо закономірними для їхньої оцінки (http://infostream.ua).

Сервіс контент-моніторингу новин Infostream слугує для знаходження та відбору в Інтернеті новин за заданою тематикою, ключовими словами, часовими межами, морфологією, сюжетами, одночасного доступу в режимі пошуку до інформації з багатьох веб-сайтів, їхньої змістової обробки і, як наслідок, мінімізації зусиль користувача для відсіювання інформації, що дублюється, так званого «інформаційного шуму», зменшує ймовірність повторів і потрапляння до моніторингу застарілої чи неверифікованої інформації.

Головними перевагами системи InfoStream порівняно з традиційними мережевими інформаційно-пошуковими системами та зі звичайними новинними вебсайтами є:

1) оперативність — бази даних системи поповнюються кожні 15 хвилин, джерела скануються у мережі в міру їхнього оновлення, в той час як період індексації традиційних інформаційно-пошукових систем може вимірюватися тижнями;

2) доступність ретроспективного фонду — навіть якщо інформація видалена з веб-сайту джерела, вона збережена в інформаційному сховищі;

3) можливість селекції «дублів» — система здійснює автоматичне маркування ідентичної за змістом новинної інформації;

4) охоплення джерел — користувач має доступ до новин, що цікавлять його, одночасно з великої кількості веб-сайтів, зокрема і тих вибраних, які він звик переглядати щодня;

5) доступність ретроспективного фонду.

6) безперервність розвитку списку джерел — система InfoStream сканує понад 10000 джерел. Усі основні інформаційні сайти України та СНД, а також провідні закордонні інтернет-ресурси;

7) розширений доступ до інформації — користувачам системи InfoStream доступні не тільки заголовки або анонси, але і повні тексти новинних повідомлень, посилання на подібні документи тощо.

У процесі дослідження проаналізовано та відібрано із зазначеного переліку щоденні видання, які активно протягом трьох місяців публікували інформацію на своїх ресурсах.

При дослідженні стабільності та ефективності джерел, які публікують інформацію виявлені такі види процесів, що відбуваються з ресурсами під час їхнього життєвого циклу (рис. 1):

— майже не змінний процес публікувань джерелом (рис. 1,*а*);

— стрімке зменшення кількості публікацій ресурсом майже до його зупинки (рис. 1,*б*);

— короткострокове збільшення кількості публікацій джерелом (рис. 1,*в*);

— збільшення кількості опублікувань джерелом, що відбулося на постійній основі (рис. 1,*г*).

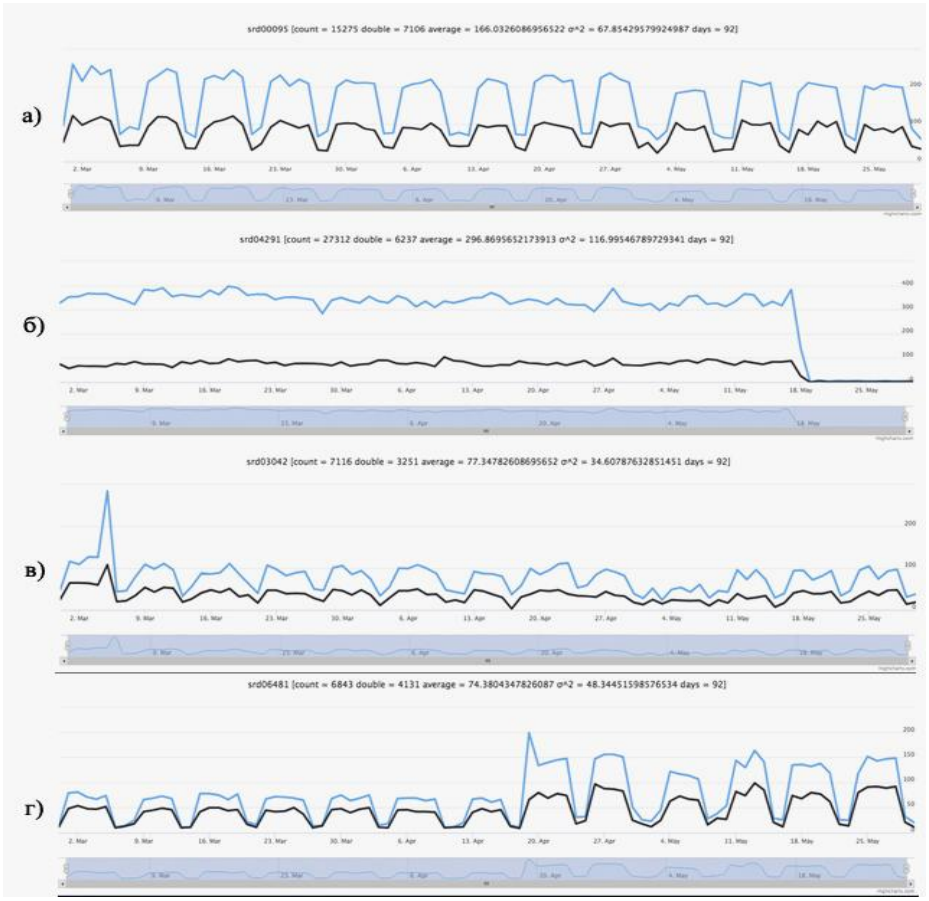

Рис. 1. Типовий приклад процесів, що можуть відбуваються з інформаційним джерелом під час життєвого циклу (верхні графіки — унікальні публікації, нижні — публікації-дублі з інших джерел)

Розглянемо джерело (рис. 1,*а*) з майже не змінним процесом публікувань упродовж усього періоду. Оцінивши вищевказаний графік, наглядно видно, що відображений ресурс достатньо стабільно публікував інформацію протягом 3 місяців, зниження темпу опублікувань відбувалося тільки на вихідні дні. У результаті розрахунку показника Херста та середньоквадратичного відхилення за даним ресурсом, було отримано результат, що дозволяє оцінити дане інформаційне джерело як стабільний ресурс.

Наступний вид процесу (рис. 1,*б*) — стрімке зменшення кількості публікацій ресурсом майже до його зупинки. На даному графіку візуально зображено процес зменшення кількості опублікувань інформаційним ресурсом, що свідчить про нестабільність даного джерела. Розрахувавши показник Херста та середньоквадратичне відхилення за даним ресурсом, отримано результат, що дозволяє оцінити дане інформаційне джерело як критичне інформаційне джерело, яке потребує постійного контролю.

Далі розглянемо випадок короткострокового збільшення кількості публікацій джерелом (рис. 1,*в*). На даному графіку візуально зображено короткотривале збільшення кількості опублікованої інформації ресурсом. Даний тип процесу ще називають «інформаційним вибухом», оскільки кількість опублікованої інформації у певний проміжок часу збільшується в рази, і таке явище триває недовго.

Візуально оцінивши графік (рис. 1,*в*), наглядно видно, що впродовж усього періоду даний ресурс стабільно опубліковував інформацію, але в певний період часу даним ресурсом опубліковано інформації в рази більше його середньодобового значення.

Дослідивши інформаційні ресурси, було визначено, що існують джерела, які підтримуються для інформаційних атак у сфері ЗМІ в необхідний період часу. Зазвичай, такі інформаційні джерела перебувають у режимі спокою, тобто кожного дня, як і звичайні джерела, публікують певну невелику кількість новин. Для простоти такі джерела також можуть використовувати новини, вже опубліковані на інших сайтах.

Наступним кроком розглянемо такий вид процесу як збільшення кількості опублікувань джерелом, яке відбулося на постійній основі (рис. 1,*г*). На даному графіку візуально зображено інформаційне джерело, яке активно збільшило кількість своїх публікацій і підтримує заданий поріг на постійній основі. Розрахувавши показник Херста та середньоквадратичне відхилення за даним ресурсом, отримано результат, що дозволяє оцінити дане інформаційне джерело як критичне.

Так як вищезазначене джерело збільшило кількість щоденних публікацій то це негативно відобразилося на показнику Херста, і даний факт не дозволяє повністю довіряти такому ресурсу, оскільки невідомі цілі, що призвели до таких змін.

Особливий інтерес викликає той факт, що кількість центральних ЗМІ, які публікують новини державного рівня, не збільшується. Зріст спостерігається тільки в сегменті регіональних і спеціалізованих ЗМІ, які потенційно можуть брати участь у проведенні інформаційних атак.

Проаналізувавши отримані дані, виявлено, що основна маса джерел мають показник Херста $H > 0,5$. Даний результат свідчить про стабільність таких джерел і те, що вони являються не критичними. Тому для оцінювання та дослідження

необхідно використовувати джерела з $H \le 0,5$. Такі видання є ненадійними і можуть використовуватися для інформаційних атак.

Також, слід відмітити, що під час дослідження виявлено особливість, що інформаційні видання зменшують кількість публікацій на вихідні дні, і тим самим збільшується показник середньоквадратичного відхилення кількості опублікованої інформації джерелом, і це впливає на загальний результат оцінювання.

Для більш ефективного оцінювання необхідно нормалізувати вхідні дані за тиждень щодо кількості публікацій кожного інформаційного видання. У результаті цього отримаємо такий вираз:

$$y_i = \frac{x_{i-3} + \ldots + x_i + \ldots + x_{i+3}}{7}, \tag{3}$$

$$z_i = \frac{y_i}{\sum_{k=1}^{N} y_k}, \tag{4}$$

де y_i — кількість публікацій від інформаційного джерела, що досліджується за день i; y_k — кількість публікацій від інформаційного джерела, що досліджується за день k; N — дні, за які відбуваються спостереження.

Середньоквадратичне відхилення σ у цьому випадку розраховується за формулою

$$\sigma = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(z_i - \bar{z})^2} \,\| \,\|, \tag{5}$$

де $\bar{z}$ — середнє арифметичне ряду спостережень z за N днів; N — дні, за які відбуваються спостереження; z_i — кількість публікацій від інформаційного джерела, що досліджується за день i.

Так як показник Херста являється оцінкою щодо стабільності та передбачуваності дій інформаційного джерела за період проведення аналізу, тому для дослідження необхідно використати отриманий раніше показник Херста до відношення середньоквадратичного відхилення з виразу (5).

Дослідивши отримані результати (рис. 2), візуально видно, що показник середньоквадратичного відхилення кількості створеної інформації майже для всіх джерел змінився. При цьому, слід відмітити, зміна середньоквадратичного відхилення пов'язана з тим, що в основному видання зменшували кількість публікацій на вихідні дні.

Далі, необхідно провести дослідження отриманих результатів і визначити вузли з ознаками «фейків» або ІО. Так як отримані результати показника Херста та середньоквадратичного відхилення за кількістю опублікованої інформації джерелом є ключовими параметрами, і виділити більш значимий з яких неможливо, тому необхідно застосувати метод, що дозволить з використанням цих параметрів провести оцінку вузлів, щоб виявити ті, які розповсюджували недостовірну інформацію.

У процесі дослідження закономірностей розповсюдження інформації джерелами ЗМІ глобальної мережі Інтернет розроблено алгоритм, який дозволяє оціню-

вати інформаційні джерела за двома критеріями та виділяти їх у групи, що потребують особливої уваги та є ненадійними.

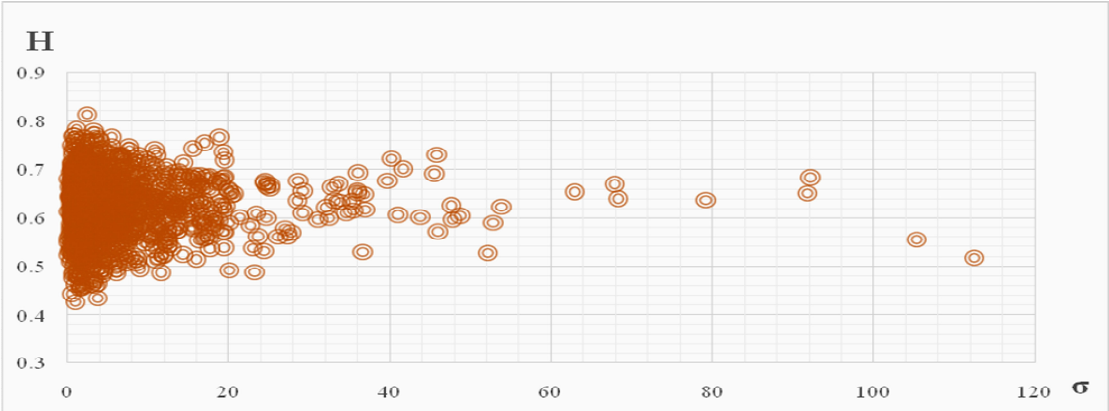

Рис. 2. Розподіл показника Херста із використанням нормалізації даних (вісь ординат) відносно середньоквадратичного відхилення кількості створених повідомлень джерелом (вісь абсцис)

Розробка алгоритму

Алгоритм містить наступні етапи (рис. 3).

1. Введення вхідних даних:

$\{source_i\}$ — дані про інформаційні джерела, складовими яких є середньоквадратичне відхилення, показник Херста, кількість унікальних опублікованих повідомлень за весь період, кількість інформації, яка дублюється на інших джерелах за весь період, текст усіх повідомлень, які публікувалися даним інформаційним джерелом;

$[result_i]$ — масив вихідних даних інформаційних джерел;

i — лічильник кількості кроків повторення;

s — інформаційне джерело, що досліджується;

t — поточне інформаційне джерело.

2. Сортування даних про інформаційні джерела в порядку зростання середньоквадратичного відхилення. В даному блоці відбувається перетворення множини даних про інформаційні джерела $\{source_i\}$ в масив $[source_i]$ у порядку збільшення показника зростання середньоквадратичного відхилення.

3. Перевірка умови, за якої значення довжини масиву $[result_i]$ має бути більше 0.

4. Присвоєння початкового значення змінній i, яке дорівнює довжині масиву $[source_i]$.

5. Присвоєння початкового значення змінній s, що дорівнює останньому елементу масиву $[source_i]$, який має найбільший показник середньоквадратичного відхилення, при цьому з масиву забирається даний елемент.

6. Додавання до масиву $[result_i]$ значення змінної s.

7. Присвоєння значення змінній i на одиницю менше поточного значення.

8. Перевірка умови, за якої значення змінної i має бути більше 0.
9. Вивід інформації з масиву $[result_i]$ та повна його очистка.

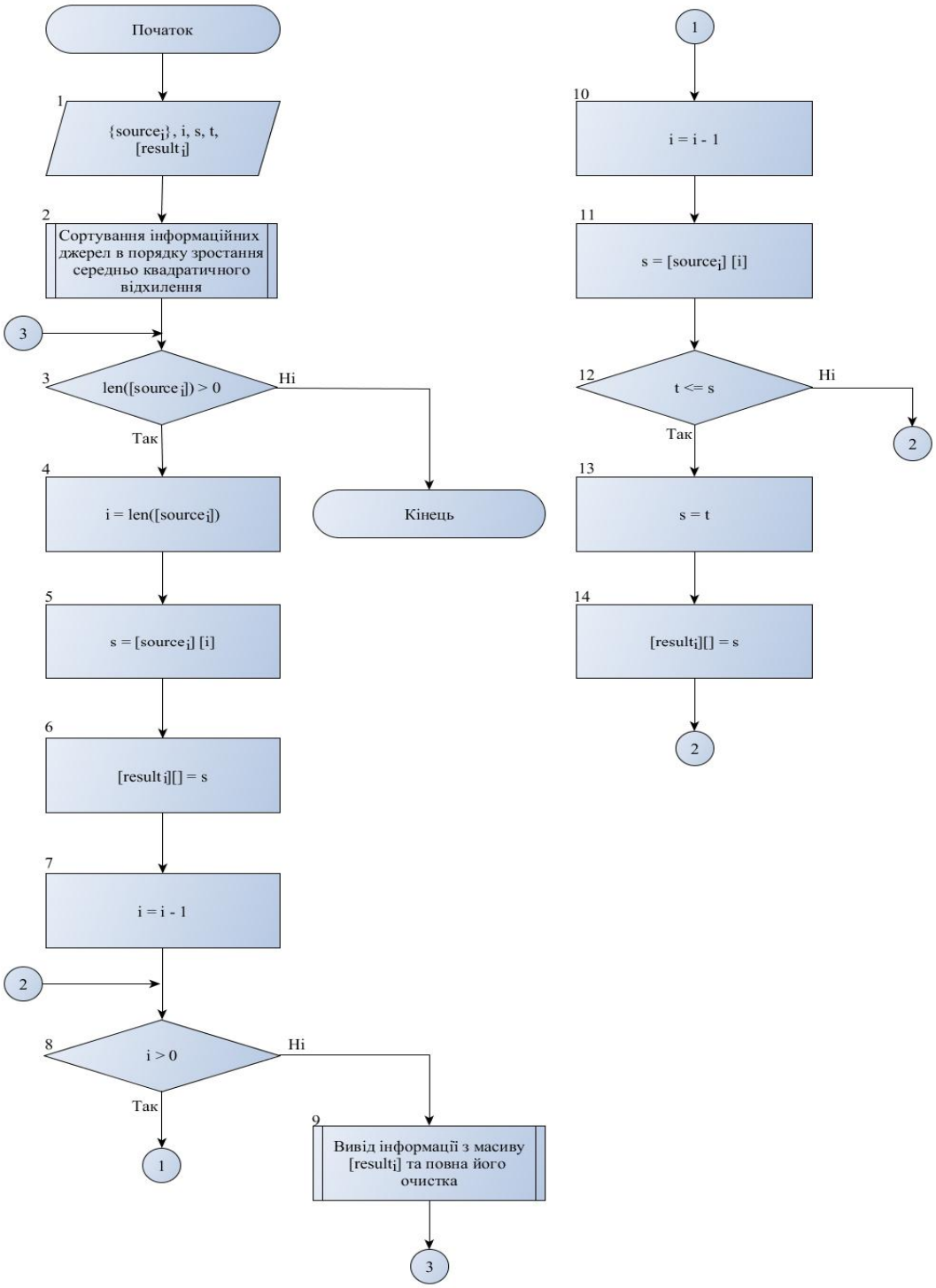

Рис. 3. Блок-схема алгоритму для оцінки інформаційного джерела за двома критеріями

10. Присвоєння значення змінній i на одиницю менше поточного значення.

11. Присвоєння значення змінній t, яка дорівнює значенню елемента з масиву $[source_i]$ під індексом i.

12. Перевірка умови, за якої значення змінної t має бути менше або дорівнювати значенню змінної s. При порівнянні двох змінних t та s порівнюються значення показника Херста та середньоквадратичного відхилення між собою у цих змінних.

13. Присвоєння значення змінній s, яка дорівнює значенню змінної t.

14. Додавання до масиву $[result_i]$ значення змінної s.

Для проведення дослідження інформаційних джерел використаємо вищевказаний алгоритм і проаналізуємо отримані дані. Після завершення роботи даного алгоритму, необхідно взяти перші 3 групи виведених результатів з даними про всі накопичені інформаційних джерела ЗМІ глобальної мережі Інтернет, так як з кожним наступник рівнем роботи алгоритму вірогідність знаходження інформаційних джерел, що проводять ІО, зменшується. Слід відмітити, що інформаційні джерела з показником Херста $H \le 0,5$ є такими, що змінюють спрямованість у процесі створення та розповсюдження інформації, також поведінку таких джерел неможливо спрогнозувати. Виходячи з цього, всі інформаційні джерела з показником Херста $H \le 0,5$ також повинні пройти дослідження експертами та поміститися в окрему групу **Layer 4**. Після проведення всіх вищезазначених кроків отримано результати, які показано на рис. 4.

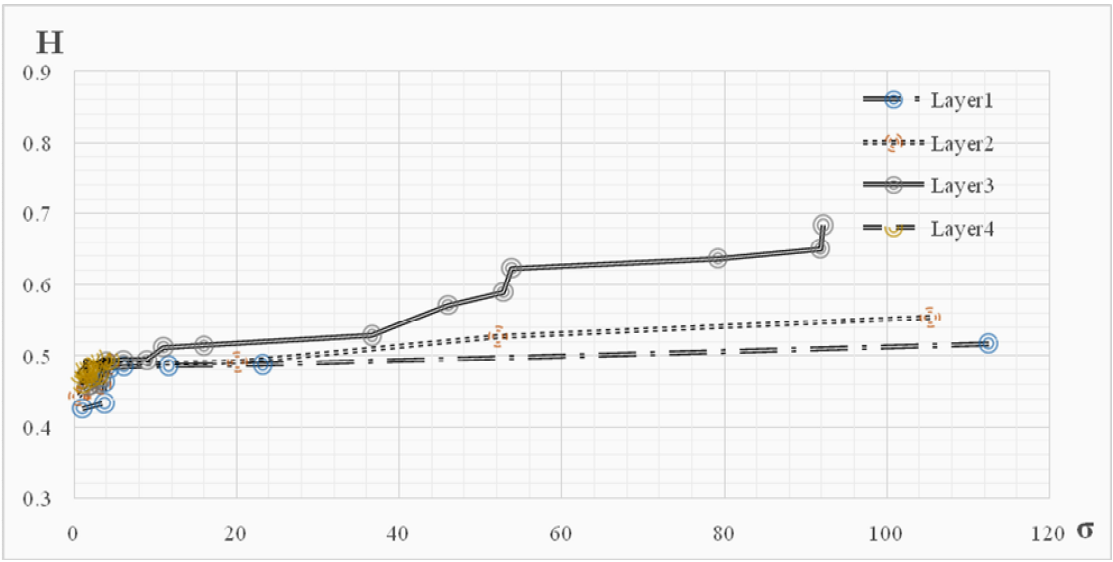

Рис. 4. Результат використання отриманого алгоритму показник Херста (вісь ординат) відносно середньоквадратичного відхилення кількості створених повідомлень джерелом (вісь абсцис)

На основі отриманих результатів (рис. 4) необхідно сформувати таблицю з даними (табл. 1).

Таблиця 1. Результати використання отриманого алгоритму для пошуку ненадійних інформаційних джерел ЗМІ глобальної мережі Інтернет

Ідентифікатор джерела	***H***	***σ***	**Кількість публікацій за період аналізу**
Layer 1			
srd04291	0,51739	112,49274	27312
srd00057	0,48767	23,23954	13508
srd00153	0,48648	11,6073	11447
srd05982	0,48543	6,10939	3119
srd05785	0,48298	4.3603	2536
srd06287	0,46456	3,74738	1410
srd06031	0,43378	3,73113	1965
srd07078	0,42595	0,98711	651
Layer 2			
srd06453	0,55404	105,3278	21573
srd01316	0,52707	52,13863	5442
srd05981	0,49112	20,09051	6010
srd06611	0,48773	4,42004	1933
srd06343	0,46043	3,42272	1508
srd05521	0,45633	1,79642	978
srd07735	0,45421	1,55245	666
srd07582	0,44333	0,56756	173
Layer 3			
srd00326	0,68345	92,14118	23182
srd00056	0,65078	91,80884	33064
srd02514	0,63729	79,17266	27761
srd00067	0,62372	53,785	11846
srd01752	0,58974	52,80888	9078
srd07931	0,57118	45,98039	6923
srd07629	0,52857	36,64814	4979
srd00080	0,51443	15,98651	8259
srd00139	0,51238	11,00949	8370
srd04612	0,49425	8,99097	3230
srd00053	0,49404	6,0819	4114
srd00541	0,49188	3,94601	2774
srd02293	0,47132	3,30473	1923
srd03734	0,46298	2,98705	1870
srd05494	0,4611	2,05512	1777
srd08136	0,45931	1,69615	1046
Layer 4			
srd05620	0,49415	4,43866	1953
srd03940	0,49226	3,43103	3411
srd04163	0,47382	3,12571	2531
srd04708	0,47085	2,14087	1495
srd02971	0,46226	0,96792	625
srd00463	0,49522	3,56686	2893
srd02115	0,48142	1,76244	1158
srd00183	0,476	1,56316	1152
srd06842	0,47576	0,69093	188
srd01543	0,49883	2,39959	860
srd05389	0,48228	1,75833	1145
srd04024	0,47797	1,3919	761

Продовження табл. 1

srd02969	0,4925	1,38766	846
srd07837	0,48051	1,3312	513
srd02318	0,48418	1,1721	764
srd01239	0,48609	0,94706	542
srd05239	0,48448	0,66684	295

Публікації інформаційних джерел з табл. 2 надані 4 експертам для порівняльної оцінки щодо виявлення в них ознак «фейків» або ІО. При цьому експерти оцінювали як зміст повідомлень, так і тенденції джерел щодо їхньої кількості опублікувань за весь період. Результати роботи експертів представлені в табл. 2.

Таблиця 2. Експертна оцінка пошуку інформаційних джерел, що проводили ІО

Етапи роботи алгоритму	**Ідентифікатор джерела**	**Посилання на джерело**
Layer 1	srd05785	http://www.business-top.info/
	srd06287	https://visti.ks.ua/
	srd06031	http://ukraine-today.net/
Layer 2	srd01316	https://www.tvr.by/
	srd05521	http://mashportal.ru/
	srd07582	http://lug-info.com/news/
Layer 3	srd01752	http://www.nakanune.ru/
	srd04612	http://evrazia.org/
Layer 4	srd04163	https://rus.azattyq.org/

Як бачимо, отримано закономірності у кількісній зміні опублікованої інформації джерелами в процесі їхнього життєвого циклу, і це дозволяє виявляти інформаційні джерела, що можуть використовуватись як інструмент інформаційного навіювання для маніпуляції у глобальній мережі.

Висновки

Запропоновано алгоритм, який дозволяє оцінити інформаційні джерела та виявити ті, в яких присутні ознаки «фейків» або ІО.

На основі експертної оцінки та розрахунку коефіцієнта ефективності можна зробити висновок, що з кожним наступним рівнем аналізу отриманих даних від використання отриманого алгоритма кількість інформаційних джерел, в яких виявлено ознаки «фейків» або ІО, за період оцінки падає. Це зв'язано з тим, що загальний рівень показника Херста з кожним рівнем збільшується, а значення середньоквадратичного відхилення зменшується, і в результаті надійність інформаційних джерел з кожним рівнем роботи алгоритму зростає.

Оцінивши результати роботи вищевказаного алгоритму та оцінку коефіцієнта його ефективності, можна зробити висновок про те, що отриманий алгоритм з ефективністю 18,4 % показав ті інформаційні джерела, в яких виявлено ознаки «фейків» чи ІО за період аналізу даних. Слід відмітити, що даний алгоритм показав інформаційні джерела ЗМІ глобальної мережі Інтернет, які в процесі своєї ро-

боти різко змінювали кількість опублікованої інформації за період свого життєвого циклу.

1. Расторгуев С.П. Информационная война. Проблемы и модели. Экзистенциальная математика: учеб. пособ. для студентов вузов, обучающихся по специальностям в области информационной безопасности. Москва: Гелиос АРВ, 2006. 240 с.

2. Lande D. and Shnurko-Tabakova E. OSINT as a part of cyber defense system. *Theoretical and Applied Cybersecurity*. 2019. No 1. P. 103–108.

3. Додонов А.Г., Ландэ Д.В. Методика аналитического исследования динамики событий на основе мониторинга веб-ресурсов сети Интернет. *Информационные технологии и безопасность: основы обеспечения информационной безопасности*. Материалы международной научной конференции ИТБ-2014. Киев: ИПРИ НАН Украины. 2014. С. 3–17.

4. Пальчук В. Сучасні особливості розвитку методів контент-моніторингу і контент-аналізу інформаційних потоків: Наук. пр. Нац. б-ки України ім. В.І. Вернадського: зб. наук. пр. / НАН України, Нац. б-ка України ім. В.І. Вернадського, Асоц. б-к України. Київ, 2017. Вип. 48. С. 360–374.

5. Потемкин А.В. Распознавание информационных операций средств массовой информации сети Интернет. Интернет-журнал «Науковедение». 2015. № 3. URL: http://naukovedenie.ru/PDF/139TVN315.pdf (свободный).

6. Почепцов Г.Г. Сучасні інформаційні війни. Київ: Вид. дім «Києво-Могилянська академія», 2015. 497 с.

7. Аверченков В.И., Спасенников В.В., Рытов М.Ю., Лексиков Е.В. Конкурентная разведка: технологии и противодействие: учеб. пособ. — Брянск: БГТУ, 2014. 200 с. (Серия «Организация и технология защиты информации»).

8. DMJ Lazer et al. The science of fake news. *Science*. 2018. Vol. 359. Issue 6380, P. 1094–1096. DOI: 10.1126/science.aao2998.

9. Nir Grinberg, Kenneth Joseph, Lisa Friedland, Briony Swire-Thompson and David Lazer. Fake news on Twitter during the 2016 U.S. presidential election. *Science*. 2019. Vol. 363. Issue 6425. P. 374–378. DOI: 10.1126/science.aau2706.

10. Anderson A. & Correa E. Critical explorations of online sources in a culture of «fake news, alternative facts and multiple truths». In G. Marks (Ed.). Proceedings of Global Learn 2019 Global Conference on Learning and Technology. 2019. P. 439–447. Retrieved August 14, 2019 from https://www.learntechlib.org/primary/p/210398/

11. Федер Е. Фракталы. Москва: УРСС, 2014. 256 с.

12. Ландэ Д.В. Фрактальные свойства тематических информационных потоков из Интернет. *Реєстрація, зберігання і оброб. даних*. 2006. Т. 8. № 2. С. 93–99.

13. Ландэ Д.В., Брайчевский С.М., Григорьев А.Н. Стабильность источников информации как один из параметров информационных потоков. *Компьютерная лингвистика и интеллектуальные технологии*: Труды международной конференции «Диалог-2006». Москва: Наука, 2006. С. 332–334.

14. Хорошко В.О., Хохлачова Ю.Є. Інформаційна війна. ЗМІ як інструмент інформаційного впливу на суспільство. Частина 1. *Ukrainian Scientific Journal of Information Security*. 2016. Т. 22. № 3. С. 283–288. DOI: 10.18372/2225-5036.22.11104.

Надійшла до редакції 10.08.2019