УДК 004.89

д.т.н., проф. **Лєнков С.В.** (ВІКНУ)
к.т.н., доц., **Джулій В.М** (ХмНУ)
Солодєєва Л.В. (ВІКНУ)

DOI: https://doi.org/10.17721/2519-481X/2022/77-09

МЕТОД ПРОТИДІЇ ПОШИРЕННЮ ТА ВИЯВЛЕННЯ ШКІДЛИВОЇ ІНФОРМАЦІЇ В СОЦІАЛЬНИХ МЕРЕЖАХ

В роботі продено дослідження задачі виявлення та протидії поширенню у соціальних мережах шкідливої інформації, в тому числі «фейкових новин». Особливо гостро стоїть необхідність протидії поширенню у соціальних мережах таких новин, що породжують хвилі паніки, які виникають під час пандемії. На теперішній час – війна в Україні. Фейкові новини поширюються у соціальних мережах у шість разів швидше, ніж правдиві дописи. Російська пропаганда стала одним з головних елементів війни в Україні, її якісно закамуфльовано під вигляд матеріалів західних ЗМІ - DW, CNN або BBC. Основна складність виявлення та протидії поширенню шкідливої інформації в соціальних мережах безпосередньо слідує із використанням на сучасному етапі тенденцій розвитку інформаційно - технологічної сфери, а саме: збільшення швидкості поширення шкідливої інформації в соціальних мережах; швидкості виникнення нових джерел поширення шкідливої інформації; збільшення об'єму інформації, що містить шкідливі повідомлення; швидкості тиражування повідомлень в мережі; кількості сценаріїв привернення уваги аудиторії; рівня гетерогенності даних. За своєю архітектурою соціальні мережі є багатокомпонентними рішеннями, в архітектурі мережі знаходяться: компоненти, які здійснюють обробку контенту; компоненти, які забезпечують функції маркетингу, адміністрування, зберігання даних. Соціальні мережі не містять окремого компонента виявлення та протидії поширенню шкідливій інформації в мережі.

Проведений аналіз та дослідження оцінювання ефективності інформаційно-аналітичних систем та інформатизації процесів, показали, що проблема виявлення та протидії поширенню в соціальних мережах шкідливої інформації не може вважатися вирішеною і вимагає на даному етапі проведення нових досліджень та дозволяє визначити загальні вимоги до системи протидії, в основу реалізації якої, покладено модельно-методичний апарат. З метою підвищення ефективності системи протидії в Інтернет - мережах вирішена задача розробки відповідного підходу підвищення обґрунтованості прийнятого рішення на протидію поширенню та виявлення шкідливої інформації за рахунок збільшення числа параметрів, що враховуються при виборі інформаційного об'єкта впливу та дійових контрзаходів. Вирішення поставленої задачі, досягається за рахунок проведення ранжування контрзаходів та аналізу джерел мережі шкідливої інформації. Запропонований метод протидії та виявлення в соціальних мережах поширенню шкідливої інформації, ґрунтується на використанні запропонованих моделей, алгоритмів, забезпечує, на відміну від аналогів, аналіз інформації соціальних мереж; формування списків інформаційних об'єктів впливу для проведення протидії об'єктам, сортування інформаційних об'єктів; надання оператору системи протидії пропонованого та альтернативних варіантів з обґрунтуванням вибору. Розроблений метод виявлення та протидії поширенню шкідливої інформації в соціальних мережах відрізняється від існуючих, використанням запропонованих алгоритмів оцінки джерел повідомлень, аналізом та ранжуванням контрзаходів, в результаті підвищується обґрунтованість прийняття рішення про протидію поширенню шкідливої інформації та вибору

контрзаходу, відповідним чином скорочується час роботи оператора системи у процесі протидії поширенню шкідливої інформації у соціальних мережах.

Ключові слова: шкідлива інформація, соціальні мережі, контрзаходи, джерела повідомлень, метод протидії, інформаційна система.

Вступ. На сучасному етапі, глибина проникнення у повсякденне життя людства, соціальних мереж є значною. Перевагою соціальних мереж є можливість оперативно висловлювати свою думку учасникам комунікації, значній кількості групі людей, публікувати медіа-, відео файли. Соціальні мережі є не лише засобом спілкування групи людей, а також інструментом поширення інформації в мережі, в тому числі шкідливої інформації. Очевидною проблемою інформаційної безпеки суспільства, сьогодення стала шкідлива інформація, також необхідно зазначити, що злочинні та терористичні угрупування беруть на озброєння, дедалі частіше, засоби інформаційного впливу, розробляють та пишуть стратегії, спрямовані на залучення нових адептів та розширення сфери впливу через соціальні мережі. Таким чином, однією зі складових надійного забезпечення інформаційної безпеки держави є проведення аналізу, виявлення, моніторинг та активна протидія розповсюдженню шкідливої інформації в соціальних мережах [1,2].

До шкідливої інформації, поширеної в соціальних мережах, частіше відносять «фейкові новини». Особливо гостро стоїть необхідність протидії поширенню у соціальних мережах таких новин, що породжують хвилі паніки, які виникають під час пандемії. На теперішній час – війна в Україні. Фейкові новини поширюються у соціальних мережах у шість разів швидше, ніж правдиві дописи. Російська пропаганда стала одним з головних елементів війни в Україні, її якісно закамуфльовано під вигляд матеріалів західних ЗМІ - DW, CNN або BBC.

Аналіз останніх досліджень та постановка задачі. Проблема виявлення та протидії поширенню у соціальних мережах шкідливої інформації, в тому числі «фейкових новин», має недостатньо науково-технічних рішень. Відомі підходи та засоби протидії виявлення в соціальних мережах шкідливої інформації не відповідають вимогам до адекватності, повноти, швидкості та точності прийнятих рішень. Дана ситуація зумовлена кількома причинами: система розділена на два не пов'язаних модулі – моніторинг та протидія, між якими знаходиться оператор. Соціальні мережі складаються з множини різнорідних повідомлень, які мають складну структуру, дана особливість повідомлень не в повній мірі враховується при виборі засобів протидії – джерело, тип повідомлення, а також інші характеристики. Необхідно обробляти надвеликі об’єми інформації в реальному масштабі часу і в стислий термін вибирати відповідний інструмент для проведення контрзаходу протидії поширенню шкідливої інформації, оператор системи протидії в ручному режимі не в змозі зупинити поширення шкідливої інформації в соціальній мережі [3,4].

На теперішній час, основна складність виявлення та протидії поширенню шкідливої інформації в соціальних мережах безпосередньо слідує із використанням на сучасному етапі тенденцій розвитку інформаційно - технологічної сфери, а саме: збільшення швидкості поширення шкідливої інформації в соціальних мережах; швидкості виникнення нових джерел поширення шкідливої інформації; збільшення об’єму інформації, що містить шкідливі повідомлення; швидкості тиражування повідомлень в мережі; кількості сценаріїв привернення уваги аудиторії; рівня гетерогенності даних. Таким чином, розглянуті тенденції поширення шкідливої інформації в Інтернет мережах, зумовлюють необхідність підвищення ефективності протидії та виявлення в соціальних мережах шкідливої інформації, враховуючи також при цьому, обґрунтованість та оперативність [5,6].

Швидкість змін в інформаційному полі суспільства є досить великою, уповільнена та невірна реакція з боку органів безпеки держави може призвести до катастрофи суспільства.

Адаптація до змін в інформаційному полі держави, потребує на сучасному етапі значних і швидких коригувань у сфері захисту інформаційного поля держави. Необхідно бути більш здатним краще протидіяти та відновлюватися після кризи, більш обізнаними щодо характеру та потенціалу кризових ситуацій.

Під категорію шкідливої інформації, з погляду забезпечення державної безпеки підлягають наступні види інформації: інформація, включена до державного списку екстремістських матеріалів [2]; інформація, що ідентифікується як заборонена до поширення в державі [7]; персональні дані; інформація для службового користування; конфіденційна інформація. Забороняється поширення інформації в Інтернет мережі, спрямованої на пропаганду війни, розпалювання релігійної, національної, расової ненависті та ворожнечі, інформації, за поширення якої передбачено адміністративну, кримінальну відповідальність.

За своєю архітектурою соціальні мережі є багатокомпонентними рішеннями, в архітектурі мереж знаходяться: компоненти, які здійснюють обробку контенту; компоненти, які забезпечують функції маркетингу, адміністрування, зберігання даних. Соціальні мережі не містять окремого компонента виявлення та протидії поширенню шкідливій інформації [8,9].

Проведений аналіз та дослідження оцінювання ефективності інформаційних систем та інформатизації процесів, показали, що проблема виявлення та протидії в соціальних мережах шкідливої інформації не може вважатися вирішеною і вимагає на даному етапі проведення нових досліджень.

Протидія поширенню шкідливої інформації у соціальних мережах є важливим елементом інформаційної безпеки особистості, суспільства, держави, проте більшість систем, на теперішній час не враховує простір функціональності системи виявлення та протидії поширенню шкідливою інформації, системи розділені на два модулі: моніторинг та протидія, необхідна автоматизація процесу протидії. Соціальні мережі мають складну структуру, параметри повідомлень та джерел не в повній мірі враховуються під час вибору засобів протидії та виявлення шкідливої інформації. При розробці методу протидії поширенню шкідливої інформації в Інтернет мережі, необхідно: в повній мірі, враховувати кількість повідомлень на сторінці, характеристики джерела, зворотній зв'язок від джерела та аудиторії повідомлень; підтримувати дві стадії роботи системи протидії: налаштування, експлуатація; ранжувати контрзаходи з урахуванням коефіцієнтів складності [1,10].

Дослідження задач побудови систем протидії поширенню та виявлення шкідливої інформації в соціальних мережах. Проведений порівняльний аналіз досліджень в області протидії та виявлення шкідливої інформації в соціальних мережах дозволив визначити загальні вимоги до системи протидії, в основу реалізації, покладено модельно-методичний аппарат [1,2,5, 7-9]. Розглянемо необхідний фундамент функціональності системи протидії поширенню та виявлення шкідливої інформація в соціальних мережах (рис. 1).

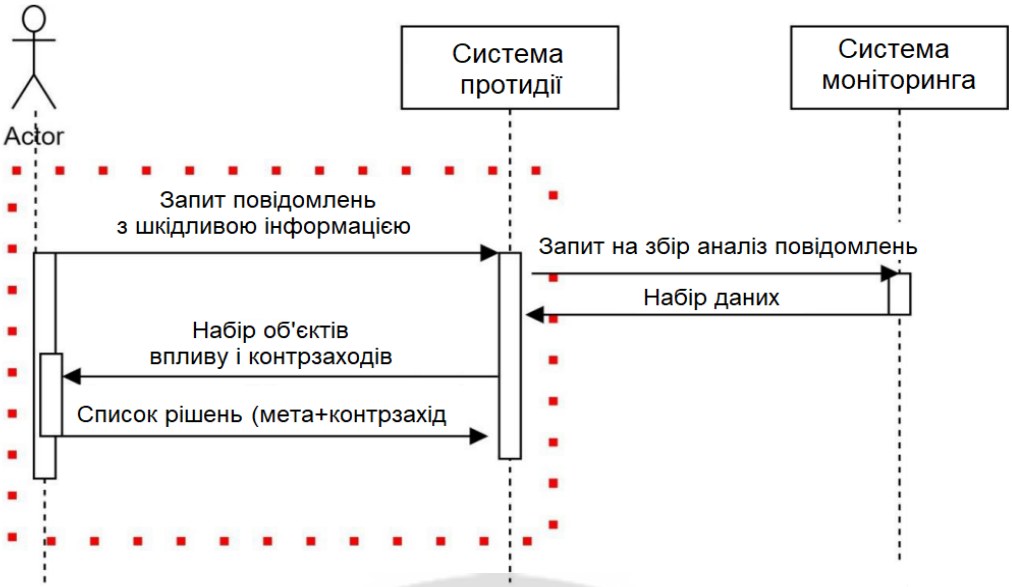

Рисунок 1 – Фундамент функціональності системи протидії поширенню та виявлення шкідливої інформації у соціальних мережах

Система протидії (рис. 1) може бути центральним елементом у процесі виявлення шкідливих повідомлень в соціальних мережах. Процеси у системі протидії та виявлення шкідливих повідомлень в Інтернет мережі можуть бути автоматизовані з використанням запропонованих алгоритмів і відповідних програмних компонентів.

Вимоги до системи протидії розділимо на дві групи: функціональні та не функціональні. Функціональні вимоги можуть бути реалізовані шляхом проектування та розробки архітектури компонентів, програмних прототипів. Функціональні вимоги - функції, які має виконувати система протидії. Не функціональні вимоги можуть бути реалізовані шляхом розробки відповідних моделей та алгоритмів. Не функціональні вимоги описують цільові характеристики системи: оперативність, вимоги щодо обґрунтованості та ресурсоспоживання.

Функціональні вимоги до системи виявлення та протидії поширенню шкідливої інформації в соціальних мережах: формування задачі на збір повідомлень; аналіз повідомлень для системи моніторингу; аналіз джерел повідомлень в отриманому наборі даних; налаштування доступних заходів виявлення та протидії поширенню шкідливоїінформації в інформаційно-аналітичній системі; сортування та ранжування об'єктів впливу на отриманому наборі даних; вибір засобів впливу для протидії; сортування та ранжування доступних контрзаходів з бази даних контрзаходів для відповідного набору отриманих даних; генерація звітів про роботу системи виявлення та протидії в адаптованому вигляді, для адміністратора системи; генерація звітів про отримані результати у адаптованому вигляді, для експерта з інформаційної безпеки організації.

Задача дослідження полягає у розробці: моделей - шкідливої інформації, джерела повідомлень та соціальної мережі; алгоритмів проведення аналізу джерел поширення шкідливої інформації у соціальних мережах та проведення ранжування контрзаходів; методу виявлення та протидії поширенню шкідливої інформації у соціальних мережах з урахуванням вимог до обґрунтованості; архітектури компонентів інформаційно-аналітичної системи протидії поширеню шкідливої інформації в соціальних мережах.

Метод протидії поширенню та виявлення шкідливої інформації в соціальних мережах. Протидія поширенню шкідливої інформації може здійснюватися на основі проведеного аналізу та дослідження джерел повідомлень [1,5,7,10]. Об'єктом деструктивного

впливу шкідливої інформації є користувачі соціальних мережі. Кожен користувач залишає відповідний слід під час перегляду повідомлення в мережі і може залишити відповідну реакцію. Таким чином, алгоритм оцінки джерел повідомлень, повинен враховувати зворотній в'язок від користувачів шкідливої інформації в соціальній мережі, у процесі інформаційного обміну. Множина $ACTIVITY$ включає всі ознаки зворотнього зв'язку від користувачів шкідливої інформації соціальної мережі (1):

$$ACTIVITY\{countrepost, countLike, countComment, countView\}, \quad (1)$$

де $countrepost$ – кількість посилань на джерело («репостів»), $countLike$ - кількість позначок, $countComment$ – кількість коментарів, $countView$ – кількість переглядів. До множини $SOURCE\{sourceID, messageURL\}$ входить ідентифікатор джерела, адреса повідомлень у соціальній мережі.

Таким чином, необхідно знайти кортеж атрибутів, на основі елементів множини $ACTIVITY$ і відношення *R*, які характеризуть $SOURCE$ (2).

$$R(SOURCE, MESSAGE) - < index_{active}, index_{viewability}, index_{impact} >, \quad (2)$$

де $index_{active}$ - індекс активності, $index_{viewability}$ - індекс перегляду, $index_{impact}$ - індекс впливу джерела повідомлень.

Значення індексів перегляду, активності, впливу джерела повідомлень знаходиться в діапазоні від 0 до 2, до значень індексів застосовується нормування – порівняльна нормалізація, ідеальне значення є максимум.

Розглянемо алгоритм оцінки джерел повідомлень соціальної мережі:

1. На вхід алгоритму подається кортеж: $< sourceID, messageURL, repostCount, likesCount, commentCount, viewCount >$.

2. Обчислення індексу активності джерел повідомлень соціальної мережі: формуються хеш-таблиці (key-value) - <sourceID, urlCOUNTER>, <messageURL, likesCount>, <messageURL, commentCount>, <messageURL, repostCount>; в наступній хеш-таблиці сумуються показники commentCount, repostCount, likesCount для messageURL, формується, в даному випадку кортеж $< message.SourceID, activityIndex >$; значення з кортежу $< message.SourceID, activityIndex >$ сумуються, результат ділиться на показник *urlCOUNTER* з першої хеш-таблиці, таким чином формується набір індексів активності джерел повідомлень, до яких застосовується нормування.

3. Обчислення індексу перегляду джерел повідомлень соціальної мережі: формуються хеш-таблиці (key-value), $\{SourceID : urlCOUNTER, messageURL : viewCount\}$. Значення viewCount всіх $messageURL$ сумуються і отриманий результат ділиться на $urlCOUNTER$. В результаті формується кортеж $< SourceID, viewIndex >$. Індекси переглядів нормуються.

4. Обчислення індексу впливу джерела повідомлень соціальних мереж: для кожного джерела повідомлень перемножуються індекси переглядів та активності, в результаті отримаємо значення індексу впливу, також для нього використаємо порівняльне нормування. На виході алгоритму оцінки джерел повідомлень соціальної мережі формується кортеж $< sourceID, activityIndex, viewIndex, impactIndex >$.

Алгоритм оцінки джерел повідомлень соціальної мережі в процесі інформаційного обміну враховує зворотній зв'язок, його кількісні характеристики від аудиторії поширення шкідливої інформації, перетворює їх у якісні індекси.

Алгоритм сортування об'єктів впливу соціальної мережі. В основі існуючих рішень, методів протидії поширенню шкідливої інформації в соціальних мережах лежать підходи виявлення із шкідливою інформацією інформаційних об'єктів. Розглянуті підходи опираються

на концепцію - «виявлення-протидія» інформаційних об'єктів [3,10]. Інформаційні об'єкти, які містять джерела шкідливої інформації в соціальних мережах - мільйони. Інформаційні об'єкти можливо поділити за індексами активності та потенціалом джерела, таким чином, можна застосувати фільтр у процесі вибору інформаційного об'єкта протидії та задати пріоритет. Алгоритм сортування інформаційних об'єктів впливу соціальної мережі пов'язаний із алгоритмами оцінкою джерел повідомлень та ранжування за потенціалом, отримує вхідні дані з них, сортує інформаційні об'єкти впливу за пріоритетом на виході. Цільова функція об'єктів впливу за пріоритетом задається наступною формулою:

$$f(S) \to l_{pr}^{s} = l_{p}^{s} + l_{i}^{s} = [0,4], \quad (3)$$

де S – джерело повідомлень, l_{pr}^{s} - пріоритет джерела повідомлень, l_{p}^{s} - потенціал, l_{i}^{s} - індекс впливу.

Правила вибору об'єкта впливу *Target:* $\left\{source \in TARGET \mid I_{pr}^{s} \cong \max\right\}$; $\left\{message \in TARGET \mid I_{pr}^{s} \cong \min\right\}$, де $TARGET$ - множина інформаційних об'єктів впливу.

Алгоритм сортування об'єктів впливу соціальної мережі наведено на рис. 2. На вхід алгоритму сортування об'єктів (рис. 2) передається набір кортежів $< messageURL, sourceID, potentialIndex, activityIndex, viewIndex, impactIndex >$. На першому етапі роботи алгоритму обчислюється середнє арифметичне індексу впливу всіх джерел повідомлень, виділяються об'єкти з низьким та високим пріоритетом. Формуються кортежі з індексом пріоритету $1 \le l_{pr}^{s} \le 3$ $< messageURL, sourceID, potentialIndex, activityIndex, viewIndex, impactIndex >$.

Результат роботи алгоритму - набір кортежів та два списки: набір кортежів *Priority_Medium*, передається оператору для вибору та додаткової оцінки інформаційного об'єкта впливу між адресою сторінки в соціальній мережі та адресою повідомлення; *Priority_High* – цілі *Target*, *sourceID* є інформаційним об'єктом впливу, для прийняття заходів протидії мають високий пріоритет; *Priority_Low* – цілі *Target*, *messageURL* є інформаційним об'єктом впливу, для прийняття заходів протидії мають низький пріоритет. Алгоритм сортування інформаційних об'єктів впливу соціальної мережі формує пріоритетні списки для протидії поширенню шкідливої інформації.

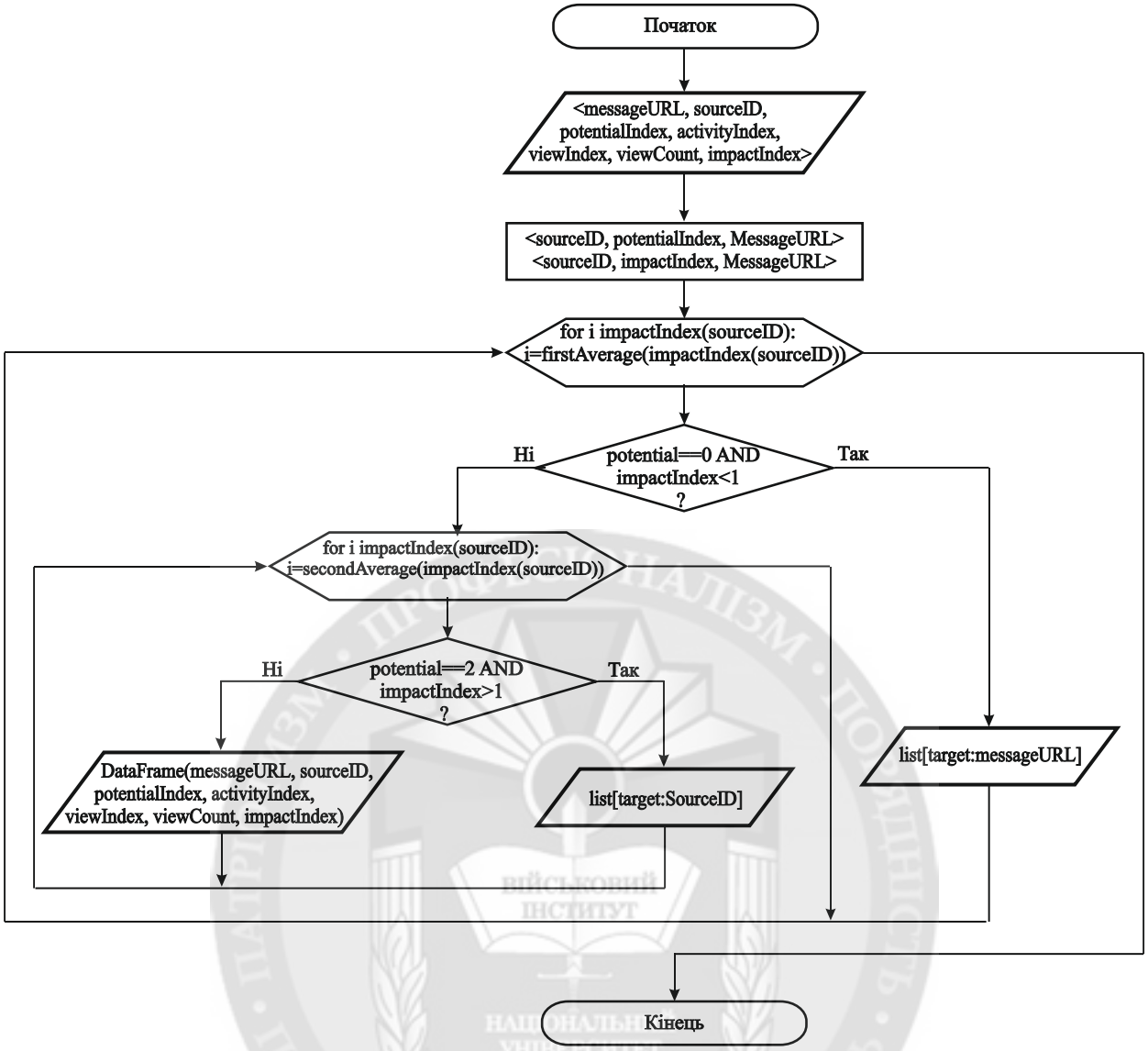

Рисунок 2 – Алгоритм сортування об'єктів впливу соціальної мережі

Метод протидії поширенню в соціальних мережах шкідливої інформації вирішує задачу інформаційної підтримки процесу ухвалення рішень та включає: проведення аналізу зібраної та обробленої інформації; вироблення, на основі проведеного аналізу повідомлень, варіантів рішень; проведення оцінки отриманих варіантів, вибір найкращого варіанта; надання обраного та альтернативних варіантів, особі, яка приймає рішення, з обґрунтуванням вибору.

Метод протидії, відповідно до життєвого циклу інформаційних систем, поділяється на два етапи: налаштування та експлуатацію. На стадії формування вхідних даних та налаштування системи протидії надаються: списки доступних у системі контрзаходів, їх коефіцієнти; списки інформаційних загроз; списки доступних агентів реалізації; формується список ранжованих контрзаходів. Стадія експлуатації включає: аналіз об'єктів впливу та їх сортування; отримання інформації від системи моніторингу; формування пар ціль-контрзахід; запуск протидії.

На рисунках 3 та 4 наведено загальне представлення методу протидії в соціальних мережах поширенню та виявлення шкідливої інформації.

Стадія налаштування методу протидії та формування вихідних даних включає:

1. Налаштування системи запитів. Оператор, відповідно до інформаційно-ознакової моделі загроз [7], формує список інформаційних загроз та їх ознак. Після отримання від

оператора інформаційних загроз та їх ознак, формується перелік загроз та ознак (табл. 1). Списки загроз та їх ознак, отриманих в результаті виконання налаштування системи запитів, зберігаються у загальному сховищі даних.

Таблиця 1

Список загроз та їх ознак

Загроза	Шкідлива інформація у соцмережах	Інформаційні ознаки
T_1	Наркотики купити	a_1
	Наркотики рецепт виготовлення	a_2
T_2	Вибуховий пристрій набір для збирання з інструкцією	b_1
T_3	Секретний алгоритм захисту телефонних дзвінків	c_1

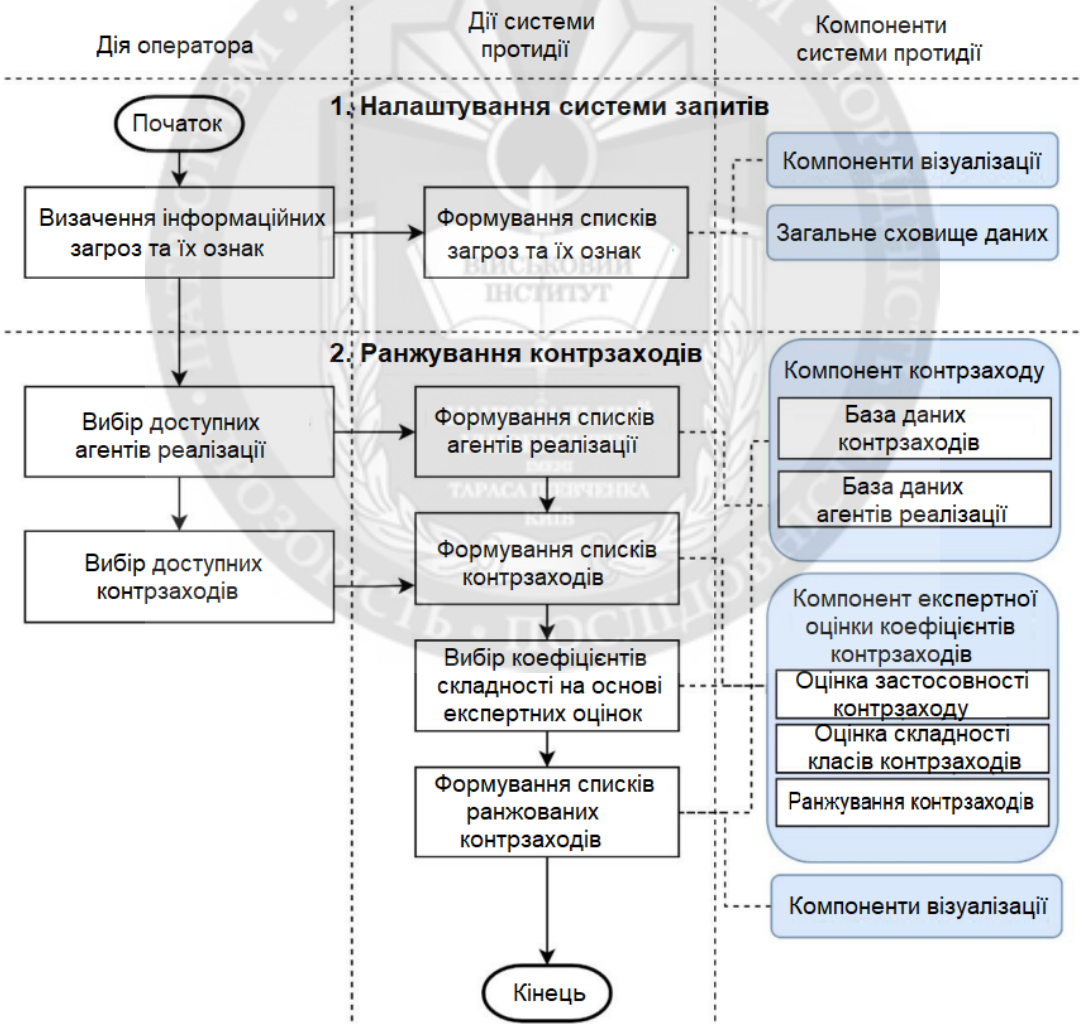

Рисунок 3 – Метод протидії в соціальних мережах поширенню та виявлення шкідливої інформації

2. Ранжування контрзаходів. Оператор вибирає доступні агенти реалізації: браузер; оператор зв'язку; black_list; антивірус; система батьківського контролю; операційна система. Формується та зберігається список доступних агентів реалізації. Оператор вибирає доступні контрзаходи: блокування через соцмережу; блокування через оператора зв'язку; блокування через спеціальне програмне забезпечення; блокування через black_list; фільтрація через систему батьківського контролю; фільтрація через антивірус. Формується список контрзаходів протидії, на основі експертних оцінок формуються коефіцієнти складності, згідно алгоритму вибору коефіцієнтів складності. Алгоритм вибору коефіцієнтів складності використовує наступні величини: вага w_i, визначає внесок у складність контрзаходу класу KC_i; рівень складності $lc_{i,j}$, визначає внесок у складність контрзаходу екземпляра класу $kc_{i,j}$; початкова складність cw_x заходу протидії. Величини залежать від кваліфікації співробітників, доступних ресурсів та задаються експертним шляхом. Для вибору значень пропонується використовувати Дельфі-метод експертних оцінок, в результаті серії дій експертів формується узагальнений результат, який дозволяє уникнути суб'єктивних оцінок [4,11].

Алгоритм вибору коефіцієнтів складності включає наступні кроки:

1. Вибір експертів. Групі експертів надаються відомості про можливі заходи протидії.

2. Голосування. Визначаються властивості які застосовуються до заходів протидії. Для кожної величини $cp_{x,i,j}$ експерти виставляють оцінки застосовності від одиниці до десяти.

3. Опрацювання результатів. Виконується усереднення отриманих значень (4):

$$cp_{x,i,j} = \frac{\sum_{l=1}^{N} cp_{x,i,j,l}}{10 \cdot N} \tag{4}$$

Отримане значення округляється до 0 чи 1, і визначається, чи застосовний даний екземпляр $kc_{i,j}$ класу властивостей заходів протидії для даного контрзаходу.

4. Голосування. Для уточнючих величин $\left(w_i, lc_{i,j}\right)$ експерти виставляють оцінки складності від 1 до 10.

5. Опрацювання результатів. Виконується усереднення отриманих значень (5):

$$w_i = \frac{\sum_{l=1}^{N} w_{i,l}}{N}$$
$$lc_{i,j} = \frac{\sum_{l=1}^{N} lc_{i,l}}{N} \tag{5}$$

6. Голосування. Експерти для заходів протидії виставляють оцінки початкової складності cw_x від 1 до 10.

7. Опрацювання результатів. Виконується усереднення для початкової складності отриманих значень (6).

$$coefficient\left(cw_i\right) = \frac{\sum_{l=1}^{N} cw_{x,l}}{N} \tag{6}$$

Результатом роботи алгоритму є отримані показники визначення складності застосування заходів протидії.

Розглянемо метод протидії в соціальних мережах поширенню та виявлення шкідливої інформації на стадії експлуатації. Етап експлуатації аналізу об'єктів впливу та запиту інформації містить наступні кроки:

1. Запит на збирання інформації (даних). Оператор із збереженого списку вибирає інформаційні загрози, задає нові інформаційні ознаки, у випадку необхідності. Оператор запускає процес збирання інформації, система протидії поширенню та виявлення шкідливої інформації надсилає запит до моніторингу зовнішніх систем та отримує, як результат, набір даних із повідомленнями, джерелами та параметрами, що містять шкідливу інформацію, необхідними для подальшого аналізу.

2. Сортування та ранжування об'єктів впливу: джерела ранжуються за потенціалом та оцінюються, формуються кортежі $< messageURL, sourceID, potentialIndex, activityIndex, viewIndex, impactIndex >$. Далі сортуються інформаційні об'єкти впливу за пріоритетом, формуються списки, які в результаті передаються оператору.

3. Протидія поширенню шкідливої інформації в соцмережах. Оператор системи отримує інформацію про потенціал джерела мережі, на яке, опублікованих на його сторінці у соціальній мережі, впливає кількість повідомлень, інформацію про пріоритет впливу, на який впливає кількість переглядів, рівень активності користувачів джерела. Оператор коригує списки об'єктів впливу, формуються пари ціль-контрзахід, перевірка відповідних пар оператором та запуск системи протидії поширенню шкідливої інформації в соціальних мережах. Оператор передає команду на запуск системи протидії поширенню шкідливої інформації в соціальних мережах, запускається через агентів реалізації, демонструє проміжні результати процесу проведення протидії оператору системи. Формується звіт про результати роботи системи протидії, інформаційній загрозі та визначеними у ході експлуатації системи об'єктів впливу протидію.

Вхідними даними методу протидії поширенню шкідливої інформації в соціальних мережах є: параметри об'єктів впливу, відповідно до яких оператор розподіляє черговість прийняття рішення про протидію; сформовані пари ціль-контрзахід для протидії поширенню шкідливої інформації у соціальних мережах через доступні агенти реалізації; контрзаходи та їх коефіцієнти, інформаційні загрози, доступні агенти реалізації заходів протидії, ознаки.

Запропонований метод протидії поширенню та виявленню шкідливої інформації в соціальних мережах, з урахуванням вимог до обґрунтованості, на різних етапах життєвого циклу дозволяє: визначити потенціал джерела повідомлень, значення якого залежить від кількості повідомлень на сторінці; оцінити індекс активності джерела повідомлень мережі, на значення впливає рівень активності користувачів повідомлень із вмістом шкідливої інформації; оцінити індекси перегляду повідомлень мережі, також джерела; визначити індекс впливу джерела повідомлень, значення залежить від активності та перегляду інформації в цілому.

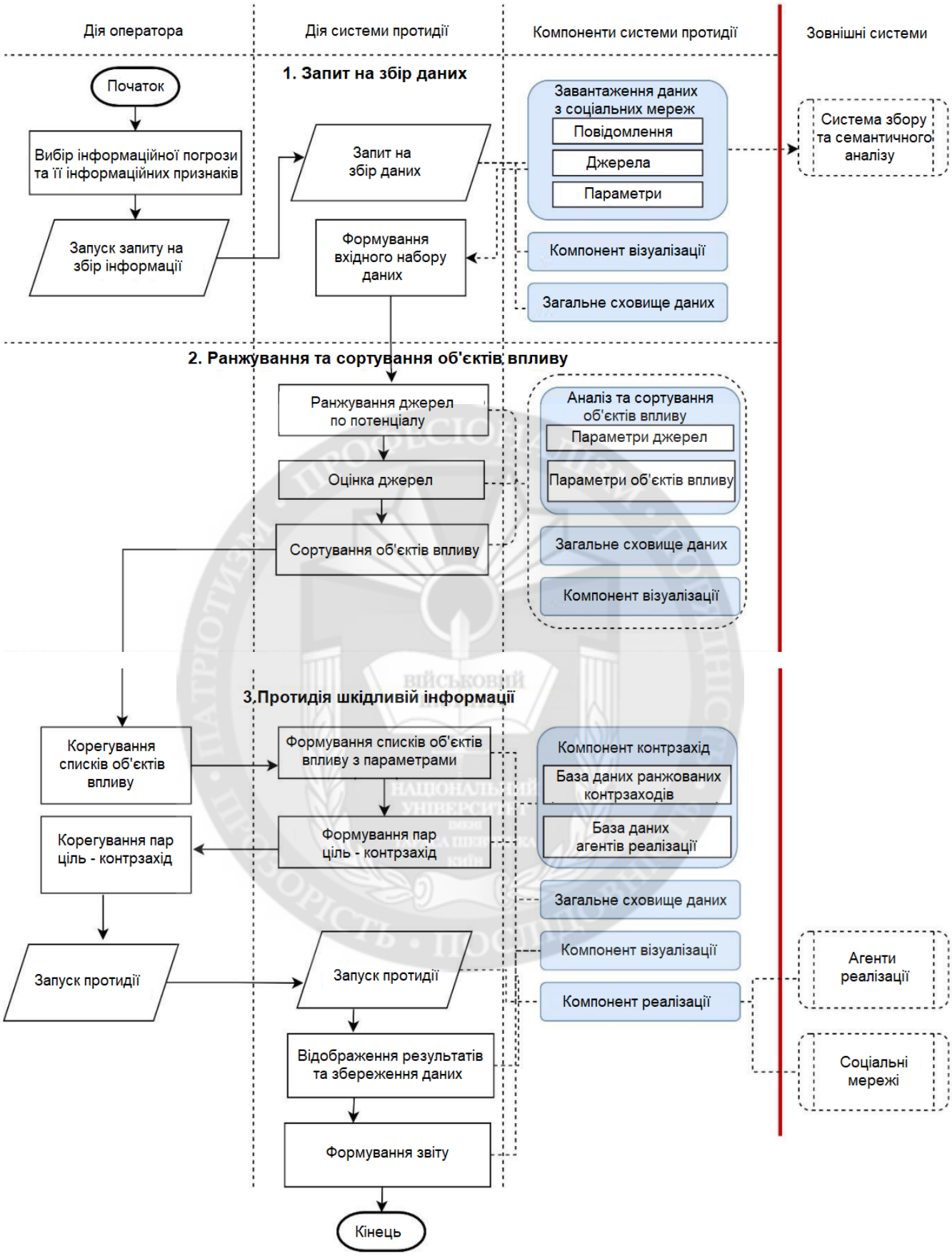

Рисунок 4 – Метод протидії в соціальних мережах
поширенню та виявлення шкідливої інформації на стадії експлуатації

Метод протидії дозволяє: визначити пріоритет об'єкта впливу протидії, на об'єкт впливу впливають індекс впливу та потенціал джерела; для підтримки прийняття рішення оператором, сортувати об'єкти впливу протидії за пріоритетом; сформувати відповідні пари ціль-контрзахід, для підтримки прийняття відповідного рішення про протидію поширення шкідливої інформації в соціальній мережі.

Висновки. З метою підвищення ефективності системи протидії в Інтернет - мережах вирішена задача розробки відповідного підходу підвищення обґрунтованості прийнятого рішення на протидію поширення та виявлення шкідливої інформації за рахунок збільшення числа параметрів, що враховуються при виборі інформаційного об'єкта впливу та дійових контрзаходів. Вирішення поставленої задачі досягається за рахунок проведення ранжування контрзаходів та аналізу джерел мережі шкідливої інформації. Запропонований метод протидії та виявлення в соціальних мережах поширення шкідливої інформації, ґрунтується на використанні запропонованих алгоритмів, моделей, забезпечує, на відміну від аналогів, аналіз інформації соцільних мереж; формування списків інформаційних об'єктів впливу для проведення протидії об'єктам впливу, сортування інформаційних об'єктів; надання оператору системи протидії пропонованого та альтернативних варіантів з обґрунтуванням вибору. Розроблений метод протидії виявлення та поширення шкідливої інформації в соціальних мережах відрізняється від існуючих, використанням запропонованих алгоритмів оцінки джерел повідомлень, ранжуванням та аналізом контрзаходів, в результаті підвищується обґрунтованість прийняття рішення про протидію поширенню шкідливої інформації та вибору контрзаходу, відповідним чином скорочується час роботи оператора системи у процесі протидії поширенню шкідливої інформації у соціальних мережах. Система протидії загрозам соціальних мереж забезпечує ранжування контрзаходів доступних у системі для протидії поширенню та виявлення шкідливої інформації в Інтернет - мережі.

ЛІТЕРАТУРА:

1. Ленков, С.В. Модель безпеки поширення забороненої інформації в інформаційно-телекомунікаційних мережах / С.В. Ленков, В.М. Джулій, В.С. Орленко, О.В. Сєлюков, А.В. Атаманюк // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2020. – Вип. №68. – С. 53-64.

2. Соціальні мережі – реальні загрози віртуального світу. [Електронний ресурс]. – Режим доступу : http://ogo.ua/ articles/view/011–02–23/26490.htm.

3. Ленков, С.В. Методы и средства защиты информации. В 2-х томах /С.В. Ленков, Д.А. Перегудов, В.А. Хорошко –К: Арий, 2008.–464с

4. Остапов С. Е. Технології захисту інформації: навчальний посібник / С.Е. Остапов, С.П. Євсеєв, О.Г. Король – Харків : Вид-во ХНЕУ, 2016. – 476 с.

5. Лєнков, С.В. Аналіз існуючих методів та алгоритмів виявлення атак в бездротових мережах передачі даних / С.В. Лєнков, В.М. Джулій, Н.М. Берназ, С.О. Божук // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2017. – Вип. № 56. – С.124-132

6. Довгий, С.О. Сучасні телекомунікації: мережі, технології, економіка, управління, регулювання / С.О. Довгий, О.Я. Савченко, П.П. Воробієнко – К.: Український Видатничій Центр, 2012. – 520 с.

7. Джулій, В.М. Інформаційно-ознакова модель шкідливої інформації в соціальних мережах/ І.В. Муляр, В.М. Джулій, В. М. Пічура, О.О Зацепіна – Вимірювальна та обчислювальна техніка в технологічних процесах № 3 (2022)-73–78с.

8. Джулій, В.М. Модель потоку текстових повідомлень тематичних інтернет-ресурсів системи прогнозування інформаційної безпеки/ В.М. Джулій, Ю.В. Хмельницький, Н.С. Петляк, О.В. Пахар– Вісник Хмельницького національного університету. Технічні науки. 2022. № 5. С. 294-300с.

9. Джулій, В.М., Кльоц Ю.П., Муляр І.В., Жилевич М.Л., Джулій А.В. Контроль додатків інтернет-трафіка комп'ютерних мереж методами машинного навчання. Вісник Хмельницького національного університету. Технічні науки. 2021. № 5. С. 22-26.

10. Джулій, В.М. Метод класифікації додатків трафіка комп'ютерних мереж на основі машинного навчання в умовах невизначеності / В.М. Джулій, О.В. Мірошніченко, Л.В. Солодєєва // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2022. – Вип. №74. – С. 73-82.

11. Лавров, Є. А. Математичні методи дослідження операцій : підручник / Є. А. Лавров, Л. П. Перхун, В. В. Шендрик – Суми : Сумський державний університет, 2017. – 212 с.

REFERENCES:

1. Lenkov, S.V. (2020), Model bezpeky poshyrennia zaboronenoi informatsii v informatsiino-telekomunikatsiinykh merezhakh / S.V. Lenkov, V.M. Dzhulii, V.S. ORLENKO, O.V. Sieliukov, A.V. Atamaniuk // Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. – K.: VIKNU. – №68. – pp. 53-64.

2. Cotsialni merezhi – realni zahrozy virtualnoho svitu. [Elektronnyi resurs]. – Rezhym dostupu : http://ogo.ua/ articles/view/011– 02–23/26490.htm

3. Lenkov, S.V. (2008), Metodyy sredstva zashchyты ynformatsyy. V 2-kh tomakh / S.V. Lenkov, D.A. Perehudov, V.A. Khoroshko –K: Aryi–464s.

4. Ostapov, S. E. (2016) Tekhnolohii zakhystu informatsii: navchalnyi posibnyk / S.E. Ostapov, S.P. Yevseiev, O.H. Korol–Kharkiv : Vyd-vo KhNEU. – 476 s.

5. Lenkov, S.V. (2017), AnalIz Isnuyuchih metodiv ta algoritmiv viyavlennya atak v bezdrotovih merezhah peredachI danih / S.V. Lenkov, V.M. Dzhuliy, N.M. Bernaz, S.O. Bozhuk // Zbirnik naukovih prats Viyskovogo Institutu Kiyivskogo natsionalnogo universitetu imeni Tarasa Shevchenka. – K.: VIKNU. – Vip. No 56. – p.124-132

6. Dovhyi, S.O. (2012), Suchasni telekomunikatsii: merezhi, tekhnolohii, ekonomika, upravlinnia, rehuliuvannia /S.O. Dovhyi, O.I. Savchenko, P.P. Vorobiienko – K.: Ukrainskyi Vydatnychii Tsentr. – 520p.

7. Dzhulii, V.M. Informatsiino-oznakova model shkidlyvoi informatsii v sotsialnykh merezhakh/ I.V. Muliar, V.M. Dzhulii, V. M. Pichura, O.O Zatsepina – Vymiriuvalna ta obchysliuvalna tekhnika v tekhnolohichnykh protsesakh № 3 (2022)-73–78s.

8. Dzhulii, V.M. Model potoku tekstovykh povidomlen tematychnykh internet-resursiv systemy prohnozuvannia informatsiinoi bezpeky/ V.M. Dzhulii, Yu.V. Khmelnytskyi, N.S. Petliak, O.V. Pakhar– Visnyk Khmelnytskoho natsionalnoho universytetu. Tekhnichni nauky. 2022. № 5. 294-300s.

9. Dzhulii V.M., Klots Yu.P., Muliar I.V., Zhylevych M.L., Dzhulii A.V. (2021), Kontrol dodatkiv internet-trafika kompiuternykh merezh metodamy mashynnoho navchannia. Visnyk Khmelnytskoho natsionalnoho universytetu. Tekhnichni nauky. – Khmelnytskyi. – №5. – pp. 22–26.

10. Dzhulii, V.M. (2022), Metod klasyfikatsii dodatkiv trafika kompiuternykh merezh na osnovi mashynnoho navchannia v umovakh nevyznachenosti / V.M. Dzhulii, O.V. Miroshnichenko, L.V. Solodieieva // Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. – K.: VIKNU. – Vyp. №74. – pp. 73-82.

11. Lavrov, Ye. A. (2017.), Matematychni metody doslidzhennia operatsii : pidruchnyk / Ye. A. Lavrov, L. P. Perkhun, V. V. Shendryk – Sumy : Sumskyi derzhavnyi universytet, – 212 p.

Doctor of Technical Science, Lienkov S.V.,
Ph.D. Dzhuliy V.M.,
Solodeeva L.V.

METHOD OF COUNTERACTION AND DETECTION OF HARMFUL INFORMATION IN SOCIAL NETWORKS

The paper studies the task of detecting and counteracting the spread of malicious information in social networks, including "fake news". There is a particularly urgent need to counter the spread of news on social media that generates panic waves during a pandemic. Currently, there is a war in Ukraine. Fake news travels six times faster on social media than the truth. Russian propaganda has become one of the main elements of the war in Ukraine, it is qualitatively camouflaged under the guise of Western media materials - DW, CNN or BBC.

The main difficulty in detecting and counteracting the spread of malicious information in social networks follows directly from the use of information technology development trends at the present stage, namely: an increase in the speed of dissemination of malicious information in social networks; the rate of emergence of new sources of dissemination of malicious information; increase in the volume of information containing malicious information; speed of replication of messages in the network; the number of scenarios for attracting the attention of the audience; level of data heterogeneity. By their architecture, social networks are multicomponent solutions; the network architecture contains: components that process content; components that provide the functions of marketing, administration, data storage. Social networks do not contain a separate component for detecting and counteracting the spread of malicious information on the network.

The analysis and study of evaluating the effectiveness of information-analytical systems and informatization of processes showed that the problem of detecting and counteracting the spread of malicious information in social networks cannot be considered solved and requires new research at this stage and allows us to determine the general requirements for the countermeasure system, as the basis for implementation which is based on the model-methodical apparatus.

In order to increase the effectiveness of the countermeasure system in Internet networks, the problem of developing an appropriate approach to improve the validity of the decision to counter the spread and detection of harmful information by increasing the number of parameters taken into account when choosing an information object of influence and effective countermeasures has been solved. The solution of the task is achieved by ranking countermeasures and analyzing the sources of the network of malicious information. A method of counteracting and detecting the spread of malicious information in social networks is proposed, based on the use of the proposed models, algorithms, provides, unlike analogues, the analysis of information from social networks; formation of lists of information objects of influence on the conduct of counteraction to objects, sorting of information objects; providing the system operator with a countermeasure to the proposed and alternative options with a justification for the choice. The developed method of detecting and counteracting the spread of malicious information in social networks differs from the existing ones by using algorithms for evaluating message sources, analyzing and ranking countermeasures, as a result, the validity of decision-making on countering the spread of harmful information and choosing a countermeasure increases, correspondingly, the time of the system operator in the process is reduced countermeasures against the spread of malicious information in social networks.

Keywords: malicious information, social networks, countermeasures, sources of messages, method of countermeasures, information system.