УДК 004.738.5

ІНФОРМАЦІЙНО-ОЗНАКОВА МОДЕЛЬ ШКІДЛИВОЇ ІНФОРМАЦІЇ В СОЦІАЛЬНІЙ МЕРЕЖІ

Судейченко Д.В.[1)], **Даньків А.В.**[2)], **Биц С.С.**[3)], **Могильська І.М.**[4)], **Олійник А.П.**[5)]
Західноукраїнський національний університет
[1)]магістрант;[2]аспірант;[3)]магістрант;[4)]студент;[5)]аспірант;

І. Постановка проблеми

Глибина проникнення соціальних мереж у повсякденне життя значна, і їхні переваги полягають у можливості учасників комунікації оперативно висловлювати свою думку великій групі людей та публікувати медіа файли. Сьогодні соціальні мережі вже не лише засіб спілкування, але й інструмент розповсюдження інформації. Проблема шкідливої інформації стала очевидною проблемою інформаційної безпеки сучасного суспільства. Терористичні та злочинні угруповання все частіше використовують засоби інформаційного впливу для розширення своєї сфери впливу та залучення нових адептів через соціальні мережі. Тому моніторинг, аналіз та активна протидія шкідливій інформації в соціальних мережах стає надзвичайно важливим для забезпечення інформаційної безпеки держави [1-3].

Проте в наш час існує недостатньо науково-технічних рішень для протидії шкідливій інформації. Існуючі засоби виявлення та протидії шкідливій інформації в соціальних мережах не відповідають вимогам до швидкості, повноти, точності та адекватності прийнятих рішень. Це зумовлено кількома причинами, включаючи розділеність системи на два не пов'язаних модулі - моніторинг та протидію, складну структуру соціальних мереж та потребу в обробці великих обсягів повідомлень в реальному часі [4-5].

Отже, основна складність протидії шкідливій інформації в соціальних мережах випливає з сучасних тенденцій розвитку інформаційної сфери, таких як збільшення обсягу та швидкості поширення шкідливої інформації. Це ставить перед науковцями та фахівцями з інформаційної безпеки виклик з підвищення ефективності протидії шкідливій інформації у соціальних мережах, зокрема за рахунок оперативності та обґрунтованості.

ІІ. Мета роботи

Метою дослідження є розробка інформаційно-ознакової моделі шкідливої інформації в соціальній мережі.

ІІІ. Інформаційно-ознакова модель шкідливої інформації в соціальній мережі

Соціальні мережі *(SN)* – сукупність взаємозалежних вузлів, якими є аканти спільноти, сторінки, пости, вкладення тощо, а зв'язки між об'єктами – це однорівневі відносини (складаються "у друзях", перебувають у співтоваристві, тощо) та відносини вкладеності (стіна містить пост, сторінка облікового запису містить посилання на пост і т.п.). Соціальні мережі асоціюються із графами, де частина об'єктів інформаційні, і є вершиною графа, а частина – зв'язки між такими об'єктами є ребра між вершинами [1-2].

У процесі аналізу основних структур даних соціальних мереж можна виділити загальні атрибути, які можуть бути застосовні для опису взаємозв'язку між джерелом, реципієнтом та шкідливою інформацією. Нехай у момент приєднання до соціальної мережі суб'єкт проходить процес реєстрації та створює мережевий профіль - обліковий запис (*account*), який належить множині *ACCOUNT*.

У процесі реєстрації облікового запису суб'єкт отримує унікальний ідентифікатор (*id*), який належить множині *ID*. Суб'єкт завжди до нього прив'язаний, хоча знаходиться на межі між віртуальним та реальним світом. Суб'єкт може не додавати про себе жодної інформації після реєстрації, проте це не заважає йому створювати та передавати інформацію в соціальній мережі [3].

Далі суб'єкт заповнює обліковий запис шляхом внесення даних про себе у мережному профілі, і тоді він заповнює свою власну сторінку (*pageac)*. Сторінка облікового запису належить множині PAGEac. Суб'єкт може створити спільноту, і в цей момент спільнота отримує свою унікальну адресу та профіль (*group*). Співтовариства в соціальних мережах утворюють множину *GROUP*, після заповнення профілю спільноти формується його сторінка ($pageg$). Сторінки груп належать множині *PAGEg*. При цьому

$$PAGE = PAGEac \cup PAGEg \quad (1)$$

У процесі аналізу будь-якого повідомлення в соціальних мережах можна визначити сторінку, де воно опубліковано. Сторінка, на якій опубліковано повідомлення із шкідливою інформацією – це джерело *(source)*. Усі джерела в соціальних мережах утворюють множину *SOURCE*. Поширення шкідливої інформації в соціальних мережах можливе шляхом публікації повідомлення (*message*). Всі повідомлення соціальних мереж утворюють множину *MESSAGE*. Повідомлення – це будь-який пост на стіні акаунта, на стіні групи, запис у коментарях тощо. Суб'єкт створює повідомлення та публікує його у відкритому доступі від імені свого облікового запису або від імені групи; він (суб'єкт) є автором (*author*). Усі пишучі суб'єкти соціальних мереж утворюють множину *AUTHOR*.

Нехай *MIO* – це інформаційний об'єкт (шкідливий інформаційний об'єкт), який містить ознаки, що дозволяють прийняти рішення про те, що інформація завдає шкоди суспільству, особистості, державі чи бізнесу. При цьому ознаки T (токени) інформаційної загрози встановлює експерт, залежно від умов. Наприклад, коли використовується система батьківського контролю, батько сам вибирає обмеження для дитини. Якщо ж представник бізнесу зацікавлений у захисті конфіденційної інформації, тоді він сам задає їх. Отже, теоретико-множинна модель шкідливої інформації у соціальній мережі включає такі базові елементи:

- *IO*- інформаційний об'єкт,
- *T*- інформаційна загроза,
- *MIO* – шкідливий інформаційний об'єкт,
- *Token*– ознака інформаційної загрози, що міститься у шкідливому інформаційному об'єкті,
- Feature – ознака наявності інформаційного об'єкта, зв'язок між об'єктами.

Теоретико-множинна модель формально представлена наступним чином:

$$IO = \{io\};\ MIO = \{io\};\ MIO_i = \{io\}$$

$$MIO \subset IO;\ \forall io \in MIO : io \in IO$$

$$MIO_i \subseteq MIO;\ \forall io \in MIO_i;\ io \in MIO$$

$$Token \subset T;\ Token = \{t\}$$

$$CheckFeature(io, t) = \{True; False\}$$

$$io \in MIO_i \Leftrightarrow \exists Token_m io_i : CheakFeature(uo, t) = True.$$

де *IO* – множина інформаційних об'єктів, io_i – один інформаційний об'єкт, *T*- множина всіх можливих ознак інформаційної загрози, t_n – одна ознака інформаційної загрози, *MIO* – множина шкідливих інформаційних об'єктів, *MIOi* - окремий клас шкідливої інформації, $Token_m$ - множина ознак характеризуючих *MIO*.

Таким чином, для протидії шкідливій інформації необхідно задати набір ознак, характерних для інформаційної загрози. Відмінною особливістю є те, що модель припускає наявність дискретних ознак у наборі ознак, таких як: дата створення інформаційного об'єкта, зв'язок інформаційного об'єкта з іншими об'єктами у соціальній мережі, частота повторення ознаки та ін.

Протидія шкідливому інформаційному об'єкту може здійснюватися лише на рівні повідомлень чи рівні джерел. Необхідно виділити такі погрози та їх інформаційні ознаки повідомлення у соціальній мережі, що характеризують його як шкідливе. Загалом під інформаційно-ознаковою моделлю [3,4] у дослідженні розуміється впорядкована сукупність відомостей про зв'язки повідомлень та їх інформаційних ознак із змістом повідомлень. У свою чергу, під інформаційними ознаками повідомлень розуміється окремі властивості повідомлень, а точніше їх зміст:

- інформаційна загроза – задається оператором системи;
- шкідлива інформація в соціальній мережі – задається оператором шляхом формування набору ключових слів;
- інформаційні ознаки, що формують множину усіх можливих ознак t.

На рисунку 1 зображено співвідношення різних рівнів інформаційно-ознакової моделі шкідливої інформації. Показано, що автор формує повідомлення та розміщує його в джерелі розповсюдження, на сторінці або обліковому записі, або групі. Повідомлення можуть містити чи не містити ознаки шкідливої інформації. Ознаки формують рівень інформаційних загроз.

Таким чином, зібравши інформацію на сторінці будь-якого джерела, можливо визначити, які з цих повідомлень належать до шкідливих. З урахуванням виявлених загроз та їх кількості може бути ухвалено рішення про протидію повідомленню або джерелу.

Розроблена інформаційно-ознакова модель шкідливої інформації дозволяє сформувати вихідні дані для протидії шкідливої інформації.

Розроблений комплекс моделей складається з моделі соціальної мережі, моделі джерела інформації, моделі шкідливої інформації та інформаційно-ознакової моделі шкідливої інформації Кожна з моделей, що входять до комплексу, містить унікальні, запропоновані автором комплексу множини, атрибути та відношення між елементами. Одночасно зцим комплекс моделей дозволяє сформувати вимоги до алгоритмів аналізу та оцінки джерел та вибору контрзаходів.

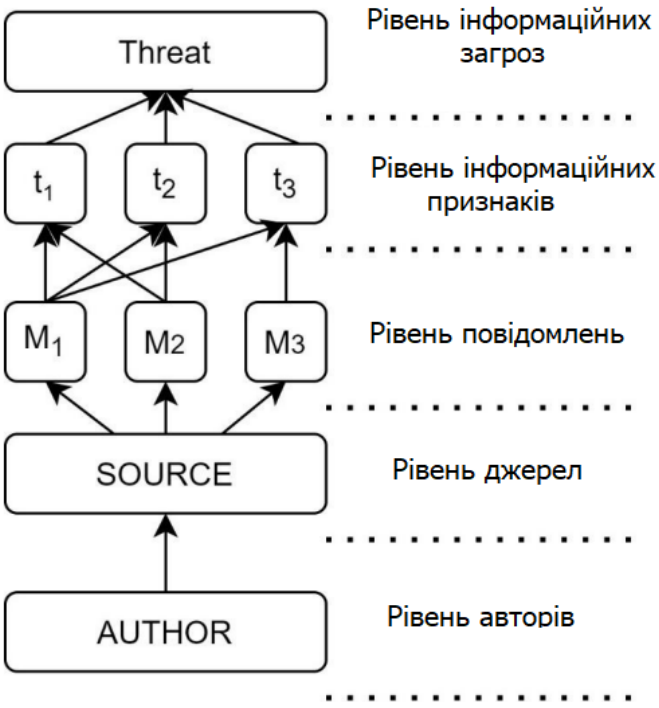

Рисунок 1 –Графічне представлення інформаційно-ознакової моделі шкідливої інформації

Висновок

В рамках цього дослідження було розроблено модель соціальної мережі, що включає повідомлення, джерела та зв'язки між ними, яка відрізняється наявністю нових структурних елементів та зв'язків. Також розроблено модель джерела, в якій вперше враховуються такі параметри, як індекс активності, потенціал, індекс впливовості та індекс перегляду. Розроблено інформаційно-ознакову модель шкідливої інформації, що складається з взаємопов'язаних об'єктів та ознак шкідливої інформації, разом формують шкідливо-інформаційні об'єкти.

Список використаних джерел

1. Войтович О. П. Модель та засіб для виявлення фейкових облікових записів у соціальних мережах / Войтович О. П., Дудатьєв А. В., Головенько В. О. // Вчені записки таврійського національного університету ім. В.І. Вернадського. Серія: Технічні науки. – Частина 1. – 2018. – № 1. –Том 29 (68). – С. 112-119.
2. Monti, F.; Frasca, F.; Eynard, D.; Mannion, D.; Bronstein, M.M. Fake news detection on social media using geometric deep learning. arXiv 2019, arXiv:1902.06673, 2019.
3. Silva, A.; Han, Y.; Luo, L.; Karunasekera, S.; Leckie, C. Propagation2Vec: Embedding partial propagation networks for explainable fake news early detection. Inf. Process. Manag. 2021, 58, 102618.
4. Barnabò, G.; Siciliano, F.; Castillo, C.; Leonardi, S.; Nakov, P.; Martino, G.D.S.; Silvestri, F. Deep active learning for misinformation detection using geometric deep learning. Online Soc. Netw. Media 2023, 33
5. Shu, K.; Mahudeswaran, D.; Wang, S.; Liu, H. Hierarchical propagation networks for fake news detection: Investigation and exploitation. In Proceedings of the International AAAI Conference on Web and Social Media, Limassol, Cyprus, 5–8 June 2020; Volume 14, pp. 626–637.