Застосування умовної ентропії для оцінювання інформаційно-психологічного впливу в соціальних мережах

Юрій Бродський
Кафедра КТіМС
Поліський національний університет
Житомир, Україна
yubrodskiy26@gmail.com

Катерина Молодецька
Кафедра КТіМС
Поліський національний університет
Житомир, Україна
kmolodetska@gmail.com

Abstract. The model of evaluation of informational and psychological influence on actors in social networks was developed. The model is based on conditional entropy, which made it possible to take into account the destructive influence not only of the content source, but also of its distribution in virtual communities. This allows to increase the level of information security of the state as a result of application of the developed model in information technologies of threat assessment.

Ключові слова: соціальні мережі, інформаційно-психологічний вплив, ентропія, загроза, інформаційна безпека.

Вступ

Зважаючи на глобальний розвиток інформаційних технологій та мережі Інтернет відбулися зміни у системі стратегічних комунікацій, де соціальні мережі перетворилися на найбільш популярний засіб масової комунікації. Внаслідок цього соціальні мережі можуть використовуватися зловмисниками для досягнення власних цілей в інформаційному просторі будь-якої держави. Наслідками реалізації інформаційно-психологічного впливу на акторів соціальних мереж можуть бути маніпулювання суспільною думкою, вплив на свободу вибору громадян, їх емоційний і психічний стан, дискредитація існуючої системи управління в державі тощо [1-4].

Зважаючи на постійне зростання кількості загроз інформаційній безпеці держави у соціальних мережах, особливої актуальності набуває проблема виявлення інформаційно-психологічного впливу на громадян в інформаційному просторі сервісів. Незважаючи на активний розвиток технологій інформаційно-психологічного впливу на акторів у соціальних мережах [5], розроблення і удосконалення методів виявлення такого впливу суттєво обмежені. Це пов'язано, зокрема, зі складністю формалізації моделей деструктивного контенту та відсутністю його сталих ознак. Тому перспективним є розроблення моделей оцінювання деструктивного впливу на акторів, що забезпечать підвищення ефективності процедури виявлення загроз інформаційній безпеці держави.

Модель оцінювання інформаційно-психологічного впливу на акторів

Створений учасниками інформаційних операцій текстовий контент, що містить інформаційно-психологічний вплив на акторів віртуальних спільнот, характеризується деякою величиною вхідної ентропії $H(x)$ або ентропією джерела контенту. Після поширення в інформаційному просторі, відбувається ознайомлення з контентом акторів віртуальних спільнот, подальше перекручування його змісту внаслідок особливостей його сприйняття споживачами і подальша публікація з додаванням суб'єктивних оціночних суджень та висновків. Як наслідок, у такому контенті збільшується рівень інформаційно-психологічного впливу на акторів, який

характеризуватиметься умовною ентропією $H(y/x)$. Тоді втрата змісту контенту після подвійного перекручування визначається величиною ентропії $H(x/y)$.

Невикривлений контент $I(x,y)$, що не містить інформаційно-психологічного впливу на акторів, формалізуємо у вигляді різниці ентропії контенту кінцевого споживача $H(y)$ та умовної ентропії $H(y/x)$, що характеризує результат перекручування контенту акторами, або через ентропію джерела контенту $H(x)$ і умовну ентропію $H(x/y)$, яка описує втрати змісту контенту внаслідок його трансформації

$$I(x,y) = H(y) - H(y/x) = H(x) - H(x/y). \quad (1)$$

При обробці великої кількості публікацій частота появи відповідних слів-індикаторів наближається до ймовірності появи ознак інформаційно-психологічний впливу [5]. Модель такого впливу доцільно описати у вигляді матриці перехідних ймовірностей. Матриця буде складатися з n^2 елементів, де n – загальна кількість ознак інформаційно-психологічного впливу на акторів. Кожний елемент матриці, залежно від змісту оцінюваного інформаційного процесу, представляє собою умовну ймовірність $p(y_j / x_i)$ або $p(x_i / y_j)$. Якщо відома матриця перехідних імовірностей, то частоти появи ознак f_j^y інформаційно-психологічного впливу на акторів у СІС на виході однозначно визначаються частотами ознак f_i^x в контенті від джерела з урахуванням імовірності відповідно до переходу $p(y_j / x_i)$ [6]. Нехай ймовірність наявності в контенті від початкового джерела деструктивного інформаційного впливу наближається до частоти появи відповідних ознак загрози, тоді

$$I(x,y) = \sum_{i=1}^{n}\sum_{j=1}^{n} f_i^x p(y_j / x_i)\Big[\log_2 p(y_j / x_i) - \log_2 \sum_{i=1}^{n} f_i^x p(y_j / x_i)\Big]. \quad (2)$$

Для інтерпретації отриманих числових значень за виразом (2) використаємо нормовані значення I_{norm} для інформації про наявність або відсутність інформаційно-психологічного впливу на акторів у контенті СІС

$$I_{norm}(x,y) = \frac{I(x,y)}{I_{\max}(x,y)}, \quad (3)$$

де $I_{\max}(x,y)$ – максимальне значення інформації.

Якісна шкала оцінки загроз інформаційно-психологічного впливу подано в табл. 1.

Таблиця 1. Рівень загрози

Клас загрози	Значення $I_{norm}(x,y)$
дуже високий	0,00–0,20
високий	0,21–0,49
значний	0,50–0,74
низький	0,75–0,90
дуже низький	0,91–1,00

Запропонована модель оцінювання інформаційно-психологічного впливу забезпечує підвищення ефективності моніторингу інформаційного простору соціальних мереж та виявлення загроз інформаційній безпеці держави.

ЛІТЕРАТУРА

[1] A. Oxley, Security risks in social media technologies: Safe practices in public service applications, Elsevier, 2013.

[2] К. В. Молодецька, "Спосіб підтримання заданого рівня попиту акторів соціальних інтернет-сервісів на контент," Радіоелектроніка, інформатика, управління, № 4(35), с. 113–117, 2015.

[3] Р. В. Гумінський, А. М. Пелещишин, "Загрози інформаційної безпеки держави в соціальних мережах," Наука і техніка Повітряних сил Збройних Сил України, 2(11), с. 192–199, 2013.

[4] R. Hryshchuk, R. Zhovnovatiuk, H. Nosova, "Hybrid threats in cyber space: factors of influence on nature of emergence," Modern Information Technologies in the Sphere of Security and Defence, 36(3), pp. 53–58, 2019.

[5] Р. В. Грищук, К. В. Молодецька-Гринчук, "Методологія побудови системи забезпечення інформаційної безпеки держави у соціальних інтернет-сервісах," Захист інформації, т. 19, № 4, с. 254–262, 2017.

[6] Y. Wang, L. Yongming, "Bayesian entropy network for fusion of different types of information," Reliability Engineering & System Safety, 195, p. 106747, 2020.