

Молодецька Катерина Валеріївна

д-р техн. наук, доцент,

керівник навчально-наукового центру

інформаційних технологій

Житомирський національний

агроєкологічний університет, м. Житомир, Україна

АНАЛІЗ ПІДХОДІВ ДО МОДЕЛЮВАННЯ КОНФЛІКТНОЇ ВЗАЄМОДІЇ АКТОРІВ У СОЦІАЛЬНИХ ІНТЕРНЕТ-СЕРВІСАХ

Поглиблення процесів інформатизації суспільства призвело до суттєвої трансформації процесів соціальної комунікації. На перший план як засіб масової комунікації вийшли соціальні інтернет-сервіси (СІС), які сьогодні використовуються користувачами (акторами) для об'єднання однодумців у віртуальні спільноти, виявлення громадянської позиції, координації дій в реальному житті та, як наслідок, впливу на політичні та суспільні процеси у державі. Світовий та український досвід використання СІС громадянами для самоорганізації у кризових ситуаціях та під час резонансних подій показав, що вони є ефективним інструментом впливу на суспільну думку, мобілізації громадян та посилення протестних настроїв у суспільстві [1, 2]. Такі явища стали можливими завдяки високому ступеню довіри акторів до інформації в СІС порівняно із традиційними ЗМІ.

Також внаслідок докорінної зміни процесів комунікації у інформаційному просторі, СІС перетворилися на дієвий засіб ведення нової форми протистояння – гібридної війни. Гібридна війна об'єднує в собі політичні, економічні, інформаційні та інші інструменти для досягнення однією державою переваги над іншою [1]. Провідна роль у веденні гібридної війни відводиться інформаційному протистоянню як суперництву соціальних систем або країн в інформаційній сфері для впливу на різні сфери суспільних відносин і встановлення контролю над джерелами стратегічних ресурсів, у результаті якого одна сторона отримує переваги, необхідні їй для подальшого розвитку. В сучасних умовах перевага в інформаційному просторі держави досягається внаслідок високої швидкості поширення контенту в СІС, який містить деструктивний інформаційний вплив на акторів, а також децентралізованому характеру зв'язків між акторами. У результаті цього СІС виступають ефективною і дієвою онлайн-платформою ведення наступальних дій в національному інформаційному просторі держави [2].

Таким чином, на сучасному етапі розвитку інформаційних технологій та формування інформаційного суспільства, СІС перетворилися на джерело загроз інформаційній безпеці держави. Внаслідок багатофункціональності СІС та в умовах глобалізації інформаційного простору й вільного обігу контенту в світі, виникає об'єктивне протиріччя між нагальною потребою практики у забезпеченні сталого розвитку інформаційного простору сервісів і проблемою науки щодо розроблення дієвих методологічних засад моделювання конфліктної взаємодії в інформаційному просторі для забезпечення інформаційної безпеки держави у СІС.

Аналіз останніх досліджень і публікацій показав, що на сучасному етапі розвитку технологій гібридна війна ведеться без застосування військового потенціалу і зброї у класичному розумінні [1]. Завдяки використанню СІС інформаційне протиборство набуває латентного характеру, не має чіткого окресленого початку і кінця, а внаслідок транскордонності взаємодії між акторами у СІС кордони держав стають розмитими. У свою чергу, поширюваний під час інформаційних операцій контент містить деструктивний інформаційний та інформаційно-психологічний вплив. Це призводить до ускладнення процедур формалізації процесів інформаційного протиборства та їх моделювання, врахування унікальних ситуацій та окремих важливих факторів.

З публікацій [3-5] відомо, що для дослідження процесів інформаційного протиборства використовуються математичні моделі, які враховують перерозподіл різних типів ресурсів, необхідних для його здійснення. Серед відомих моделей війни найбільш поширеною є модель Ланчестера [3], що розглядає кількісну динаміку бою двох угруповань як випадковий марківський процес з дискретними станами і неперервним часом. Для такого процесу можна отримати рівняння динаміки середніх і визначити для будь-якого моменту часу середні чисельності протиборчих сторін. На практиці модель Ланчестера використовується для прогнозування середньої кількості уражених і неуражених бойових одиниць кожного угруповання в будь-який момент часу. Недоліком розглянутої моделі є суттєве зменшення точності результатів моделювання при зменшенні чисельності акторів протиборчих віртуальних спільнот у СІС.

Також широкої популярності для дослідження інформаційного протиборства у СІС набула модель Лоткі-Вольтерри (або модель “хижак-жертва”) [4]. Ця модель описує популяцію, що складається з двох взаємодіючих видів. Перший з них – “хижаки”, при відсутності другого – “жертв” вимирає, при цьому другий за відсутності хижаків необмежено розмножується відповідно до закону Мальтуса. В загальному випадку ця модель

описує чисельність акторів віртуальних спільнот у СІС, які є носіями або прихильниками деякого визначеного нарративу чи формалізує взаємодію акторів. Однак, застосування моделі Лоткі-Вольтерри в задачах інформаційного протистояння віртуальних спільнот акторів у СІС обмежується тільки окремими її аспектами і, наприклад, не може формалізувати кількість акторів у протидіючих віртуальних спільнотах.

Для математичного опису і дослідження взаємодії в часі конфліктуючих сторін у СІС також застосовуються диференціальні ігри переслідування [5]. При цьому розглядаються дві групи акторів у СІС – наздоганяючі та тікаючі. Метою віртуальної спільноти наздоганяючих акторів є перехід деякого вектору на задану множину за найменший відрізок часу, а метою спільноти тікаючих акторів – збільшення тривалості такого переходу. Недоліками такого підходу є існування припущення про детермінованість поведінки противника і кожній групі повинні бути відомі можливі стратегії іншої. Також диференціальні ігри переслідування не враховують ризиків, пов'язаних з процесами соціальної комунікації у СІС, і шукані оптимальні стратегії використовують тільки один показник або критерій. Спільним недоліком розглянутих підходів до формалізації та дослідження інформаційного протидіючого віртуальних спільнот у СІС є здійснення його опису на рівні ресурсу – зокрема, чисельності акторів віртуальної спільноти. Досвід ведення гібридної війни між Україною і Російською Федерацією показує, що ефективність інформаційного протидіючого в СІС визначається не тільки кількістю прихильників деякого нарративу, але і появою емерджентних властивостей та синергетичних ефектів у соціотехнічній системі, які впливають на реальні суспільні процеси у державі. Тому моделі інформаційного протидіючого віртуальних спільнот у СІС повинні враховувати більшу кількість факторів, аніж існуючі моделі. Також у моделі “хижак-жертва” [3] не виконується головна умова конфлікту – кількість акторів у СІС залишається незмінною, а вигравш однієї віртуальної спільноти повинен дорівнювати величині програшу іншої.

Зважаючи на складність процесів взаємодії акторів у СІС в умовах постійного прихованого впливу загроз інформаційній безпеці держави, перспективним напрямком досліджень є виділення в математичній моделі інформаційного протидіючого складових рівнянь, які враховують: зміну конфліктних характеристик взаємодії акторів віртуальних спільнот; зростання рівня ресурсів внаслідок збільшення чисельності віртуальної спільноти акторів у СІС; витрати ресурсів на проведення інформаційних операцій у СІС в межах протидіючого. Тому дослідження процесів ін-

формаційного протиборства віртуальних спільнот акторів у СІС потребує розроблення математичних моделей, які забезпечать виконання сформульованої вище умови конфлікту. Таким чином, актуальним завдання є моделі конфліктної взаємодії акторів віртуальних спільнот в СІС, які дозволяють врахувати не тільки кількісну зміну акторів у спільнотах, але і перерозподіл отриманих ресурсів інформаційного простору та витрати на ведення протиборства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Грабар І. Г. Безпекова синергетика: кібернетичний та інформаційний аспекти: монографія / І. Г. Грабар, Р. В. Гришук, К. В. Молодецька; за заг. ред. д.т.н., проф. Р. В. Гришука. – Житомир : ЖНАЕУ, 2019. – 280 с.
2. Гришук Р. В. Методологія побудови системи забезпечення інформаційної безпеки держави у соціальних інтернет-сервісах / Р. В. Гришук, К. В. Молодецька-Гринчук // Захист інформації. – 2017. – Т. 19, № 4. – С. 254–262.
3. Kress M. Lanchester model for three-way combat / M. Kress, J. P. Caulkins, G. Feichtinger, D. Grass, A. Seidl // European Journal of Operational Research. – 2018. – 264(1). – PP. 46–54.
4. Barrett C. Modeling and simulation of large biological, information and socio-technical systems: an interaction based approach / C. Barrett, S. Eubank, M. Marathe // Interactive Computation; Eds. Goldin D., Smolka S.A. – Springer, Heidelberg, 2006. – PP. 353–392.
5. Hafezalkotob A. Cooperation of advertising companies in social networks: A graph and game theory approaches / A. Hafezalkotob, M. Khodabakhsh, A. Saghaei, M. Eshghipour // Computers & Industrial Engineering. – 2018. – 125. – PP. 212–220.