Підвищення інформаційної стійкості віртуальних спільнот у соціальних інтернет-сервісах

Руслан Грищук
Кафедра захисту інформації та кібербезпеки
Житомирський військовий інститут
імені С. П. Корольова
Житомир, Україна
dr.hry@i.ua

Катерина Молодецька
Навчально-науковий центр ІТ
Житомирський національний агроекологічний університет
Житомир, Україна
kmolodetska@gmail.com

Abstract. Social networking services are a source of threats to state information security. The core method is to increase the information stability of virtual communities in social networking services to destructive information influences through their hidden artificially controlled formation. The formation of information resistant virtual communities is suggested to be carried out on the basis of the critical mass principle. This approach provides their further stable development and guarantees critical perception of the content of destructive matter. In addition, for those virtual communities that have unsatisfactory quality performance indicators, it is offered to use latent synergistic management in the form of directed information influence.

Ключові слова: соціальні інтернет-сервіси, загрози, інформаційна безпека, стартап, критична маса, синергетичне управління, модель Моно, показник Херста.

Вступ

Наразі соціальні інтернет-сервіси (СІС) не тільки консолідують інструменти для обміну повідомленнями і мультимедійним контентом, але й застосовуються для самоорганізації суспільства у віртуальні спільноти та реалізації взаємодії у реальному житті [1, 2]. Зростання популярності СІС нерозривно пов'язане з появою викликів інформаційній безпеці держави (ІБД) в інформаційному просторі віртуальних спільнот. Так, СІС активно використовуються Російською Федерацією для ведення гібридної війни проти України. Метою здійснення протиборчою стороною інформаційного впливу на акторів СІС є маніпулювання особистістю, групою людей та масами, поширення дезінформації для впливу на суспільні й політичні процеси у державі, поширення хаосу серед населення тощо [3].

Аналіз останніх досліджень показав, що дієвим напрямком протидії загрозам ІБД у СІС є використання синергетичного управління [4]. Однак, невирішеним залишається завдання формування стійких до деструктивних інформаційних впливів у СІС структур віртуальних спільнот акторів. Такий підхід дозволить зменшити витрати ресурсів на неперервний моніторинг інформаційного простору СІС та протидію загрозам ІБД.

Інформаційна стійкість віртуальних спільнот

Під інформаційною стійкістю віртуальної спільноти в СІС будемо розуміти її здатність реагувати і відновлюватися після впливу загроз інформаційній безпеці, адаптуватися до змін інформаційного простору та реалізовувати свою мету функціонування. Розглянута категорія відрізняється від поняття інформаційної безпеки віртуальної спільноти врахуванням вимоги її стійкого розвитку у середовищі СІС. Досягнення інформаційної стійкості віртуальної спільноти в СІС забезпечує завчасну готовність, адекватну реакцію та успішне відновлення до заданого стану інформаційної безпеки віртуальної спільноти після реалізації загрози у СІС. Серед

факторів, які впливають на забезпечення інформаційної стійкості віртуальних спільнот у СІС, виділимо наступні:

- діяльність державних суб'єктів забезпечення інформаційної безпеки;
- соціальні норми;
- соціальні санкції;
- критичне мислення акторів.

МЕТОД ФОРМУВАННЯ ІНФОРМАЦІЙНО СТІЙКИХ ВІРТУАЛЬНИХ СПІЛЬНОТ

Штучно керований синтез стійких структур віртуальних спільнот у СІС нерозривно пов'язаний з використанням стартапу віртуальних спільнот. Проблема стартапу спільноти в СІС з'являється тоді, коли виникає потреба швидкої активації віральної петлі, що забезпечить її саморозвиток в умовах жорстких ресурсних обмежень при залученні мінімальної кількості акторів. Наразі не існує універсального підходу до визначення критичної маси акторів для стартапу віртуальних спільнот у СІС, тому скористаємося метрикою самоподібності – показником Херста [3]. Дана метрика самоподібності забезпечить виявлення не тільки трендовості у послідовності наповнення віртуальної спільноти новими акторами, а й дозволить встановити природу стартапу. Величина показника Херста опосередковано відповідатиме на питання чи досягло віртуальне співтовариство критичної маси за мінімальної кількості акторів та виділених ресурсів чи ні. На основі кількісних значень показника Херста запропоновано визначати якісні ознаки стартапу – "невдалий", "випадковий" і "вдалий". Якщо стартап віртуальної спільноти є вдалим, це створює передумови для її подальшого сталого розвитку та ефективної протидії загрозам ІБД у СІС внаслідок дії факторів, що забезпечують інформаційну стійкість.

Для випадку, коли стартап віртуальної спільноти у СІС характеризується якісними показниками "невдалий" або "випадковий", вона не здатна до самостійного функціонування і розвитку. Тому розглянемо процес формування віртуальної спільноти акторів, яка буде здатна до сталого саморозвитку завдяки активізації віральної петлі в СІС з використанням синергетичного управління. Зважаючи на високу швидкість зростання кількості акторів і віртуальних спільнот у СІС, виникнення еволюційних процесів у межах віртуальних спільнот, використаємо для опису взаємодії акторів у СІС модель мікробіологічної системи Моно. Після цього, відповідно до концепції синергетичного управління взаємодією акторів у СІС, синтезуємо модель прихованого інформаційного впливу на учасників віртуальної спільноти [3]. Внаслідок цього відбувається штучно керована самоорганізація акторів у СІС. У такій віртуальній спільноті виникають когерентні колективні процеси і спрямована самоорганізація спільноти й параметрів процесів взаємодії акторів.

Проведені експериментальні дослідження запропонованого методу формування віртуальних спільнот підтвердили, що синтезована спільнота здатна самостійно поширювати мультимедійний контент із заданим наративом, що дозволить ефективно протидіяти загрозам ІБД у СІС. Така віртуальна спільнота є інформаційно стійкою до впливу загроз ІБД в інформаційному просторі СІС.

ЛІТЕРАТУРА

[1] M. Salehan, D. J. Kim, C. Koo, "A study of the effect of social trust, trust in social networking services, and sharing attitude, on two dimensions of personal information sharing behavior," The Journal of Supercomputing, 74(8), pp. 3596-3619, 2018.

[2] А. М. Пелещишин, Р. В. Гумінський, "Модель інформаційного середовища віртуальної спільноти," Eastern-European Journal of Enterprise Technologies, 2(68), с. 10-16, 2014.

[3] І. Грабар, Р. Грищук, К. Молодецька, Безпекова синергетика: кібернетичний та інформаційний аспекти, Житомир: ЖНАЕУ, 2019.

[4] А. А. Колесников, Синергетические методы управления сложными системами: теория системного синтеза, Москва: Едиториал УРСС, 2005.