Роль соціальних інтернет-сервісів у процесі забезпечення інформаційної безпеки держави

Катерина Молодецька

Кафедра комп'ютерних технологій і моделювання систем, Житомирський національний агроекологічний університет, УКРАЇНА,
м. Житомир, бульвар Старий, 7,
E-mail: kmolodetska@gmail.com

Проаналізовано особливості функціонування і різновиди сучасних соціальних інтернет-сервісів (СІС). Встановлено, що СІС є об'єктом реальних і потенційних загроз інформаційній безпеці держави й, в свою чергу, виступають ефективним інструментом комунікації та координації учасників дестабілізуючих акцій. Обґрунтовано необхідність розробки цілісної методології забезпечення інформаційної безпеки держави у СІС.

Ключові слова – соціальний інтернет-сервіс, актор, деструктивний інформаційний посил, віртуальна спільнота, інформаційна безпека держави.

На сучасному етапі розвитку суспільства соціальні інтернет-сервіси (СІС) є ефективним інструментом для комунікації учасників віртуальних спільнот – акторів, і обміну між ними контентом різного типу [1-3]. СІС впливають на всі сфери суспільного життя – економічну, соціальну, політичну і духовну. Істотний вплив на суспільство пояснюється тим, що СІС ґрунтуються на використанні соціальних взаємозв'язків між особами, які, наприклад, мають спільні інтереси, діяльність або утворюють реальні чи віртуальні об'єднання. З [1] відомо, що СІС використовуються для суспільних перетворень шляхом створення об'єднань громадян і координації їх спільної діяльності внаслідок процесів самоорганізації.

Системний аналіз ролі СІС в інформаційному просторі держави і особливостей їх функціонування [1, 3-5] показав, що вони є об'єктом реальних і потенційних загроз інформаційній безпеці людини й громадянина, суспільства та держави. Поширення в СІС неповного, недостовірного чи упередженого контенту у поєднанні із сугестивними технологіями впливу на індивідуальну і масову свідомість може мати наслідком прояв у суспільстві соціальної напруженості, міжнаціональної ворожнечі, протестних настроїв, незадоволення існуючою системою управління в державі.

Аналіз світового і вітчизняного досвіду показав, що СІС відігравали одну з ключових ролей в організації подій «арабської весни», «революції парасольок», гібридній війні на сході України та інших дестабілізуючих акцій. Так, на початку 2011 року в Тунісі відбувалися антиурядові демонстрації, що мали на меті проведення реформ у державі, які отримали назву «Жасминова революція». Особливістю протестних акцій було актовне використання СІС, а саме *Facebook* і *Twitter*, для організації, координації дій, висвітлення ситуації у ЗМІ. Події в Тунісі викликали лавиноподібне поширення акцій протесту з метою повалення диктаторських режимів у інших арабських країнах – Єгипті, Ємені, Лівії, Сирії тощо і супроводжувалися використання СІС як інструмента

комунікації. У вересні 2014 року в Гонкогу відбулися демонстрації студентів проти планів китайського уряду фільтрувати кандидатів на гонконгських виборах 2017 року. Для обміну інформацією учасники протестів використовували *Instagram* і *Twitter*, а також месенджер *FireChat* для пошуку акторів на відстані без використання мережі Інтернет. Отже, можна зробити висновок, що активними учасниками протестів були соціально активні громадяни, які використовували для комунікації СІС з метою поширення протестних настроїв, організації демонстрацій, їх координації та інформування міжнародної громадськості.

Події гібридної війни на сході України показали, що СІС активно використовувалися на етапах підготовки і безпосередньо під час її ведення. У соціальних мережах *Facebook*, *Vkontakte*, *Одноклассники* було створено віртуальні спільноти *Антимайдан*, *Новороссия*, *Русская весна* тощо для поширення деструктивних інформаційних посилів, які мали на меті спотворення інформації про реальні події, деструктивних змін свідомості акторів, корекції їх поведінки. Актори таких віртуальних спільнот стали об'єктом сугестивного впливу для подальшого забезпечення сприятливих умов реалізації атакуючих дій у всіх сферах суспільної діяльності в режимі офлайн. Також соціальні мережі використовувалися для збирання інформації про осіб, які становлять інтерес для агресора, розвідувальної діяльності для встановлення противником державної належності та ідентифікації об'єктів, навігаційного забезпечення операцій тощо. Засобами СІС агресором відстежувалися настрої в суспільстві, виконувалася нейтралізація джерел контрпропаганди. Таким чином, в Україні відсутня цілісна методологія забезпечення інформаційної безпеки держави в СІС. Існуючі засоби та підсистеми протидії недостатньо забезпечені відповідним інструментарієм моніторингу, виявлення і протидії загрозам, а їх взаємодія здійснюється із запізненням. В результаті держава і її громадяни стають суб'єктами деструктивних інформаційних впливів у СІС.

Література

1. Earl J. Digitally Enabled Social Change: Activism in the Internet Age / J. Earl, K. Kimport. – Cambridge: MIT, 2011. – 170 p.; 2. González-Bailón S. Networked discontent: The anatomy of protest campaigns in social media / S. González-Bailón, N. Wang // Social Networks. – № 44. – 2016. – PP. 95–104.; 3. Процеси управління інтерактивними соціальними комунікаціями в умовах розвитку інформаційного суспільства: монографія / А. М. Пелещишин, Ю. О. Сєров, О. Л. Березко, О. П. Пелещишин, О. Ю. Тимовчак-Максимець, О. В. Марковець; ред. А. М. Пелещишин. – Львів : Вид-во Львів. політехніки, 2012. – 368 с. – ISBN 978-617-607-198-3; 4. Даник Ю. Мобільні соціальні Інтернет-сервіси як один із різновидів масової комунікації на сучасному етапі / Ю. Даник, Р. Грищук, О. Самчишин // Безпека інформації. – 2015. – Т. 21, № 1. – С. 16–20.; 5. Молодецька К. В. Загрози інформаційній безпеці держави в соціальних інтернет-сервісах / К. В. Молодецька // Інформаційна безпека та комп'ютерні технології: зб. тез доп. міжнар. наук.-практ. конф., 24–25 берез. 2016 р. – Кіровоград : КНТУ, 2016. – С. 55.