DOI 10.33099/2618-1614-2019-8-3-36-39
УДК 354.42.44

В. М. Шемаєв,
доктор військових наук, професор,
головний науковий співробітник
Національного інституту стратегічних досліджень,

М. М. Присяжнюк,
кандидат технічних наук, старший науковий співробітник,
професор кафедри національної безпеки
Національної академії Служби безпеки України,

А. П. Онофрійчук,
кандидат економічних наук, заступник директора
з економічних питань ТОВ «БК СЕРВІСРЕМБУД»

Соціальні мережі в аспекті інформаційної безпеки

У статті розглядається забезпечення інформаційної безпеки в соціальних мережах. Досліджуються соціальні мережі як середовище маніпулятивного впливу та розкриваються причини й наслідки негативного впливу в соціальних мережах.

Ключові слова: соціальна мережа, маніпулятивний вплив, інформаційна безпека.

Постановка проблеми. Стрімкий розвиток інформатизації прискорив процеси інтеграції світового масштабу. Новітні інформаційно-комунікаційні технології та соціальні мережі стали ефективним знаряддям розвитку суспільства і взаємовідносин між державами. Серед користувачів мережі Інтернет важко знайти людину, яка б не мала профілю або навіть кількох у соціальних мережах. Проте зростання їхнього суспільного значення зумовлює і зростання вразливості елементів інформаційної інфраструктури до негативних впливів. Інформаційна інфраструктура стала об'єктом інформаційної агресії та інформаційних воєн. А це, у свою чергу, призводить до того, що суспільство може піддаватися сугестивному маніпулятивному впливу в глобальному інформаційному просторі.

Тому тему наукової статті «Соціальні мережі в аспекті інформаційної безпеки» можна вважати актуальною й такою, що потребує детального дослідження.

Аналіз останніх публікацій показав, що забезпечення інформаційної безпеки в соціальних мережах стало предметом конкретних наукових досліджень. Проблеми негативного впливу на людей у соціальних комунікаціях розглянуті в роботах таких науковців, як Я. А. Деркаченко, А. М. Пелещишин, О. Шклярська та ін.

Метою цієї статті є розкриття сутності соціальних мереж в аспекті інформаційної безпеки.

Об'єктом дослідження є соціальні мережі.

Предметом дослідження є інформаційна безпека в соціальних мережах.

Виклад основного матеріалу. Сучасні інформаційно-комунікаційні технології дають змогу створювати в Інтернеті як постійні, так і тимчасові соціальні структури, об'єднані єдиними нормами, спільними інтересами та комунікаційними можливостями. На відміну від традиційних ЗМІ мережеві співтовариства мають соціальний характер, формуються на основі емпатії (співчуття) та мають певні переваги: доступність, відкритість, оперативний обмін інформацією, зворотний зв'язок, можливість установлення нових зв'язків, неформальне спілкування, полегшений пошук необхідного користувача соціальної мережі тощо.

У поширеному розумінні соціальна мережа – це спільнота людей, об'єднана загальними інтересами чи загальною справою для безпосереднього спілкування між собою. Соціальні мережі є авторитетним джерелом інформації та через свою доступність і популярність налічують найбільше число акаунтів (користувачів) у глобальній мережі Інтернет. Потік інформації в них має двосторонній напрямок, тому учасники спілкування можуть бути одночасно як комунікаторами, так і реципієнтами. Соціальні мережі часто виступають у ролі неформальних ЗМІ, де будь-який користувач може опублікувати новинне повідомлення про події. У відвідувачів соціальних мереж формується відчуття власної можливості впливу на соціально-політичні процеси в державі.

Близько 78% людей довіряють інформації із соціальних мереж, оскільки аудиторія може залучатися до інформації надією розв'язати будь-які проблеми.

Сучасні соціальні мережі є одними з найбільш відвідуваних ресурсів. Вони дають можливість одночасно передавати інформацію на будь-яку відстань у реальному масштабі часу значній аудиторії в усьому світі. Згідно з даними компанії comScore, їх використовують близько 80% усіх користувачів Інтернету.

Проте ця особливість може використовуватися також з метою цілеспрямованих деструктивних впливів на національний інформаційний простір. Виникає загроза соціальної небезпеки, пов'язаної із застосуванням технологій штучної зміни поведінкових реакцій людини і впливу на свободу її волевиявлення. З'явилися нові загрози, пов'язані з неусвідомлюваними інформаційними впливами, формуванням штучної психічної залежності та маніпулюванням суспільною свідомістю, що розглядається як психологічний вплив, майстерна реалізація якого веде до прихованого збудження в користувача соціальних мереж намірів, котрі не збігаються з її реальними бажаннями.

У контенті соціальних мереж містяться надзвичайно великі об'єми інформації, яка не завжди є якісною, достовірною та об'єктивною. На додачу самі ж користувачі зазначають правдиві відомості про себе та оприлюднюють власні фото заради того, щоб краще дізнатися про життя інших. Тож сьогодні постали дві ключові проблеми, а саме: щодо захисту користувачів від впливів інформації, яка несе певний прихований зміст, і захисту інформації самих же користувачів.

З іншої боку, соціальні мережі є новою й недостатньо освоєною технологією інформаційного обміну в суспільстві, тому в ньому зростає вразливість до можливих негативних інформаційних впливів. Сучасні соціальні мережі, крім цілей міжособистісної комунікації, часто використовуються маніпуляторами для збурення суспільних протестів, спричинення збройного протистояння та захоплення влади насильницьким шляхом. Задля того, щоб керувати і впливати на людину використовуються спеціальні маніпулятивні технології.

Можна виокремити такі ознаки маніпулятивного впливу в соціальних мережах, як:

- прихованість маніпулятивного впливу;
- уміле оперування інформацією;
- латентний вплив на здійснення вибору;
- переважний акцент робиться на «масових людей»;
- ідея «прибирання до рук», перетворення об'єкта маніпулювання на «ідеального раба»;
- спонукання до певної поведінки за допомогою обману або гри на передбачуваних слабкостях іншого;
- створення ілюзорного бажання пристосуватися до чогось нового, що лежить в основі сугестії;
- майстерність застосування прийомів впливу;
- ставлення до іншого як до засобу, об'єкта, знаряддя, мішені;
- прихований примус, програмування думок, намірів, почуттів, відносин, установок, поведінки;
- управління і контроль, експлуатація іншого, використання його як об'єкта, предмета;
- збереження ілюзії самостійності об'єкта маніпулювання [1].

Робота в соціальних мережах впливає на центр задоволення в мозку. Бажання повторного отримання цих емоцій змушує людину проводити там дедалі більше часу. Людина отримує багато різновидів інформації дрібними порціями за короткий проміжок часу. До такого режиму роботи мозок звикає дуже швидко. Зручність, швидкість і доступність соціальних мереж і є факторами формування залежності. Саме через надання контенту дрібними порціями в потрібній тональності досягається нейролінгвістичне програмування. Це дає можливість поширювати чутки, які надаються маніпуляторами зазвичай «вирваними» кусками інформації, та викликати в користувачів необхідну емоційну реакцію.

Часто соціальні мережі використовуються з метою здійснення маніпулятивного впливу на суспільну свідомість населення країни та для інформаційного протиборства на міжнародному рівні.

В умовах гібридної війни Російської Федерації проти України небезпечний деструктивний інформаційно-психологічний вплив, спрямований на розпалювання національних, релігійних та інших протиріч, ненависті й непокори, здійснюється в таких найпопулярніших соціальних мережах, як «ВКонтакте», «Одноклассники», Facebook тощо.

Факторами цього небезпечного впливу є:

- неспроможність відвідувачів соціальних мереж аналізувати великі масиви інформації та перевіряти її на достовірність;
- недостатня технічна підготовка реципієнтів масової комунікації для отримання із соціальних мереж якісної інформації.

Це призводить до того, що відвідувачі соціальних мереж можуть піддаватися впливу деструктивних маніпулятивних технологій, ворожої пропаганди, спеціальних інформаційних операцій тощо, які активно проводяться в глобальному інформаційному просторі.

Тому сьогодні маніпулятивний вплив на психіку людини в соціальних мережах став можливим не лише під час безпосереднього контакту, а й через Інтернет-ресурси.

Основним завданням маніпуляторів є внесення «сенсаційної» інформації в середовище користувачів соціальних мереж із метою подальшої трансляції ними цієї інформації ширшому загалу, представляючи при цьому її як суспільну думку та настрої певної частини людей.

Сучасні інформаційні технологи в соціальних мережах використовують різні прийоми маніпулятивного впливу. Одним з них є *прийом соціального доказу*, розрахований на використання групового інстинкту «масової людини», яка переймає нав'язану їй ілюзорну

поведінку більшості. Спрацьовує так званий «ефект натовпу» – «як більшість, так і я». При цьому немає необхідності витрачати додатковий час і напружувати мізки для перевірки отриманої інформації на достовірність.

Часто в соціальних мережах маніпулятори використовують технології нейролінгвістичного програмування (НЛП), які демонструє *прийом дзеркального повернення*, коли маніпулятор спілкується з реципієнтом «його мовою». Для ефективного інформаційного впливу та переконання реципієнта маніпулятор здійснює підлаштування – процес установлення і підтримання «рапорту» (мовою НЛП – контакту) з іншою людиною шляхом приєднання до її моделі світу, мови, ідеалів, цінностей, справжніх переживань [2].

З метою збурення населення, підтримки акцій протесту й масової непокори на території України в соціальних мережах використовується *прийом «вмонтованих» мовних команд*. Цей прийом характеризується смисловим наголошенням вмонтованої інформації, що являє собою фрагмент вислову, здатного викликати у відвідувачів соціальних мереж певні емоції та змінити їхні думки в напрямі, потрібному маніпулятору. Соціальні мережі дають змогу забарвлювати текстовий матеріал потрібною емоційною інтерпретацією, тим самим визначаючи своє ставлення до змісту наданої інформації, що важливо при формуванні громадської думки. Як правило, маніпулятори подають цю інформацію з різним змістом, проте з одним емоційним забарвленням.

Ефективним для маніпулятивного впливу є також прийом «вкидання частини інформації». Ця частина інформації сформована так, що підштовхує індивіда самому доповнювати зміст повідомлення в необхідному для маніпулятора напрямі.

Маніпулятори соціальних мереж запозичили відомий ще із часів міністра пропаганди фашистської Німеччини Й. Геббельса *прийом багаторазового повторення*, який базується на постійному повторенні певного твердження, що призводить до сприйняття його мережевим співтовариством як єдино правильного.

Варто зазначити, що крім зазначених маніпулятивних прийомів у соціальних мережах також використовуються технології інформаційного впливу звичайних ЗМІ.

Крім цього, для приховування смислового змісту, інформація в соціальних мережах подається маніпуляторами певними порціями та в несистематизованому вигляді, що викликає в користувачів утруднення щодо аналізу її значення та сутності.

Соціальні мережі збирають біографічні дані, щоб допомогти користувачам легко знаходити один одного. Така інформація також залучає мисливців за персональними даними. Існує чимало спеціальних програм стеження і зламу. Деякі з них можна безкоштовно скачати в Інтернеті, а складніші – купити. Наприклад, одна з найпопулярніших програм Spy Recon не лише фіксує все, що було введено з клавіатури, в тому числі паролі, а й записує чати, які велися з використанням комп'ютера (ICQ, Skype, MSN).

Виявити такого електронного зломщика вкрай важко. Тому для забезпечення власної безпеки варто обмежити особисту інформацію в соціальних мережах. Сучасні технології дають змогу виявити персональні дані в соціальній мережі, не використовуючи незаконні засоби [3].

Не слід також забувати про масу різних вірусних програм і троянів, здатних фіксувати все, що відбувається на екрані, та запам'ятовувати порядок введення символів з клавіатури персонального комп'ютера чи смартфона. Як наслідок, паролі й логіни, необхідні для входу в той чи інший акаунт, а згодом персональна інформація та вміст потрапляють до рук зловмисників.

Існують також фальшиві акаунти, які фахівці називають ботами (скорочення від «робот»), головне завдання яких – керувати настроями людей у соціальних мережах.

Такими послугами активно користуються політичні та громадські діячі. Політтехнологи у 90% політичних проектів купують лайки, проплачують коментарі та загалом організовують цілі піар-кампанії в соціальних мережах. Прикладом цього є популярність сторінок окремих політичних чи громадських діячів, які мають десятки тисяч підписантів, але їхні записи не набирають більше десятків «лайків» [4].

До негативних наслідків варто віднести також залежність від соціальних мереж як одну з найгостріших особливостей комунікацій.

Статистика на сьогодні така: понад 10% усіх Інтернет-користувачів страждають на залежність від соціальних мереж, і найчастіше залежними стають люди від 18 до 24 років. Залежність від соціальних мереж дійшла до того, що люди «сидять» у них постійно – на роботі, у транспорті, під час навчання та обіду, спілкуються в соціальних мережах, перебуваючи на відстані кількох метрів один від одного.

Виникає нагальна потреба забезпечення інформаційної безпеки особи, окремих груп і населення загалом від негативних інформаційно-психологічних впливів у соціальних мережах.

Висновки

Сучасні соціальні мережі є важливим інструментом комунікації. Проте вони також є середовищем для поширення матеріалів маніпулятивного впливу. Це може призвести до виникнення (корегування) певних уявлень, суджень, вчинків чи організації соціальних протестів, які використовуються внутрішніми і зовнішніми конкістадорами для досягнення різного роду цілей.

Основним об'єктом негативного впливу обирається молодь, серед якої найбільша частка користувачів соцмереж і якій притаманні такі якості, як нігілізм і бунтарство, що маскують під національну ідею [5].

Варто зауважити, що наслідками деструктивних маніпулятивних прийомів є негативний вплив на свідомість і підсвідомість користувачів соціальних мереж, який може спричинити придушення їхньої волі та навіть призвести до зміни індивідуальності. У результаті довготривалого інформаційно-психологічного впливу можуть виникати зазомбовані групи, готові до будь-яких дій, керованих ззовні, а це, у свою чергу, може спричинити реальну загрозу національній безпеці.

Попри те, що сучасні новітні інформаційно-комунікаційні технології та соціальні мережі стали ефективним знаряддям розвитку суспільства і взаємовідносин між державами, виникають нові загрози, пов'язані з використанням соціальних мереж для здійснення деструктивних маніпулятивних інформаційних впливів, порушення життєво важливих інтересів людини, суспільства й держави та створення загроз інформаційній інфраструктурі та національній безпеці України загалом.

Саме тому постає питання ефективного забезпечення інформаційної безпеки як важливої складової національної безпеки.

Перелік літератури

1. Інформаційна безпека (соціально-правові аспекти) : підручник / В. В. Остроухов, В. М. Петрик, М. М. Присяжнюк, Я. М. Жарков та ін.; за заг. ред. Є. Д. Скулиша. – К. : КНТ, 2010. – 776 с.

2. Сугестивні технології маніпулятивного впливу: навч. посіб / [В. М. Петрик, М. М. Присяжнюк, Л. Ф. Компанцева, О. Д. Бойко, В. В. Остроухов]; за заг. ред. Є. Д. Скулиша. – К. : ВІПОЛ, 2011. – 248 с.

3. Шпигунство в соціальних мережах : Інтернет-конференція кафедри інформаційних технологій НУ «ОЮА» / А. О. Яцишин [Електронний ресурс]. – Режим доступу : http://conf.inf.od.ua/doklady-konferentsii/spisok-materialov-konferentsii/56-yatsishin-a-o-student-2-go-kursu-institutu-prokuraturi-ta-slidstva-nu-oyua-naukovij-kerivnik-k-t-n-dotsent-zaderejko-o-v-shpigunstvo-v-sotsialnikh-merezhakh.

4. Знайомтесь, це боти: Завдяки їм політики намагаються підвищувати свій рейтинг / Є. Коляда // Експрес-онлайн [Електронний ресурс]. – Режим доступу : https://expres.online/archive/news/2016/11/25/214655-znayomtes-boty-zavdyaky-yim-polityky-namagayutsya-pidvyshchuvaty-sviy-reytyng.

5. Соціальні мережі як середовище для технологій маніпулятивного впливу / ІССС – Міжнародний центр протидії кіберзлочинності / Я. А. Деркаченко [Електронний ресурс]. – Режим доступу : https://iccc.pro/ article/socialni-merezhi-yak-seredovyshche-dlya-tehnologiy-manipulyatyvnogo-vplyvu.