Національна безпека

УДК 336.72

Присяжнюк Микола Миколайович
Кандидат технічних наук, старший науковий співробітник
Навчально-науковий інститут інформаційної безпеки
Національної академії Служби безпеки України
Парасунько Микола Миколайович
Студент 2-го курсу магістратури навчальної групи І-151М
Навчально-науковий інститут інформаційної безпеки
Національної академії Служби безпеки України

Присяжнюк Николай Николаевич
Кандидат технических наук, старший научный сотрудник
Учебно-научный институт информационной безопасности
Национальной академии Службы безопасности Украины
Парасунько Николай Николаевич
Студент 2-го курса магистратуры учебной группы І-151М
Учебно-научный институт информационной безопасности
Национальной академии Службы безопасности Украины

Prysiazhniuk M.
Candidate of Technical Sciences, Senior Research Fellow
Educational and Scientific Institute of Information Security
National Academy of Security Service of Ukraine
Parasunko M.
Student 2-year student of Master Study Group I-151M
Educational and Scientific Institute of Information Security
National Academy of Security Service of Ukraine

СОЦІАЛЬНІ МЕРЕЖІ ЯК ЕФЕКТИВНИЙ ІСТРУМЕНТ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ВПЛИВУ ІНОЗЕМНИМИ СПЕЦСЛУЖБАМИ

СОЦИАЛЬНЫЕ СЕТИ КАК ЭФФЕКТИВНЫЙ ИНСТРУМЕНТ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОГО ВОЗДЕЙСТВИЯ ИНОСТРАННЫМИ СПЕЦСЛУЖБАМИ

SOCIAL NETWORKING AS AN EFFECTIVE INSTRUMENT INFORMATION-PSYCHOLOGICAL INFLUENCE OF FOREIGN INTELLIGENCE SERVICES

Анотація: *У статті розкриваються нові технології впливу в соціальних мережах на населення певної держави, також розкриваються особливості розвідувально-підривної діяльності іноземних розвідок в мережі Інтернет, до яких було віднесено: цілеспрямованість і плановість застосування; конкретність визначення об'єкта впливу; збір інформації для подальшого визначення, конкретність поведінки, що ініціюється. Досліджується ключові етапи збору інформації для подальшого використання маніпулятивниго впливу на свідомість людини в Інтернеті. Розкриваються причини ефективності технологій підбурювання користувачів в мережі Інтернет та найбільш впливові техніки впливу.*

Ключові слова: *Інтернет; соціальні мережі; інформаційний простір; розвідувально-підривна діяльність; конфіденційна інформація; маніпулювання свідомістю.*

Аннотация: *В статье раскрываются новые технологии влияния в социальных сетях населения данного государства, также раскрываются особенности разведывательно-подрывной деятельности иностранных разведок в сети Интернет, в которых были отнесены: целеустремленность и плановость применения; конкретность определения*

объекта воздействия; сбор информации для дальнейшего определения, конкретность поведения, инициируется. Исследуется ключевые этапы сбора информации для дальнейшего использования манипулятивниго воздействия на сознание человека в Интернете. Раскрываются причины эффективности технологий подстрекательство пользователей в сети Интернет и наиболее влиятельные техники воздействия.

Ключевые слова: *Интернет; социальные сети; информационное пространство; разведывательно-подрывная деятельность; конфиденциальная информация; манипулирования сознанием.*

Summary: *The article describes the impact of new technologies on social networks on the population of a state, and the peculiarities of intelligence and subversive activities of foreign intelligence services on the Internet, which could include commitment and planning applications; Receptor specificity determination; gathering information to further identify, concrete behaviors initiated. We study the key stages of collecting information for later use manipulyatyvnyho impact on the human mind online. Reasons efficiency technologies inciting users to the Internet and most influential technology influence.*

Keywords: *Internet; social networks; information space; reconnaissance and subversive activities; confidential information; manipulation.*

Постановка наукової проблеми. Разом з розвитком інформаційного суспільства та сучасними досягненнями в галузі інформаційних технологій розвивається мережа Інтернет. Однак, Інтернет-середовище часто використовується для здійснення всякого роду маніпулювань для досягнення певних результатів в сфері політики та національної оборони певних держав. Зважаючи на інтенсивний розвиток інформаційних технологій і те, що Інтернет є основним способом інформаційно-

психологічного впливу, виникає необхідність поглибленого дослідження цього феномену. Активна динаміка розвитку інформаційного суспільства та вживання маніпулятивних технологій зокрема в соціальних мережах обумовлюють актуальність дослідження.

Аналіз останніх публікацій. Дослідженням соціальних мереж як середовища інформаційно-психологічного впливу займалася значна кількість вітчизняних і зарубіжних вчених. Проблеми впливу засобів технологій на свідомість і підсвідомість окремими аспектами розглянуті в роботах таких науковців як Н. В. Слухай, Л. Ф. Компанцева, Р.В. Гумінський, В.Д. Гавловський та ін. Проте, технології інформаційно-психологічного впливу в соціальних мережах ще не стали предметом конкретних наукових досліджень.

Метою статті є розкриття сутності наукових дослідженнях, пов'язаних з протидією деструктивному інформаційно-психологічному впливу.

Для досягнення мети в статті вирішуються такі *завдання*:

1)дослідження проблем створення систем контент-моніторингу соціальних ресурсів мережі Інтернет з метою розвідки та інформаційного протиборства;

2)роз'яснення методів і алгоритмів проведення інформаційних операцій у відкритих (закритих) ресурсах Інтернету.

Об'єктом дослідження є глобальний інформаційний простір з позицій соціальних комунікацій.

Предмет дослідження – механізми впливу в соціальних мережах, які використовуються в інформаційних кампаніях.

Викладення основного матеріалу дослідження. У системі загальної протидії розвідувально-підривній діяльності іноземних спецслужб проти України, зокрема, і вчиненню протиправних дій проти громадян

України з боку таких суб'єктів, пріоритетне місце природно закріплене за Службою безпеки України.

Характерною особливістю діяльності іноземних спецслужб на сучасному етапі, безсумнівно, є намагання використовувати для здобування розвідувальної інформації можливостей, що утворилися завдяки розвитку науки та техніки.

Беззаперечним є факт, що об'єктивно інтенсивний розвиток протягом останніх десятиліть глобальних інформаційних мереж має бути визнаний одним із визначальних факторів загальних інтеграційних процесів у суспільстві. З одного боку, саме завдяки сучасним інформаційним технологіям створено реальні умови для загального доступу: до різноманітних інформаційних ресурсів незалежно від фактичної відстані між джерелом інформації та особою, зацікавленою в її отриманні, а, з іншого, штучно створюються реальні можливості для несанкціонованого, тобто безконтрольного, з боку власників персональної інформації, а, отже, протиправного її використання (систематизації, обробки, аналізу).

Значну потенційну небезпеку тут становлять соціальні мережі, сучасний стан накопичення та зберігання персональних даних особи в яких створює плідне підґрунтя як для втягування наших співгромадян іноземними спеціальними службами у протиправну (розвідувально-підривну, терористичну та іншу) діяльність [1, с. 253], так і для збору іншої різнопланової розвідувальної інформації. При цьому, діюча на сьогодні в Україні система захисту особи не спроможна забезпечити ефективний захист наших співгромадян від протиправних дій з використанням інформаційно-маніпулятивних технологій в соціальних мережах. Розглядаючи інформаційно-психологічний вплив віртуальних спільнот на національні інтереси держави, суспільства виділяють три етапи формування інформаційного впливу віртуальних спільнот [2, с. 27]:

перший етап – створення активного соціального сегмента незадоволеного політичним режимом;

другий етап – інтенсивна інформаційна пропаганда цієї незадоволеності в інформаційному просторі;

третій етап – блокування соціальних груп, які не підтримують ідеологію цього соціального сегмента.

При цьому повинні вирішуватися такі завдання:

– розбудити (підвищити) активність масової свідомості;

– утримати активність (агресивність) на певному рівні, не виходячи за його межі;

– озброїти своїх прихильників аргументацією для бесід з їхніми супротивниками.

Для більш ефективного використання інформаційних технологій впливу потрібно проводити детальний аналіз вікової групи на який буде скерована основна інформаційна атака. Для цього потрібний значний обсяг конфіденційної інформації інтернет користувачів які самі викладають інформацію в соціальних мережах.

Власна конфіденційна інформація користувачів у соціальних мережах має не просто різноплановий, а і в ряді випадків завершений характер. Користувач фактично сам складає на себе досьє: повні установчі та автобіографічні дані, відомості про професійну діяльність, особисті уподобання, нахили, спосіб життя, фотографії тощо, а також фактично повні відомості про своє оточення – тобто так званий «список зв'язків», і з повним «досьє» на кожного суб'єкта цього списку. Якщо додати сюди можливість обробки, систематизації та аналізу інформації за різноманітними пошуковими реквізитами, можна отримати майже ідеальний для будь-якої спецслужби пошуково-довідковий інформаційний масив для виявлення осіб, які становлять оперативний інтерес, їх вивчення та розробки тощо. Дійсно, якщо за інших умов на збір аналогічної персональної інформації

спецслужби мали б використовувати колосальні гласні та негласні сили і засоби, час, ставити під загрозу оперативну розробку через її можливу розшифрування внаслідок задіяння великої кількості людей, то використання в якості засобу та джерела отримання такої інформації соціальних мереж робить цей процес швидким і дешевим, а крім того, майже унеможливлює розшифрування об'єкта оперативної зацікавленості.

Не викликає сумнівів той факт, що у соціальних мереж є технічні можливості відслідковувати інформацію про своїх користувачів, їх активність у мережі Інтернет незалежно від того знаходяться чи не знаходяться вони в соціальній мережі, тобто після виходу зі сторінок соціальної мережі, а також про користувачів мережі Інтернет, які взагалі не мають акаунта в соціальній мережі, шляхом створення профілів незареєстрованих користувачів.

Звертає на себе увагу і той факт, що деякі соціальні мережі майже ідеально створені для прикриття розвідувально-пошукової діяльності спецслужб щодо збору різнопланової, придатної для наступного аналітичного дослідження інформації [3, с. 257]. Проте, це, на жаль, не єдина демаскуюча ознака, що свідчить на користь того, що іноземні спеціальні служби давно та плідно використовують соціальні мережі в якості засобу для збору розвідувальної інформації.

Досить показовим з точки зору підтвердження факту відслідковування, збирання та систематизації інформації, що містить персональні дані та конфіденційну інформацію про користувачів інформаційно-телекомунікаційного простору, є аналіз документальних матеріалів щодо цього аспекту діяльності соціальної мережі Facebook.

Зокрема, те як Facebook стежить за відвідувачами мережі Інтернет досить наочно описав А. Роозендааль (Тілбургский університет, Нідерланди) [4, с. 231]. Це підтвердив Н. Кубріловік, проаналізувавши HTTP-заголовки запитів, що відправляються браузерами на facebook.com,

він виявив наявність видозмінених cookie-файлів, що з'являються після виходу зі сторінки Facebook [5, с. 54].

Той факт, що Facebook створює досьє як на користувачів цієї соціальної мережі, так і на тих, хто ще не зареєстрований на сервісі був підтверджений після перевірки компанії Facebook Ireland ірландським відомством, яке займається захистом персональних даних – Офісом уповноважених із захисту персональних даних і приватності [6, с. 543].

У свою чергу, німецьке агентство Data Protection Authority опублікувало доповідь, в якій викриває соціальну мережу Facebook у відслідковуванні навіть тих користувачів, які видалили свою сторінку і покинули цей Інтернет-проект. Зокрема, було заявлено, що для відслідковування Facebook використовує cookie-файли, здатні передавати інформацію про комп'ютер користувача та його переміщення по всесвітній павутині [7, с. 73].

До того ж Центр захисту недоторканності особистого життя в Німеччині оприлюднив заяву, в якій вказувалося, що керівництво соціальної мережі передає особисту інформацію про користувачів третім особам у США. «Користувачі Facebook повинні знати, що вони відслідковуються компанією», – заявили представники Центру, відзначивши, що це порушення закону Євросоюзу із захисту особистої інформації [8, с. 122].

Про тотальне відслідковування даних користувачів наголошує і Д. Ассанж, засновник Wikileaks. Він відмічає, що користувачі додаючи контакт у свій Facebook, працюють на американські розвідки, оновлюючи їх бази даних. Інші розвідки можуть або зламати Facebook, або отримати цю інформацію від американців у обмін на якісь послуги [9, с. 137].

У ряді випадків факти використання соціальних мереж спеціальними службами отримують і офіційне підтвердження. Так, директор розвідувального центру при ЦРУ США Open Source Ctyter Даг Накуін повідомив журналістам, що ввірений йому підрозділ стежить за змістом

соціальних мереж практично в усьому світі, зокрема, щоденно фільтрується до п'яти мільйонів твістів [10, с. 49]. Крім того, за повідомленням офіційного сайту ЦРУ, із грудня 2006 року цей підрозділ використовує мережу Facebook для вербування кандидатів для роботи у національних секретних службах [11, с. 87]. Аналогічна інформація надходить про використання соціальних мереж спецслужбами Великобританії, зокрема, розвідувальною службою MI-6 [12, с. 68]. Збір цих даних дає можливість будувати цілісну систему матрицю впливу на певний тип населення враховую національність , стать, релігійні переконання та вікова категорія. В сукупності за допомогою цих технологій інформаційних атак можна будувати цілі кампанії, які прозвали «кольорові революції».

Сьогодні геополітики активно вивчають феномен «кольорових революцій», оскільки саме з їх допомогою відбувається перерозподіл простору влади в нестабільних регіонах світу. Експерти виділяють такі відмітні риси «кольорових революцій»:

1) використання переважно невійськових засобів досягнення цілей - інформаційно-психологічних впливів, мирних політичних акцій, легітимних методів зміни режиму. Вельми благодатний ґрунт для «кольорових революцій» представляють вибори, адже необхідна умова безкровної революції - масову участь в ній населення;

2) головна ударна сила «кольорової революції» - не революційний більшість народу, а так звана п'ята колона, фінансована з-за кордону;

3) на відміну від традиційних, «кольорова революція» - це мережний процес, що працює за принципом мережевого і активно використовує всі канали ЗМІ для легітимації своїх цілей і завдань. Таким чином, в певному сенсі «кольорові революції» можна розглядати як особливу форму інформаційної війни.

Дуже важливо визначити причини, генеруючі даний феномен. Сьогодні ні для кого не секрет, що головним каталізатором «кольорових

революцій» стають зовнішні фактори і ресурси. Необхідною умовою здійснення таких революцій є наявність активних зарубіжних спонсорів, які фінансують молодіжні організації і опозиційні політичні партії, лідери яких заявляють про свою підтримку західної моделі демократії. Цілком очевидна зв'язок активістів революцій з грантами або стипендіями таких організацій, як Інститут «Відкрите суспільство» (Фонд Джорджа Сороса), Гарвардський університет, Інститут Альберта Ейнштейна, Міжнародний республіканський інститут, Національний демократичний інститут (США), Міжнародний центр ненасильницьких конфліктів, Міжнародний інститут стратегічних досліджень у Лондоні та багатьох інших.

Відомо, що значні фінансові ресурси на організацію «кольорових революцій» надходили через американський фонд «Підтримки демократії у Східній Європі» (Support for East European Democracy - SEED). Витрати SEED - частина бюджету держдепартаменту США. Загальні фінансові надходження через SEED в Сербію склали близько 90 млн дол. В українську «помаранчеву революцію» США вклали понад 85 млн дол.

До речі, і у вітчизняних спеціальних наукових джерелах останнім часом оприлюднюються думки про те, що спецслужби іноземних держав мають певні можливості для цілеспрямованого моніторингу соціальних мереж з метою виявлення серед громадян України корисних їм, у тому числі придатних для конфіденційного співробітництва [13, с. 88], та про те, що загрози несанкціонованого збирання персональних даних і побудови прихованих каналів зв'язку можуть бути реалізовані на рівні спеціальних служб та інших силових структур, що мають протиправні наміри з різним рівнем мотивації. Для їх активізації використовуються різні методи, які для розв'язання цих задач не відрізняються від класичних методів інформаційно-психологічного впливу і починаються з атаки на масову свідомість з використанням класичних методів інформаційних війн [14, с. 189]:

За цілями:

– методи пропаганди;

– методи контрпропаганди.

Методи пропаганди націлені на те, щоб донести до населення необхідні ідеї, тобто сформувати на певній ділянці інформаційного простору потрібні інформаційні сутності. Відповідно, методи контрпропаганди спрямовані на дискредитацію ворожих ідей, руйнування шкідливих інформаційних сутностей і недопущення їх виникнення надалі.

За характером дії:

– явні методи;

– неявні (приховані) методи.

Явні методи відрізняються від неявних тим, що в них мету і характер впливу не приховують від супротивника. Серед основних моделей ведення інформаційного противоборства у соціальних мережах варто виділити такі:

– модель мережевих атак;

– модель із залученням користувачів;

– модель тотального блокування.

Підсумовуючи, вважаю за необхідне зазначити, що фактично ми маємо говорити про системне використання іноземними спецслужбами та організаціями соціальних мереж, діяльність яких перебуває і юридично і фактично поза межами правового регулювання нашої держави, в якості прикриття своєї розвідувальної (розвідувально-підривної) діяльності проти України. Отже, йдеться про наявність нової реальної загрози національній безпеці України, на протидію та нейтралізацію якій має бути спрямована діяльність низки складових структурних елементів механізму держави, а основну організаційну функцію тут природно має реалізовувати саме Служба безпеки України, як спеціально уповноважений орган державної влади у сфері контррозвідувальної діяльності.

Висновки. Підсумовуючи, вважаю за необхідне зазначити, що фактично ми маємо говорити про системне використання іноземними спецслужбами та організаціями соціальних мереж, діяльність яких перебуває і юридично і фактично поза межами правового регулювання нашої держави, в якості прикриття своєї розвідувальної (розвідувально-підривної) діяльності проти України. Отже, йдеться про наявність нової реальної загрози національній безпеці України, на протидію та нейтралізацію якій має бути спрямована діяльність низки складових структурних елементів механізму держави, а основну організаційну функцію тут природно має реалізовувати саме Служба безпеки України, як спеціально уповноважений орган державної влади у сфері контррозвідувальної діяльності.

Література:

1. Гавловський В.Д. До питання захисту персональних даних у соціальних мережах / В. Д. Гавловський // Б-ба з орг. злоч. (теорія і практика) : наук.-практ. журнал. – К.: МНДЦ при РНБО України, 2011. – № 24. – С. 252–262.
2. Доценко Е. Л. Психология манипуляции: феномены, механизмы и защита. – М.: ЧеРо, 1997. – 344 с.
3. Остроухов В.В. Інформаційна безпека (соціально-правові аспекти): підруч. / [Остроухов В.В., Петрик В.М., Присяжнюк М.М. та ін.; за заг. ред. Є.Д.Скулиша]. – К. : КНТ, 2010. – 776 с.
4. Наукові записки. Серія «Філологічні науки» (Ніжинський державний університет імені Миколи Гоголя) / відп. ред. проф. Г. В. Самойленко. – Ніжин: НДУ ім. М. Гоголя, 2013. – Кн. 3. – 235 с.
5. Сугестивні технології маніпулятивного впливу: навч. посіб. / В.М. Петрик, М.М. Присяжнюк Л.Ф. Компанцева, О.Д. Бойко, В.В. Остроухов / заг Ред. Є. Д. Скулиша. – К.: ВІПОЛ, 2011. – 248 с.

6. Рябоконь О. Маніпуляції масовою свідомістю в політичному сегменті соціальних мереж / О. Рябоконь // Наукові праці Національної бібліотеки України ім. В. І. Вернадського. – 2012. – Вип. 33. – С. 543-553. – Режим доступу: http://nbuv.gov.ua/UJRN/npnbuimviv_2012_33_50.
7. Сугестивні технології маніпулятивного впливу : навч. посіб. / М.М. Присяжнюк, Л.Ф. Компанцева, Є. Д. Скулиш [та ін.] ; ред.: Є.Д. Скулиша; Нац. акад. СБУ. – Київ, 2010. – 247 с.
8. На Facebook подают в суд в Калифорнии: соцсеть тоже шпионила за пользователями / [Електронний ресурс]. – Режим доступу: http://hitech.newsru.com/article/03Oct2011/fcbksuit.
9. Facebook постоянно следит за пользователями / [Електронний ресурс]. – Режим доступу: http://www.versii.com.ua/news/240639.
10. Facebook збирає досьє на тих, хто ще не зареєстрований / [Електронний ресурс]. – Режим доступу: http://vidgolos.com/119526-facebook-zbiraye-dosye-na-tix-xto-shhe-ne.html.
11. Германия обвиняет Facebook в слежке за пользователями / [Електронний ресурс]. – Режим доступу: http://infox.ru/hi-tech/internet/2011/11/03/Gyermaniya_obvinyayephtml.
12. Facebook постоянно следит за пользователями / [Електронний ресурс]. – Режим доступу: http://www.versii.com.ua/news/240639.
13. «Шпионы кардинала»: за нами следят «айфоны», «андроиды», социальные сети и даже ФСБ. Паникуем? / [Електронний ресурс]. – Режим доступу: http://www.aif.ru/techno/article/42864.
14. Спецслужбы раскинули социальные сети / [Електронний ресурс]. – Режим доступу: http://www/pravda.ru/society/hov/08-11-2011/1097800-cru-0.