УДК 355/359.07

к.політ.н. **Турченко Ю.В.** (ВІКНУ)

ВИКОРИСТАННЯ СОЦІАЛЬНИХ МЕРЕЖ У ЗДІЙСНЕННІ ДЕСТРУКТИВНИХ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИХ ВПЛИВІВ НА ОСОБОВИЙ СКЛАД ВІЙСЬК (СИЛ) ТА ОРГАНИ ВІЙСЬКОВОГО УПРАВЛІННЯ

Встановлено можливість використання соціальних мереж у здійсненні деструктивних інформаційно-психологічних впливів на особовий склад військ (сил) та органи військового управління. З'ясовано, що ефективність використання соціальних мереж для здійснення інформаційно-психологічного впливу, в першу чергу пов'язана із можливістю створення у них різних віртуальних спільнот (груп) за певними інтересами. Доведено можливість здійснення впливу через соціальні мережі та доцільність здійснення моніторингу загроз у таких мережах. Обґрунтовано необхідність розробки та впровадження на озброєння ЗСУ сучасних інформаційних систем для забезпечення виконання завдань протидії негативному інформаційно-психологічному впливу, як на етапі виявлення, так і на етапі нейтралізації його проявів.

Ключові слова: соціальні мережі, моніторинг загроз, інформаційні процеси (дії), негативний інформаційно-психологічний вплив, протидія, воєнна сфера, інформаційна безпека, інформація.

Постановка проблеми. Морально-психологічний стан особового складу військ (сил) та органів військового управління є однією із основних складових, які забезпечують можливість реалізації придбаних практичних навичок та умінь у ході виконання ними службових обов'язків та бойових завдань. Рівень такого стану залежить від психологічних особливостей кожної людини, ступеню її готовності до спротиву зовнішнім деструктивним інформаційно-психологічним впливам (ІПсВ), який забезпечується відповідною підготовкою, що ведеться перед призначенням на відповідні посади, та підтримується відповідними структурами Міністерства оборони (МО) України.

Враховуючи постійну потребу людини в отриманні інформації кожна особа, у будь-якому випадку, сприймає повідомлення позитивного, нейтрального та деструктивного характеру. Сукупність таких повідомлень формує базу знань особи для оцінювання поточної обстановки, її можливого розвитку. Такі дані є основою для прийняття рішень щодо подальшої послідовності дій, які, в залежності від ступеню загроз реалізації особистих потреб, можуть сприяти або знижувати якість виконання посадових обов'язків.

Пріоритетним завданням військової політики економічно розвинених держав світу на сучасному етапі є інформатизація збройних сил. Перевага у ступені інформованості стає неодмінною умовою перемоги у війні, що переконливо доводить досвід збройних конфліктів і локальних війн, а також проведення антитерористичної операції силовими структурами України. Разом з тим, стрімкий розвиток і впровадження інформаційних технологій у системах управління військами та зброєю обумовлює появу широкого спектру загроз інформаційній безпеці таких систем. За рахунок охоплення телекомунікаційними системами практично будь-якого місця можливого перебування людини та портативні засоби підключення до них створюють умови здійснення постійного ІПсВ на неї. Це особливо загострює актуальність розробки тематики удосконалення системи протидії деструктивним інформаційним впливам.

Одним із можливих шляхів запобігання деструктивних впливів на особовий склад є своєчасне виявлення доступних для сприйняття деструктивних загроз в інформаційній сфері. Реалізувати таке завдання можливо шляхом вдосконалення системи виявлення негативного ІПсВ на особовий склад військ та органів військового управління.

Аналіз останніх досліджень і публікацій. Застосування інструментарію соціальних мереж у здійсненні інформаційно-психологічного впливу широко дискутується дослідниками. Серед провідних теоретиків, які вивчали проблематику впливу на суспільну свідомість, зокрема і під час проведення інформаційних операцій, варто назвати Г. Почепцова, Г. Ортега-і-Гасета, Д. Ольшанського, Г. Лебона, Г. Тарда, Е. Фрома, І. Панаріна, М. Лібікі, М. Маклюена, К. Юнга, С. Кара-Мурзу, С. Московічі тощо. Серед вітчизняних та зарубіжних праць щодо оцінювання морально-психологічного стану особового складу різних військових формувань і в цілому військ (сил), слід виділити дослідження І. Замаруєвої, В. Остроухова, Г. Перепелиці, які мають суттєве теоретичне та практичне значення [14-16].

Метою статті є використання інструментарію соціальних мереж у здійсненні деструктивних інформаційно-психологічних впливів на особовий склад військ (сил) та органи військового управління.

Виклад основного матеріалу. Останнім часом Інтернет стає пріоритетним середовищем здійснення інформаційного впливу на формування громадської думки, прийняття політичних, економічних і військових рішень. Можливість ефективного впровадження методів деструктивного ІПсВ в мережі Інтернеті пов'язано з тим, що, в інформаційному суспільстві на базі соціальних мереж створюються віртуальні спільноти (групи), які набувають своєї популярності завдяки широкому спектру можливостей щодо обміну різнотипної інформації серед користувачів мережі [6]. Під *соціальною мережею* мається на увазі соціальна структура, яка складається з множини агентів (користувачів, груп, та суспільств) та визначеної на ній множини відносин (інформаційної взаємодії, знайомств, участі у групах та суспільствах). У рамках даних відносин у мережі відбуваються різні інформаційні процеси. Таким чином, користувачі є реальними суб'єктами інформаційного діяльності, що може призводити до провокування виникнення конфліктів у суспільстві [9, С. 192-199].

Ефективність використання соціальних мереж для здійснення ІПсВ пов'язана із можливістю створення у них різних віртуальних спільнот (груп) за певними інтересами, завдяки яким можливо наповнити інформаційний простір необхідними даними, приховуючи при цьому конкретні цілі певних осіб. Створена віртуальна спільнота (група), свідчить про наявність осіб, здатних до сприйняття ідей, що поширюються, а зростання чисельності групи

показує можливий рівень ефективності ІПсВ. Сформована віртуальна спільнота людей може стати основою для утворення реальних організацій терористичної чи кримінальної спрямованості зі структурою, яку складно виявити [4, с. 28-35].

Аналізуючи соціальні мережі в контексті інформаційних війн, слід приділити увагу психологічним явищам, які роблять мережі привабливими для здійснення інформаційно-психологічного впливу на користувачів. Окремо, доцільно виділити наступні явища, такі як: явище "Спіраль мовчання" (Е. Ноель-Нойман); стадний інстинкт у соціальних мережах; довіра всьому опублікованому в мережі; присутність лідерів думок; прагнення самореалізації чи заміни реальності. Таким чином, модель комунікації німецької Е. Ноель-Нойман полягає в тому, що мас-медіа можуть маніпулювати громадською думкою за рахунок надання слова представникам меншості і замовчування думок більшості. Пов'язаним із вищезгаданою моделлю є явище "стадного інстинкту". Сам принцип стадного інстинкту полягає в тому, що людина за своєю природою – істота колективна, групова. І один з механізмів виживання в групі полягає в тому, щоб у більшості випадків вести себе так само, як і всі, а також переймати досвід інших [13]. "Стадний інстинкт" безпосередньо проявляється в тому, що людина, спостерігаючи велику кількість відгуків, надає такому повідомленню більшого значення та приєднується до більшості, а при наявності малої кількості відгуків частіше залишає повідомлення без достатньої уваги.

Б. Ковалевич зазначає, "що подібне відбувається і з діяльністю груп: людина із більшим задоволенням приєднається до групи, аудиторія якої складає кілька десятків тисяч, аніж до маленької групи із декількома десятками учасників. Цікавим залишається явище повної довіри всій інформації, яка публікується в мережі. Користувач переважно не перевіряє отриману інформацію і приймає її за достовірну, тільки на основі того, що вона публікується солідною групою із значною аудиторією. У цьому аспекті варто зауважити і явище виникнення "лідерів думок", які можуть бути представлені, як окрема незалежна особистість або ж група чи сторінка в соціальній мережі. Саме їм користувач довіряє беззаперечно, навіть іноді вважаючи їх найбільш достовірним джерелом у певних питаннях, упускаючи те, що вони можуть і не бути спеціалістами в даній сфері. За допомогою таких "лідерів думок" держава чи корпорація може забезпечувати прихильність користувача до них або ж переконувати користувачів у власних ідеях, нав'язуючи їм власне бачення конкретних важливих подій, явищ у різних сферах функціонування держави та суспільства"[11]. Слід зазначити, що важливим залишається прагнення користувача до самореалізації в мережі, примірити на себе іншу роль або ж вільно виголошувати свої думки, прикриваючись анонімністю, яку надає мережа. В той же час віртуальність життєдіяльності людини посилюється за рахунок відчуття того, що віртуальна реальність є менш агресивною до людини і в значній мірі підконтрольна їй. Також прагнення людини до віртуалізації свого життя часто обумовлене бажанням зробити своє життя більш яскравим, таким, що містить цікаві події та сильні емоційні почуття [1]. Вищезазначені дії призводять до того, що кількість користувачів соціальних мереж збільшується з кожним роком. Користуючись конкретними даними, зазначимо, що аудиторія соціальної мережі "Facebook" становить більше одного мільярда користувачів, "Twitter", "Google+", "Vk.com" – більше 200 мільйонів, "LinkedIn" та "Odnoklassniki.ru" – більше 100 мільйонів.

Крім того, що одним з головних факторів, що пояснює можливість здійснення ІПсВ на користувача соціальної мережі є залежність користувача від соціальних мереж, яка викликана певною зацікавленістю. Зацікавленості об'єктів соціальними мережами обумовлена наступними причинами: можливості отримання різноманітної інформації; верифікація ідей через участь у взаємодії у соціальній мережі; соціальна вигода від контактів; рекреація; стирання традиційних обмежень реального життя; формування самобутньої культури спілкування; можливість постійної зміни статусу учасників комунікації; особливості взаємодії текстового і візуального контенту; психологічний ефект.

Виявити ІПсВ у соціальній мережі можливо шляхом побудови її моделі. Маючи модель інформаційного впливу можливо ставити та вирішувати завдання інформаційного

управління – якими повинні бути інформаційні впливи, щоб досягнути від суб'єкта необхідної поведінки. Об'єкту впливу надається інформація про ситуацію та процес, що склався, при цьому іншу інформацію намагаються зробити для нього недоступною. В таких умовах об'єкт змушений обирати лінію поведінки, орієнтуючись головним чином на цю інформацію. У такий спосіб йому нав'язується упереджене ставлення до ситуації, що склалася.

На практиці виділяють такі основні елементи мережі (рис. 1.) [12]:

– зовнішній вузол (ЗМІ, інші інформаційні джерела);

– зовнішній суб'єкт, який здатний впливати на процеси у соціальній мережі (політичний діяч, представники партії, комерційна організація);

– соціальна мережа у цілому або підмережа (множина вузлів, яка виділена за конкретною ознакою та зв'язки між ними);

– користувачі мережі;

– вузол мережі (агент);

– інформаційне повідомлення (пост, коментар, повідомлення);

– інформаційний об'єкт – подія, персона;

– інформація – опис деяких інформаційних об'єктів у інформаційному повідомлені;

– думка (розсуд по деякому питанню, точка зору на об'єкт, оцінка).

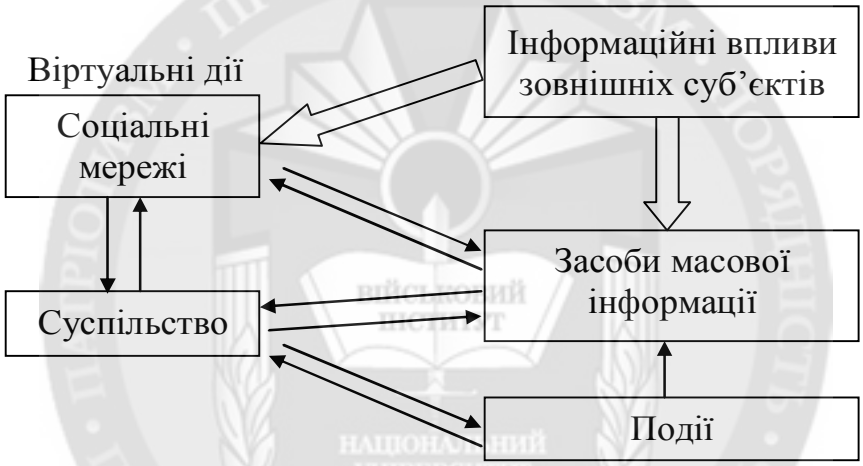

Рис. 1. Спрощена модель соціальної мережі

Вплив на процеси у соціальній мережі здійснюють зовнішні фактори (події) з боку зовнішніх суб'єктів. Зовнішні суб'єкти можуть бути зацікавлені у досягненні мережею певного цільового стану: необхідного ступеня зв'язку (або навпаки роз'єднаності) мережі, формуванні необхідної інформованості у мережі, формуванні певної суспільної думки у мережі.

Зовнішній вплив, може призвести до впливу на користувача соціальної мережі, у результаті чого користувач може публікувати інформаційні повідомлення (пости, коментарі, записи) на своїй сторінці, які містять відповідні інформаційні об'єкти (події, персоналії). Публікація інформаційних повідомлень призводить до поступового формування думок та тверджень відносно інформаційних об'єктів (при цьому користувачі формують та змінюють свою думку за тими чи іншими питаннями під впливом інших членів мережі, які мають більш високий авторитет). У подальшому думки та твердження здатні викликати конкретні дії (наприклад, різке зростання попиту на деякий товар, стихійну масову акцію протесту, флешмоби тощо).

Таким чином, процес формування інформаційного простору в соціальних мережах можливо представити сукупністю наступних елементів (рис. 1.):

– *агенти зовнішнього впливу* – це Інтернет-ЗМІ, блоги політиків, відомих людей, які функціонують у інформаційному просторі Інтернет та є суб'єктами управління віртуальними

спільнотами щодо їх інформаційного наповнення, формування ідеології віртуальних спільнот;

– *віртуальні спільноти*, які функціонують у інформаційному просторі соціальних мереж з метою досягнення визначених цілей (деструктивного, конструктивного характеру). Характеризуються наступними інформаційно-психологічними зв'язками:

– одностороннім зв'язком з агентами зовнішнього впливу, як об'єкт ІПсВ;

– одностороннім зв'язком з тіню віртуальної спільноти, як суб'єкт ІПсВ;

– двостороннім зв'язком з іншими віртуальними спільнотами, з метою конкуренції ідеології віртуальних спільнот в інформаційному просторі.

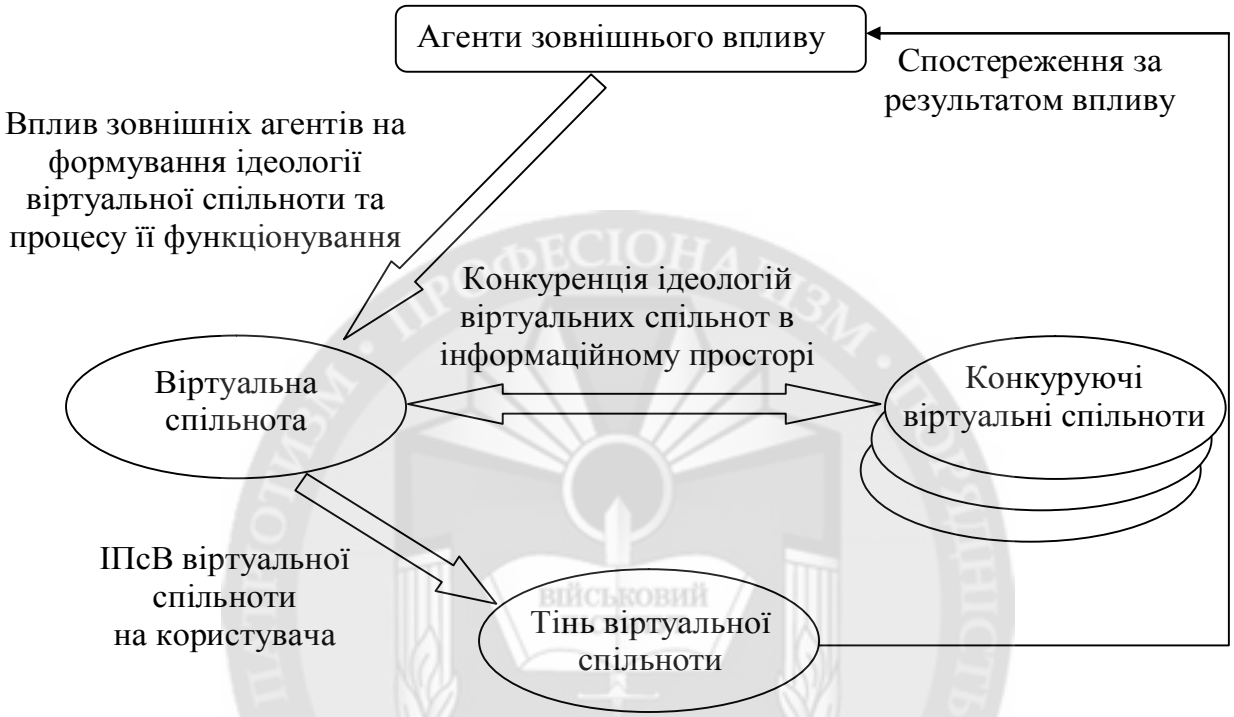

Рис. 1. Формування інформаційного простору в соціальних мережах

Тінь віртуальної спільноти – користувачі соціальних мереж, які не являються елементами віртуальної спільноти (не беруть участі у процесі функціонування віртуальної спільноти).

У такому представлені моделі соціальної мережі можливо визначити наступні типи відносин:

– відносини інформаційної взаємодії (цитування, коментарі);

– відносини знайомств (різного роду контакти у соціальних мережах);

– відношення участі у групах та суспільствах.

Зазначені типи відносин важливі з точки зору розповсюдження інформації та формування думок у соціальних мережах. Усі інші види відносин неявні (наприклад, користувачі неявно пов'язані між собою, якщо вони підписані на однакових користувачів, пишуть на однакові теми), дані види відносин можуть виявлятися за необхідністю при вирішенні конкретних завдань щодо здійснення ІПсВ.

Таким чином, аналіз можливостей використання соціальних мереж для розповсюдження носіїв ІПсВ потребує розгляду особливостей організації інформації у соціальній мережі. Важливим етапом функціонування користувача у соціальній мережі є оформлення профілю користувача. При реєстрації у соціальній мережі користувач повинен надати, відповідно до наданого адміністрацією мережі формуляра, інформацію для ідентифікації. Майже всі системи вимагають введення адреси електронної пошти і перевіряють її працездатність, висилаючи лист з кодом активації облікового запису. Якщо

адреса, то активувати запис може тільки адміністратор системи. Такий підхід гарантує до певного ступеня унікальність учасника [4].

На відміну від персональної сторінки в Інтернеті, яку людина може оформити на власний розсуд та викласти на неї будь-яку інформацію, профілі користувачів в соціальних мережах, як правило, уніфіковані і в більшості соціальних мереж у даний час не допускають значної варіативності оформлення і викладання тієї або іншої інформації. За процесом введення достовірної і реальної інформації, що викладається, а також за її строгою відповідністю відповідним полям профілю даних, постійно стежать адміністратори соціальних мереж. Наприклад, у багатьох соціальних мережах стежать за реальністю імен та прізвищ. Не допускається використання "нікнеймів" замість імен і прізвищ, не допускається створення очевидно надуманих (наприклад, профілів відомих політиків) або фантастичних профілів (наприклад, персонажів фантастичних фільмів, книг або ігор). Крім того, адміністратори мереж стежать за реальністю фотографій, що викладаються, видаляючи профілі користувачів, що викладають яке-небудь стороннє зображення, як свої особисті фотографії. При цьому достовірність інформації, яку повідомляє користувач адміністрації не завжди однозначна (наприклад, є можливість видати себе за іншу особу). Уніфікація профілів соціальної мережі робить її величезною базою даних людей з великою кількістю різної, але суворо структурованою інформацією про них. Це надає змогу будь-якому абоненту соціальної мережі знайти конкретну особу, використовуючи в якості критеріїв пошуку дані профілю. Все це сприяє при плануванні здійснення ІПсВ оцінити обстановку у конкретних віртуальних спільнотах – наявність конкретних осіб, кількість осіб з відповідними характеристиками [10].

Процес передачі інформації в більшості соціальних мережах є обміном повідомленнями перш за все між абонентами, між якими вже встановлені зв'язки якого-небудь роду. Аналізуючи найбільш відомі соціальні мереж можно визначити основні типи зв'язків між абонентами:

– *дружні зв'язки* між знайомими людьми. Знайомі люди додають один одного в друзі, і ця інформація відображається в їх профілі. Таким чином, для будь-якої людини-вузла мережі із загальної маси інших вузлів мережі виділяється група вузлів, з якими він отримує додатковий програмний зв'язок, що дає йому нові можливості, найбільш важлива з яких для здійснення ІПсВ – можливість масової розсилки повідомлень спрямованого змісту та масового запрошення друзів в групу. Окрім списку своїх безпосередніх друзів будь-який користувач також має доступ до списків друзів своїх друзів, таким чином, маючи можливість бачити вузли мережі, не пов'язані з ним безпосередньо, але пов'язані з його друзями. Таким чином, користувач, побачивши цікавого, але незнайомого йому іншого користувача, може легко зрозуміти, через яких саме людей він може з ним зв'язатися;

– *зв'язки між учасниками групи*. У віртуальних соціальних мережах користувачі можуть не тільки спілкуватися один з одним тет-а-тет, але й об'єднуватися в групи з певної тематики. Для групи створюється свій окремий профіль, аналогічний профілю користувача. У разі об'єднання людей в групи повідомлення одного члена групи, розміщене ним у профілі групи, бачать усі члени групи. Таким чином, профіль групи стає деяким аналогом Інтернет-форуму;

– *зв'язки між людьми за певними даними із профілю*. Це призводить до можливості спрямування ІПсВ у соціальній мережі на особу із конкретними характеристиками, які зазначені у її профілі, при цьому ці дані виступають як критерії пошуку.

Особливістю спілкування у соціальній мережі є те, що люди об'єднуються у деякі соціальні групи. Головне глобальне ділення відбувається за проектами, усередині яких цільова аудиторія розбивається на неформальні групи за певними ознаками. Кожен користувач (абонент) соціальної мережі формує свій "віртуальний світ" виходячи з психічних, психологічних та соціальних особливостей, отже набір груп або проектів, до яких долучається у процесі використання соціальної мережі користувач, носить індивідуальний характер. У даному випадку присутній зворотній зв'язок із користувачем. Тобто зазначені

групи, які мають свої особливості можуть піддаватися впливу самого абонента так само, як і впливати на нього (його поведінку, настрої, уподобання тощо) [9].

Слід зазначити, що низький рівень захисту приватних даних користувача соціальної мережі та оприлюднення діалогів під час спілкування призводять до високої уразливості абонента соціальної мережі від прихованого ІПсВ.

Враховуючи вищезазначене можливо стверджувати, що ефективність використання обраної соціальної мережі, як засобу для здійснення спрямованого ІПсВ на користувача також пов'язана із характеристиками (індикаторами) мережі:

– розмір мережі – число прямих зв'язків, включених в індивідуальні об'єднання. Даний показник використовується при вимірюваннях величини суспільств мережі. Розмір мережі встановлюється, як правило, на основі апріорних допущень, проте він повинен визначатися на основі порівняльних постійних зв'язків за певний період часу;

– щільність мережі – загальна кількість зв'язків між одиницями мережі;

– центральність та централізація – ступінь ієрархій мережевих зв'язків, яка обумовлена комунікаційною активністю абонентів мережі, можливостями контролю поведінки і наявністю непрямих зв'язків;

– ранг мережі – довжина загального багатоступінчатого зв'язку (маршруту), в якому один абонент мережі пов'язаний з іншими абонентами. Ранг можна оцінити як через розмір мережі, так і через її щільність;

– ідентифікація – первинні відомості про абонента (анкетні дані);

– репутація – можливість абонента формувати репутацію інших (стіна відгуків, система репутації);

– присутність – відкритий доступ до інформації про наявність абонента у мережі в конкретний момент часу, склад його "віртуального світу" (відношення до груп та спільнот, активність дій в їх рамках та у межах особистого профілю);

– ступінь відносин – відкритий доступ до інформації про прямі контакти абонента (коло спілкування з зазначенням рівнів доступу кожного з прямих контактів, ступінь доступу інших абонентів);

– наявність відкритого доступу до діалогів – можливість відкритого або закритого спілкування як між прямими контактами, так і з будь-яким іншим абонентом або спільнотою;

– ступінь впливу дій абонента на інших користувачів.

Досвід проведення оперативної роботи дослідників в галузі інформаційної безпеки, щодо виявлення деструктивного впливу у соціальних мережах дозволив виявити закономірності, які використовувалися:

– середовищем для здійснення ІПсВ обираються групи у соціальних мережах, де можливо відшукати об'єктивну інформацію, яка спрямована на велику аудиторію із максимальною кількістю користувачів, які ведуть активне обговорення подій. Ці групи вносяться у список, який буде періодично оновлюється; зміст фото та відеоматеріалів, які використовуються для здійснення ІПсВ, стосувалися не тільки втрат протиборчої сторони, але й постраждалих мирних жителів, своїх військ; матеріали, які використовуються мають бути розміщені на легкодоступних ресурсах, що дозволить забезпечити легке розповсюдження серед користувачів мережі; для розміщення матеріалів спрямованого змісту необхідно створити підґрунтя – публікації множини постів, які відображують реальну картину подій; підвищення ступеню сприйняття інформації, що оприлюднюється, здійснюється шляхом використання цитувань відомих людей – лідерів суспільної думки, не обов'язково політиків; коментарі щодо певних тематик висловлюються у різних інтерпретаціях; збільшення кількості аудиторії, яка може важливим є формування посилань на інших користувачів, які висловлюють правильні на ваш погляд думки.

З метою збільшення кількості аудиторія, яку необхідно залучити до інформації ІПсВ, необхідно додати посилання на сторінці користувача та в доступних користувачу співтовариствах, а саме: необхідно постійно наповнювати сторінку певними враженнями, які

виражені невеликими, але цікавими записами; необхідно створювати тематичні групи у соціальних мережах. Запрошувати туди усіх знайомих та зацікавлених користувачів; для збільшення кола зацікавлених користувачів необхідно організовувати розсилку інформації по ICQ або по електронній пошті.

Слід зазначити, що соціальна мережа є не тільки платформою для спілкування, а й комерційним продуктом, отже розробники соціальної мережі намагаються привабити якомога більше користувачів різноманіттям можливостей використання мережі та варіантами організації інформації у ній, створенням альтернативних проектів. При всьому зазначеному, у своєї більшості, представлення інформації на сторінках соціальних мереж залишається уніфікованою. Тому, подальший розгляд питання визначення рівня деструктивного ІПсВ у соціальній мережі пропонується проводити для найпопулярніших за рейтингом соціальних мереж. [5].

Таким чином, для визначення рівня деструктивного ІПсВ пропонується розробити систему показників, які у числовому значенні будуть характеризувати ступінь інформаційної вразливості користувача мережі. Спираючись на особливості організації інформації у соціальній мережі, показники доцільно представити трьома групами:

– перша група – характеризує вразливість за повнотою та достовірністю інформації про персональні дані користувача, які подаються ним особисто під час проходження процедури реєстрації;

– друга група – характеризує вразливість за інформацією у групах, до яких долучений абонент;

– третя група показників враховує кількість прямих контактів абонента та характеризує ступінь вразливості залежно від кількості отриманих повідомлень.

Висновки. Соціальні мережі зі стрімким розвитком інформаційних технологій можуть істотно підвищити ефективність механізмів громадської самоорганізації, сприяючи розвитку "громадянського суспільства". Нові форми комунікації держави та суспільства створюють передумови розвитку інститутів і організацій громадянського суспільства. Крім того, слід відзначити і негативні моменти впливу соціальних мереж на свідомість людини. Охоплюючи значну аудиторію, соціальні мережі перетворюються на інструментарій ведення інформаційних війн та здійснення впливу на громадськість.

Проведений аналіз можливостей здійснення впливу через соціальні мережі продемонстрував доцільність здійснення моніторингу потенційних загроз у таких мережах. Це дозволить забезпечити більш повні дані для оцінювання потенційних загроз для кожної особи, а також врахувати її реакцію на ті чи інші інформаційні приводи. Отже, здійснення оцінки морально психологічного стану особового складу військ (сил) та органів військового управління є важливим завданням військової сфери, вирішення якого, потребує активної участі зі сторони військового керівництва держави.

ЛІТЕРАТУРА:

1. Бойко Г.А. Віртуальність як частина життєдіяльності людини сучасності [Електронний ресурс] / Г.А. Бойко. – Режим доступу: http://intkonf.org/boyko-ga-virtualnist-yak-harakteristika-zhittediyalnostilyudini-21-stolittya. – Назва з екрана.

2. Боровиков В.П. Statistica: искусство анализа данных на компьютере. Для профессионалов. / В. Боровиков // Питер. – Санкт-Петербург. – 2001. – 656 с.

3. Гнатієнко Г.М. Експертні технології прийняття рішень / Г. Гнатієнко, В. Снитюк // Маклаут. – Київ. – 2008. – 444 с.

4. Губанов Д. А. Модели информационного влияния и информационного управления в социальных сетях / Д. А. Губанов, Д. А. Новиков, А. Г. Чхартишвили // Проблемы управления. 2009. – №5. – С. 28-35.

5. Губанов Д. А. Концептуальный подход к анализу онлайновых социальных сетей / Д.А. Губанов, А.Г. Чхартишвили / Управление большими системами. Выпуск №45. М.: ИПУ РАН, 2013. – С. 222-236.

6. Дюбуа П. MySQL. – М.: ИД Вильямс, – 2004. – 1056 с.

7. Жарков Я.М. Інформаційно-психологічне протиборство в сучасному світі: проблемно-історичний аналіз / Я. Жарков, М. Онищук // Вісник Київського національного університету імені Тараса Шевченка. – 2007. – № 16-17. – С. 101-104.

8. Жарков Я.М. Інформаційно-психологічне протиборство в сучасному світі: проблемно-історичний аналіз / Я. Жарков, М. Онищук // Вісник Київського національного університету імені Тараса Шевченка. – 2007. – № 16-17. – С. 101–104.

9. Загрози інформаційної безпеки держави в соціальних мережах / А. М. Пелещишин, Р. В. Гумінський // Наука і техніка Повітряних Сил Збройних Сил України . - 2013. - № 2. - С. 192-199. [Електронний ресурс]. - Режим доступу: http://nbuv.gov.ua/j-pdf/Nitps_2013_2_42.pdf.

10. Киселев Н. Социальные сети как инструмент PR (2008) / Н. Киселев / [Электронный ресурс] – Режим доступа: http://www. pr-club.com/assets/files/pr_lib/pr.../KisSocSeti.doc.

11. Ковалевич Б.В. Соціальні мережі як новий інструмент ведення інформаційних війн у сучасному світі / Б.В. Ковалевич / [Електронний ресурс]. – Режим доступу: file:/// /Grani_2014_4_24.pdf.

12. Сазанов В. М. Социальные сети – публичная сфера. / В. М. Сазанов / Том 1. Основы, анализ и моделирование. – М.: 2012. – 224 с.

13. Стадний інстинкт допомагає маніпулювати масами [Електронний ресурс]. – Режим доступу: http:// ykrnews.com/tainstvenoe/stadnii-nstinkt-dopomaga-man-pulyuvati-masami.html.

14. Петрик В. Соціально-правові основи інформаційної безпеки : навч. посіб. / В. М. Петрик, А. М. Кузьменко, В. В. Остроухов, О. А. Штоквич, В. І. Полевий; Укр. акад. наук. – К. : Росава, 2007. – 496 с. – Бібліогр.: с. 489-495.

15. Почепцов Г. Інформаційна війна як інтелектуальна війна [Електронний ресурс] / Г.Почепцов. – Режим доступу: http://osvita.mediasapiens.ua/material/13303.

16. Перепелиця Г. Інформаційні війни і національна безпека [Електронний ресурс] / Г.М. Перепелиця. – Режим доступу:http://gazeta.zn.ua/POLITICS/informatsionnye_voyny.html.

17. Шумка А.В. Інформаційно-мережева війна – нова форма міждержавного протиборства початку XXI ст. [Електронний ресурс] / А.В. Шумка, П.П. Черник. – Режим доступу: http://www.asv.gov.ua/content/nauka/editions/19/2013-19/243-255.pdf.

Рецензент: к.психол.н. Мась Н.М., Військовий інститут Київського національного університету імені Тараса Шевченка

к.полит.н. Турченко Ю.В.

ИСПОЛЬЗОВАНИЕ СОЦИАЛЬНЫХ СЕТЕЙ В ОСУЩЕСТВЛЕНИИ ДЕСТРУКТИВНОГО ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОГО ВОЗДЕЙСТВИЯ НА ЛИЧНЫЙ СОСТАВ ВОЙСК (СИЛ) И ОРГАНОВ ВОЕННОГО УПРАВЛЕНИЯ

Установлена возможность использования социальных сетей в осуществлении деструктивных информационно-психологических воздействий на личный состав войск (сил) и органы военного управления. Выявлено, что эффективность использования социальных сетей для осуществления информационно-психологического воздействия, в первую очередь связана с возможностью создания в них различных виртуальных сообществ (групп) по определенным интересам. Доказана возможность оказания влияния через социальные сети и целесообразность осуществления мониторинга угроз в таких сетях. Обоснована необходимость разработки и внедрения на вооружение ВСУ современных информационных систем для обеспечения выполнения задач противодействия негативному информационно-психологическому воздействию, как на этапе выявления, так и на этапе нейтрализации его проявлений.

Ключевые слова: социальные сети, мониторинг угроз, информационные процессы (действия), отрицательное информационно-психологическое воздействие, противодействие, военная сфера, информационная безопасность, информация.

Ph.D. Turchenko Yu.V.

USING SOCIAL NETWORKS TO MAKE DESTRUCTIVE INFORMATION AND PSYCHOLOGICAL IMPACT ON TROOPS (FORCES) PERSONNEL AND MILITARY AUTHORITIES

The author has explored the possibility of using social networks to make a destructive information and psychological impact on troops (forces) personnel and military authorities. It was stated that the efficiency of using social networks in making information and psychological impact is primarily related to the ability to create different virtual interest communities (groups). The possibility to influence through social networks and feasibility to provide monitoring of threats in such networks was proved. The necessity to develop and implement modern information systems for the AFU materiel was proved to ensure the fulfillment of tasks of countering the negative information and psychological impact at the stage of detection and neutralization of its manifestations.

Keywords: social networks, monitoring of threats, information processes (actions), negative information and psychological impact, counter, military sector, information security, information.