Загальні питання

УДК 004.738

А.М. Пелещишин [1], Р.В. Гумінський[2]

[1] *Національний університет "Львівська політехніка", Львів*
[2] *Академія сухопутних військ ім. гетьмана. Петра Сагайдачного, Львів*

ЗАГРОЗИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ В СОЦІАЛЬНИХ МЕРЕЖАХ

В статті проведено аналіз особливостей розвитку та характерних рис віртуальних спільнот, як суб'єктів інформаційної безпеки Держави. Розглянуто загрози інформаційної безпеки та інформаційний вплив віртуальних спільнот. Визначені напрямки протидії Держави від інформаційного впливу віртуальних спільнот та запропонована модель моніторингу віртуальних спільнот.

Ключові слова: *віртуальні спільноти, соціальні мережі, інформаційна безпека, система моніторингу, інформаційні загрози.*

Постановка проблеми

На даний час Інтернет все активніше і масштабніше використовується в інтересах інформаційного впливу. Він надає широкі можливості в плані надання впливу на формування громадської думки, прийняття політичних, економічних і військових рішень, впливу на інформаційні ресурси противника і поширення спеціально підготовленої інформації (дезінформації).

Активне використання мережі Інтернет для ведення інформаційного протиборства обумовлено наявністю суттєвих переваг перед звичайними засобами і технологіями:

Оперативність. Розміщення і регулярне оновлення інформації не вимагають значного часу на підготовку матеріалів в електронному вигляді. При цьому користувачі отримують її в режимі реального часу (на відміну, наприклад, від читачів періодичних видань).

Економічність. Є наслідком залучення невеликої кількості персоналу і матеріальних засобів для вирішення поставлених завдань.

Скритність джерела впливу. Як правило, акт агресії в глобальній мережі важко відрізнити від дії звичайних комп'ютерних хуліганів. Підготувати та провести кібератаку з використанням Інтернету може досить широке коло осіб - від військових і розвідувальних структур іноземних держав до партизанських формувань, злочинців, промислових конкурентів, хакерів або просто озлоблених людей. Відстежити ж джерело досить складно.

Дистанційний характер впливу на комп'ютерні системи в різних регіонах світу. В оглядах порушень мережевої безпеки регулярно повідомляється про виявлені наслідки ефективних дистанційних впливів на комп'ютерні мережі різних країн.

Масштабність можливих наслідків. Крім впливу на формування громадської думки, на позиції офіційних осіб, які приймають найважливіші рішення, використання глобальної мережі для деструктивних впливів може призвести до порушення нормальної роботи або тривалого виводу з ладу життєво важливих об'єктів і систем в окремих районах, країнах або регіонах.

Комплексність подачі інформації та її сприйняття. На Інтернет-сторінках розміщується як текстова, так і графічна інформація в найбільш зручному для сприйняття вигляді, а її обсяг може бути в багато разів більше, ніж у будь-якого друкованого видання, радіопередачі або телевізійної програми. Використання ж сучасних мультимедійних технологій, що дозволяють демонструвати документальні свідчення, фото-та відеоматеріали при спеціально підібраному супроводі (коментарі, музика), надає на користувачів додаткове емоційний вплив.

Доступність інформації. Користувачі Інтернету отримують доступ до інформації, наявної на серверах різних країн, минаючи прикордонні, цензурні й інші бар'єри. При цьому будь-який користувач може розмістити власну інформацію (нерідко безкоштовно) на серверах, зареєстрованих в інших державах.

Поширення спеціально підібраної інформації (дезінформації). Воно здійснюється шляхом: розсилки електронних листів e-mail; організації ВС; створення форумів для обміну думками; розміщення інформації на окремих сторінках або в електронних версіях періодичних видань та мережного мовлення (трансляції передач радіо-і телестанцій).

Наряду з перевагами використання Інтернет для інформаційно-психологічного впливу було обумовлено наступними чинниками:

перехід засобів масової інформації (ЗМІ) в Інтернет середовище. Становлення нового типу Інтернет – ЗМІ [17]. Сайти новин охопили близько 90% Інтернету;

створення сервісів соціальних мереж;

розвиток соціальних мереж стало передумовою інтеграції Інтернет – ЗМІ в соціальні мережі, що трансформує їх у соціальні медіа [18]. Виникає феномен соціальної журналістики. Формується нова медіасистема, в якій професійна та соціальна журналістика вступають у взаємодію, а нові інтерактивні канали поширення новин – соціальні мережі дозволяють подолати односторонній, розірваний характер комунікації традиційних медіа, роблять можливим відповідь аудиторії. Розвиток соціальних медіа та дедалі зростаюча роль аудиторії дозволяє говорити про формування нового цифрового публічного простору який надає суспільству можливість контролювати владу, безпосередньо висловлювати свою думку з найважливішим для нього питань за допомогою нових цифрових каналів комунікації, і дозволяє в значній мірі впливати на соціальні та політичні процеси в державі;

зростання рівня довіри до соціальних медіа з боку аудиторії (в середньому у декілька разів більше ніж традиційні ЗМІ) [19];

використання соціальних мереж в політичній діяльності. Основними майданчиками для об'єднання протестуючих стали не юридично зареєстровані організації а їх сайти в Інтернеті;

використання соціальних мереж в організаційних цілях для розповсюдження інформації, як засоби масових комунікацій [20]. Виникає поняття "Твіттерної – революції". Яскравим прикладом є події в країнах Північної Африки, Близького та Середнього сходу, що привело до масових заворушень, відставкам урядів та зміні політичних режимів.

Аналіз останніх конфліктів [4 – 7] засвідчили зростання використання Інтернету до інформаційних війн. Перехід від традиційних засобів впливу листівки, радіо, телебачення до соціальних медіа та інструментів Інтернет простору з метою інформаційного впливу на учасників конфлікту та світової думки (табл. 1).

Таким чином Інтернет простір став новим майданчиком щодо інформаційно-психологічного впливу, що має ряд суттєвих переваг над класичними методами впливу. Засоби інформаційно-психологічного впливу Інтернет простору дозволяють впливати на думку починаючи від особистості окремо до всесвітньої аудиторії.

Таблиця 1

Аналіз використання Інтернет простору в збройних конфліктах

Військовий конфлікт	Використання Інтернет середовища
Перша Чеченська війна (1994 по 1996)	Вперше використовується Інтернет простір. Створений Інтернет сайту «Кавказ».
Війна в Югославії (24.03-10.06.1999)	В Інтернет просторі для підтримки військової операції НАТО було розміщено близько 300 тис. сайтів, які були присвячені косовській проблемі та військовій операції Альянсу.
Війна в Іраку 20.03.03 - 15.12.11	Великомасштабне використання Інтернет – ЗМІ багатьох країн світу для інформаційно-психологічного впливу на світову громадську думку, населення та армію Іраку. Блокування інформаційних каналів, які об'єктивно висвітлювали ситуацію в зоні конфлікту. Виявлення і припинення роботи інформаційних ресурсів мережі Інтернет незалежно від національної приналежність у разі поширення інформації антиамериканської спрямованості. Широкомасштабна адресна психологічна операція проти іракського військового керівництва за допомогою електронної пошти з метою внесення розколу в ряди іракського політичного і військового керівництва.

Аналіз останніх досліджень

Віртуальні спільноти в соціальних мережах сучасні дослідники вивчають переважно або як соціальний феномен нової культури, що формується на засадах використання Інтернету, або з точки зору специфіки психологічних рис учасників таких спільнот, їх інформаційного наповнення, або з огляду на те, яку роль вони можуть відігравати у житті суспільства взагалі [10 – 15].

З погляду інформаційної безпеки держави дослідники визначають загальні риси суб'єктів інформаційної безпеки та надають загальні рекомендації щодо напрямків діяльності Держави, державних установ в інформаційному протиборстві [3,16].

Мета дослідження. Для визначення мети дослідження необхідно уточнити основні терміни та визначення, що будуть застосовуватися.

В даній статті під **соціальною мережею** розуміємо інтернет-сервіс за допомогою якої люди можуть здійснювати зв'язок між собою та об'єднуватися за специфічними інтересами. Завдання такого сервісу полягає у тому, щоб забезпечити користувачів всіма можливим шляхами для взаємодії один з одним.

Предметом дослідження є процес функціонування віртуальних спільнот в інформаційному просторі, як суб'єкта інформаційної безпеки Держави, які використовують сервіси соціальних мереж (форуми, блоги).

Метою дослідження є визначення характерних властивостей ВС, як суб'єктів інформаційної безпеки держави, правила протиборства Держави в інформаційному просторі соціальних мереж та побудови загальної моделі моніторингу та інформаційного протиборства Держави з ВС, як суб'єктами інформаційної безпеки.

Обмеженням дослідження є:

аналіз ВС в процесі їх функціонування в Інтернет просторі, як суб'єкта інформаційної безпеки Держави в аспекті їх інформаційно-психолігічного впливу на інформаційний простір;

під інформацією в даному випадку розуміємо ідеї, мету існування а також ідеології, що служать чинником формування навколо них віртуальних спільнот (відносин).

Основна частина

1. Віртуальні спільноти, як суб'єкти інформаційної безпеки Держави

У сучасному інформаційному суспільстві відбувається зародження і становлення соціальних формацій – віртуальних спільнот (ВС), що володіють принципово іншими (в порівнянні з традиційними формами впливу на соціальні структури в індустріальному суспільстві) можливостями з надання впливу на традиційні громадські та державні структури, поява яких пов'язана з програмами створення оперативного доступу по каналах відкритих телекомунікаційних мереж до розподілених інтелектуальних і матеріальних ресурсів в будь-якій точці земної кулі.

Віртуальні спільноти (англ. virtual communities, e- communities) – новий тип спільнот, які виникають і функціонують в електронному просторі (перш за все за допомогою мережі Інтернет) з метою сприяння вирішенню своїх професійних, політичних задач, задоволення своїх інтересів у мистецтві, дозвіллі, тощо [1].

Термін «віртуальні спільноти» (Virtual Community) запропонував Г.Рейнгольд, який надав йому таке визначення: «Віртуальні спільноти є соціальними об'єднаннями, які виростають з Мережі, коли група людей підтримує відкрите обговорення достатньо довго і людяно, для того, щоб сформувати мережу особистих стосунків в кіберпросторі» [2].

Сучасні ВС дослідники розділяють на декілька основних категорій [3]:

- співтовариства інтересів, які збирають людей з однаковими інтересами (такими, як політичні, соціальні, культурні, економічні тощо) або є спеціалізованими (співтовариства молодих батьків, клуби любителів певних марок автівок тощо);

- ігрові співтовариства, які дають своїм користувачам можливості створювати власне середовище, історії і персонажі в придуманих світах;

- географічні співтовариства, засновані на географічному розташуванні або місцевості (часто такі співтовариства об'єднуються за допомогою локальних мереж);

- співтовариства взаємин, які сформовані навколо певного життєвого досвіду, де люди можуть ділитися своїм досвідом і обмінюватися думками;

- комерційні співтовариства, де стосунки побудовані на купівлі та продажі онлайнових товарів і послуг;

- віртуальні держави.

По відношенню до оточуючого суспільства та Держави виділяють наступні типи ВС [24]:

Індиферентні – налаштовані до суспільства за принципом: «ми вас не чіпаємо і ви нас не чіпайте».

Ізоляціоністські – в якійсь мірі є різновидами індиферентних ВС. Це структури типу закритих клубів за інтересами. Вони намагаються повністю відокремитись від взаємодії з суспільством або обходитися мінімумом контактів.

Конструктивні – навпаки, прагнуть активно взаємодіяти з суспільством, маючи на меті поліпшення життя як суспільства в цілому, так і окремих соціальних груп та індивідів.

Деструктивні ВС, як і конструктивні, також не ізолюються від суспільства, але, на відміну від останніх, намагаються з цим співтовариством боротися усілякими, не завжди законними, методами. Об'єктом агресії деструктивних ВС є суспільство в цілому або прихильники тих чи інших соціальних груп, як правило, вороже налаштованих до цієї самої деструктивної ВС.

Соціально-мобілізаційна активність деструктивного характеру, а також акції протесту, що організовуються із застосуванням інструментарію соціальних мереж (рухи, демонстрації, флеш-моби, перекриття трас тощо) стають повсякденними у житті сучасного суспільства.

Таким чином ВС в інформаційному просторі є принципово новою стійкою формою існування соціальних відносин, які перевершують соціальні соціуми за ступенем організованості та впливу.

Аналізуючи процес функціонування ВС дослідники визначають, що ВС володіють загальними признаки суб'єктів інформаційного протистояння, а саме [8, 9]:

- наявність у суб'єкта в інформаційно-психологічному просторі власних інтересів;

- наявність у складі суб'єкта спеціальних сил (структур), функціонально призначених для ведення інформаційного протиборства або уповноважених на ведення інформаційного протиборства;

- володіння та/або розробка інформаційної зброї, засобів її доставки і маскування;

- під контролем суб'єкта знаходиться сегмент інформаційного простору, в межах якого він володіє переважним правом встановлювати норми регулювання інформаційно-психологічних відносин (на

правах власності, закріплених нормами національного та міжнародного законодавства) або державним суверенітетом (національний сегмент інформаційного простору як частина державної території);

- існування в офіційній ідеології положень, що допускають участь суб'єкта в інформаційному протиборстві.

Визначимо характерні риси ВС, як суб'єктів інформаційної безпеки держави:

- за метою створення:

- створюються з метою досягнення визначених цілей на території вибраної держави або групи держав із елементів їх соціальних структур;

- за структурою:

- включають в свою структуру, об'єднають матеріальні та інтелектуальні ресурси інших соціальних систем;

- мають ознаки децентралізованої ієрархії (принцип багатокерівництва), часткові лідери, кожний з яких має спеціалізовану роль і функцію;

- найбільші, глобальні за масштабами своєї діяльності та впливу на суспільні процеси мають ознаки суверенної держави - суверенітет; екстериторіальність; наявність власних силових структур; участь в міжнародних організаціях, що зближує їх стратегічні інтереси з національними інтересами традиційних держав, залучаючи до геополітичної конкуренції за сферами впливу;

- за проникаючою та заповнюючою здатністю:

- миттєво отримувати з структур соціального суспільства і концентрувати розподілені інтелектуальні та матеріальні ресурси в будь-якій точці інформаційного простору;

- висока здатність заповнювати нестачу сил і засобів і втрати в інтелектуальних і матеріальних ресурсах, черпаючи їх прямо з соціальних структур (держав з розвиненою інформаційно-телекомунікаційною інфраструктурою), які не беруть участь в конфлікті на стороні даної віртуальної спільноти;

- мають проникаючу здатність в будь-які соціальні структури і, в разі залучення в інформаційний конфлікт (інформаційно-психологічну війну), здатні завдати своєму противнику удар зсередини, використовуючи його комунікаційні мережі та соціальні структури держави;

- за здатністю реорганізації:

- при розпаді (наприклад, в результаті досягнення поставлених цілей або зміни пріоритетів) вона припиняє своє існування в якості самостійного суб'єкта міжнародної діяльності (або геополітичної конкуренції), а її структурні елементи повертаються на своє колишнє місце в ті соціальні системи, з яких вони були вилучені;

- здатні в найкоротші терміни повністю змінити свій вид, форму існування в інформаційно-психологічному просторі, свою структуру і методи діяльності, змінити внутрішню ієрархію і систему взаємодії та взаємовідносин окремих елементів усередині спільноти і в результаті цих змін взагалі стати іншим суб'єктом діяльності;

- володіють здатністю тимчасово припиняти своє існування, розчинятися в просторі соціальних систем;

- за вразливістю:

- головною вразливістю віртуальних спільнот є ідеологія, що об'єднує розрізнені елементи в єдиний організм (систему) і створює мотивацію участі кожного з цих елементів у спільній діяльності з метою досягнення цілей під загальним централізованим віртуальним керуючим впливом.

Зважаючи на можливості і притаманні властивості ВС крім виконання функцій підтримки спілкування, обміну думками, отримання інформації їх членами, організації і ведення бізнесу останнім часом все частіше стають об'єктами і засобами зовнішнього інформаційно-психологічного управління і ареною інформаційного протиборства на різних рівнях. Вони стали ідеальним інструментом впливу на національні інтереси держави в інформаційному просторі.

2. Інформаційні загрози національної безпеки держави в процесі функціонування віртуальних спільнот, як суб'єкта інформаційної безпеки

Згідно до законодавства України поняття "інформаційна безпека" має таке визначення:

"*стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації.*" [21].

На сучасному етапі основними реальними та потенційними загрозами інформаційній безпеці України визначені в Доктрині інформаційної безпеки України [22]. При розгляді ВС, як суб'єктів інформаційної безпеки Держави доцільно розглядати наступні інформаційні загрози:

- у зовнішньополітичній сфері:

- поширення у світовому інформаційному просторі викривленої, недостовірної та упередженої інформації, що завдає шкоди національним інтересам України;

- зовнішні негативні інформаційні впливи на суспільну свідомість;

- у сфері державної безпеки:

- негативні інформаційні впливи, спрямовані на підрив конституційного ладу, суверенітету, територіальної цілісності і недоторканності кордонів України;

- пропаганда сепаратизму за етнічною, мовною, релігійною та іншими ознаками.

Відповідно до інформаційних загроз серед найбільш серйозних за своїми наслідками задач, які можуть бути вирішенні за допомогою інформаційного-психологічного впливу ВС, дослідники виділяють наступні [25]:

створення атмосфери бездуховності та аморальності, негативного відношення до культурної спадщини;

маніпулювання суспільною свідомістю і політичною орієнтацією соціальних груп населення країни з метою створення політичної напруженості та хаосу;

дестабілізація політичних відносин між партіями, об'єднаннями і рухами з метою провокації конфліктів, розпалення недовіри, підозрілості, загострення політичної боротьби, провокування репресій проти опозиції, провокація взаємознищення;

зниження рівня інформаційного забезпечення органів влади та управління, інспірація помилкових управлінських рішень;

дезінформація населення про роботу державних органів, підрив їхнього авторитету, дискредитація органів управління;

провокування соціальних, політичних, національних та релігійних зіткнень;ініціювання страйків, масових заворушень та інших акцій економічного протесту; утруднення прийняття органами управління важливих рішень;

підрив міжнародного авторитету держави, його співробітництва з іншими країнами; нанесення шкоди життєво важливим інтересам держави в політичній, економічній, оборонній та інших сферах.

3. Інформаційний вплив віртуальних спільнот на національні інтереси Держави

Виділяють наступні етапи формування та інформаційного впливу ВС [26]:

перший етап - створення активного незадоволеного даними політичним режимом соціального сегмента;

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

третій етап - блокування соціальних груп, які не розділяють ідеологію даного соціального сегменту.

При цьому повинні вирішуватися наступні задачі:

- розбудити (підняти) активність масової свідомості;
- утримати активність (агресивність) на певному рівні, не виходячи за його межі;
- озброїти своїх прихильників аргументацією для бесід з їхніми супротивниками.

Методи для вирішення цих задач не відрізняється від класичних методів інформаційного впливу і починається з атаки на масову свідомість використовуючи класичні методи інформаційних війн:

- за цілями:

1) методи пропаганди.
2) 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 націлені на дискредитацію ворожих ідей, руйнування шкідливих інформаційних сутностей і недопущення їх виникнення в подальшому.

- за характером дії.

1) явні методи.
2) неявні (приховані) методи.

Явні методи відрізняються від неявних тим, що в них мета і характер впливу не ховаються від супротивника. Наприклад, агітація - це приклад явної пропаганди, а інформаційний вірус - прихованою.

Вже зараз потенціал ВС є достатнім, аби з їх допомогою влаштувати повномасштабний соціальний катаклізм, загальнонаціональну акцію, організувати громадський або політичний рух тощо. Згадуючи події 2012 року в Україні, що пов’язані із закриттям файлообменніку EX.UA можна стверджувати, що це був виклик національній безпеці.

Також необхідно зазначити на суттєвий вплив ВС на політику. Соціальні мережі полегшують можливість об’єднання осіб, що ставлять перед собою захоплення влади, у тому числі і незаконного. Інтернет простір може використовуватися як місце спілкування, розробки і обговорення злочинних планів. Таке спілкування набагато безпечніше «фізичних» зустрічей в оффлайні. Крім того ВС можуть непомітно підривати деякі державні основи шляхом створення так званих «віртуальних держав», що мають майже усі атрибути держави за винятком території. Яскравим прикладом є революції в Тунісі, Лівії, Єгипті, Ємену, які призвели до усунення глав цих держав.

Але, коли ми кажемо про ВС як виклик національній безпеці не треба забувати, що існує «подвійна» роль віртуальних спільнот яка виявляється у тому, що вони водночас прискорюють та гальмують потенційне настання «революційної ситуації». Віртуальні спільноти можуть діяти як колективний симулятор протестного руху. Вони дуже часто створюють ілюзію опозиційної політичної активності, поглинаючи енергію, яка інакше могла б вилитися у «фізичні» протести на вулицях.

4. Правила протидії Держави від інформаційного впливу віртуальних спільнот

Досвід інформаційного впливу ВС переконливо свідчить про необхідність посиленої уваги з боку держави до діяльності та розвитку «соціальних мереж». Водночас, така увага не повинна порушувати права людини, зафіксовані у законодавстві.

Можна виділити такі напрямки щодо протидії інформаційного впливу ВС:

- силові методи – закриття серверів;
- юридично-правові методи – притягнення до кримінальної відповідальності учасників ВС;

- Інтернет – цензура;
- моніторинг ВС та протидія методами інформаційного впливу.

Перші два методи є більш ефективними в короткостроковій перспективі. Але їх недоліками щодо недопущення правопорушень в інформаційній сфері зумовлена багатьма об'єктивними причинами, які витікають з характерних властивостей ВС, як суб'єктів інформаційної безпеки, серед яких насамперед доцільно виділити:

1) відсутність географічних кордонів та обмежень для миттєвого поширення, збирання, обробки та використання інформації, внаслідок чого Інтернет з його глобальними комунікаціями залишається поза сферою правового регулювання законів будь-якої держави, яка завжди має певну обмежену територію, на яку поширюється її суверенітет (поняття юрисдикції або дії нормативно-правового акта у просторі);

2) анонімність, яка підриває традиційне застосування юридичної відповідальності за скоєне правопорушення або злочин в інформаційній сфері, що забезпечує високий рівень латентності та низький рівень розкриття правопорушень;

3) легкодоступна змінюваність інформації в електронній формі: на відміну від стабільної документально оформленої інформації електронна інформація не має форми, сталої у часі та просторі.

Основною особливістю і головною небезпекою деструктивних ВС пов'язана з тим, що визнати за законом їх діяльність як деструктивну в умовах дії норм свободи слова, друку, віросповідання можливо тільки після реалізації в реальному світі їх учасниками якихось заходів, здійснених під дією інформаційного впливу. Тільки тоді дії події можуть бути співвіднесені з нормами чинного законодавства та кваліфіковані відповідним чином.

Ще одно із проблемних питань щодо неефективності використання силових методів є те, що українські соціальні мережі дуже сильно інтегровані в російській або мировий Інтернет (з 10 найбільш відвідуваних сайтів в Україні – два українських).

Інтернет цензура в Україні – згідно чинного законодавства цензурі в Інтернет просторі підлягає інформація, яка в собі містить елементи дитячої порнографії. Законодавчої бази щодо цензури в інших питаннях (інформаційної безпеки Держави, суспільства) не має.

Метод моніторингу віртуальних спільнот є більш ефективним в довгостроковій перспективі щодо інформаційної протидії ВС, але потребує залучення фахівців різних галузей науки. Виходячи з характерних рис ВС (здатності реорганізації) основною задачею моніторингу ВС є не знищення ВС, які представляють загрозу для інформаційної безпеки Держави, а управління та контроль діяльністю ВС методами інформаційного впливу.

5. Основні завдання системи моніторингу віртуальних спільнот

Для визначення основних задач системи моніторингу ВС необхідно провести аналіз інформаційно-психологічного впливу ВС, як об'єкта та суб'єкту інформаційної безпеки.

На рис. 1 відображено формування інформаційного простору в соціальних мережах.

Рис. 1. Формування інформаційного простору в соціальних мережах

Формування інформаційного простору в соціальних мережах включає в себе наступні елементи:

1. Агенти зовнішнього впливу (Інтернет – ЗМІ, блоги політиків, відомих людей), які функціонують і інформаційному просторі Інтернет середовища та є суб'єктами управління ВС щодо їх інформаційного наповнення та формування ідеології ВС. Агенти зовнішнього впливу будуть характеризуватися одностороннім зв'язком інформаційно-психологічного впливу на ВС.

2. ВС, які функціонують в інформаційному просторі соціальних з метою досягнення визначених цілей (деструктивного, конструктивного характеру). Будуть характеризуватися наступними інформаційно-психологічними зв'язками:

– одностороннім зв'язком з Агентами зовнішнього впливу, як об'єкт інформаційно-психологічного впливу;

– одностороннім зв'язком з тіню віртуальної спільноти, як суб'єкт інформаційно-психологічного впливу;

– двостороннім зв'язком з іншими ВС, з метою конкуренції ідеологій ВС в інформаційному просторі.

Тінь віртуальної спільноти - користувачі соціальних мереж, які не являються елементами віртуальної спільноти (не приймають участь в процесі функціонування ВС) але зацікавлені ідеологією ВС. Відповідно за проникаючою та заповнюючою здатністю ВС тінь віртуальної спільноти може стати мобілізаційним ресурсом ВС.

Таким чином основними завданнями системи моніторингу є:

1. Виявлення деструктивних ВС діяльність яких несе інформаційну загрозу національній безпеці Держави.

2. Аналіз виявленої деструктивної ВС, її зв'язків з іншими ВС (деструктивними, конструктивними) та вплив зовнішніх факторів.

3. Створення ВС яка включає в свою структуру елементи ВС, яка несе інформаційну загрозу національній безпеці Держави та ВС зв'язаних з нею.

4. Застосування методів інформаційного впливу (створеною ВС та зовнішніх факторів) з метою управління та контролю діяльності ВС, яка несе інформаційну загрозу національній безпеці Держави.

Для вирішення задач система моніторингу повинна включати наступні підсистеми:

- підсистема моніторингу ВС призначена для моніторингу інформаційних ресурсів, згідно заданої тематики інформаційного потоку та надання статистичної інформації;

- підсистема аналізу та прогнозування призначена для аналізу ВС, її інформаційного наповнення, етапів розвитку та її зв'язків (агенти зовнішнього впливу, конкуруючих віртуальних спільнот, тінь віртуальних спільнот) та прогнозування функціонування ВС в залежності від інформаційного впливу;

- підсистема прийняття рішення та управління призначена щодо визначення інформаційних загроз; розробка пропозицій щодо інформаційного впливу; на підставі результатів прогнозування. В підсистему прийняття рішень можуть входити елементи систем прийняття рішень.

Висновки

Українське суспільство уже сьогодні достатньо глибоко інтегроване у міжнародні мережні віртуальні спільноти й вітчизняна аудиторія соціальних мереж збільшується рекордними темпами. Це зумовлює необхідність проаналізувати і оцінити динаміку, напрямки й тенденції даних процесів в Україні в контексті глобального розвитку соціальних мереж, дослідити глобальні громадсько-політичні рухи у соціальних мережах та їх вплив на політичні процеси сучасності.

Перед українською владою з розвитком соціальних мереж у контексті викликів національній безпеці постають наступні проблеми:

поява та структурізація віртуальних спільнот у вітчизняних соціальних мережах;

пошук та вироблення адекватних відгуків на кинутий виклик;

обмеженість механізмів державного регулювання даного соціального феномену, яка виявляється у спробах силової або адміністративної боротьби з новими викликами з боку органів державної влади.

Найбільш ефективним механізмів державного регулювання є моніторинг віртуальних спільнот (соціальних мереж) що ставить ряд наукових та організаційних задач перед Державою, а саме: створення відповідних структур щодо моніторингу Інтернет середовища з залученням фахівців різних галузей наук, удосконалення та розробка науково-методичного апарату щодо аналізу, прогнозування розвитку та діяльності віртуальних спільнот.

Метою подальших наукових досліджень є аналіз та удосконалення методів інформаційного впливу з метою контролю та управління діяльності ВС з урахуванням їх особливостей.

Список літератури

1. Вікепедія: [Електронний ресурс]. – Режим доступу: http://uk.wikipedia.org.

2. Кремлева С.О. Сетевые сообщества / С.О. Кремлева [Електронний ресурс] – Режим доступу: http://www.follow.ru/print.php?id=116&page=1.

3. Дзюндзюк В. Б. Віртуальні співтовариства: потенційна загроза для національної безпеки // Державне будівництво [Електронне видання]. – 2011. – № 1. – Режим доступу до журн. : http:// www.kbuapa.kharkov.ua.

4. Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве. М.: МОРФ, 2011,14 с.

5. Ефремов В.В. Особенности организации и ведения информационной войны в период первой и второй чеченской кампаний / В.В. Ефремов, А.Г. Караяни, А.Н. Размазнин, В.А. Целыковский. [Електронний ресурс]. – Режим доступу: http://www.scef.ru/index.php/ru/compjnent/csef/project/842-features-of-the-organization-and-information-warfare-between-the-first-and-second-chechen-campaigns.htm.

6. Гриняев С.Н. Особенности информационной войны во время агрессии НАТО против Югославии [Електронний ресурс] – Режим доступу: http://nvo.ng.ru/spforces/2000-11-10/7_war.html.

7. Гриняев С.Н. Информационная война в ходеагрессии США, Великобритании и их союзников против Ирака/ С.Н. Гриняев, Аналитический доклад – М.: Центр стратегических оценок и прогнозов, 2010. – 118 с.

8. Манойло А.В. Государственная информационная политика в особых условиях, монография. — М.: Изд. МИФИ, 2003, 388 с., ил.

9. Манойло А.В., Петренко А.И., Фролов Д.Б. Государственная информационная политика в условиях информационно-психологической войны, монография. — М.: Горячая линия — Телеком, 2003, 541 с., ил.

10. Белинская Е. П. К проблеме групповой динамики сетевого сообщества. 2-ая Российская конференция по экологической психологии. Тезисы. Москва, 12 – 14 апреля 2000 г. М.: Экопсицентр РОСС. - С. 249 – 251.

11. Войскунский А. Е. (1997) Групповая игровая деятельность в Интернете // Психологический журнал, т. 20. С. 126 – 132.

12. Иванов Д. В. Виртуализация общества // Социология и социальная антропология. СПб: Изд. „Петербургское Востоковедение", 2000. 96 с.

13. Кастельс М. Становление общества сетевых структур // Новая постиндустриальная волна на Западе. Антология. Под ред. В.Л. Иноземцева, 1999. – С. 494 – 505.

14. Круглов А. Ю. Компьютеро-опосредованное общение как социальное явление / Автореферат диссертации на соискание ученой степени кандидата социологических наук, Санкт-Петербург, 2000.

15. Нестерова Е. И., Нестеров В. Ю. Некоторые аспекты коммуникационных процессов в Сети с точки зрения культурологии // 5-я Международная научно-практическая конференция Информационные системы и технологии „Виртуальный мир Инфосферы: практическое использование человеком". Владивосток, 1998.

16. Горбулін В.П., Додонов О.Г., Ланде Д.В. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання, монографія. – К.: Інтертехнологія, 2009. – 163 с.

17. Муратова Н.Ф. Интернет-сми как отдельный вид в системе средств массовой информации: лексическое и этимологическое обозначения понятия// Филологические науки. Вопросы теории и практики, № 2 (6). – С. 118-120.

18. Панченко Е. Интеграция Интернет - СМИ и социальных сетей в Рунете: Новая публичная сфера или пространство контроля? // Digital Icons: Studies in Russian, Eurasian and Central European New Media – 2011. – №5. – С. 87-118.

19. Лосева Н. Социальные сети и СМИ: как жить дальше? Круглый стол «Будущее журналистики: количество против качества». Тезисы. Москва 10 мая 2011, Связь-Экспокомм-2011. [Електронний ресурс] – Режим доступу: http://vid-1.rian.ru/ig/fmf/Social_media_2011.pdf

20. Подцероб А.Б. Арабская смута: роль пропаганды и современных информационных технологий // Институт ближнего востока [Електронне видання]. – 2012. – Режим доступу до журн.: http://www.iimes.ru/?p=15619

21. Конституція України.: прийнята на п'ятій сесії Верхов. Ради України 28 черв. 1996 р. – К. : Велес.

22. Доктрина інформаційної безпеки України : затверджена Указом Президента України № 514/2009 від 8 липня 2009 року [Електронний ресурс]. – Режим доступу : http://www.president.gov.ua/documents/9570.html.

23. Сазонов В.М. Социальные сети – публичная сфера, монография. – М.: Изд. Лаборатория СВМ, 2011. – 223 с.

24. Матвиенко Ю.А. Деструктивные сетевые социальные структуры как средство информационной войны и угроза безопасности России// Информационно-аналитеческий портал Геополитика [Електронне видання]. – 2011. – Режим доступу до журн.: http://old.geopolitica.ru/Articles/1218/

25. Гриняев С.Н. Проблемы внутренней безопасности России в XXI веке / С.Н.Гриняев. [Електронний ресурс]. – Режим доступу: http://www.agentura.ru/equipment/psih/info/inter.

26. Почепцов Г. Контроль над разумом / Георгій Почепцов – К: ВД Києво-Могилянська академія. 2012. – 350 с.

Надійшла до редколегії 12.03.2013

Рецензент: д-р техн. наук с.н.с. М.Ю. Яковлєв, Академія сухопутних військ ім. гетьмана. Петра Сагайдачного, Львів.

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА В СОЦИАЛЬНЫХ СЕТЯХ

А.Н. Пелещишин, Р.В. Гуминский

В статье проведен анализ особенностей развития и характерных черт виртуальных сообществ, как субъектов информационной безопасности государства. Рассмотрены угрозы информационной безопасности и информационное воздействие виртуальных сообществ. Определены направления противодействия государства от информационного воздействия виртуальных сообществ и предложена модель мониторинга виртуальных сообществ.

Ключевые слова: *виртуальные сообщества, социальные сети, информационная безопасность, система мониторинга, информационные угрозы.*

THREATS TO THE INFORMATION SECURITY OF THE STATE IN SOCIAL NETWORKS

A.M. Peleschyshyn, R.V. Huminskiy

The article provides analysis of development peculiarities and characteristic features of virtual communities as entity of State informational security. Threats to international security and informational effect of virtual communities have been investigated. State counteractions against virtual communities' effect have been defined and model of virtual communities monitoring has been offered.

Keywords: *virtual communities, social networks, informational security, monitoring system, information threats.*