УДК 355.40;355.34

**Ю. М. Супрунов**

# НАПРЯМИ ТА ОКРЕМІ ПРОБЛЕМИ ВИКОРИСТАННЯ СОЦІАЛЬНИХ СЕРВІСІВ ІНТЕРНЕТУ В КОНТЕКСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

*Розглядаються напрями та окремі проблеми поширення і розвитку блогосфери Інтернету в контексті її значення як глобального інформаційного середовища для моніторингу і виявлення інформаційно-психологічного впливу (ІПсВ), каналу ефективного диференційованого ІПсВ на визначені об'єкти соціотехнічного середовища. Аналіз проводиться на основі відкритих джерел на прикладі деяких провідних країн світу (у першу чергу США), в яких сформовано основні нормативні та організаційні засади використання кіберпростору як нового бойового середовища.*

**Постановка проблеми.** Розвиток інформаційного суспільства як інформаційної складової глобалізації перш за все визначає прискорений розвиток і впровадження інформаційних технологій (ІТ). До певної міри прихованим чинником форсованого розвитку ІТ є необхідність тотального моніторингу і контролю всіх видів ресурсів (матеріальних, інформаційних, демографічних тощо), оперативної обробки отриманої інформації, диференційованого ІПсВ на суспільство для вирішення завдань контролю й управління (обробка суспільної думки, керування формуванням змін менталітету, індивідуальної та суспільної свідомості тощо). Без досягнення критично необхідного рівня впровадження цифрових технологій спостереження виконання цих завдань не можливе.

Під технологіями спостереження розуміємо цифрові ІТ, які можна використовувати для виявлення, збору, накопичення, обробки, архівації та обміну інформацією про особистість, певні соціальні групи і суспільство в цілому, державні (корпоративні) структури й ресурси з можливістю їх подальшого оперативного використання. Оскільки практично всі технології спостереження є окремими сервісами чи інтегровані з глобальною мережею (ГМ) Інтернету, то і ГМ у цілому можна вважати комплексною глобальною технологією спостереження. Це суттєво впливає на темпи і напрямки розвитку ГМ. Основний обсяг інтернет-трафіка припадає на соціальні сервіси Інтернету (ССІ), тому дослідження заходів нормативного, організаційного, технологічного та кадрового забезпечення використання ССІ в інтересах забезпечення інформаційної безпеки особистості, суспільства і держави є вкрай актуальним.

**Огляд останніх досліджень.** Визначені проблеми в Україні та російськомовних джерелах розглядаються переважно на рівні інформаційних повідомлень з першоджерел, термінологічного визначення та врахування в нормативних документах [1, 6, 7, 9, 12 – 20, 22] і до деякої міри на рівні системного аналізу наслідків упровадження систем кібернетичного нападу [2, 5, 8, 11, 21]. На даний час узагальнений аналіз проблем розвитку та можливого використання ССІ в інтересах забезпечення інформаційної безпеки особистості, суспільства і держави практично не проводився.

**Завдання дослідження** полягає у визначенні та аналізі напрямів і деяких проблем розвитку та можливого використання ССІ в інтересах забезпечення інформаційної безпеки особистості, суспільства і держави. До них можна віднести такі:

проблеми поширення і розвитку блогосфери Інтернету в контексті її значення як глобального інформаційного середовища для моніторингу і виявлення ІПсВ, каналу ефективного диференційованого ІПсВ на визначені об'єкти соціотехнічного середовища;

проблеми дослідження національних сегментів блогосфери для виявлення її ролі та соціальних медіа, створення "портретів" і карт блогосфери для дослідження через мережні структури ролі соціальних, культурних і політичних сил у визначеній країні з метою їх можливого використання для цілей ІПсВ;

проблеми спотворення інформаційної картини соціуму, природного сприйняття інформації, інформаційного дисонансу, який виникає між спільнотою активних блогерів і користувачів інформаційних ресурсів блогосфери та рештою населення, яке користується традиційними інформаційними ресурсами, що може визначати вразливості країни від зовнішнього ІПсВ;

проблеми підготовки фахівців для здійснення консолідуючої діяльності (ІПсВ) у блогосфері, у тому числі із залученням додаткового соціального ресурсу (на основі аналізу заходів у провідних країнах світу).

**Виклад основного матеріалу.** За даними Internet World Stats на червень 2012 року в ГМ було більше 2,4 млрд користувачів. Їх кількість подвоїлась з 2007 року (1,1 млрд), тільки Азія забезпечила 53% зростання. За оцінками, до 2015 року кількість мережних пристроїв може перевищити 15 млрд, що в два рази більше населення нашої планети, а обсяг інтернет-трафіка до 2015 року зросте в 4 рази і досягне 966 ексабайтів на рік.

Значний обсяг інтернет-трафіка припадає на ССІ, під якими розуміють віртуальні майданчики, які зв'язують людей у мережні спільноти за допомогою програмного забезпечення, комп'ютерів, об'єднаних у ГМ і мережі документів. Відповідно мережна спільнота – це група людей, яка підтримує спілкування і здійснює спільну діяльність за допомогою комп'ютерних мережних засобів. Завдячуючи мережним зв'язкам, довільно чи шляхом направленого впливу формуються нові соціальні об'єднання. Саме за рахунок розвитку ССІ динаміка чисельності сайтів у ГМ набула експоненціального характеру і за оцінками моніторингової компанії Netcraft на травень 2012 року становила 678 млн сайтів і блогів. Їх частка, що належить до ССІ, отримала загальне визначення як блогосфера Інтернету.

На даний час ССІ надають користувачам інтегровані інформаційні можливості друкованих засобів масової інформації (ЗМІ), радіо і телебачення, рекламних агенцій, довірчого корпоративного, професійного, дружнього та сімейного спілкування, певного самоствердження. Динамічною тенденцією стає використання ССІ для реалізації соціальної (політичної) активності соціуму. Такі вражаючі можливості і перспективи використання ССІ не могли залишитись поза увагою військово-політичного керівництва і фахівців інформаційно-психологічного протиборства (ІПсП) провідних країн, а також більшості екстремістських і терористичних структур.

Бурхливий розвиток ССІ на даний час характеризується принципово якісними перетвореннями, серед яких виділяються:

інтеграція ССІ, їх баз даних, у першу чергу, на основі технічних можливостей найбільших ССІ та пошукових систем, об'єднання мереж на міжлінгвістичному рівні (створення "всесвітнього соціального простору" – Бред Фітцпатрік, автор програми "Social graf");

активне заохочення користувачів до розміщення на індивідуальних сторінках (блогах) різнопланової інформації з поступовим переходом до примусових сервісів, спонукання розміщувати особисту інформацію з можливістю її неконтрольованого накопичення;

поєднання різнотипних ССІ, пошукових, платіжних та інших систем для утворення універсальних інтернет-сервісів, умовами використання яких є певне декларування особистої (корпоративної) інформації та згода з "політикою конфіденційності" ССІ;

заохочення в рамках державної політики формування інформаційного суспільства до участі в ССІ державних службовців, активізація взаємодії ССІ з рекламними компаніями, а також зі спеціальними службами, що визначає їх відповідну трансформацію;

використання ССІ для ІПсВ на суспільство з боку спеціальних структур (у т. ч. створення псевдоприватних блогів та їх супроводження численними фахівцями різних новостворених кіберкомандувань тощо).

ССІ стали потужним конкурентом офіційним ЗМІ й ареною боротьби за громадську думку, ідеальним середовищем для інтернет-розвідки з боку різних структур і приватних осіб. Так, можливість створювати віртуальні співтовариства у військовій сфері (вказувати військові частини й установи в структурі даних сайту "Одноклассники.ру") надала можливість викрити базування військових частин і установ збройних сил (ЗС) колишнього СРСР, країн СНД з їх географічною і часовою локалізацією, а також поширити іншу інформацію про них. Аналогічна ситуація має місце і в іншомовних ССІ. Проводиться моніторинг користувачів ССІ – військовослужбовців ЗС США, Великобританії, інших країн, що беруть участь в операціях в Іраку та Афганістані. З березня 2010 року було зірвано військову операцію армії Ізраїлю на Західному березі річки Йордан після розміщення військовослужбовцем ЦАХАЛа інформації в соціальній мережі (СМ) Facebook про його участь у рейді на палестинських територіях. Спроби обмеження доступу до Інтернету зі службових комп'ютерів були компенсовані новими можливостями доступу з мобільних пристроїв. Це визначає цінність таких ресурсів, як джерела розвідки, і відповідно суттєву інформаційну загрозу державним (корпоративним) інтересам.

Загальний обсяг інформації тільки на серверах "Одноклассники.ру" (без відеоконтенту) становить один петабайт — це кілька сотень тисяч DVD-дисків. Користувачі "ВКонтакте" щоденно відправляють 730 млн особистих повідомлень, створюють 80 млн публічних записів, завантажують 40 млн фотографій і відеозаписів. Зі СМ можна дізнатись багато детальної інформації про людину, а шляхом її узагальнення (інтегрування інформації з різних СМ) – важливу соціологічну інформацію, яку можна використовувати для диференційованого впливу на соціум.

Важливим чинником для використання блогосфери з метою спотворення інформаційної картини світу є те, що пошукові системи використовують СМ для так званого "соціального елемента ранжування". При цьому для прискорення індексації сайту (просування інформації) має місце певна диференціація ССІ відповідно до пошукових систем, наприклад: на Yandex – twitter, на Google.com – facebook і Google+.

Фактично ССІ вже є ареною інформаційного протиборства, що визначає проблеми інформаційної безпеки як особистості, суспільства, так і держави. Це визначає й адекватні заходи зі створення спеціальних структур для інформаційної боротьби в кіберпросторі. Однією з ознак можливого переносу інформаційного протиборства до ССІ є емоційна реакція федеральних та спеціальних структур США на оприлюднення колишнім співробітником Агентства національної безпеки США (АНБ США) Е. Сноуденом конфіденційної інформації щодо використання ССІ для потреб АНБ США.

Аналіз показує, що проблеми використання ССІ в інтересах ІПсП вирішуються шляхом нормативно-правового, організаційно-технічного і кадрового забезпечення діяльності в ССІ.

США намагаються ефективно використати переваги країни, яка практично одноосібно контролює ГМ через компанію ICANN (підпорядковану Міністерству торгівлі США) та значною мірою визначає політику і технологічні засади його розвитку.

У першу чергу це стосується намагань максимального поширення ССІ без обмежень та регулювання доступу населення країн світу національними урядовими структурами та відповідного забезпечення можливості ІПсВ в інтересах США та їх союзників. Так, ще 23.10.07 комітетом з іноземних справ палати представників Конгресу США був схвалений законопроект "Global Online Freedom Act of 2013" ("Акт про глобальну мережну свободу"), який передбачає заборону компаніям США "допомагати режимам, які обмежують доступ в Інтернет", та визначає заходи з підтримки вільного доступу користувачів національних сегментів блогосфери попри обмеження національних урядів. Спроби прийняття різних варіацій цього законопроекту продовжуються практично кожний рік (останній раз – 04.02.13). Проте, не чекаючи на прийняття даного нормативного документа, для забезпечення умов поширення власного ІПсВ на інтернет-користувачів у країнах, що вживають обмежувальні заходи, керівництво США у взаємодії з ІТ-компаніями створюють та поширюють спеціальне програмне забезпечення і технології.

За заявою колишнього державного секретаря США Хілларі Клінтон від 09.03.10 влада США "пом'якшила" правила експорту інтернет-технологій до низки таких країн, як Іран, КНДР, Куба, Судан, щодо яких Вашингтон має власні ембарго. Цей крок має на меті допомогти користувачам ГМ обходити запроваджені в цих країнах інформаційні блокади й таким чином "розвивати в них громадянські суспільства". Одним з прикладів такого спеціального програмного забезпечення є продукт Collage Технологічного інституту Джорджії для використання стеганографії у ССІ.

У травні 2011 року у США прийнято "Міжнародну стратегію кібербезпеки", яка передбачає можливість застосування ЗС у відповідь на кіберзагрози США. У контексті цього документа серед можливих "кіберзагроз" окремі експерти визначають і намагання суверенних країн контролювати національні сегменти Інтернету та обмежувати деструктивний контент.

Щодо заперечення окремими експертами поняття національних сегментів Інтернету, то про їх формування наочно свідчить гіперболічна карта Інтернету, яка показує нормовану кількість з'єднань між автономними системами – квадратами, які утворюють національні сегменти (рис. 1).

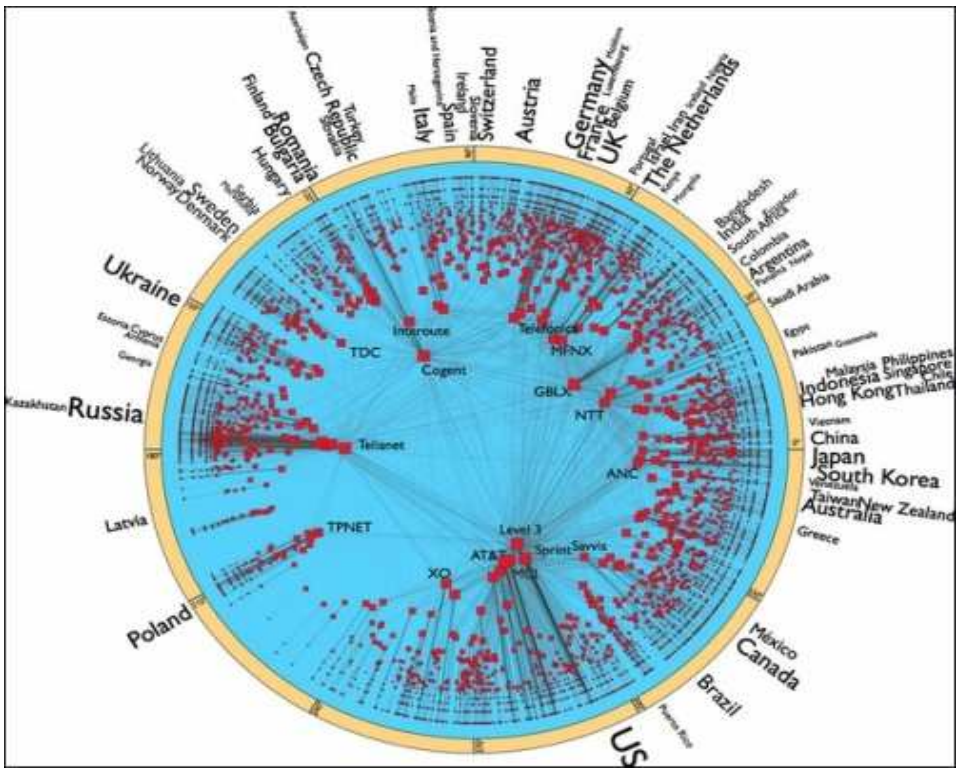


*Рис. 1. Гіперболічна карта Інтернету*

Використовуючи як інформаційне забезпечення суспільний резонанс після бостонських терактів палата представників Конгресу США вже 19 квітня 2013 року прийняла один з найбільш суперечливих проектів закону, що обмежує право на приватність: Акт про розповсюдження і захист даних кіберрозвідки (Cyber Intelligence Sharing and Protect Act – CISPA), який може надавати державним органам законну можливість доступу до будь-яких баз даних, збираючи різноманітну інформацію про своїх та іноземних громадян. Як пояснює Деклан Маккаллоу, редактор CNet, проект закону "уповноважує" федеральні агентства проводити незадекларований пошук і збір будь-яких даних у ССІ та вимагати дані від інтернет-провайдерів. Передбачається, що активність користувачів у ГМ буде алгоритмічно аналізуватись на відповідність якимось "критеріям злочинної поведінки", які ніде не прописані.

Законодавство більшості демократичних країн регулює доступ до приватної, корпоративної інформації та інформації, що є власністю держави, у тому числі і в ГМ. У той же час, фахівці Cisco Systems О. Бессараб і В. Литовка в інтерв'ю "proIT" вважають, що епоха мережного нейтралітету закінчується, хоча в країнах ЄС ця політика ще діє на законодавчому рівні. Оператори формально не можуть втручатися в трафік. Але у вітчизняних операторів немає юридичних обмежень щодо використання засобів обробки різних типів трафіка. Тому на даний час практично всі великі оператори в Україні застосовують технологію глибокої інспекції пакетів (Deep Packet Inspection), впровадили відповідні апаратно-програмні засоби та мають можливість вирішувати завдання з перехоплення визначеного трафіка відповідно до чинного законодавства.

Можливо дійти до висновку, що розвиток найбільших ССІ проходив не без уваги спеціальних служб. Так, компанія Facebook свого часу отримала інвестування від компанії

Accel Partners. Один з її менеджерів – Гілман Луї, президент компанії In-Q-Tel, заснованої ЦРУ для розробки "технологій добування інформації", інший менеджер Аніта Джоунс була керівником науково-дослідного відділу Міністерства оборони США, радником міністра оборони з питань Агентства з перспективних оборонних науково-дослідних розробок США (DARPA). У складі DARPA є відділ володіння інформацією (BBI), в інтересах якого працює компанія In-Q-Tel. Заявленою метою BBI є "збір якомога більшої кількості інформації про кожну людину, у централізованому місці для зручного вивчення, у т.ч.: її активність і спрямованість дій в Інтернеті, кредитні історії, стан здоров`я, освіта, платежі, податки, переміщення, зв`язки та інші дані"…

Серед технологічних потреб ЦРУ, визначених для In-Q-Tel у 1999 – 2001 роках:

використання Інтернету для потреб ЦРУ, безпечне отримання інформації;

анонімний серфінг, анонімна передача інформації;

мережні комунікації та Інтернет; автоматична ідентифікація та візуалізація користувачів;

пошук у відкритих джерелах усіх ресурсів Інтернету, а не тільки проіндексованої інформації в основних пошукових системах;

інтеграція різних методів пошуку та розширення пошуку з використанням XML тощо.

Серед сучасних технологій BBI – "аналіз соціальних мереж і механізмів формування моделі поведінки", для чого потрібний велетенський обсяг чітко спрямованого збору даних, що й забезпечує Facebook.

ЦРУ уклало з компанією Visible Technologies (моніторинг у ССІ) угоду з розробки системи, що дозволяє отримувати аналітично оброблену інформацію про відібрані повідомлення (позитивні, негативні, змішані, нейтральні), оцінити вплив автора на погляди аудиторії та вийти з ним на контакт. 04.02.10 компанія Google й АНБ США домовились про співробітництво у галузі кібербезпеки.

Це підтверджують свідчення Е. Сноудена (у публікаціях "Вашингтон пост" та "Гардіан" від 06.06.13) про комплексну систему моніторингу Інтернету, яка впроваджена спеціальними службами США у взаємодії з відповідними службами найближчих союзників, зокрема про функціонування секретної програми АНБ PRISM, у рамках якої можна контролювати електронну пошту, чати, голосові скайп-переговори, отримувати доступ до будь-яких особистих даних користувачів більшості ССІ, у першу чергу Google, Facebook, Skype, Yahoo, YouTube тощо (PRISM – державна комп'ютерна програма США, яка прийнята АНБ у 2007 році на заміну програми Terrorist Surveillance Program).

За оцінками "Вашингтон пост" (ще від 2010 року), щодобово системи збору інформації АНБ (у тому числі PRISM) перехоплювали і записували біля 1,7 млрд телефонних розмов та електронних повідомлень. Guardian з посиланням на надані Е. Сноуденом документи пише, що Microsoft надавала АНБ можливість обходити власний криптографічний захист для того, щоб отримувати доступ до листів і чатів поштового клієнта Outlook. Співробітники спецслужб отримали прямий доступ до "хмарного сховища" файлів SkyDrive. Один з листів АНБ підтверджує, що відомство почало отримувати метадані популярного сервісу Skype, починаючи з 06.02.11.

Компанія Microsoft, що купила Skype в травні 2011 року, забезпечила сервіс технологією законного прослуховування. Будь-якого абонента можна переключити на особливий режим, в якому ключі шифрування генеруються не на пристрої користувача, а

на сервері. Як пояснив Максим Емм, виконавчий директор компанії Peak Systems, таку послугу Microsoft надає спецслужбам багатьох країн, у т.ч. Росії й України. Газета Bloomberg Businessweek писала про те, що в китайській версії Skype (TOM-Skype) є опція для відстеження дій абонента (впроваджений так званий "клавіатурний шпигун", що дозволяє перевіряти набрані в Skype повідомлення на наявність у них "небажаних" слів в інтересах спецслужб). До передачі прав на Skype компанії Microsoft вважалось, що цей сервіс – один з найбільш захищених соціальних сервісів.

Журналіст The Guardian Глен Гринвальд розповів, що АНБ за допомогою DNI Presenter (спеціальної програми для злому електронної пошти) здійснювало перехоплення інформації державних структур різних країн, зокрема Президентів Бразилії і Мексики. АНБ США прослуховувало 38 іноземних дипломатичних установ, у тому числі своїх союзників по НАТО Франції та Італії.

Аналіз нормативного забезпечення діяльності систем кібербезпеки провідних країн свідчить про пріоритетне визначення ССІ серед об’єктів їх діяльності. Серед деяких задекларованих завдань об’єднаного кіберкомандування ЗС США (USCYBERCOM) та деяких інших федеральних структур:

підтримка доменних областей .mil, .gov і .com.;

проведення "війни ідей в Інтернеті" ("створенні глобального середовища, ворожого до насильницького екстремізму";

проведення спостереження за електронними ЗМІ та інтернет-блогами, виявлення каналів зв’язку терористичних груп та боротьба з "неточним" відображенням подій.

Застосування ССІ (Facebook, Diplopedia, Twitter, LinkedInTM, Communities@State) у контексті політики Digital Diplomacy передбачено "Стратегічним планом використання інформаційних технологій на 2011–2013 рр." Із жовтня 2008 року (за заявою заступника держсекретаря США з публічної дипломатії Джеймса Гласмана) "війна ідей" поширена і на російськомовну блогосферу введенням до складу "команди цифрових зовнішніх контактів" відповідних фахівців. Для координації діяльності федеральних, корпоративних і громадських структур з цього напряму в уряді США створено спеціальний підрозділ – "Політичний координаційний комітет зі стратегічних комунікацій", який підпорядкований Президенту. Для поточної розробки стратегії та оперативного керівництва діяльності за напрямом в уряді створено також Центр з глобальної стратегічної взаємодії, до якого входять "представники держдепартаменту, міністерства оборони і розвідки, з яким взаємодіє Національний контртерористичний центр, а також нова структура для координації й усунення конфліктів при проведенні таємних операцій".

Крім того, у США є практика передачі частини повноважень спецслужб у сфері ІПсП найнятим за контрактом приватним військовим компаніям, які спеціалізуються у галузі "управління сприйняттям" (маніпуляції інформацією). За оцінками експертів, комплексна система контролю Інтернету, яка створена у США, надає можливість за контентом ССІ у тій чи іншій країні визначити момент соціального вибуху з похибкою у 2 – 3 дні.

У Доктрині інформаційної безпеки Російської Федерації (РФ), затвердженої Президентом Російської Федерації 09.09.2000 р.), визначено:

"*…Источником внешней угрозы информационной безопасности Российской Федерации является разработка рядом государств концепций информационных войн,*

*предусматривающих создание средств опасного воздействия на информационные сферы других стран мира… Одним из приоритетных направлений противодействия является совершенствования методов и средств активного противодействия психологическим операциям вероятного противника…*"

У "Концептуальных взглядах на деятельность Вооруженных Сил Российской Федерации в информационном пространстве" (2011 р.) визначено, що: "*ВС РФ руководствуются следующими правилами разрешения военных конфликтов в информационном пространстве:*

*…3. В условиях эскалации конфликта в информационном пространстве и перехода его в кризисную фазу воспользоваться правом на индивидуальную или коллективную самооборону с применением любых избранных способов и средств, не противоречащих общепризнанным нормам и принципам международного права;*

*…5. В интересах индивидуальной и коллективной самообороны размещать свои силы и средства обеспечения информационной безопасности на территории других государств, в соответствии с соглашениями, выработанными ими на добровольной основе в ходе переговоров, а также в соответствии с международным правом*".

У липні 2009 р. створено Центр інформаційних технологій ОДКБ, а в жовтні прийнято рішення про створення спеціального інформаційно-пропагандистського центру Міністерства оборони (МО) РФ для інформаційної протидії у сфері ІТ. Центр інформаційного забезпечення (ЦІЗ) МО РФ активно використовує можливості Інтернету, у першу чергу через офіційний сайт МО РФ, абонентські пункти ГМ органів інформаційного забезпечення Збройних Сил (ЗС) РФ, сайти центрів зарубіжної воєнної інформації та сайти військових ЗМІ.

Відповідно до відомчої цільової програми "Забезпечення інформацією з соціально значущих тем у сфері молодіжної політики" у 2010 р. створювались державні школи блогерів (Томськ, Дагестан, Астрахань та ін.). 21 березня 2012 року віце-прем'єр Уряду РФ Дмитро Рогозін оголосив про плани створення Кіберкомандування ЗС РФ.

Для ефективного проведення заходів ІПсВ у блогосфері Інтернету дуже важливим є її вивчення, аналіз відповідними фахівцями для визначення цільових аудиторій, створення (мобілізації, підготовки) мереж блогерів, управління ними в ході ІПсВ тощо. Активно проводиться розробка засобів моніторингу соціальних мереж. Так ізраїльська компанія "Amdocs" запропонувала російським компаніям впровадити свій продукт Social Network Gateway – засіб моніторингу соціальних мереж. Ключові особливості програми:

відслідковування згадувань про компанії в блогах і соціальних мережах, інших інформаційних акціях у режимі реального часу;

ранжування важливості повідомлень залежно від авторитетності джерела (цитування блогера і його геолокації, аудиторії "передплатників" тощо);

наявність інструментів аналізу даних, що отримуються, для оцінювання ефективності інформаційних акцій.

Принциповим є те, що впровадження Social Network Gateway передбачається найбільшими операторами телекомунікаційних послуг "ВымпелКом", за кордоном – "Vodafon". Впровадження засобів аналізу компаніями, що надають телекомунікаційні послуги, робить їх потенційно можливими засобами протидії інформаційним акціям в Інтернеті, оскільки факт ІПсВ стає відомим ще до того, як повідомлення потрапить до соціальної мережі, що дозволяє застосовувати оперативну фільтрацію контенту.

Компанія "Медіалогія" пропонує створений кілька років тому програмно-технічний комплекс "Призма" ("Управління репутацією і ризиками в соціальних медіа"). "Призма" призначена для керівників федеральних і регіональних органів влади, корпоративних структур. Це інструмент оперативного аналізу соціальних медіа для виявлення реальних проблем і ризиків та своєчасного реагування на них. За твердженнями директора "Медіалогії" з розвитку Фарита Хусноярова, "система може відслідковувати 60 млн джерел (окремих блог-сфер) і основні соціальні мережі, аналізує тональність висловлювань з похибкою 2 – 3% (при використанні інтернет-сленгу достовірність аналізу знижується) практично у реальному часі. До моніторингу потрапляють практично всі основні ССІ, у тому числі блоги на LiveJournal, Twitter, YouTube, Facebook.

Служба зовнішньої розвідки РФ оголосила 3 закритих тендери для розробки нових методик моніторингу блогосфери, розповсюдження повідомлень у соціальних мережах, щоб формувати суспільну думку. Тендери були проведені в січні – лютому 2012 року. За інформацією газети "Комерсант", ці роботи, що розбиті за різними тендерами, функціонально пов'язані між собою. "Планируется, что сначала мониторить блогосферу будет система "Диспут"... Затем полученную информацию будет анализировать система "Монитор-3"... На основе полученных данных вбрасывать нужную информацию в социальные сети начнет система "Шторм-12"... Цель: "массовое распространение информационных сообщений в заданных социальных сетях, используя имеющиеся учетные записи пользователей, с целью формирования общественного мнения", "сбор статистики и анализ эффективности распространения информационной волны", "анализ пригодности наиболее популярных сервисов социальных сетей для инициирования информационных волн различной тематической, социальной и прочей направленности", – пише "Комерсант". Безпосереднім виконавцем з усіх трьох конкурсів стала компанія "Итеранет".

У Китаї проводиться політика жорсткого контролю за інтернет-провайдерами та користувачами їх послуг. Законом заборонені анонімні блоги, обов'язковою є реєстрація користувачів. Як повідомляє China Tech News, з 2009 року всі інтернет-кафе обладнані спеціальними фотокамерами і сканерами документів. Інформація про кожного відвідувача передається в "центри моніторингу охорони культурного правопорядку". Фільтрується контент Інтернету, блокуються окремі ССІ. Країна до певної міри вже забезпечує інформаційні потреби влади та населення власними засобами обчислювальної техніки та програмного забезпечення. Навіть ті ж смартфони та планшетні комп'ютери не передбачають використання запозиченого програмного забезпечення і сервісів Google. Важливою умовою впровадження ІТ-технологій у Китаї був дозвіл користуватись іноземними ССІ тільки до тих пір, доки не буде розроблений їх китайський аналог. На даний час Facebook у КНР не працює, замість нього XiaoNei, замість Twitter – Weibo.

Технологічною умовою цього є те, що сервери китайських аналогів знаходяться в Пекині. У Китаї, творчо інтегруючи досвід США і Росії, крім створення спеціальних військових структур (оперативних об'єднань) для ведення інформаційної війни, не забувають теорію народної війни і народної армії, що передбачає участь у веденні ІПсП не тільки військових фахівців, але й широких мас навченого населення. Керівництво КНР розгорнуло широку кампанію з підготовки й інформаційного виховання свого населення, адаптуючи його до умов життя в інформаційному світі. Це забезпечує можливість

залучення до організованої діяльності у блогосфері мільйонів підготовлених та мотивованих користувачів. У США рух активістів блогосфери у Китаї навіть назвали "50-ти центовою армією"…

У той же час у США з використанням досвіду молодіжної політики у СРСР з 2009 року (відповідно до п. 8 "Комплексної національної ініціативи забезпечення кібербезпеки", 2008) розгорнута програма "Кіберпатріот" (CyberPatriot – The National High School Cyber Defense Competition), яка передбачає проведення навчання – змагання протягом року максимально широкого кола учнів старших класів шкіл, ліцеїв, кадетських корпусів (у сезоні 04.2013 – 03.2014 – 3000 команд США і Канади) для актуалізації проблеми кібербезпеки країни та пошуку і відбору талановитої, мотивованої молоді до роботи (служби) у відповідних структурах національної системи кібербезпеки.

Розумінням того, що спеціальні державні структури не в змозі самостійно вирішити питання ІПсП у блогосфері, є й розгортання руху "Кібердружин" у Росії. 27 квітня 2013 року пройшов Перший Всеросійський зліт учасників руху "Кібердружина", в якому взяли участь більше 400 активістів з усієї Росії, які представляли більше 20 тисяч учасників руху, представники правоохоронних органів, адміністрації Президента, уряду, громадських організацій, бізнес-структур. Учасники працювали у трьох тематичних сесіях: інформаційні війни; інформаційна безпека (у т.ч. боротьба з розповсюдженням дитячої порнографії тощо); Росія он-лайн. Аналогічні молодіжні програми при урядовій підтримці реалізуються в Ізраїлі та інших країнах.

Міжнародний саміт з питань безпеки кіберпростору, який проведено у грудні 2012 р. в Дубаї (ОАЕ), показав, що протиріччя, пов'язані з розвитком і використанням міжнародних телекомунікацій, загострюються і можуть перейти у фазу нової "холодної" війни між США, Канадою, Великою Британією, Францією та ін., з одного боку, та Китаєм, Росією, Бразилією, Індією, ЮАР та ін., з іншого боку. Секретар спеціалізованої установи ООН – Міжнародного союзу електрозв'язку (МСЕ, 193 країни) Хамадун Туре заявив, що світ знаходиться у стані інформаційної війни і для багатьох урядів практика шпигунства в ГМ вже стала звичайною справою. Основне протиріччя між одноосібним (США, компанія ICANN) чи міжнародним (ООН, МСЕ) контролем Інтернету, а також між "глобальною інтернет-свободою" (в умовах контролю США) та певними механізмами суверенітету в національних сегментах Інтернету для запобігання його використання як каналу зовнішнього ІПсВ.

Наслідками значного міжнародного резонансу після публікацій "Вашингтон пост" та "Гардіан" зі свідченнями Е. Сноудена стали відповідні заходи з інформаційної безпеки у різних країнах світу. Серед них:

рішення країн Південноамериканського спільного ринку (МЕРКОСУР) на позачерговому саміті щодо неприпустимості кібершпигунства з боку США та інших країн;

рішення міністрів оборони Аргентини та Бразилії щодо поєднання зусиль для захисту від кіберзагроз з боку США;

рішення уряду ФРН про офіційне припинення дії договору про моніторинг телекомунікаційних систем національних спецслужб зі спецслужбами США, Великої Британії і Франції, впровадження системи "національної маршрутизації";

денонсація Європарламентом договору про міжнародну банківську систему SWIFT, яка надавала США доступ до інформації європейських банків;

різке зменшення користувачів Facebook і Google+ у США і Великій Британії тощо.

Для виявлення ролі блогосфери та соціальних медіа, дослідження через Інтернет ролі соціальних, культурних і політичних сил у визначеній країні (регіоні, соціальному середовищі…) розроблено технології створення "портретів" і карт блогосфери. Так, за допомогою унікальної методології групи Morningside Analytics група аналітиків Центру Беркмана при Гарвардському університеті виконала дослідження "Публічний дискурс в російській блогосфері: аналіз політики і мобілізації в Рунеті".

Порівняльний аналіз блогосфер Росії і США продемонстрував дуже різні структури, з різним ступенем централізованості і різними розмірами "блог-сфер". Російськомовний сегмент блогосфери згідно з первинним аналізом являє собою кілька ізольованих кластерів (чисельність проаналізованих блогів – 5 млн). Більш глибокий аналіз на основі активного "дискусійного ядра" (12 тис.) навпаки показує відсутність фрагментації блогосфери, ядро якої практично збігається з картою одного із сегментів загальної блогосфери: блог-платформою "Живой журнал" (ті ж самі 12 тис. в ядрі). Структура американської блогосфери чітко показує поділ між групами консерваторів і лібералів. А ось на російській карті відразу видно цілісну "блог-сферу", в якій немає ізольованих груп. Тобто маємо "штучний актив" російської блогосфери, який до того ж тяжіє до ліберальних електронних ЗМІ. А ставляться до цього активу звичайні користувачі по-різному, маємо 4 фрагменти різної направленості.

Після визначення загальної структури "дискусійного ядра" дослідники ідентифікували сегменти "блог-сфери". На базі аналізу змісту 1200 блогів (10% ядра) було виявлено 4 основних внутрішніх кластери "дискусійного ядра":

політичні і громадські відношення; культура (література, кіно та ін);

регіональні блогери (блогери з Білорусі, України, Вірменії, Ізраїлю та ін);

інструментальні блогери (блогери, що активно використовують блог для заробітку).

Всередині групи політичних і громадських відношень виявлено групу "демократичної опозиції", а також групу "націоналістів". Саме в цих двох групах були виявлені ознаки політичної і соціальної мобілізації. У той же час не знайшли чіткого вираження представники державницьких патріотичних груп, які переважно знаходяться на місцях загальної дискусії на суспільно-політичні теми, але практично не формують "дискусійне ядро". Тобто державницькі і патріотичні групи активістів російськомовної блогосфери ще не зайняли належних активних позицій у формуванні суспільної думки, більше обмежуються негативним чи позитивним сприйняттям тих чи інших інформаційних проявів з боку "дискусійного ядра".

Технологія дозволяє також отримувати індивідуальні карти найбільш активних і відомих блогерів, наприклад О. Навального. В основі карти – аналіз груп блогів, які посилаються на даний блог. Тобто є можливість оцінити перспективу й ефективність задіяння певного блогу для ІПсВ на певну цільову аудиторію! Без сумніву, що такі технології вже використовуються певними структурами для організації ІПсВ під час суспільно-політичної мобілізації у тих чи інших країнах (виборчі компанії тощо).

Для виявлення, залучення до співпраці та навчання активістів-блогерів з метою створення "заряджених блог-мереж" та їх подальшого використання в інтересах ІПсП провідними країнами (у першу чергу США) реалізуються численні міжнародні проекти в галузі соціальних медіа. У тому ж Центрі Беркмана відкрито курси для блогерів з різних країн світу. Для зв'язку між блогерами з усього світу створено сайт Global Voices Online. Цей ресурс дозволяє отримувати пости (повідомлення) від блогерів, перекладати їх на різні мови, розповсюджувати в ГМ відібраний матеріал, використовуючи адреси блогерів, для ініціювання інформаційних хвиль визначеної спрямованості.

Для більш повного врахування особливостей цільової аудиторії при проведенні ІПсВ у блогосфері необхідне також більш чітке розуміння відмінностей підходів до питань "масовізації людини в медіапросторі" і суб'єктів масової комунікації (МК). Представники медіацентричного підходу вважають, що МК становить замкнену цілісну систему, що функціонує за власними законами. Об'єктом її впливу є масова аудиторія як носій громадської думки; як суб'єкти виступають власники ЗМІ, журналісти, а також структури, які їх контролюють.

Соціоцентрична модель, в якій суб'єктами є різні соціальні групи, передбачає дещо більш складний механізм. Суб'єктами МК як такої є "соціальні групи, які реалізують потреби і умови свого існування та розвитку", що потребує впровадження в масову свідомість певних духовних значень і установок. При такому підході масова аудиторія є самостійним суб'єктом, який детермінує МК і висловлює (узгоджує) через її канали свої погляди. Такий підхід, за поглядами деяких фахівців, зокрема С. Г. Корконосенка, є найбільш перспективним і актуальним, у першу чергу для аудиторії МК у країнах СНД. Ця особливість, за умов забезпечення населення країн СНД елементарними знаннями ризиків життя в інформаційному суспільстві – здатності до інформаційного самозахисту (у т.ч. у блогосфері), може бути додатковим чинником інформаційної безпеки. При цьому необхідно сприяти консолідації правлячих еліт, державницьких сил, ліберальної інтелігенції та основної маси активного населення країни.

**Висновки**

1. Прискорений розвиток блогосфери Інтернету визначає її важливе значення як глобального інформаційного середовища для моніторингу і виявлення ІПсВ, каналу ефективного диференційованого ІПсВ на визначені об'єкти соціотехнічного середовища.

2. Провідні країни проводять комплекс заходів щодо нормативного, організаційно-технічного та кадрового забезпечення діяльності у блогосфері Інтернету з метою захисту власного інформаційного простору та досягнення інформаційної переваги над суперниками для вирішення геополітичних, економічних та військових задач.

3. Створені комплексні системи кібербезпеки у провідних країнах дозволяють оперативно відслідковувати процеси, що призводять до зростання соціальної напруженості, провокування безладу, протесні й електоральні настрої в соціальних медіа щодо основних політичних партій, обговорення суспільно значущих проблем, діяльність екстремістських і терористичних угрупувань, прояви комп'ютерної злочинності та злочинів проти моралі тощо, оперативно реагувати на них.

4. Аналіз останніх подій у світі свідчить про критичний рівень інформаційних загроз для країн, які неспроможні контролювати і захищати власний інформаційний простір. Це вимагає від таких країн прийняття комплексу нормативних, організаційно-технічних та кадрових заходів для забезпечення інформаційної безпеки особистості, суспільства і держави.

5. Проведений аналіз свідчить про необхідність:

створення дієвих механізмів комплексного системного контролю з боку державних і громадських структур за впровадженням ІТ, моніторингу ССІ, прогнозування та виявлення інформаційних загроз та їх наслідків для особистості, суспільства і держави;

розробки та впровадження нормативних освітніх програм ("Інформаційна безпека держави", "Основи безпеки інформаційного середовища" тощо), підготовки фахівців з вищою освітою всіх напрямів з метою надання населенню України здатності до інформаційного самозахисту.

## СПИСОК ЛІТЕРАТУРИ

1. Про Доктрину інформаційної безпеки України : Указ Президента України від 08.07.2009 № 514/2009 [Електронний ресурс]. – Режим доступу : http://www.president.gov.ua.

2. Дубов Д. В. Сучасні тренди кібербезпекової політики: висновки для України : аналітична записка відділу досліджень інформаційного суспільства та інформаційних стратегій Національного інституту стратегічних досліджень при Президентові України [Електронний ресурс] / Д. В. Дубов. – Режим доступу : http://www.niss.gov.ua/articles/294.

3. H.R. 624: Cyber Intelligence Sharing and Protection Act [Electronic resource]. – Node of access : http://www.govtrack.us/congress/bills/113/hr624.

4. H.R. 491: Global Online Freedom Act of 2013 [Electronic resource]. – Node of access : http://www.govtrack.us/congress/bills/113/hr491/text.

5. Брюс Этлинг. Публичный дискурс в российской блогосфере: анализ политики и мобилизации в Рунете. Исследования Центра Беркмана No. 2010 – 2011, 19 октября 2010 г. [Электронный ресурс] / Брюс Этлинг. – Режим доступа : http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Public_Discourse_in_the_Russian_Blogosphere-RUSSIAN.pdf.

6. Доктрина информационной безопасности Российской Федерации [Электронный ресурс]. – Режим доступа : http://www.rg.ru/oficial/doc/min_and_vedom/mim_bezop/doctr.shtm.

7. Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве (2011 г.) [Электронный ресурс]. – Режим доступа : http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle.

8. Корконосенко С. Г. Свобода личности в массовой коммуникации / С. Г. Корконосенко, М. Е. Кудрявцева, П. А. Слуцкий ; под ред. С. Г. Корконосенко. – СПб. : Изд-во СПбГЭТУ "ЛЭТИ", 2010. – 308 с.

9. Тараскин М. М. Взгляды высшего военно-политического руководства ведущих иностранных государств на противодействие угрозам кибернетических войн

[Электронный ресурс] / М. М. Тараскин, С. А. Чешуин // Научные материалы научно-исследовательского центра "Наука-XXI". Бюллетень "Проблемы безопасности". – Режим доступа : http://www.nic-nauka.ru/material.

10. Мониторинг сети спецслужбами [Электронный ресурс]. – Режим доступа : http://www.mywebs.su/blog/safety/7051.html.

11. Дубов Д. В. Майбутнє кіберпростору та національні інтереси України: нові міжнародні ініціативи провідних геополітичних гравців : аналітична доповідь відділу досліджень інформаційного суспільства та інформаційних стратегій Національного інституту стратегічних досліджень при Президентові України [Електронний ресурс] / Д. В. Дубов, М. А. Ожеван. – Режим доступу : http://www.niss.gov.ua/content/articles/files/Kyberprostyr-17541.pdf.

12. Илья Барабанов. Разведка ботом [Электронный ресурс] / Илья Барабанов, Иван Сафронов, Елена Черненко // Коммерсантъ. – 2012. – 27 серпня (№ 158/П (4943)). – Режим доступа : http://www.kommersant.ru/doc-y/2009256.

13. Российский бизнес контролирует блогосферу. OpenMediaNews, 19 мая 2011 г. [Электронный ресурс]. – Режим доступа : http://www.omn.ru/?p=12355.

14. Як влада читає ваші блоги: розслідування Forbes [Електронний ресурс]. – Режим доступу : http://ipress.ua/mainmedia/yak_vlada_chytaie_vashi_blogy_rozsliduvannya_forbes_6363.html.

15. Кирилл Князев. Реальность и мифы об инспектировании трафика [Электронный ресурс] / Кирилл Князев. – Режим доступа : http://proit.com.ua/article/internet/2013/03/05/173726.html.

16. Правительство США распространит "войну идей" на Рунет [Электронный ресурс]. – Режим доступа : http://govorim-vsem.ru/viewtopic.php?f=1&t=41589.

17. In-Q-Tel: венчурный фонд ЦРУ. Исследовательское сообщество Московского физико-технического института [Электронный ресурс]. – Режим доступа : http://government.fizteh.ru/darpa/in-q-tel_fund.html.

18. Страны объединяются в борьбе с кибершпионажем США [Электронный ресурс]. – Режим доступа : http://inpress.ua/ru/politics/16361-strany-obedinyayutsya-v-borbe-s-kibershpionazhem.

19. Алексей Зверев. Русская РУНЕТка [Электронный ресурс] / Алексей Зверев. – Режим доступа : http://www.osfsb.ru/File.ashx?ID=177.

20. USAID створює успішні організації, що підтримують ЗМІ. [Електронний ресурс]. – Режим доступу : http://ukraine.usaid.gov/ua/programs/demokratiya-ta-vryaduvannya-uk/rozvytok-zmi-uk/usaid-stvoryuye-uspishni-organizatsiyi-shcho.

21. Панченко В. М. Соціальні інтернет-сервіси як засіб прихованого інформаційного впливу [Електронний ресурс] / В. М. Панченко // Інформаційна безпека людини, суспільства, держави : зб. наук. праць. – К. : НА СБУ, 2012. – Вип. 1 (8). – Режим доступу : http://archive.nbuv.gov.ua/portal/Soc_Gum/iblsd/2012_1/_private/11pvmlii.pdf.

22. The Comprehensive National Cybersecurity Initiative. National Security Council [Electronic resource]. – Node of access : http://www.whitehouse.gov/administration/eop/nsc/cybersecurity.

Подано 01.08.13

**Ю. М. Супрунов**

**НАПРАВЛЕНИЯ И ОТДЕЛЬНЫЕ ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ СОЦИАЛЬНЫХ СЕРВИСОВ ИНТЕРНЕТА В КОНТЕКСТЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА**

*Рассматриваются направления и отдельные проблемы распространения и развития блогосферы Интернета в контексте ее значения как глобальной информационной среды мониторинга и выявления информационно-психологического воздействия (ИПсВ), канала эффективного дифференцированного ИПсВ по определенным объектам социотехнической среды. Анализ проблем проводится на примере некоторых ведущих стран мира (в первую очередь США), в которых сформированы основные нормативные и организационные основы использования киберпространства в качестве новой боевой среды.*

**Y. M. Suprunov**

**TRENDS AND SOME PROBLEMS OF INTERNET'S SOCIAL SERVICES USE IN THE CONTEXT OF INFORMATION SECURITY OF STATE**

*Trends and some problems of proliferation and development of the Internet's blogosphere in the context of its importance as a global information environment of monitoring and identification of information and psychological influence, channel of effective differentiated information-psychological influence on certain objects of social and technical environment are under consideration. The problems' analysis is conducted on the example of several leading countries of the world (especially the U.S.), where the main regulatory and organizational framework for the use of cyberspace as a new combat environment was formed.*