УДК 159.98

Р.М.Федоренко

КОНТЕНТ-МОНІТОРИНГ ІНФОРМАЦІЙНОГО ПРОСТОРУ ЯК ЧИННИК ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ У ВОЄННІЙ СФЕРІ

Стаття присвячена питанням впровадження контент-моніторингу інформаційного простору у воєнній сфері України. Розглянуто основні об'єкти, загрози та негативні фактори забезпечення інформаційної безпеки у воєнній сфері, а також наявний рівень автоматизації процесів моніторингу інформаційного простору в Україні. Реалізація контент-моніторингу дасть змогу підвищити ефективність забезпечення інформаційної безпеки України у воєнній сфері та сприятиме переходу від прийняття окремих рішень до вироблення комплексних сценаріїв, коли кожне окреме рішення підпорядковано забезпеченню довгострокових цілей держави.

Ключові слова: інформаційна безпека; контент-моніторинг інформаційного простору; інформаційно-психологічні операції; автоматизовані системи моніторингу.

Вступ. На Україну здійснюється потужний інформаційний вплив шляхом поширення неповної або упередженої інформації. Це зумовлено, насамперед, прагненням керівництва іноземних держав впливати на зовнішню та внутрішню політику України. Сьогодні актуальним завданням для України є моніторинг загроз інформаційній безпеці для реалізації інформаційної політики, спрямованої на забезпечення національних інтересів.

Постановка проблеми. Актуальність контент-моніторингу інформаційного простору з метою виявлення ознак інформаційно-психологічних операцій для забезпечення інформаційної безпеки України у воєнній сфері обумовлена новими геополітичними викликами, що набули особливої гостроти в умовах інформаційної війни та військових конфліктів на сході України.

Аналіз останніх досліджень і публікацій. Проблематику інформаційної безпеки та інформаційних воєн досліджували такі вчені як О. Бодрук, М. Биченок, В. Горбулін, Т. Дзюба, В. Кацалап, В. Корендович, О. Литвиненко, Г. Перепилиця, В. Петрик, П. Рогов, А. Рось, П. Сніцаренко, В. Толубко та інші. У цих дослідженнях інформаційна безпека визначається як безпека об'єкта від інформаційних загроз або негативних впливів, пов'язаних з інформацією. Суб'єктами забезпечення інформаційної безпеки є відповідні державні органи, які гарантують постійну наявність даних для прийняття стратегічних рішень та захист інформаційних ресурсів країни. Захист інформаційних ресурсів країни та наявність даних для прийняття стратегічних рішень є важливими умовами забезпечення інформаційної безпеки.

Метою статті є підвищення ефективності забезпечення інформаційної безпеки України у воєнній сфері за рахунок впровадження контент-моніторингу інформаційного простору з метою виявлення ознак інформаційно-психологічних операцій.

Виклад основного матеріалу. Інформаційний простір є однією з основних категорій інформаційної безпеки. Національний інформаційний простір являє собою сферу інформаційних обмінів щодо створення нової інформації, її захисту та використання. Розбудова власного інформаційного простору є однією з передумов соціально-економічного, політичного й культурного розвитку держави.

Інформаційна політика держави має реалізовуватися на чотирьох основних напрямах: розвиток національного інформаційного простору (ЗМІ), розвиток інформаційного суспільства (Е-уряд, Е-банкінг), розвиток офіційної комунікації (інформування громадськості, формування позитивного іміджу держави) та забезпечення інформаційної безпеки держави (захист інформаційного суверенітету, забезпечення інформаційних прав та свобод громадян, визначення режимів функціонування інформації тощо).

Контент-моніторинг – це змістовний аналіз інформаційних потоків з метою отримання необхідних якісних та кількісних зрізів, що проводиться безперервно в часі [1].

Аналіз нормативно-правового забезпечення інформаційної безпеки в Україні. Базовими нормативно-правовими актами, що визначають засади державної політики у сфері

інформаційної безпеки, є Закон України “Про основи національної безпеки України”, Закон України “Про засади внутрішньої і зовнішньої політики”, Закон України “Про інформацію”, Указ Президента України “Про Стратегію національної безпеки”, Указ Президента України “Про Воєнну Доктрину України” тощо.

В Законі України «Про інформацію» № 2657-XII від 02.10.1992 (у поправках після 2002 р.) вперше у правовій площині з’являється поняття «інформаційний суверенітет». Законом передбачено, що основою інформаційного суверенітету України є національні інформаційні ресурси.

У 1998 році було підготовлено проект Закону України «Про інформаційний суверенітет та інформаційну безпеку України» реєстраційний № 1207 від 07.07.1998, але він і досі ще не прийнятий. Слід зазначити, що проекти документів щодо інформаційної безпеки орієнтовані переважно на гуманітарну сферу, а проблеми технологічного розвитку та захисту інформаційної інфраструктури мало представлені.

Забезпечення інформаційної безпеки у воєнній сфері має бути спрямовано на такі основні об’єкти, як:

– інформаційна інфраструктура центральних органів військового управління та органів управління видів Збройних Сил України, родів військ, об'єднань, військових частин, установ і організацій;

– інформаційні ресурси підприємств оборонного комплексу і науково-дослідних установ, що виконують державні оборонні замовлення або займаються оборонною проблематикою;

– програмно-технічні засоби автоматизованих і автоматичних систем управління військами та зброєю;

– особовий склад та обслуговуючий персонал.

Сьогодні Україна опинилась перед загрозою втрати власного суверенітету в інформаційному просторі. Проведення інформаційно-психологічних операцій та інформаційних війн безпосередньо впливає на стан захищеності інформаційної безпеки та завдає шкоди національним інтересам.

Основними негативними факторами реалізації державної політики щодо забезпечення інформаційної безпеки у воєнній сфері є:

– відсутність єдиного, ефективно діючого міжвідомчого органу з координації діяльності суб’єктів сектору безпеки і оборони України та інших органів державної влади в інформаційній сфері;

– недостатній розвиток інформаційної інфраструктури у воєнній сфері для своєчасного отримання, обміну та використання інформаційних ресурсів органами військового управління;

– витік секретної інформації щодо планування та проведення військових операцій, структури та чисельності військ, їх передислокації тощо.

Таким чином, наявні проблеми вимагають загальносистемного вирішення та інтеграції дій відповідних державних інституцій з метою забезпечення інформаційної безпеки у воєнній сфері.

Загрозами інформаційній безпеці України у воєнній сфері в сучасних умовах можна визначити наміри, явища або процеси по відношенню до елементів інформаційної інфраструктури сектору безпеки і оборони України, яка підтримує сталість єдиного інформаційного простору держави у воєнній сфері [2]. Наслідками реалізації загроз інформаційній безпеці України у воєнній сфері може бути неотримання потенційно важливих та необхідних інформаційних ресурсів (зменшення об'єму інформаційного простору), несанкціонований витік інформації, блокування доступу до інформаційних ресурсів тощо. Основними загрозами інформаційній безпеці України у воєнній сфері є:

– недосконалість законодавчого та нормативного регулювання процесів інформаційної взаємодії силових структур щодо обміну оперативно-розшуковою, довідковою, криміналістичною та іншою інформацією;

– зростаюче відставання від розвинутих країн за рівнем інформатизації та автоматизації в усіх сферах життєдіяльності людини, суспільства і держави (Україна на 71 з 143 позицій в рейтингу розвитку інформаційного суспільства в світі) [3];

– інформаційно-пропагандистська діяльність деяких держав та політичних сил, що поширюють викривлену або брехливу інформацію про Україну;

– діяльність комерційних структур щодо впровадження комп'ютерно-телекомунікаційних систем в державному секторі на основі імпортних програмно-технічних засобів та технологій;

– руйнація вітчизняних наукоємних і високотехнологічних виробництв у галузі мікроелектроніки та комп'ютерно-телекомунікаційних засобів оборонно-промислового комплексу;

– падіння престижності військової служби, відвертання молоді від військово-технічних професій, втрата професійних знань і досвіду попередніх поколінь військовослужбовців.

З метою забезпечення державних інтересів, збереження ладу та стабільності у настроях українського суспільства необхідно швидко та ефективно реагувати на ці загрози та виклики інформаційній безпеці.

Аналіз інформаційних загроз показує, що потрібно враховувати умови і чинники, які впливають на процес виникнення та розвиток загроз. Якщо узагальнити ці процеси, то можна визначити динаміку розвитку інформаційного впливу: чинник інформаційної загрози – проява інформаційної загрози – реалізація загрози (інформаційний вплив) – результати впливу.

Моніторинг інформаційного простору з метою виявлення загроз інформаційній безпеці України у воєнній сфері. На стан інформаційної безпеки впливає безліч різних факторів, які або перешкоджають, або сприяють забезпеченню безпеки держави. При невірному або несвоєчасному реагуванні на негативні фактори інформаційного впливу (поширення неправдивої або негативної інформації) відбувається їх перехід у дестабілізуючий стан, при цьому фактор визначається вже як загроза. Своєчасне втручання в розвиток факторів інформаційної безпеки сприяє запобіганню появі кризових ситуацій, що є найбільш ефективним розвитком подій.

Актуальність контент-моніторингу інформаційного простору обумовлюється необхідністю передбачення ситуацій переростання факторів дестабілізації в загрози безпеці та збереження безпечного рівня стану об'єкта безпеки. Оптимальним порядком дій по забезпеченню інформаційної безпеки у воєнній сфері є своєчасне виявлення, класифікація та контроль факторів дестабілізації, ідентифікація загроз та розробка і виконання заходів щодо їх нейтралізації.

Контент-моніторинг інформаційного простору має бути спрямований на виявлення інформаційно-психологічних операцій, об'єктами впливу яких можуть бути: інформаційно-технічні та аналітичні системи, бази даних та інформаційні ресурси, психіка людини, настрої суспільства та імідж Збройних Сил і держави в цілому.

Для своєчасного виявлення інформаційно-психологічних операцій необхідно уважно стежити за динамікою публікацій щодо відповідної тематики з урахуванням їх тональності користуючись доступними інформаційно-аналітичними засобами моніторингу. При цьому варто враховувати моделі проведення інформаційних атак, наприклад, якщо ця модель охоплює фази: «фонові публікації» – «затишок» – «артпідготовка» – «затишок» – «атака», то вже за першими трьома компонентами можна з великою ймовірністю передбачити майбутні події (рис. 1) [4].

Рис. 1. Типова поведінка рядів інтенсивності тематичних публікацій

Таким чином, з метою своєчасного виявлення та ефективної протидії інформаційно-психологічним операціям доцільним є реалізація наступних етапів моніторингу:

– первинний аналіз інформації в засобах масової інформації щодо визначеної тематики та об'єкту;

– часовий аналіз появи публікацій, побудова графіків та визначення критичних точок;

– детальний аналіз динаміки публікацій з визначенням моментів, тривалості, періодичності повідомлень у критичних точках, прив'язка моментів появи повідомлень до інших подій, виявлення взаємозв'язків;

– визначення джерел, що публікують найбільшу кількість негативу;

– визначення «першоджерел» публікацій та ймовірних «замовників»;

– оцінка ймовірних наслідків та прогнозування подальших кроків;

– організація інформаційної протидії.

Автоматизація процесів моніторингу інформаційного простору. Для аналізу інформаційних операцій у середині минулого століття існували вузькоспеціалізовані програми для проведення окремих розрахунків або програми загального користування (системи керування базами даних).

Сучасний рівень контент-моніторингу (змістовий аналіз інформаційних потоків) реалізує виявлення взаємозв'язків окремих категорій у повідомленнях, групування цих категорій, їх візуалізацію. При цьому використовуються методи кластерного аналізу, що дають змогу на основі виявлення латентних ознак формувати компактні групи категорій, виявляти головні з них, візуалізовувати взаємозв'язки [5].

Існуюче програмне забезпечення дає змогу визначати такі характеристики інформаційних повідомлень, як:

– кількісна динаміка (кількість подій за одиницю часу);

– визначення основних сюжетів публікацій у ЗМІ щодо обраного явища;

– ранжирування та аналіз динаміки розвитку окремих проявів;

– статистичний, кореляційний аналіз загальної динаміки та динаміки окремих проявів;

– прогнозування розвитку явища й окремих його проявів.

Для дослідження взаємозв'язку реальних подій і публікацій щодо них у мережі Інтернет створено послуги моніторингу, систематизації та аналізу інформації (Інформаційна система InfoStream, Інформаційно-аналітичне агентство «Контекст Медіа», Автоматичний

інформаційний сервіс «Стрічка.ком» тощо) із забезпеченням доступу до оперативної інформації та аналітичною роботою (побудова таблиць, діаграм).

Успішно вирішуються й завдання моніторингу соціальних мереж (Hootsuite, YouScan, Twitalyzer, WildFire, у тому числі безкоштовні: Socialmention, SocialSeek). Для аналізу даних про атаки, прив'язані до географічних карт існують рішення DShield (www.dshield.org) або Internet Storm Center (http://isc.sans.org).

Таким чином, контент-моніторинг є обов'язковим для оперативного аналізу інформаційної обстановки, оскільки він забезпечує оперативність, повноту джерел та містить необхідні аналітичні засоби, зокрема визначає інтенсивність публікацій. Вибір засобу контент-моніторингу залежить від цілей та бюджету організації. Очевидно, що для сектору безпеки і оборони України необхідною є розробка власної аналітичної платформи контент-моніторингу інформаційного простору з відповідними засобами захисту від несанкціонованого доступу.

Висновки й перспективи подальших досліджень. Організований інформаційно-психологічний вплив на людей є специфічним явищем сучасності, важливим і ефективним засобом досягнення різних цілей на тактичному, оперативному і стратегічному рівнях. Негативний інформаційно-психологічний вплив інформаційних повідомлень все частіше використовується як зброя.

Контент-моніторинг інформаційного простору з метою виявлення ознак інформаційно-психологічних операцій дасть змогу підвищити ефективність забезпечення інформаційної безпеки України у воєнній сфері та сприятиме:

- підвищенню ефективності оцінки, прогнозування розвитку суспільно-політичної та соціально-економічної обстановки в державі, в регіоні та в світі в цілому;
- розробці та контролю здійснення заходів щодо попередження або мінімізації ризиків в кризових ситуаціях та в особливий період;
- оперативній оцінці наслідків різних рішень і обирати з них найбільш раціональні в кризових ситуаціях та в особливий період;
- визначенню області ризику з найбільшою можливістю і величиною збитку у випадку реалізації ризиків;
- переходу від прийняття окремих рішень до вироблення комплексних сценаріїв (загальносистемних рішень), коли кожне окреме рішення підпорядковано забезпеченню довгострокових цілей держави.

Таким чином, проведення контент-моніторингу інформаційного простору та виявлення загроз інформаційній безпеці у воєнній сфері надаватиме якісну оцінку рівню інформаційного впливу на елементи інформаційної інфраструктури сектору безпеки і оборони України, а це, у свою чергу, дасть змогу розробляти адекватні контрзаходи з нейтралізації інформаційних загроз.

Література:

1. Григорьев А. Н., Ландэ Д. В., Бороденков С. А. и др. InfoStream. Мониторинг новостей из Интернет: технология, система, сервис: Научно-методическое пособие. – К., ООО "Старт-98", 2007. – 40 с.

2. Биченок М. М. Проблеми моніторингу комп'ютерно-телекомунікаційних загроз. Національна безпека: український вимір. / М. М. Биченок, С. П. Іванюта, О. С. Метельська // Ін-т пробл. нац. безпеки. Щоквартальний науковий збірник № 5 (24). – К., 2009.

3. Global Information Technology Report 2015. World Economic Forum. http://reports.weforum.org/global-information-technology-report-2015/

4. Горбулін В. П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: Монографія / В. П. Горбулін, О. Г. Додонов, Д. В. Ланде. – К.: Інтертехнологія, 2009. – 164 с.

5. Берко А. Ю., Кісь Я. П., Суховерський В. І. Система контент-моніторингу новинних Інтернет ресурсів. // Національний університет "Львівська політехніка". – 2011. – № 699. – С. 13-20.

Надійшла 19.05.2015 р. Рецензент: д.т.н., проф. Богданович В.Ю.