УДК 316.658.2

І.В. Замаруєва, д-р техн. наук, проф.,
А.О. Рось, д-р техн. наук, проф.

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ У ВОЄННІЙ СФЕРІ ПРИ ЗАПОБІГАННІ І СТРИМУВАННІ ВОЄННОГО КОНФЛІКТУ

У статті надано аналіз інформаційних загроз національним інтересам України у воєнній сфері. Запропоновано основні напрями ведення інформаційної боротьби при запобіганні і стримуванні воєнного конфлікту на всіх етапах його розвитку.

Ключові слова: інформаційна загроза, національна безпека, воєнний конфлікт, запобігання, стримування, інформаційна боротьба.

In the article it is presented the analysis of information threats to national interests of Ukraine in the military sphere. Basic directions of conduct of information srtuggle for forestaling and inhibition of military conflict on all stages of its development.

Key words: information threat, national security, military conflict, forestaling, inhibition, information srtuggle

Виходячи із загроз національним інтересам України в сфері національної безпеки, договірних обмежень, міжнародних угод та ресурсних можливостей держави, чинною Державною програмою розвитку Збройних Сил України на перспективу до 2015 року серед основних завдань Збройних Сил визначені такі:

- запобігання терористичним актам на важливих державних, промислових та військових об'єктах на території України у випадках, передбачених законодавством;
- запобігання збройним конфліктам та підтримання миру і стабільності у кризових регіонах світу в рамках міжнародного військового співробітництва та надання військової допомоги іншим державам;
- стримування та недопущення поширення збройних конфліктів з території суміжних держав та втягування України в прикордонні збройні конфлікти;
- участь Збройних Сил у загальнодержавних стабілізаційних заходах з проведенням спеціальних дій, спрямованих на недопущення поширення на територію України неконтрольованих деструктивних процесів, які пов'язані із широкомасштабною дестабілізацією суспільно-політичної обстановки в суміжній державі;
- стримування та відсіч збройній агресії шляхом оборони національної території держави при втягуванні України у воєнний конфлікт.

Обґрунтування функцій запобігання і стримування власних збройних сил окремої держави має спиратися на керівні положення і вимоги вищих концептуальних державних документів – Концепції національної безпеки (Закону про національну безпеку), Стратегії національної безпеки і Воєнної доктрини. Такий підхід цілком адекватний досвіду розвинених країн світу. В основі положень зазначених документів лежать національні інтереси держави і загрози останнім.

Саме на загрозах національним інтересам держави ґрунтується визначення (моделювання) ймовірного (евентуального) противника. Наведемо типові загрози національним інтересам держави, з появою яких виникає потреба в запобіжних діях, у тому числі з використанням збройних сил.

Зовнішні загрози [1]**:**

- наявність таких територіальних претензій до держави, які офіційно висловлюються одним чи декількома суб'єктами міжнародних відносин;
- намагання одного чи декількох суб'єктів міжнародних відносин до втручання у внутрішні справи держави та реальні дії щодо практичної реалізації цих намагань;
- дії одного чи декількох суб'єктів міжнародних відносин, які за змістом є такими, що зачіпляють політичні, економічні та інші інтереси держави, а за формою суперечать міжнародному праву і світовим традиціям міждержавних відносин;
- створення ворожих осередків, які є носіями задуму про збройну агресію проти держави, на територіях поблизу державного кордону останньої;
- дії сусідніх та інших країн, пов'язані з розгортанням (нарощуванням) угруповань військ (сил) на територіях (акваторіях), що є прилеглими до території держави, і які порушують узаконений міждержавними угодами баланс сил у регіоні (субрегіоні);
- наявність процесів, які пов'язані з посиленням ворожих до держави воєнних союзів;
- воєнні дії на сусідніх для держави територіях, особливо, якщо такими діями порушуються інтереси спільних етносів;
- агресія проти країн, які є союзниками держави за воєнно-політичними чи оборонними міждержавними утвореннями;
- створення, оснащення і вишкіл на територіях інших держав збройних формувань, метою яких є протиправні дії на території держави;
- напади на об'єкти держави, що розташовані на територіях інших країн, з метою завдати шкоди або створити провокаційну ситуацію;
- інструментальні, інформаційні, психологічні дії, які здійснюються з територій інших країн та спрямовані на порушення нормального функціонування систем державного і військового управління, небезпечних промислових об'єктів держави;
- дискримінаційні та інші незаконні дії проти прав і свобод громадян держави на територіях інших держав;
- терористичні дії проти держави поза її територією.

Внутрішні загрози [1]**:**

- початок підготовки будь-якої політичної групи (будь-яких політичних груп) до здійснення дій щодо насильницької зміни конституційного ладу в державі;
- прояви протиправної діяльності екстремістських, націоналістичних, етнічних, релігійних, сепаратистських і терористичних організацій і структур, яка спрямована на порушення територіальної цілісності держави та дестабілізацію внутрішньополітичної обстановки в країні відкрито силовими або терористичними діями;
- планування будь-якими організаціями або структурами дій, спрямованих на дезорганізацію функціонування органів державної влади, матеріальна підготовка до таких дій та початок їх ведення, у тому числі й напади на об'єкти державного і військового управління, промислові, сільськогосподарські, інформаційні та інші важливі для безпеки держави об'єкти;
- незаконні силові дії проти структур громадянського суспільства, населення, окремих громадян, у тому числі бандитські й диверсійні акції;
- створення, оснащення та підготовка до дій незаконних збройних формувань;
- незаконне розповсюдження на території держави зброї, боєприпасів, вибухових речовин, хімічних і біологічних засобів, у тому числі наркотиків, які можуть бути

використані для здійснення диверсій, терористичних актів та інших протиправних дій;

• прояви організованої злочинності, тероризму, контрабанди.

Отже, на теперішній час участь у запобіганні та стримуванні воєнного конфлікту стає вираженою функцією, а не побічною якістю збройних сил.

Як випливає зі змісту наведених зовнішніх і внутрішніх загроз національній безпеці держави, реалізаційною основою їх значної частини є інформаційна. Необхідність нейтралізації цих загроз, а також протидії інформаційному впливу з боку країни-агресора, спрямованому на розв'язання конфліктної ситуації шляхом збройного насильства, обумовлює особливу значущість забезпечення інформаційної безпеки держави у воєнній сфері. Наведемо декілька визначень.

Інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається завдання шкоди через неповноту, невчасність та невірогідність інформації; негативний інформаційний вплив, негативні наслідки застосування інформаційних технологій, несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [2].

Інформаційна безпека держави у воєнній сфері – стан захищеності національних інтересів у воєнній сфері в умовах впливу зовнішніх і внутрішніх і інформаційних загроз, який забезпечується шляхом здійснення комплексу заходів інформаційно-психологічного та інформаційно-технічного характеру.

Забезпечення інформаційної безпеки держави у воєнній сфері – скоординовані дії інформаційно-психологічного та інформаційно-технічного характеру, які здійснюють держави, збройні сили й інші структури в інтересах воєнної безпеки держави.

Інструментом забезпечення інформаційної безпеки держави у воєнній сфері, у тому числі при запобіганні і стримуванні воєнного конфлікту є інформаційна боротьба.

Аналіз існуючого доробку з проблем ведення інформаційної боротьби в інтересах запобігання і стримування воєнного конфлікту [3, 4] свідчить про необхідність його розвитку в напрямі уточнення змісту заходів, що мають при цьому проводитися.

Метою статті є визначення основних напрямів ведення інформаційної боротьби при запобіганні і стримуванні воєнного конфлікту на всіх етапах його розвитку.

Основні зусилля інформаційної боротьби у **фазі зародження воєнного конфлікту** повинні зосереджуватися за такими напрямами:

• створення сприятливого міжнародного клімату навколо країни;

• моніторинг стану інформаційної безпеки країни, виявлення інформаційних загроз та їх нейтралізація;

• консолідація населення, особового складу Збройних Сил навколо політики держави;

• введення противника в оману відносно намірів та можливостей держави щодо відбиття можливої агресії.

Основними складовими інформаційної боротьби у цей період мають бути заходи з інформаційно-психологічної боротьби, зокрема заходи з протидії інформаційно-психологічному впливу з боку країни-агресора, який може бути спрямованим, наприклад, на таке:

• обґрунтування необхідності розв'язання конфліктної ситуації шляхом збройного насильства;

• переконання світової спільноти у справедливості своїх претензій до країни-об'єкта агресії;

• створення коаліції країн-союзників для підтримання своїх намірів, які можуть бути реалізованими цими країнами на будь-якому рівні – політичному, економічному, військовому тощо;

• підтримання міжнародними організаціями доцільності залучення військових контингентів для розв'язання конфліктної ситуації в інтересах забезпечення міжнародної безпеки у певному регіоні;

• переконання населення, особового складу військ країни-об'єкта агресії у неправомірності її воєнно-політичного керівництва щодо відстоювання і захисту своїх національних інтересів, які є предметом конфлікту, тощо.

З метою зриву агресивних планів протидіючої сторони, усунення або зниження воєнно-політичної напруги основні зусилля інформаційної боротьби слід зосередити на здійсненні державними органами, силовими відомствами, іншими структурами комплексу заходів, спрямованих на розв'язання конфліктної ситуації на інформаційному рівні (несиловими методами). Так, адекватною протидією інформаційно-психологічному впливу з боку країни-агресора у комплексі з іншими заходами може бути посилення у засобах масової інформації, зокрема у мережі Internet, пропагандистської кампанії за такими напрямами:

• своє населення – для забезпечення моральної готовності до захисту держави, психологічної стійкості та здатності діяти в умовах проведення противником інформаційно-психологічних операцій;

• свої війська – для забезпечення їх високих морально-психологічних якостей і готовності до виконання завдань, психологічної стійкості до застосування противником інформаційно-психологічної та психотронної зброї;

• населення противника та його союзників – з метою розкриття істинних задумів державного і військового керівництва агресора та формування й підтримання антивоєнних думок і настроїв, негативного ставлення до завдань та мети прогнозованої збройної агресії, небажання прямо чи опосередковано брати участь у конфлікті;

• збройні сили противника – для введення їх в оману відносно планів воєнно-політичного і військового керівництва щодо застосування військ (сил) в операції з ліквідації (локалізації, нейтралізації) збройного конфлікту у разі його розв'язання; погіршення їх морально-психологічного стану, зниження готовності до виконання завдань;

• дружні держави – для отримання від них реальної воєнної, матеріально-технічної, економічної, політичної й інших видів допомоги та впливу на агресора;

• нейтральні держави – для залучення їх на свій бік та формування позитивної суспільної думки відносно ролі своєї країни в конфлікті, розгортання на території нейтральних та дружніх держав своїх центрів інформаційної боротьби.

Для цього доцільно спланувати і провести комплекс відповідних заходів дипломатичного характеру, організувати серію теле- і радіопередач на загальнодержавних і приватних теле- і радіоканалах, а також публікувати у пресі як усередині країни, так і за її межами серії статей, в яких відобразити суворе дотримання державою принципів ООН, ОБСЄ з національних і територіальних питань, намагання її керівництва розв'язати суперечку шляхом відкритих переговорів відповідно до міжнародних законів.

Основною формою ведення інформаційної боротьби в інтересах запобігання воєнній агресії є інформаційно-психологічна операція (ІПсО), яка має проводитися на державному рівні. Враховуючи багатоплановість напрямів інформаційної боротьби, одночасно, послідо-

вно або комбіновано може вестися декілька ІПсО, об'єднаних єдиними цілями і замислом. Взаємозв'язану сукупність цих операцій доцільно розглядати як інформаційно-психологічну кампанію. Термін "інформаційно-психологічна кампанія", незважаючи на те, що нині активно вживається представниками Генерального штабу саме у цьому сенсі, сьогодні ще не набув офіційного статусу. Разом з цим цей термін відбиває поняття, яке за змістом і обсягом (об'єднання декількох ІПсО, трансконтинентальний характер ведення ІПсО, значна тривалість у часі), а також за логікою їх проведення (підпорядкування єдиним цілям і замислу, взаємоузгодженість у просторі і часі) обумовлює правомірність його застосування на державному рівні як форми ведення інформаційної боротьби в інтересах запобігання і стримування воєнного конфлікту. Іншими формами ведення інформаційної боротьби в інтересах запобігання і стримування воєнного конфлікту є інформаційно-психологічні дії та акції.

Основні зусилля інформаційної боротьби на рівні Збройних Сил на цьому етапі зосереджуються на участі в заходах, які проводяться на державному рівні, вивченні інформаційної складової противника, забезпеченні власної інформаційної безпеки.

Участь в інформаційно-психологічній операції (кампанії) повинна бути спрямована на створення позитивного іміджу Збройних Сил. З цією метою доцільно організувати висвітлення в ЗМІ діяльності Збройних Сил у загальнодержавних заходах щодо запобігання воєнному конфлікту. При цьому показати, що Збройні Сили своєчасно реагують на можливу загрозу, мають високу готовність до відсічі збройним підривним діям і агресії та надання допомоги населенню держави (незалежно від етнічної належності), якщо воно постраждає або зазнає збитків внаслідок зазначених подій.

Важливим є вивчення інформаційної складової противника, що передбачає:

- виявлення уразливих місць інформаційної інфраструктури органів державного і військового управління, каналів впливу на інформаційні ресурси автоматизованих і автоматичних систем управління військами й зброєю, озброєння і військової техніки, оснащених засобами інформатизації;
- створення психологічних портретів керівного й особового складу збройних сил, населення противника.

Основними завданнями інформаційної боротьби щодо забезпечення інформаційної безпеки Збройних Сил є:

- захист особового складу Збройних Сил від негативного інформаційного впливу;
- забезпечення встановленого регламенту збирання, обробки, збереження і передачі інформації, яка знаходиться в штабах і установах Міністерства оборони;
- забезпечення надійності функціонування систем і засобів інформатизації;
- забезпечення прихованості управління, режиму секретності, безпеки зв'язку;
- комплексний захист інформації в комп'ютерних мережах;
- адаптація системи інформаційно-аналітичної підтримки прийняття рішень керівним складом органів управління до умов ведення інформаційної боротьби;
- протидія технічній розвідці противника тощо.

У фазі загострення конфлікту проводяться так самі дії, що й у фазі його зародження, але з подальшим нарощуванням інтенсивності заходів щодо інформаційно-психологічного впливу на всіх напрямках ведення інформаційної боротьби.

У загрозливий період інформаційна інфраструктура країни підпорядковується вирішенню завдань інформаційної боротьби, у повному обсязі розгортається система управління з урахуванням забезпечення її максимальної прихованості. Важливим елементом стратегічної інформаційно-психологічної операції стають демонстративні дії Збройних Сил. Розпочинається проведення комплексу заходів маскування, пов'язаного з підготовкою до локалізації району конфлікту, посиленням охорони державного кордону, важливих об'єктів державного управління й економіки, інформаційної інфраструктури. У ЗМІ посилюється інформаційно-пропагандистська кампанія, спрямована на нейтралізацію негативного інформаційно-психологічного впливу противника, консолідацію суспільства і підтримку дій військово-політичного керівництва країни. Особливого значення при цьому набуває створення керованої системи надання інформації. За умови використання противником заходів комп'ютерно-телекомунікаційної боротьби, спрямованих на дезорганізацію систем державного і військового управління, доцільне проведення адекватних дій.

Основними особливостями ведення інформаційної боротьби в цей період є такі:

- гранична обмеженість у використанні сил, способів і засобів інформаційного впливу на противника;
- дотримання існуючих норм міжнародного права на обмеження радіоелектронного придушення певних частот і систем;
- тісна взаємодія силових відомств та інших державних структур у проведенні заходів інформаційної боротьби.

У фазі кризи умовою виходу з конфлікту може бути втручання міжнародних організацій або якоїсь впливової держави. Отже, ефективна дипломатична активність і переконання міжнародної громадської думки в тому, що дії держави є правомірними і не суперечать моралі, під час проведення заходів з використанням власних збройних сил є важливою умовою запобігання воєнному конфлікту.

На цьому етапі інформаційна боротьба стає одним з вирішальних механізмів запобігання. Для її ведення необхідно залучити всі можливі канали, сили і засоби.

Основні зусилля інформаційної боротьби на рівні Збройних Сил повинні зосереджуватись на дезорганізації системи державного і військового управління противника, мереж зв'язку незаконно створених збройних формувань (НСЗФ), а також підриві морально-психологічного стану військовослужбовців, населення противника, членів НСЗФ та їх лідерів.

Проблеми організації і ведення інформаційної боротьби в інтересах запобігання, стримування воєнних конфліктів:

1. Відсутність бачення інформаційної боротьби як одного з найефективніших засобів забезпечення воєнної безпеки держави, вирішення завдань запобігання і стримування воєнної агресії з боку інших країн.

2. Недостатнє відображення ролі інформаційної боротьби при забезпеченні національних інтересів і воєнної безпеки держави у законодавчій і нормативній базі.

У Сполучених Штатах така база створена і розвинена, більш того у кожному виді збройних сил є своя доктрина або настанова з інформаційних операцій.

Особливого значення набуває участь у розробленні пакетів законів і нормативно-правових актів, спрямованих на регулювання механізмів контролю інформаційного простору з боку Генерального штабу в умовах надзвичайного стану (об'єктів інформаційної інфраструктури державної власності, об'єктів інформаційної ін-

фраструктури приватної і сумісної з іноземними компаніями власності тощо).

3. Виявлення ознак інформаційно-психологічних операцій (дій, акцій), спрямованих на розв'язання воєнної агресії проти України, на ранній стадії з метою здійснення превентивних заходів.

4. Відсутність координуючого органу з питань організації і ведення інформаційної боротьби на державному рівні.

Основними завданнями такого органу мають бути:

- координація заходів з моніторингу, спрямованого на виявлення ознак ведення інформаційної боротьби проти держави, інформаційних загроз національним інтересам України, а також заходів щодо їх нейтралізації;
- координація зусиль міністерств та інших центральних органів виконавчої влади з питань підготовки і ведення інформаційної боротьби щодо забезпечення національних інтересів у політичній, воєнній, економічній, інформаційній та інших сферах національної безпеки;
- планування й організація підготовки і ведення інформаційної боротьби на державному рівні;
- ініціювання та безпосередня участь у розробленні нормативно-правових документів, що регулюють механізми здійснення контролю інформаційного простору країни у загрозливий і воєнний періоди, оперативного підпорядкування об'єктів інформаційної інфраструктури Генеральному штабу;
- організація і проведення міжвідомчих спільних навчань з питань підготовки і ведення інформаційної боротьби на державному рівні.

5. Відсутність координуючого органу для координації заходів інформаційної боротьби на рівні Збройних Сил.

Необхідність цього органу обумовлена тим, що заходи інформаційної боротьби на рівні Збройних Сил мають комплексний характер. До їх проведення залучаються відповідні структурні підрозділи Міністерства оборони та Генерального штабу. Тому на координуючий орган доцільно покласти такі завдання:

- сприяння державним органам у здійсненні заходів інформаційної боротьби в інтересах вирішення завдань національної безпеки;
- вироблення замислу ведення інформаційної боротьби в інтересах воєнної безпеки держави та реалізації функцій Збройних Сил;
- планування й організація підготовки і ведення інформаційної боротьби в Збройних Силах;
- організація і безпосередня участь у створенні нормативно-правового забезпечення підготовки і ведення інформаційної боротьби в Збройних Силах;
- організація взаємодії між структурними підрозділами Міністерства оборони та Генерального штабу, а також з міністерствами і відомствами країни з питань підготовки і ведення інформаційної боротьби;
- участь у створенні механізмів контролю за інформаційним простором держави в особливий період.

Вирішення вищерозглянутих проблем сприятиме суттєвому підвищенню рівня інформаційної безпеки держави в цілому та збройних сил зокрема.

1. Основи стратегії національної безпеки та оборони держави: підруч. / Раденький В.Г., Дузь-Крятченко О.П., Лисицин Е.М., ін. 2-ге вид., доп. і випр. – К.: НУОУ, 2010. – 592 с. 2. Закон України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки" від 09.01.2007 № 537-V. 3. Вагапов В.Б., Лисицин Е.М. До проблеми запобігання воєнним конфліктам і стримування їх. – Наука і оборона. – 2004. – №1. – С.12–19. 4. Фомін В.О., Жук С.Я. Інформаційна боротьба в підготовці воєнного конфлікту та запобіганні йому і стримуванні. – Наука і оборона. – 2004. – №4. – с.12–18.

Надійшла до редколегії 30.05.12

УДК 327.8

М.І. Онищук, канд. істор. наук, доц.,
В.П. Лещук

РОЛЬ СОЦІАЛЬНИХ МЕРЕЖ В ПОЛІТИЧНИХ ПРОЦЕСАХ НА БЛИЗЬКОМУ СХОДІ ТА В ПІВНІЧНІЙ АФРИЦІ

У статті вивчається роль соціальних мереж в мобілізації протестних настроїв громадян арабських країн Північної Африки та Близького Сходу на початку 2011 року. Розглядаються події революцій в Тунісі і Єгипті, аналізуються основні причини масових протестів та заворушень. Розглядаються заходи, прийняті в деяких країнах для запобігання розвитку аналогічних соціальних протестів.

Ключові слова: соціальні мережі, протестні настрої, Північна Африка, антиурядові демонстрації, акції протесту.

The article is dedicated to the role of social networks in mobilising protest moods of the citizens of Arab countries in North Africa and the Middle East in early 2011. The author analyses the revolutions in Tunisia and Egypt and considers the main reasons for these mass protests. He studies measures taken in some countries in order to prevent such social protests.

Keywords: social networks, protest moods, North Africa, antiauthority demonstration, protest action.

Постановка проблеми в загальному вигляді. Події, що відбулися на рубежі 2010-2011 рр. в Тунісі, ще зовсім недавно досить стабільній країні прозахідної орієнтації, – так званої "Жасминової революції", що поклала кінець 23-річному періоду правління президента Зін ель-Абідіна Бен Алі, – стали своєрідним детонатором, що підірвали ситуацію в багатьох державах Північної Африки і Близького Сходу.

Багатотисячні антиурядові демонстрації з вимогами радикальних політичних реформ в січні-березні 2011 р. пройшли в Алжирі, Бахрейні, Джібуті, Єгипті, Йорданії, Іраку, Ємені, Лівані, Мавританії, Марокко, Сирії, Судані, Султанаті Оман. Спроби їх проведення мали місце в Кувейті. Громадянська війна розгорілася в Лівії.

Відмінною рисою практично всіх виступів народних мас в країнах Північної Африки та Близького Сходу стало активне використання учасникам протестів глобальної мережі Інтернет, зокрема, різних соціальних мереж для мобілізації протестних настроїв, координації своїх дій, інформування світової громадськості про події.

Значний інтерес представляє використання опозиційними силами соціальних мереж при поваленні державної влади в Тунісі та Єгипті, а також заходи, вжиті в деяких країнах, в першу чергу в Китаї, для запобігання розвитку аналогічних соціальних протестів.

Викладення основного матеріалу. Фахівцями наголошується, що головні події революції в Тунісі розгорталися одночасно на вулицях міст країни і на Інтернет сторінках: основною відмінною рисою туніської революції стало використання соціальних мереж "Facebook" і "Twitter", де її учасники поширювали новини, за допомогою яких організовували протести, що дозволило