УДК 327.84

В.Ю. Богданович, М. С. Дудар

УЗАГАЛЬНЕНА МОДЕЛЬ УПРАВЛІННЯ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОЮ БЕЗПЕКОЮ ВЕЛИКИХ ГРУП ЛЮДЕЙ В УМОВАХ НИЗЬКОГО РІВНЯ СОЦІАЛЬНО-ПОЛІТИЧНОЇ СТАБІЛЬНОСТІ В КРАЇНІ

В статті розглядається методологічний підхід до побудови узагальненої моделі управління інформаційно-психологічною безпекою (ІПсБ) великих груп людей в умовах низького рівня соціально-політичної стабільності в державі. Обгрунтовуються мета, завдання, цільова функція управління. Розглядаються основні завдання, що покладаються на складові узагальненої моделі, а також методичний підхід до формування ієрархічної системи показників оцінювання поточного рівня ІПсБ. Сформульовані умови забезпечення достатнього рівня інформаційно-психологічної безпеки та показані особливості великих груп населення, що проявляються в умовах низького рівня соціально-політичної стабільності в державі.

Ключові слова: інформаційно-психологічна безпека, модель управління, деструктивний інформаційно-психологічний вплив, психологічна безпека, загрози психологічного характеру, управління інформаційно-психологічною безпекою, протидія інформаційно-психологічному впливу, спеціальна інформаційна операція, велика група населення.

Постановка проблеми. Стаття присвячена проблемі захисту широких верств населення від деструктивних інформаційно-психологічних впливів в умовах сучасного інформаційного протиборства. Актуальність проблеми обумовлена недостатньою розробленістю науково-методологічного апарату організації ефективної протидії деструктивним інформаційно-психологічним впливам з боку недружніх держав, що негативно впливає на забезпечення соціально-політичної стабільності в державі.

Аналіз останніх досліджень і публікацій. Проблема інформаційно-психологічної безпеки населення останнім часом знаходить відображення в працях багатьох вчених і фахівців різних галузей (С.Г. Кара-Мурза, Г.В. Грачев, Г.Г.Почепцов, Г.Л. Смолян, Г.М. Зараковський, В.Е. Лепський, В.Н. Лопатін, В.В. Остроухов і ін.). Необхідність створення цілісної системи інформаційно-психологічної безпеки особи, суспільства і держави як складової загальної системи безпеки усвідомлюється і на державному рівні (підтверджують це Доктрина інформаційної безпеки України, Стратегія національної безпеки України і ін.).

В монографії [1] досліджена природа маніпуляції свідомістю як окремих особистостей, так і великих груп людей, але проблема управління інформаційно-психологічною безпекою детально не розглянута. У монографії [2] наводяться фактори, які визначають ефективність психологічної операції, спрямованої на невеликі групи людей. Серед показників виділені прямі і непрямі. Але по цим показникам неможливо коректно оцінювати виявлені деструктивні інформаційно-психологічні впливи, у тому числі спеціальні інформаційно-психологічні операції (СІО), що проводяться проти населення країни.

В публікаціях [3-7] дається загальна характеристика інформаційно-психологічних операцій, але питання оцінювання їх ефективності в цих публікаціях не розглянуті, тому не представляється можливим виявити найбільш суттєві характеристики інформаційних операцій, обґрунтувати критерії оцінювання їх ефективності і, відповідно, обґрунтувати стратегічні вимоги до системи протидії таким операціям з тим, щоб організувати управління інформаційно-психологічною безпекою великих груп людей.

У статті [8] запропонована граф-модель процесу організації протидії спеціальним інформаційним операціям. Проблема організації управління інформаційно-психологічною безпекою великих груп людей не розглянута.

Невирішена раніше проблема. У наведених публікаціях та інших наукових працях, з якими змогли ознайомитися автори, відсутня науково обгрунтована система критеріїв інформаційно-психологічної безпеки великих груп населення, а також діагностичний інструментарій для її оцінювання та організації управління.

Метою даної статті є розробка узагальненої моделі управління інформаційно-психологічною безпекою населення в умовах низького рівня соціально-політичної стабільності в країні.

Викладення основного матеріалу. Проблема психологічної безпеки почала активно розроблятися у зв'язку зі зростанням ролі засобів масової комунікації у житті суспільства. Особлива зацікавленість проявляється до інформаційно-психологічної безпеки великих груп населення. Під великою групою населення будемо розуміти кількісно не обмежену умовну спільноту людей, яка може бути виокремлена на основі певних соціальних ознак, таких як класова приналежність, стать, вік, національність тощо, це може бути також організована спільнота людей, що залучені до деякої суспільної діяльності (наприклад, колектив великого підприємства, політична організація, фанати футбольної команди, члени релігійної секти і ін.) [18].

Під управлінням інформаційно-психологічною безпекою великих груп населення (людей) будемо розуміти процес захисту структури цінностей, історичних, культурних, сімейних та інших традицій, мотивів, цілей, устремлінь, психічного здоров'я, світогляду як окремих осіб, так і всієї групи від деструктивних інформаційно-психологічних впливів (загроз), у тому числі руйнівного та деформуючого характеру.

Інформаційно-психологічну безпеку особи та великої групи населення (ВГН) будемо розглядати з позицій прояву інформаційного та психологічного впливів на індивідуальну та суспільну свідомість, які відображають відношення ВГН та їх окремих членів до навколишнього сьогодення та майбутнього.

Результати проведених досліджень свідчать про те, що досягнення поставлених цілей у сфері забезпечення інформаційно-психологічної безпеки практично неможливе без розробки і послідовного проведення єдиної гнучкої державної політики, без створення і впровадження в життя єдиної системи взаємоузгоджених і всебічно зважених заходів економічного, політичного, інформаційного і організаційного характеру, адекватних загрозам життєво важливим інтересам суспільства і держави [9].

Безперечно, що всебічне дослідження можна провести лише за допомогою відповідних моделей, для чого і пропонується розробити узагальнену модель управління інформаційно-психологічною безпекою (УМУІПсБ) великих груп людей, яка б враховувала особливості, що проявляються в умовах низького рівня соціально-політичної стабільності в країні.

У основу побудови **УМУІПсБ** повинні бути закладені наступні принципи:

• принцип відкритості моделі, що дає можливість нарощувати модель додатковими модулями у разі потреби, використовувати єдину базу даних і гарантувати надійний інформаційний захист від різного роду інформаційних дій;

• принцип генерації сценаріїв, що дозволяє моделювати альтернативні сценарії розвитку соціально-політичної ситуації в країні;

• принцип фільтрації запропонованих заходів, що дає можливість обгрунтовувати варіанти стратегічних рішень на підставі певних критеріїв, пріоритетності використання несилових методів вирішення проблем у сфері забезпечення інформаційно-психологічної безпеки держави, гарантій, що діють, і обмежень в системі забезпечення інформаційної безпеки України;

• принцип адаптації до реального інформаційно-психологічного протиборства, що дає можливість обгрунтовувати заходи щодо забезпечення інформаційно-психологічної безпеки, адекватні рівню, напряму, характеру і масштабу реальних інформаційно-психологічних загроз;

• принцип модульності, відповідно до якого допускається заміна окремих часткових моделей (модулів) точнішими і вдосконаленими, а також нарощування загальної моделі.

У зв'язку з цим до **УМУІПсБ** висуваються такі основні вимоги:

• забезпечення об'єктивної оцінки рівня інформаційно-психологічної безпеки вибраних ВГН та тенденцій його зміни в часі і просторі;

• прогнозування розвитку інформаційно-психологічного протиборства за участю вибраних ВГН, виявлення найбільш критичних сценаріїв деструктивних інформаційно-психологічних впливів;

• оцінка ефективності заходів, які пропонуються для підвищення рівня інформаційно-психологічної безпеки в системі забезпечення інформаційної безпеки держави;

• проведення розрахунків достатнього рівня ІпсБ ВГН для нейтралізації розглянутих загроз, у разі потреби з оцінками необхідних для цього фінансових і матеріальних ресурсів;

• обґрунтування рекомендацій щодо адаптації політики національної, інформаційної безпеки держави, та політики забезпечення ІПсБ ВГН до реального характеру інформаційно-психологічного протиборства, в яке залучена держава на конкретний проміжок часу і на перспективу.

УМУІПсБ розробляється на методології системного аналізу, методах дослідження операцій, аналізу ієрархій, теорії імовірності і прогнозування, експертного оцінювання і моделювання і може використовуватися вищим політичним керівництвом держави в ситуаційних центрах управління при плануванні і здійсненні цілеспрямованої політики по забезпеченню необхідного рівня ІПсБ держави, окремих ВГН, а також в учбових, наукових і дослідницьких установах при вивченні проблем протидії деструктивним інформаційно-психологічним впливам.

Оскільки практична розробка **УМУІПсБ** виходить за рамки даної публікації, то обмежимося в основному лише її узагальненою структурною схемою, рис.1, і короткими коментарями щодо призначення, вимог, вирішуваних завдань, вхідної інформації і вихідних даних для окремих модулів моделі.

Для розробки **УМУІПсБ** необхідно сформувати модель вектора (системи) загроз. В даний час немає досить обгрунтованої і детальної загальної класифікації загроз інформаційно-психологічній безпеці і їх джерел. Це пов'язано з новизною і складністю цієї проблематики, а також з тим, що сама процедура і результат класифікації залежать від тих завдань, які необхідно вирішити, і у зв'язку з цим - від обираних підстав і критеріїв, які використовуються при класифікації [19].

При розробці УМУІПсБ нас більше цікавитимуть загрози від дій тих людей, які, переслідуючи власні цілі, використовуючи різні способи інформаційно-психологічної дії на інших, без врахування їх інтересів, а частенько, просто вводячи в оману, діючи врозріз з їх інтересами, завдають їм збитку. Це діяльність різних осіб - від політичних лідерів, державних і суспільних діячів, представників засобів масової комунікації, літератури і мистецтва, до повсякденних партнерів по міжособовій взаємодії. До цих осіб відносяться ті з них, хто, надаючи на тих, що оточують, інформаційно-психологічну дію, майстерно змішуючи брехню з правдою, збільшують міру неадекватності інформаційного середовища суспільства і тим самим розширюють ілюзорну суб'єктивну реальність.

Доступ до широкомасштабного використання нових інформаційних технологій і контролю за засобами масової комунікації, впровадження і функціонування інститутів так званого громадянського суспільства, що фінансуються іншими державами, багато разів підсилює можливості інформаційно-психологічної дії на людей за допомогою зміни інформаційного середовища суспільства. Найбільшою мірою це можливо для ВГН - різних об'єднань людей, соціальних груп, суспільних, політичних і державних структур, деяких соціальних інститутів суспільства.

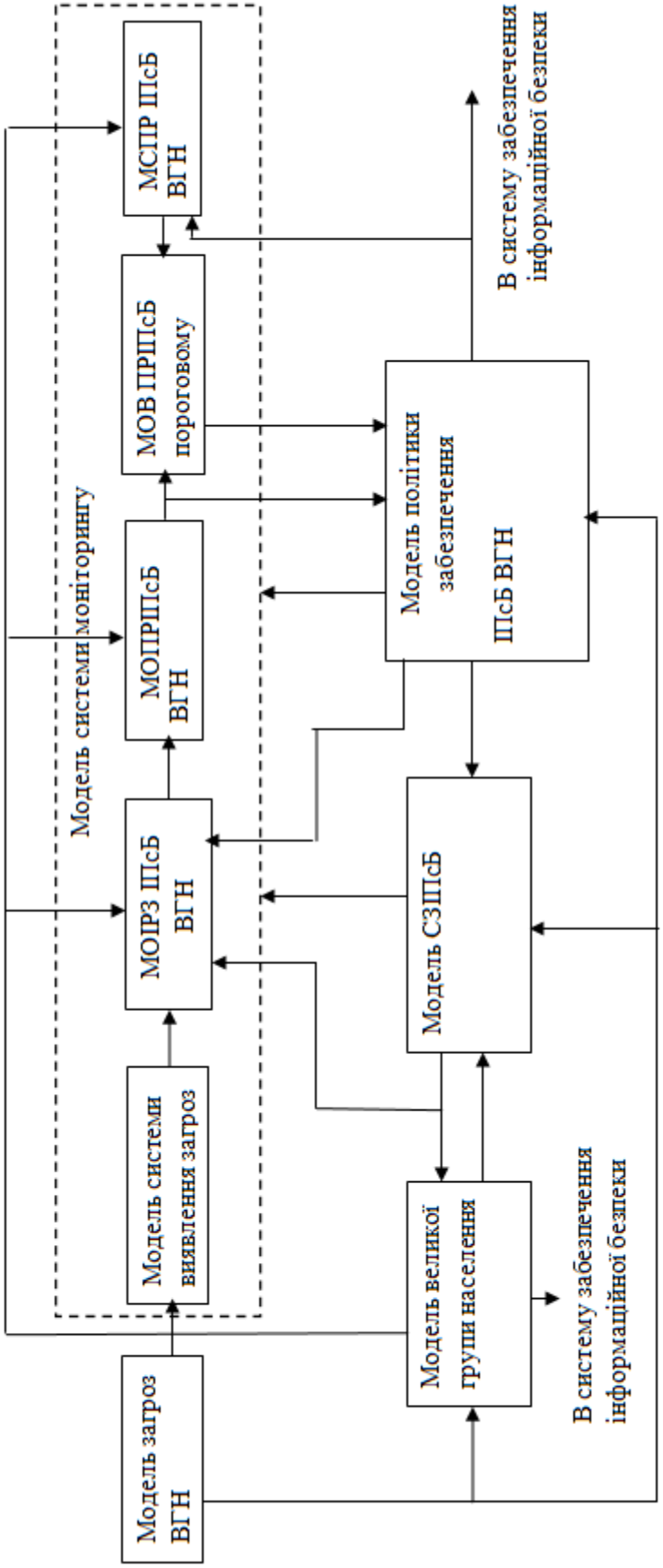

Рис. 1. Узагальнена модель управління інформаційно – психологічною безпекою (ІПсБ) великих груп населення (ВГН): МОІРЗ – модель оцінювання інтегрального рівня загроз ІПсБ ВГН; МОПРІПсБ – модель оцінювання поточного рівня ІПсБ; МОВ – модель оцінювання відповідності; СЗІПсБ – система забезпечення ІПсБ; МСПР – модель системи порогових рівнів.

У зв'язку з цим виділяються три відносно самостійних групи джерел загроз ІПсБ. Так, для особи і ВГН може представляти інформаційно-психологічну небезпеку діяльність різних угруповань і об'єднань людей, зокрема, деяких політичних партій, інститутів, центрів, суспільно-політичних рухів, націоналістичних і релігійних організацій, фінансово-економічних і комерційних структур, груп лобістів і мафіозних і тому подібне.

Їх діяльність стає небезпечною, коли для досягнення своїх цілей вони починають застосовувати різного роду засоби інформаційно-психологічної дії, змінюючи за допомогою цього поведінку людей в своїх ціях. Як ще одне джерело загроз інформаційно-психологічній безпеці і особи і ВГН за певних умов можна виділити саму державу, органи державної влади і управління. Це пов'язано з діями державних лідерів, правлячої еліти. Небезпека виникає, коли вони, реалізовуючи власні інтереси, а інколи і просто амбіції, використовують потужність державного апарату для надання інформаційно-психологічної дії на людей, маскуючи свої дії і дійсні цілі, які не відповідають інтересам держави, суспільства і населення країни. Як найважливіше джерело небезпек такого роду, що діє постійно і усе більш активно і могутньо, можуть розглядатися також інші держави, що ведуть масовані спеціальні інформаційні (психологічні) операції (СІО) проти населення або окремих ВГН країни, вибраної як їх "мішень" (об'єкту дії), або що здійснюють зовнішнє управління цією країною.

З врахуванням викладеного, система загроз інформаційно-психологічного характеру може бути представлена зовнішніми та внутрішніми негативними інформаційними пливами на суспільну свідомість через засоби масової інформації, а також мережу Інтернет [20]:

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

• використання засобів масової інформації, а також мережі Інтернет для пропаганди сепаратизму за етнічною, мовною, релігійною та іншими ознаками;

• інформаційно-психологічний вплив на населення України, у тому числі на особовий склад військових формувань, з метою послаблення їх готовності до оборони держави та погіршення іміджу військової служби;

• негативні інформаційні впливи, в тому числі із застосуванням спеціальних засобів, на індивідуальну та суспільну свідомість;

• поширення суб'єктами інформаційної діяльності викривленої, недостовірної та упередженої інформації;

• поширення в засобах масової інформації невластивих українській культурній традиції цінностей і способу життя, культу насильства, жорстокості, порнографії, зневажливого ставлення до людської і національної гідності;

• тенденція до витіснення з інформаційного простору та молодіжної культури українських мистецьких творів, народних традицій і форм дозвілля;

• послаблення суспільно-політичної, міжетнічної та міжконфесійної єдності суспільства;

• відставання рівня розвитку українського кінематографу, книговидання, книгорозповсюдження та бібліотечної справи від рівня розвинутих держав;

• дезорганізація і руйнування системи накопичення і збереження культурних цінностей, включаючи архіви;

• обмеження доступу громадян до відкритих державних інформаційних ресурсів органів державної влади, іншої суспільно значимої інформації;

• зниження духовного, етичного і творчого потенціалу ВГН.

До системи загроз психологічного характеру слід віднести:

• ескалація рівня психологічної напруженості населення унаслідок збільшення числа стресових ситуацій в населених пунктах, в колективах, на виробництві, в сім'ях;

• підвищення психологічної напруженості в населення унаслідок посилення відчуття соціальної незахищеності;

• зіставлення поколінь на основі відмінності сповіданих цінностей, різниці в умовах життя і мотивації;

• інформаційне нав'язування "західних" стереотипів сприйняття, мислення, поведінки, упроваджуваних в свідомість ВГН без врахування особливостей українського менталітету;

• втрата віри в професіоналізм, чесність і порядність політичних лідерів;

• зростання числа психічних захворювань;

• зростання вжитку алкоголю, поширення наркоманії;

• формування культу багатства (за рахунок придбання матеріального благополуччя будь-якими засобами), агресії і насильства, і, як наслідок цього, втрата орієнтації на етичні, духовні і культурні цінності.

В умовах низького рівня соціально-політичної стабільності підвищується навіюваність людей, і, відповідно, зростає схильність до інформаційно-психологічних дій. Вона також зростає в умовах знаходження особи в масових скупченнях людей, в натовпі, на мітингу, демонстрації.

Модель системи виявлення загроз (МСВЗ) є складовою моделі системи моніторингу загроз. В основу її функціонування закладається метод співставлення розглядаємих фактів, подій з загрозами, що внесені в реєстр загроз інформаційно-психологічного характеру [9].

Модель оцінювання інтегрального рівня загроз (МОІРЗ) інформаційно-психологічній безпеці ВГН є другою складовою моделі системи моніторингу загроз. МОІРЗ повинна налаштовуватися на вибраний вектор загроз, враховувати вимоги політики безпеки щодо забезпечення достатнього рівня ІПсБ вибраної ВГН [9], а також ефективність впроваджених технологій захисту та додаткових або скорегованих заходів, що реалізуються в системі забезпечення ІПсБ ВГН.

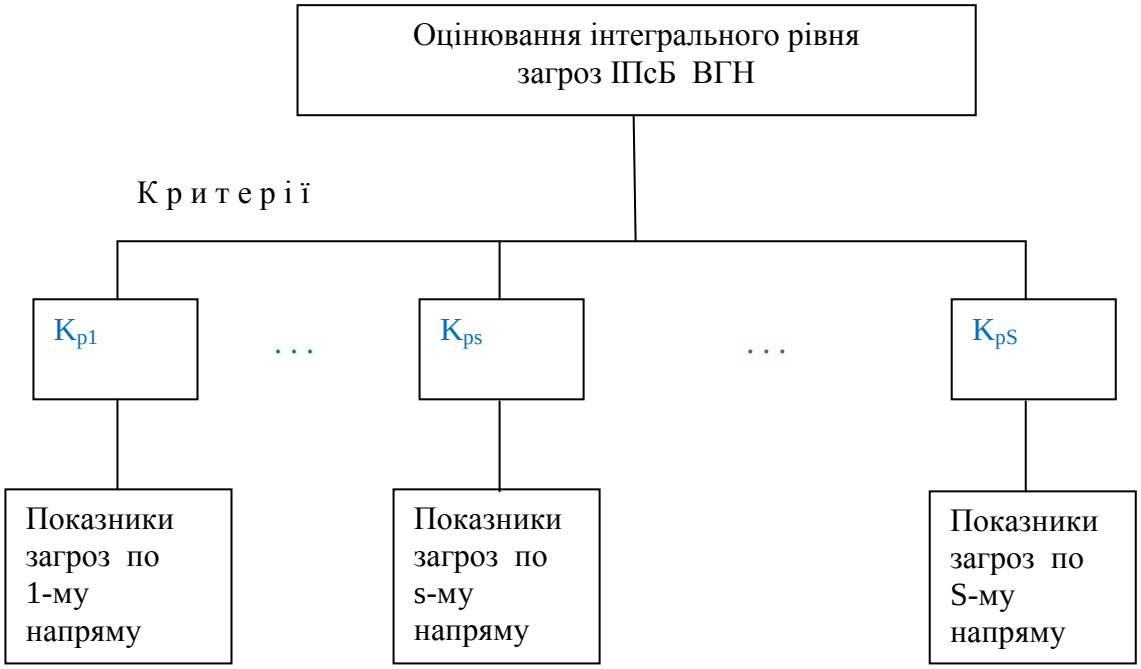

Рис.2. Трирівнева модель оцінювання інтегрального рівня загроз інформаціно-психологічній безпеці великої групи населення.

МОІРЗ доцільно будувати на основі удосконаленого методу аналізу ієрархій (MAI) у вигляді трирівневої ієрархії [9,15], рис.2., де на першому рівні визначена мета - оцінювання інтегрального рівня загроз ІПсБ вибраної ВГН; на другому рівні- Критерії (напрями) деструктивних інформаційно-психологічних впливів Kps, s=1,S , де S –кількість критеріїв

(напрямів). На третьому рівні для кожного s-го критерія розміщуються показники (індикатори) ступеня деструктивного інформаційно-психологічного впливу. Детально процедура побудови трирівневої ієрархії описана в [9]. Для кількісного оцінювання інтегрального рівня загроз ІПсБ може бути використана комп'ютерна технологія М7 [9] , яка дозволяє отримувати як поточні оцінки, так і прогнозні в межах від 0 до 1.

Модель оцінювання поточного рівня (МОПР) ІПсБ є третьою складовою моделі системи моніторингу загроз, у залежності від оціненого інтегрального рівня загроз на момент часу $\mathbf{t_{оц}}$ формує кількісну оцінку поточного рівня ІПсБ ВГН $B_{ps}(\mathbf{t_{оц}})$ в інтервалі від 0 до 1 ($0 \leq B_{ps}(\mathbf{t_{оц}}) \leq 1$).

Модель системи порогових рівнів (МСПР) є четвертою складовою моделі моніторингу загроз, містить порогові (допустимі) рівні деструктивних інформаційно-психологічних впливів за вибраними напрямами, по яким оцінюється пороговий рівень ІПсБ ВГН $B_{psp}(\mathbf{t_{оц}})$ ($B_{psp}(\mathbf{t_{оц}}) < 1$).

У моделі оцінювання відповідності поточного рівня (МОПР) ІПсБ пороговому проводиться порівняння поточного рівня $B_{ps}(\mathbf{t_{оц}})$ з пороговим $B_{psp}(\mathbf{t_{оц}})$. Якщо поточний рівень $B_{ps}(\mathbf{t_{оц}}) > B_{psp}(\mathbf{t_{оц}})$, то вважається, що політика забезпечення ІПсБ достатня і не потребує корегування, а система забезпечення ІПсБ активного втручання.

Якщо $B_{ps}(\mathbf{t_{оц}}) \leq B_{psp}(\mathbf{t_{оц}})$, то формується сигнал щодо корегування політики забезпечення ІПсБ. Зазначені умови визначають зміст цільової функції системи управління ІПсБ великих груп населення. Слід зазначити, що в умовах низького рівня соціально-політичної стабільності в державі порогові рівні психологічної безпеки суттєво знижуються. Напрями політики, а також зміст і масштаб потрібного реагування системою забезпечення ІПсБ буде визначатися величиною невідповідності $\Delta(\mathbf{t_{оц}})$ та характером загроз, яким при оцінюванні поточного рівня ІПсБ надано найбільші пріоритети. Більш детально ці процедури будуть описані в наступних публікаціях.

Література

1.Кара-Мурза С.Г. Манипуляция сознанием.-М.: Изд-во: Эксмо, 2005.-832 с.

2.Почепцов Г. Информационные войны [інформаційний ресурс] / Г.Почепцов –Монографія.- Режим доступу: www.novsu.ru/file/145368

3.Литвиненко О.В. Спеціальні інформаційні операції та пропагандистські кампанії: монографія / О.В.Литвиненко.- К.: ВКФ «Сатсанга», 2000.-225с.

4.Литвиненко О.В. Інформаційні впливи та операції. Теоретико-аналітичні нариси: монографія / О.В.Литвиненко.- К.: НІСД, 2003.-240с.

5. Круглов В. Концепция информационно-ударной операции в современной войне / В.Круглов, Д.Ловцов // М.: Обозреватель. – 1999.- № 12.- С. 49-51.

6.Жуков В. Взгляды военного руководства США на ведение информационной войны / В.Жуков // Зарубежное военное обозрение.- 2002.- № 1.-С.3-5.

7. Вепринцев В. Операции информационно-психологической войны [електронний ресурс] / В. Вепринцев, А.Манойло, А.Петренко, Д.Фролов // Режим доступу: http://psyfactor.org/psyops/psyops4.htm

8.Богданович В.Ю., Міщенко Д.А. Граф-модель процесу організації протидії спеціальним інформаційним операціям / В.Ю.Богданович, Д.А.Мішенко.-К.: НА СБУ Інформаційна безпека людини, суспільства, держави.- №1 (8), 2012.-с.58-64.

9. Богданович В.Ю., Свида І.Ю., Скулиш Є.Д. Теоретико-методологічні основи забезпечення національної безпеки України: Монографія. : у 7 т..-Т.1.Теоретичні основи, методи й технології забезпечення національної безпеки України / В.Ю.Богданович, І.Ю.Свида, Є.Д.Скулиш; за заг. ред. Є.Д.Скулиша.-К.:Наук.-вид. відділ НА СБ України, 2012.-548с.

10. Указ Президента України від 12 лютого 2007 року №105. Стратегія національної безпеки України «Україна у світі, що змінюється» (в редакції Указу Президента України від 8 червня 2012 року № 389/2012).

11. Богданович В.Ю. Методичний підхід до агрегування засобів інформаційно-аналітичного забезпечення протидії інформаційним загрозам / В.Ю.Богданович, А.Л.Висідалко // К.: Наук.-вид. відділ НА СБ України, 2012, №3 (10). с. 18-28.

12. Богданович В.Ю. Забезпечення безпеки інформаційних процесів безпекового супроводу реалізації національних інтересів / В.Ю.Богданович, А.Л.Висідалко // Київ: ДУТ: Сучасний захист інформації, №3, 2013, с.60-66.

13. Богданович В.Ю. Концептуальна модель інформаційно-моніторингової системи національної безпеки / В.Ю.Богданович, А.Л.Висідалко // Київ: НАУ: Захист інформації, Том 16, №1, 2014, с.81-88.

14.Манойло А.В. Государственная информационная политика в особых условиях / А.В. Манойло: Монография.- М.: МИФИ, 2003. – 388 с.

15.Богданович В.Ю. Критерії, модель та методика оцінювання ефективності протидії спеціальним інформаційним операціям / В.Ю.Богданович, Д.А.Міщенко.- К.: НА СБУ Інформаційна безпека людини, суспільства, держави.- №2 (9), 2012.-с.78-87

16. Thomas L. Saaty. Multi-decisions decision-making: In addition to wheeling and dealing, our national political bodies need a formal approach for prioritization / Thomas L. Saaty // University of Pittsburgh, 322 Mervis Hall, Pittsburgh, PA 15260, United States / Mathematical and Computer Modelling 46 (2007) 1001–1016. [Електронний ресурс]. - Режим доступу: www.elsevier.com/locate/mcm.

17.R. Whitaker. Validation examples of the Analytic Hierarchy Process and Analytic Network Process / R. Whitaker // Pittsburgh, PA, USA / Mathematical and Computer Modelling 46 (2007) 840–859. [Електронний ресурс]. - Режим доступу: www.elsevier.com/locate/mcm.

18. Понятие и виды больших социальных групп [інформаційний ресурс] / Режим доступу: http://psyera.ru/5370/ponyatie-i-vidy-bolshih-socialnyh-grupp.

19. Грачев Г.В. Информационно-психологическая безопасность личности: состояние и возможности психологической защиты /Г.В.Грачев [інформаційний ресурс] / Режим доступу: http://bookap.info/psywar/grachev/gl7.shtm

Надійшла 14.11.2014 р. Рецензент: д.т.н., проф. Шевченко В.Л.