УДК 007 + 159.98 **doi: 10.26906/SUNZ.2018.6.116**

Серпухов О. В.[1], Макогон О. А.[1], Новік С. А.[2], Клімов О. П.[1], Ковальов І. О.[1], Базелюк В. М.[1]

[1] Військовий інститут танкових військ НТУ "ХПИ", Харків, Україна
[2] Національний технічний університет "Харківський політехнічний інститут", Харків, Україна

ДОСЛІДЖЕННЯ МОДЕЛІ МІЖНАРОДНОГО ІНФОРМАЦІЙНОГО ПРОСТОРУ З МЕТОЮ ПОШУКУ ЕФЕКТИВНИХ МЕХАНІЗМІВ ЗАХИСТУ НАЦІОНАЛЬНОГО ІНФОРМАЦІЙНОГО СУВЕРЕНІТЕТУ

Предметом вивчення в статті є процес виникнення та розвитку інформаційних загроз безпеці України у воєнній сфері. **Метою дослідження** є аналіз деструктивних впливів на національний інформаційний суверинитет, пошук ефективних шляхів протидії і механізмів захисту. **Задачі:** на основі структурно-функціонального аналізу моделі міжнародного інформаційного простору (МІП) визначити загрози та потенційні небезпеки інтеграції України у міжнародний інформаційний простір, смоделювати процес проведення інформаційних атак, що здійснюються у МІП, та розробити оптимальний порядок профілактичних заходів щодо забезпечення інформаційної безпеки та інформаційного суверинитету у воєнній сфері. Використовуваними є **методи** системного аналізу та статистичної обробки даних. Отримані такі **результати.** За умов глобальної інтеграції та жорсткої міжнародної конкуренції МІП стає ареною зіткнень і боротьби різновекторних національних інтересів. У зв'язку з цим дослідження реальних та потенційних загроз негативних впливів на Україну у міжнародному інформаційному просторі та створення дієвої системи захисту і протидії дискредитації України на міжнародному рівні набувають значимої актуальності. Застосування "м'якої" сили у сучасних інформаційних технологіях дає змогу реалізувати власні інтереси у МІП. Контент-моніторинг МІП 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. Основними профілактичними заходами щодо забезпечення інформаційної безпеки та інформаційного суверинитету у воєнній сфері є своєчасне виявлення, класифікація та контроль факторів дестабілізації, ідентифікація загроз та розробка і виконання заходів щодо їх нейтралізації. Ефективне здійснення заходів захисту національного інформаційного суверинитету та протидії дискредитації України на міжнародному рівні неможливе без виховання інформаційної культури суспільства у цілому, і у майбутніх офіцерів зокрема. **Висновки.** У роботі проведено дослідження моделі міжнародного інформаційного простору з метою аналіза деструктивних впливів та пошуку шляхів протидії дискредитації України на міжнародному рівні. На основі аналізу умов і чинників, які впливають на процес виникнення та розвиток інформаційних загроз, визначено таку динаміку розвитку інформаційного деструктивного впливу: "чинник інформаційної загрози – проява інформаційної загрози – реалізація загрози (інформаційний вплив) – результати впливу". В якості профілактичного заходу щодо забезпечення інформаційної безпеки та інформаційного суверинитету у воєнній сфері пропонується контент-моніторінг МІП. У роботі розглядаються шляхи реалізації основних етапів контент-моніторингу МІП із своєчасного виявлення та ефективної протидії інформаційно-психологічним операціям. Крім того, зазначено необхідність виховання інформаційної культури майбутніх офіцерів у фокусі проблем інформаційної безпеки України та протидії деструктивним інформаційним впливам.

Ключові слова: модель міжнародного інформаційного простору, контент-моніторинг, ынформаційний суверинитет.

Вступ

Постановка проблеми та завдання дослідження. Конфлікти політичних та економічних інтересів держав загострюють проблеми у сфері інформаційних відносин, формування інформаційних ресурсів і користування ними. У теперішній час найбільш актуальною формою конфронтації між державами стають так звані "гібридні" війни. Методи саме такої війни активно використовують могутні країни в сучасному міжнародному інформаційному просторі для впливу на супротивника.

Питання забезпечення інформаційної безпеки України та протидії деструктивним інформаційним впливам сьогодні набуває актуальность, оскільки основними загрозами, визначеними Стратегією національної безпеки України, є ведення інформаційної війни проти нашої країни та відсутність цілісної комунікативної політики держави, недостатній рівень медіакультури суспільства [1].

Створення потужного національного інформаційного простору (НІП) як головного аспекту присутності держави в міжнародному інформаційному просторі є стратегічним завданням інформаційної безпеки України. Таке завдання включає створення системи захисту власного інформаційного суверинитету.

З цього приводу пріоритетними завданнями забезпечення інформаційної безпеки держави дослідники вважають: виявлення, оцінку та прогнозування поведінки джерел загроз інформаційній безпеці; вироблення, координацію та введення єдиної державної політики у галузі інформаційної безпеки; створення та експлуатацію систем забезпечення інформаційної безпеки; розробку, координацію та запровадження єдиної державної політики у галузі міжнародних інформаційних відносин, зокрема у напрямку формування іміджу держави [5].

Аналіз останніх досліджень і публікацій. Специфіка забезпечення інформаційної безпеки знайшла відображення в Законі України "Про національну безпеку України" [2], в Законі України "Про національну програму інформатизації" [3], у Концепції національної програми інформатизації, схваленої Законом України "Про Концепцію Національної програми інформатизації" [4].

Проблемам інформаційної безпеки у цілому та України зокрема присвятили свої наукові розробки М. Галамба, Ф. Медвідь, В. Остроухов, В. Петрик, М. Присяжнюк та інші вчені [6 – 9].

Незважаючи на значну увагу до дослідження інформаційного компоненту гібридних війн, механізми протидії дискредитації України у міжнародному інформаційному просторі та запобігання порушенню національного інформаційного суверинитету, вивчені недостатньо.

Метою роботи є дослідження моделі міжнародного інформаційного простору з метою аналіза деструктивних впливів на національну безпеку та пошуку шляхів протидії дискредитації України на міжнародному рівні і ефективних механізмів захисту національного інформаційного суверинитету.

Виклад основного матеріалу

1. Основні чинники використання міжнародного інформаційного простору в деструкційних цілях. Міжнародний інформаційний простір (МІП) визначається як сума складних інформаційних технологій, які є основою і визначальним компонентом промислово-економічного комплексу транснаціональних спільнот, які впливають на формування світоглядних процесів у суспільстві [10].

Основними структурними складовими моделі інформаційного простору в синергетичному поданні є інформаційні поля та інформаційні потоки.

Використаня МІП у деструктивних цілях може характеризуватися такими чинниками:

- територія розповсюдження інформації за допомогою глобальної системи комунікацій;
- інфраструктура або технологічні засоби і можливості зберігання, обробки і розповсюдження інформації по вертикалі та горизонталі;
- наявність міжнародної та національної інформаційної політики, комплексу норм і принципів, що регулюють функціонування та використання міжнародної інформації;
- наявність міжнародних угод в галузі комунікацій, які базуються на розумінні світової ролі МІП, і його впливу на розвиток цивілізацій;
- доступ до інформації світової громадськості і участь суб'єктів міжнародних відносин у загальній системі зв'язку.

1.1 Міжнародний інформаційний простір як об'єкт інформаційно-психологічних операцій. У наш час очевидно, що інформація стала чинником, здатним призвести до масових протестних акцій, проявів сепаратизму, військових конфліктів, дезорганізації державного управління, тощо [6].

Саме формування іноземними засобами масової інформації альтернативної до дійсності викривленої інформаційної картини світу, в тому числі через призму подій в Україні, приниження української мови і культури, фальшування української історії тощо, є однією з форм ведення ін формаційної війни проти нашої держави [1].

В умовах формування міжнародного інформаційного простору в сучасних конфліктах з'явилася нова фаза – інформаційно-психологічна війна. Також необхідно збереження негативну тенденцію до розміщення публікацій з гострими і упередженими висловлюваннями іноземних громадських та державних діячів, що межують із відвертим нехтуванням вимог міжнародного та українського права. Головними інформаційним спрямуваннями іноземних країн, які використовують МІП не тільки для пропагування власних інтересів, а й у деструктивних цілях на територіях, що являються об'єктами геополітичних інтересів суміжних держав, є наступні:

- підрив авторитету вищих органів державної влади в Україні;
- ідеологічне обґрунтування федералізації України із трактуванням приналежності в минулому окремих регіонів України до суміжних країн;
- поширення автономістських та сепаратистських настроїв у регіонах геополітичних інтересів;
- інформаційна підтримка громадських об'єднань та рухів радикального і сепаратистського налаштування з відвертою антиукраїнською ідеологією;
- створення передумов виникнення конфліктів на національному підґрунті, що може бути використано для "виправдання" самопроголошення нових територіальних автономних утворень.

Основними складовими МІП, які становляться об'єктами деструктивного інформаційного впливу, визначеними В. Остроуховим, є:

- ідеологічно-психологічне середовище суспільства, пов'язане з використанням інформації, інформаційних ресурсів та інформаційної інфраструктури для здійснення впливу на психіку й поведінку людей;
- ресурси, які розкривають духовні, культурні, історичні, національні цінності, традиції, надбання держави, нації в різних сферах життя суспільства (кінематограф, художнє мистецтво, література, тощо);
- інформаційна інфраструктура, тобто усі проміжні ланки між інформацією та людиною;
- система формування суспільної свідомості (світогляд, політичні погляди, загальноприйняті правила поведінки тощо);
- система формування громадської думки;
- система розроблення та прийняття політичних рішень;
- свідомість та поведінка людини [9].

1.2 Загрози та потенційні небезпеки інтеграції України у міжнародний інформаційний простір. 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.

Основними напрямками реалізації інформаційної політики можна вважати такі:

- розбудова національного інформаційного простору (ЗМІ);
- розвиток інформаційного суспільства (е-уряд, е-банкінг);

- розвиток офіційної комунікації (інформування громадськості, формування позитивного іміджу держави);

- забезпечення інформаційної безпеки держави (захист інформаційного суверенітету та інформаційних прав та свобод громадян, визначення режимів функціонування інформації, тощо).

Аналізуючи весь спектр засобів для реалізації зовнішньої інформаційної експансії, можна стверджувати, що головними потенційними небезпеками для України можуть бути наступні:

1.3 Використання Інтернет-ресурсів з метою дискредитацію України на міжнародному рівні. Поруч із застосуванням традиційних засобів масової інформації, варто також відзначити важливу роль у розгортанні та проведенні інформаційних війн через можливості Інтернет-ресурсів, соціальних мереж та блогосфери. Як свідчить аналіз останніх подій в Україні та за її межами, широкого застосування набули соціально орієнтовані інформаційно-комунікаційні сервіси – соціальні мережі, мікроблоги, блоги, відеоблоги. Якщо раніше використання таких сервісів розглядалося як виняток, то на сьогодні цей механізм перетворився на технологію, яка становить загрозу національній безпеці. З огляду на транскордонний характер Інтернет-сервісів, майданчиком для застосування подібної технології може стати будь-яка держава. Соціально орієнтовані інформаційно-комунікаційні сервіси забезпечують швидке, анонімне (за винятком окремих випадків), майже безкоштовне оповіщення великої кількості людей.

З урахуванням мобільності клієнтських пристроїв інформацію щодо координації дій розрізнених груп людей можна оперативно змінювати. Соціальні сервіси забезпечують самоорганізацію користувачів у "групи за інтересами", що зумовлює ефективність інформаційного впливу: завдяки сегментації соціального простору є можливість абсолютно точно вибирати цільову аудиторію. 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 деструктивного впливу: "чинник інформаційної загрози – проява інформаційної загрози – реалізація загрози (інформаційний вплив) – результати впливу".

Загалом, механізми, які впроваджуються для здійснення інформаційного тиску як на населення України, так і на країни-"союзники", є тотожними, вирізняючись тільки інформаційним наповненням залежно від поставленої мети у той чи інший період.

Для досягнення кінцевого результату, який полягає у створенні вигідного інформаційного поля, використовуються підконтрольні ЗМІ, представники еліти, політичні партії, фінансовий сектор, неурядові організації, експертне та культурне середовище.

1.4 Механізми використання МІП у деструктивних цілях. Характеризуючи можливі інструменти, які застосовуються країнами-агресорами як для модерації українських та закордонних інформаційних потоків, так і для "знешкодження небажаних", варто виокремити такі:

- розрив комунікацій (купівля рейтингових ЗМІ, блокування роботи "ворожих" ЗМІ, їх дискредитація, адміністративний тиск, організація DDoS-атак на інформаційні Internet-сайти, тощо);

- інформаційна деморалізація (залякування населення шляхом поширення суперечливих і взаємовиключних даних, підкуп авторитетних експертів-спікерів для їх участі в інформаційних проектах, систематична дезінформація населення і керівництва "ворожих" держав, тощо);

- розбалансування системи управління інформаційним полем (поширення компромату на провідні ЗМІ та журналістів, придбання і створення власних позицій у адміністративно-регуляторному секторі та ін.).

В цьому контексті слід також згадати поняття "м'якої" сили, застосування якої спрямовано на досягнення переваг внаслідок використання інформаційно-психологічних впливів дипломатичного, політично-пропагандистського та суспільно-культурного характеру.

У "м'якій силі" в концентрованому вигляді знаходить своє вираження національна ідея країни та її місія в глобальному світі. Сукупність даних факторів сприяє створенню привабливого й ефективного іміджу країни на міжнародному рівні. Саме процеси глобалізації у МІП, розвиток новітніх інформаційних технологій радикально підвищили значення комунікаційних процесів та інформаційних впливів. Так, подальших досліджень потребують як питання протидії зовнішньої "м'якої" силі так і вибудування власної стратегії розвитку стратегії "м'якої" сили через реалізацію гуманітарного потенціалу, пропаганду культурних цінностей, ідей демократії і т.ін. [11].

Викладене вище схематично можна проілюструвати схематично, виділивши структуру міжнародного та національного інформаційного простору як показано на рис. 1.

Рис. 1. Модель міжнародного та національного інформаційного простору

2. Заходи щодо протидії дискредитації України на міжнародному рівні. Враховуючи сучасний стан захисту національного інформаційного простору, а також особливості ведення сучасної інформаційної війни, її методи та механізми реалізації деструктивних інформаційних акцій, Україні доцільно вибудувати ефективну стратегію захисту інформаційного суверинитету із врахуванням усіх наявних викликів та загроз, особливо у воєнній сфері.

Фахівці зазвичай поділяють заходи щодо зміцнення інформаційного суверинитету на 4 рівня: *законодавчий* (закони, нормативні акти, стандарти, тощо); *адміністративний* (дії загального характеру з боку керівництва установи); *процедурний* (конкретні заходи стосовно людей); *програмно-технічний* (конкретні технічні заходи) [4].

На сьогоднішній день методи і способи реалізації цих заходів опрацьовані в достатньому обсязі. Але у більшості випадків вони мають переважно технікоприкладний характер та орієнтовані на розв'язання конкретних науково-технічних задач. Тим не менш, необхідною умовою для їх ефективного втілення на практиці є розробка ефективної процедури моніторингу інформаційного простору та формування в суспільстві інформаційної культури.

2.1 Контент-моніторинг міжнародного 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. Саме при невірному або несвоєчасному реагуванні на негативні фактори інформаційного впливу (поширення неправдивої або негативної інформації) проявляється посилення їх дестабілізуючого впливу, а сам фактор при цьому 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 МІП обумовлюється необхідністю передбачення ситуацій переростання факторів дестабілізації в загрози безпеці та збереження інформаційного суверенитету в цілому.

Оптимальним порядком дій по забезпеченню інформаційної безпеки та інформаційного суверинитету у воєнній сфері є своєчасне виявлення, класифікація та контроль факторів дестабілізації, ідентифікація загроз та розробка і виконання заходів щодо їх нейтралізації.

Контент-моніторинг МІП 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.

На основі проведеного дослідження можна смоделювати процес проведення інформаційних атак, що здійснюються у МІП, та виділити такі їх умовні фази: "фонові публікації", "затишок", "артпідготовка", "затишок", "атака". Типову хронологічну послідовність тематичних публікацій та поведінку їх рядів інтенсивності показано на рис. 2. 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. 2) [12, 13].

Рис. 2. Типова поведінка рядів інтенсивності тематичних публікацій

2.2 Визначення оптимального порядку профілактичних заходів щодо забезпечення інформаційної безпеки та інформаційного суверинитету у воєнній сфері. Основними профілактичними заходами є своєчасне виявлення, класифікація та контроль факторів дестабілізації, ідентифікація загроз та розробка і виконання заходів щодо їх нейтралізації. З метою своєчасного виявлення та ефективної протидії інформаційно-психологічним операціям доцільним є реалізація таких 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 у інтенсивності тематичних публікацій;

–детальний аналіз динаміки публікацій з визначенням моментів, тривалості;

– 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.

2.3 Виховання інформаційної культури майбутніх офіцерів у фокусі проблем інформаційної безпеки. Ефективне здійснення заходів захисту національного інформаційного суверинитету та України на міжнародному рівні неможливе без виховання інформаційної культури суспільства у цілому, і у майбутніх офіцерів зокрема.

Інформаційну культуру пропонується визначати як певний рівень знань, що дає людині змогу вільно орієнтуватися в інформаційному просторі, брати участь в його формуванні та сприяти здійсненню інформаційних комунікацій [10]. Критеріями

сформованості інформаційної культури можна вважати наступні: уміння адекватно формулювати свою потребу в інформації, ефективно здійснювати пошук потрібної інформації; уміння переробляти інформацію і створювати нову; вміння адекватно відбирати та оцінювати інформацію; наявність комп'ютерної грамотності [15]. Найбільш ефективно сформувати інформаційну культуру у закладі вищої військової освіти можливо за умови максимального використання потенціалу предметів гуманітарного циклу – правознавства, іноземної мови, соціальної військової педагогіки, військової психології та ін.

Вивчення цих дисциплін дає можливість курсанту навчитися думати, розвивати інтелектуальні здібності, прораховувати і моделювати життєві ситуації; аналізувати інформацію та ідентифікувати ідеологічні впливи "неекологічного" контенту; засвоїти культуру обміну інформацією як складову норму морально-етичної поведінки у суспільстві. Засобами, які би забезпечили таку міждисциплінарну взаємодію, повинні стати єдиний підхід та єдність понятійного апарату. Так, викладачам слід спрямувати зусилля на те, щоб прищепити майбутнім офіцерам знання основних законів функціонування інформаційних потоків в суспільстві та прийоми та методи аналітико – синтетичної переробки інформації.

Висновки

Питання забезпечення інформаційної безпеки України та протидії деструктивним інформаційним впливам сьогодні набуває актуальності, оскільки ведення інформаційної війни проти нашої країни, відсутність цілісної комунікативної політики держави, недостатній рівень медіакультури суспільства становить загрозу національній безпеці країни. Створення потужного національного інформаційного простору як головного аспекту присутності держави в міжнародному інформаційному просторі є стратегічним завданням інформаційної безпеки України. Таке завдання включає створення системи захисту власного інформаційного суверинитету.

Важливу роль у розгортанні та проведенні інформаційних війн відіграє застосування "м'якої" сили як традиційними засобами масової інформації так і через можливості Інтернет-ресурсів, соціальних мереж та блогосфери.

У роботі проведено дослідження моделі міжнародного інформаційного простору з метою аналіза деструктивних впливів та пошуку шляхів протидії дискредитації України на міжнародному рівні.

На основі аналізу умов і чинників, які впливають на процес виникнення та розвиток інформаційних загроз, визначено таку динаміку розвитку інформаційного деструктивного впливу: "чинник інформаційної загрози – проява інформаційної загрози – реалізація загрози (інформаційний вплив) – результати впливу".В якості профілактичного заходу щодо забезпечення інформаційної безпеки та інформаційного суверинитету у воєнній сфері пропонується контент-моніторінг МІП.

У роботі розглядаються шляхи реалізації основних етапів контент-моніторингу МІП із своєчасного виявлення та ефективної протидії інформаційно-психологічним операціям.

Крім того, зазначено необхідність виховання інформаційної культури майбутніх офіцерів у фокусі проблем інформаційної безпеки України та протидії деструктивним інформаційним впливам.

СПИСОК ЛІТЕРАТУРИ

1. Про рішення Ради національної безпеки і оборони України від 6 червня 2015 року № 287/2015 "Про Стратегію національної безпеки України" [Електронний ресурс]: Указ Президента України від 26.05.2015 № 287/2015. Законодавство України // Платформа LIGA:ZAKON. URL: http://search.ligazakon.ua/l_doc2.nsf/link1/U287_15.html.
2. Про національну безпеку України: Закон України від 19 червня 2003 року № 2469-VIII в редакції від 21 червня 2018 року. *Відомості Верховної Ради (ВВР),* 2018. – № 31, ст.241.
3. Про національну програму інформатизації: Закон України від 4 лютого 1998 року № 74/98-ВР. *Відомості Верховної Ради України,* 1998. – № 27–28. ст. 181.
4. Про концепцію національної програми інформатизації : Закон України від 4 лютого 1998 року № 75/98-ВР. *Відомості Верховної Ради України*, 1998. – № 27-28. ст. 182.
5. Бондаренко В. О. Інформаційна безпека сучасної держави: концептуальні роздуми / В. О. Бондаренко, О. В. Литвиненко // Стратегічна панорама. – 1999. –№ 1–2. – С. 127–133.
6. Галамба М. Інфор ма ційна без пека Украї ни: поняття, сутн ість та загрози/ М. Галамба, В. Петрик // Юридичний журнал. – 2006 – № 12. — С. 133-136.
7. Медвідь Ф. М. Інформаційна безпека України: ґенеза і становлення / Ф. М. Медвідь // Наукові праці МАУП / редкол.: В. Б. Захожай (гол. ред.) та ін. – К. : ДП Вид. дім "Персонал", 2010. – Вип. 2(25). – С. 116–122.
8. Присяжнюк М.М. Інформаційна безпека України в сучасних умовах / М. М. Присяжнюк, Я. С. Бєлошевич // Вісник Київського національного університету імені Тараса Шевченка. □ 2013. □ Вип. 30. □ С.42-46.
9. Інформаційна безпека (соціально-правовіаспекти): підручник / [Остроухов В. В., Петрик В. М., Присяжнюк М. М. та ін.] ; за заг. ред. Є. Д. Скулиша. – К. : КНТ, 2010. – 776 с.
10. Шрейдер, В.Г. Теорія комунікацій / В.Г. Шрейдер. – К. : Ваклер, 1998. – 395 с.
11. Гай-Нижник П. П. Росія проти України (1990–2016 рр.): від політики шантажу і примусу до війни на поглинання та спроби знищення / Павло Гай-Нижник. – К.: "МП Леся", 2017 – 332 с.
12. 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.
13. Федоренко Р. М.. Контент-моніторинг інформаційного простору як чинник забезпечення інформаційної безпеки держави у воєнній сфері/ Сучасний захист інформації Київ, 2015. – №2. – С. 21-26.13
14. Медведева Е. А. Основы информационной культуры / Е. А. Медведєва // СоцИс. –1994. – №11. – С. 52-67.
15. Матвійчик О. Є. Формування інформаційної культури викладача//Комп'ютер у школі та сім'ї. – 2006. – №6. – С. 16-17.

Рецензент: д-р техн. наук, проф. О. О. Можаєв,
Харківський національний університет внутрішних справ, Харків
Received (Надійшла) 03.10.2018
Accepted for publication (Прийнята до друку) 21.11.2018

Исследование модели международного информационного пространства с целью поиска эффективных механизмов защиты национального информационного суверинитета

А. В. Серпухов, Е. А. Макогон, С. А. Новик, А. П. Климов, И. А. Ковалев, В. Н. Базелюк

Предметом изучения в статье является процесс возникновения и развития информационных угроз безопасности Украины в военной сфере. **Целью исследования** является анализ деструктивных воздействий на национальное информационное суверинитет, поиск эффективных путей противодействия и механизмов защиты. **Задачи:** на основе структурно-функционального анализа модели международного информационного пространства (МИП) определить угрозы и потенциальные опасности интеграции Украины в международное информационное пространство, смоделювать процесс проведения информационных атак, осуществляемых в МИП, и разработать оптимальный порядк профилактических мероприятий по обеспечению информационной безопасности и информационного суверинитета в военной сфере. Использованы **методы** системного анализа и статистической обработки данных. **Получены следующие результаты.** В условиях глобальной интеграции и жесткой международной конкуренции МИП становится ареной столкновений и борьбы разновекторных национальных интересов. В связи с этим исследования реальных и потенциальных угроз негативных воздействий на Украине в международном информационном пространстве и создание действенной системы защиты и противодействия дискредитации Украины на международном уровне приобретают значимую актуальность. Основными профилактическими мероприятиями по обеспечению информационной безопасности и информационного суверинитет в военной сфере является своевременное выявление, классификация и контроль факторов дестабилизации, идентификация угроз и разработка и выполнение мероприятий по их нейтрализации. Эффективное осуществление мер защиты национального информационного суверинитет и противодействия дискредитации Украины на международном уровне невозможно без воспитания информационной культуры общества в целом, и в будущих офицеров в частности. **Выводы**. В работе проведено исследование модели международного информационного пространства с целью анализа деструктивных воздействий и поиска путей противодействия дискредитации Украины на международном уровне. На основе анализа условий и факторов, влияющих на процесс возникновения и развития информационных угроз, определено такую динамику развития информационного деструктивного воздействия: “фактор информационной угрозы - проявление информационной угрозы - реализация угрозы (информационное воздействие) - результаты влияния”. В качестве профилактической меры по обеспечению информационной безопасности и информационного суверинитет в военной сфере предлагается контент-мониторинг МИП. В работе рассматриваются пути реализации основных этапов контент-мониторинга МИП по своевременному выявлению и эффективного противодействия информационно-психологическим операциям. Кроме того, отмечена необходимость воспитания информационной культуры будущих офицеров в фокусе проблем информационной безопасности Украины и противодействия деструктивным информационным воздействиям.

Ключевые слова: модель международного информационного пространства, контент-мониторинг, информационный суверинитет.

Study of the international informational space model with the goal of the search for efficient mechanisms of national information sovernight protection

O. Serpukhov, H. Makogon, S. Novik, A. Klimov, I. Kovalov, V. Bazeliuk

The **subject matter** of the article is the process of the emergence and development of information threats to Ukraine's security in the military sphere. The **goal** of the study is to analyze the destructive effects on national informational sverinitet, the search for effective ways of counteraction and mechanisms of protection. The **tasks** to be solved are: on the basis of structural and functional analysis of the model of the international information space (IIS), to identify the threats and potential dangers of Ukraine's integration into the international information space, to simulate the process of information attacks carried out in the IPP and to develop the optimal order of preventive measures to ensure information security and information superstitions in the military sphere. The **methods** of system analysis and data statistical processing are used. The following **results** are obtained. Under the conditions of global integration and tight international competition, the IIS becomes an arena of collisions and the struggle between different national interests. In this regard, the study of real and potential threats of negative influences on Ukraine in the international information space and the creation of an effective protection system and counteraction to Ukraine's discreditation at the international level are becoming relevant. Using of “soft” force in modern information technologies allows you to realize your own interests in the IIS. The content monitoring of the IIS should be aimed at identifying information and psychological operations, the objects of influence of which may be: information and technical and analytical systems, databases and information resources, the human psyche, the mood of society and the image of the Armed Forces and the state as a whole. The main preventive measures to ensure information security and information security in the military sphere are the timely detection, classification and control of the factors of destabilization, identification of threats and development and implementation of measures to neutralize them. Effective implementation of measures to protect national information superstition and counteracting the discredit of Ukraine at the international level is impossible without raising the information culture of society as a whole, and future officers in particular. **Conclusions**. The article examines the model of the international information space in order to analyze destructive influences and to find ways to counter Ukraine’s discredit on the international level. On the basis of the analysis of the conditions and factors influencing the process of the emergence and development of information threats, the following dynamics of the development of information destructive influence are determined: “the factor of the information threat - the manifestation of the information threat - the realization of the threat (information influence) - the results of influence”. Content monitoring of IIS is proposed as a preventive measure to ensure information security and information security in the military sphere. The paper considers ways of realization of the main stages of the content-monitoring of the IIS on timely detection and effective counteraction to information-psychological operations. In addition, the necessity of raising the informational culture of future officers in the focus of Ukraine's information security and counteracting destructive information influences is noted.

Keywords: model of the international information space, content-monitoring, informational supercontinue.