УДК 355.40: 356.35

**Сніцаренко П. М., д-р техн. наук, ст. наук. співроб. (ORCID 0000-0002-65257064);**
**Грицюк В. В. (ORCID 0000-0002-3146-1956)**

Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського, Київ

# Аналіз стану виявлення та оцінювання негативного інформаційного впливу на особовий склад Збройних Сил України в системі протидії такому впливу

**Анотація**. У статті розглянуто досвід армій передових країн світу та України з питань побудови, завдань і функціоналу систем протидії негативному інформаційному впливу. Проаналізовано сучасний стан вітчизняних структур і підрозділів, що можуть бути задіяні до процесу моніторингу інформаційного простору для виявлення та оцінки негативного інформаційного впливу на особовий склад Збройних Сил України. Визначено актуальність і необхідність автоматизації процесу виявлення та оцінки такого впливу на основі класифікації інформаційних подій.

**Ключові слова**: інформаційний вплив, виявлення та оцінка, протидія, морально-психологічний стан Збройних Сил України.

**Постановка проблеми.** Протидія негативному інформаційному впливу – невід'ємна складова забезпечення інформаційної безпеки України, зокрема у воєнній сфері. Особливої важливості для України ця обставина набула напередодні та в період агресії з боку Російської Федерації, коли гостро та відчутно виявилися наслідки негативного зовнішнього інформаційного впливу, зокрема на особовий склад Збройних Сил України (ЗС України). Особливим, складним, а тому малорозвиненим є процес моніторингу інформаційного простору в інтересах протидії. Виокремленими питаннями до того ж слід вважати виявлення, оцінювання та аналіз інформаційних подій і можливі шляхи підвищення ефективності (оперативності) цих процесів.

**Аналіз останніх досліджень і публікацій.** Питання протидії негативному інформаційному впливу на особовий склад ЗС України розглядалося в працях вітчизняних науковців В. Толубка, І. Руснака, В. Телелима, А. Рося, Т. Дзюби, Г. Пєвцова та інших [0-0]. Аналіз показує, що на сьогодні теорія протидії такому впливу обмежена на рівні концептуально-декларативних положень, тому для практики є недосконалою. У ній бракує чітких формальних методів і методик для кількісних оцінок певних аспектів цієї сфери, зокрема щодо виявлення та оцінювання рівня негативного інформаційного впливу на особовий склад ЗС України. З цієї причини його кількісна оцінка не проводиться, а оцінювання морально-психологічного стану ЗС України, який є наслідком, зокрема, і такого впливу, здійснюється за якісними показниками на основі результатів моніторингу у військових частинах і підрозділах відповідно до діючих інструкцій [0], тобто вже після наслідків інформаційних впливів. Зазначене не дає змогу проводити випереджувальні заходи для підтримки морально-психологічного стану військ (сил), отже ефективно протидіяти такому впливу.

**Метою статті** є розгляд умов і чинників до створення автоматизованої підсистеми виявлення та оцінювання рівня негативного інформаційного впливу на особовий склад ЗС України на основі кількісних показників із властивостями реалізації дій випереджувального характеру як складової перспективної системи протидії такому впливу.

**Викладення основного матеріалу**. Військовим стандартом, який затверджує термінологію з питань інформаційної безпеки у воєнній сфері [0], визначається, що під *інформаційним впливом слід розуміти організоване цілеспрямоване втручання у свідомість (підсвідомість) чи фізичний стан цільової аудиторії та/або в процес функціонування технічних об'єктів інформаційної інфраструктури шляхом застосування інформаційних засобів і технологій*.

Відомо [0, 0], що за характером дії інформаційний вплив може бути поділений на два види – інформаційно-технічний та інформаційно-психологічний. Розглядаючи надалі питання інформаційного впливу на цільову аудиторію, якою є особовий склад військ (сил) та органи військового управління, дотримуємося його розуміння в сенсі інформаційно-психологічного впливу.

Зауважимо, що Концепцією кадрової політики в Збройних Силах України визначено: "*особовий склад Збройних Сил –*

військовослужбовці та працівники Збройних Сил, які виконують свої обов'язки у межах, визначених Конституцією України та законами України" [0]. У контексті цієї концепції "органи військового управління" також є особовим складом. Тому надалі використано узагальнене поняття "особовий склад військ (сил)", зважаючи також на те, що методи дії інформаційного впливу на військову цільову аудиторію є ідентичними незалежно від ролі і посад особового складу військ (сил).

Негативний інформаційний вплив на таку цільову аудиторію спричиняє зниження рівня її морально-психологічного стану, що, відповідно, знижує загальну боєздатність військових формувань. Активна протидія негативному інформаційному впливу на особовий склад військ (сил) має розпочинатися у разі загрози такого впливу або його здійснення з боку противника [0]. Результат протидії досягається через реалізацію взаємопов'язаного процесу, який за сутністю є управлінським, з такими обов'язковими фазами: виявлення впливу; оцінка рівня впливу; формування висновків з оцінки та прийняття рішення щодо необхідності протидії впливу; планування заходів протидії, затвердження плану заходів протидії; реалізація заходів протидії відповідно до плану; контроль дієвості реалізованих заходів протидії та їх коригування.

Успішність та належна результативність зазначеного управлінського процесу потребує чіткої алгоритмізації дій на усіх фазах його реалізації. Особливо відповідальними для якісної реалізації усього управлінського процесу протидії, його своєрідним фундаментом, є перші дві фази – виявлення негативного інформаційного впливу та об'єктивна оцінка рівня цього впливу на армійську цільову аудиторію. Для оцінювання набутого досвіду розглянемо практику побудови таких систем протидії, як в Україні так і за її межами, зосередивши увагу на фазах виявлення та оцінювання рівня такого впливу.

Останніми роками у провідних країнах світу, насамперед США, країнах ЄС, РФ, є певні досягнення щодо організації та ведення дій в інформаційному просторі у воєнних конфліктах, зокрема заходів протидії інформаційного впливу противника [0–0]. Так, у *Сполучених Штатах Америки* така протидія, відповідно до Доктрини "Інформаційні операції" (JP 3-13), здійснюється в межах ведення інформаційних операцій, що являють собою комплекс заходів збройних сил США щодо впливу на людські й матеріальні ресурси противника з метою ускладнити або унеможливити прийняття ними вірних рішень з одночасним захистом своїх інформаційних систем [0]. Поряд з іншим, основними складовими інформаційних операцій вважаються психологічні операції (операції з інформування та впливу – MISO) та заходи щодо забезпечення безпеки власних сил і засобів, що передбачає протидію інформаційному впливу противника на особовий склад власних військ (сил).

На сьогодні можливості MISO для проведення заходів інформаційно-психологічної протидії суттєво розширено завдяки створенню військової компоненти національної системи кібернетичної безпеки – Об'єднаного кібернетичного командування збройних сил США (USCYBERCOM), яке інтегрує за єдиним задумом і планом наявні сили і засоби формувань збройних сил США, зокрема можливості структур ведення психологічних операцій (MISO), зокрема щодо моніторингу електронних ЗМІ та інтернет-блогів, а також боротьби з "неточним відображенням подій".

Водночас слід відзначити, що проведення збройними силами США інформаційних операцій передбачає використання великої кількості експертів та може свідчити про переважання експертних методів в оцінюванні ситуацій і, очевидний дефіцит відповідних формалізованих методик, що стосуються як моніторингу інформаційного простору, так і здійснення активного контрвпливу. Проте розроблення таких методик, зокрема лінгвістичних комп'ютерних програм моніторингу соціальних мереж у регіонах уваги США для виявлення загроз місіям їх збройних сил, проводиться.

Досвід *європейських країн-членів НАТО* зводиться до того, що воєнно-політичне керівництво НАТО надає важливе значення психологічному забезпеченню діяльності Об'єднаних збройних сил НАТО як в мирний, так і воєнний час. Особливо зростає роль цього виду забезпечення в умовах, пов'язаних з місіями за участю національних військових контингентів у локальних збройних конфліктах і міжнародних миротворчих операціях під егідою НАТО або ООН у різних регіонах світу. Найрозвиненішими такі служби є у Великобританії, Франції, Федеративній Республіці Німеччини, Італії, де значна увага приділяється, зокрема, протидії негативному інформаційному впливу противника, включаючи активні заходи моніторингу

інформаційного простору для виявлення такого впливу [0, 0, 0].

Типовою моделлю сил психологічних операцій, адаптованою до вимог НАТО, є служба психологічних операцій Війська Польського при координації 5-го відділу психологічних операцій (у складі Головного управління військової розвідки Генерального штабу Війська Польського), якому оперативно підпорядкована Центральна група психологічних дій (у складі сил спеціальних операцій командування сухопутних військ). Ця група безпосередньо реалізує завдання щодо проведення інформаційно-психологічних операцій. Зокрема вона займається збором і обробкою публікацій у пресі, різних періодичних виданнях, тематичної друкарської продукції, повідомлень радіо і телебачення, розміщених в Інтернеті даних, на основі чого готує матеріали для військово-політичного керівництва, яке приймає рішення, зокрема, щодо протидії негативному інформаційному впливу. За необхідності до роботи цієї групи залучаються нештатні експерти (етнографи, соціологи, психологи, педагоги та ін.).

У збройних силах *Російської Федерації* (РФ) протидія негативному інформаційному впливу реалізується в системі інформаційно-психологічного забезпечення бойових дій військ (сил). Таке забезпечення здійснюється на стратегічному, оперативному і тактичному рівнях структурними підрозділами психологічної боротьби, які отримали назву підрозділів "психологічного забезпечення", а останнім часом – "психологічних операцій". Органи психологічних операцій діють у всіх загальновійськових об'єднаннях російської армії, починаючи від корпусу, мають завдання постійного всебічного відстеження інформаційної обстановки в різних регіонах, здатні до швидкого розгортання та досягнення готовності виконувати поставлені завдання за будь-яких умов. Такі підрозділи зосереджені в розвідувальних органах.

Координацію інформаційно-психологічних дій у сфері оборони здійснює управління пресслужби та інформації міністерства оборони РФ. До того ж інформаційно-пропагандистський центр міністерства оборони спільно з центром інформаційного забезпечення мають здійснювати заходи інформаційної протидії в кібернетичному просторі, активно використовуючи для цього можливості Інтернету, насамперед, через офіційний сайт міністерства оборони РФ, абонентські пункти глобальної мережі в органах управління її збройних сил, сайти центрів зарубіжної воєнної інформації та сайти військових ЗМІ. Для ефективного виконання цього завдання в центрі інформаційного забезпечення, зокрема, передбачено потужний програмно-технічний комплекс моніторингу й аналізу інформації з відкритих джерел для виявлення в інформаційному просторі можливих загроз державі та її збройним силам (такий комплекс може відслідковувати до 60 млн джерел, аналізує тональність висловлювань з похибкою 2–3 % практично у реальному часі – до моніторингу потрапляють основні соціальні сервіси: Facebook, Twitter, Viber, Instagram, Vkontakte).

Отже, у провідних країнах світу, зокрема суміжних з Україною, приділяється обов'язкова увага проведенню психологічних операцій як одного з найважливіших чинників досягнення успіху у воєнному конфлікті національними збройними силами. До того ж інформаційні заходи (дії) обов'язково передбачають постійний моніторинг інформаційного простору та добування даних в інтересах оцінювання інформаційної ситуації для протидії інформаційному впливу противника.

Аналіз підтвердив, що процес моніторингу інформаційного простору, у тому числі кіберпростору, є складним проблемним завданням, яке сьогодні вирішується за участю експертного середовища, а автоматизація його виконання на основі комп'ютерного лінгвістичного аналізу знаходиться в стадії активного розвитку.

Особливості функціонування існуючої *вітчизняної системи протидії негативному інформаційному впливу на особовий склад Збройних Сил України* виявляються в діяльності структурних підрозділів МО України та ЗС України, функції, завдання і можливості яких є дотичними до організації та проведення заходів такої протидії, яка має бути координована на загальнодержавному рівні (рис. 1), про що наголошується зокрема в роботі [0].

*У структурі МО України* підрозділами, які відповідно до повноважень можуть бути причетними до сфери протидії негативному інформаційному впливу, можна віднести Головне управління розвідки, Департамент військової освіти, науки, соціальної та гуманітарної політики, Управління інформаційних технологій, Управління комунікацій та преси і Відділ координації стратегічних комунікацій та моніторингу. Серед них завдання моніторингу інформаційного простору в інтересах протидії

негативному інформаційному впливу виконують Головне управління розвідки, Управління комунікацій та преси і Відділ координації стратегічних комунікацій та моніторингу.

Відповідно до Закону України "Про розвідувальні органи України" [0], на Головне управління розвідки покладаються, зокрема, такі завдання [0]:

добування, аналітична обробка та надання визначеним законом органам державної влади розвідувальної інформації;

здійснення спеціальних заходів, спрямованих на підтримку національних інтересів і державної політики України в економічній, інформаційній сферах, зміцнення обороноздатності.

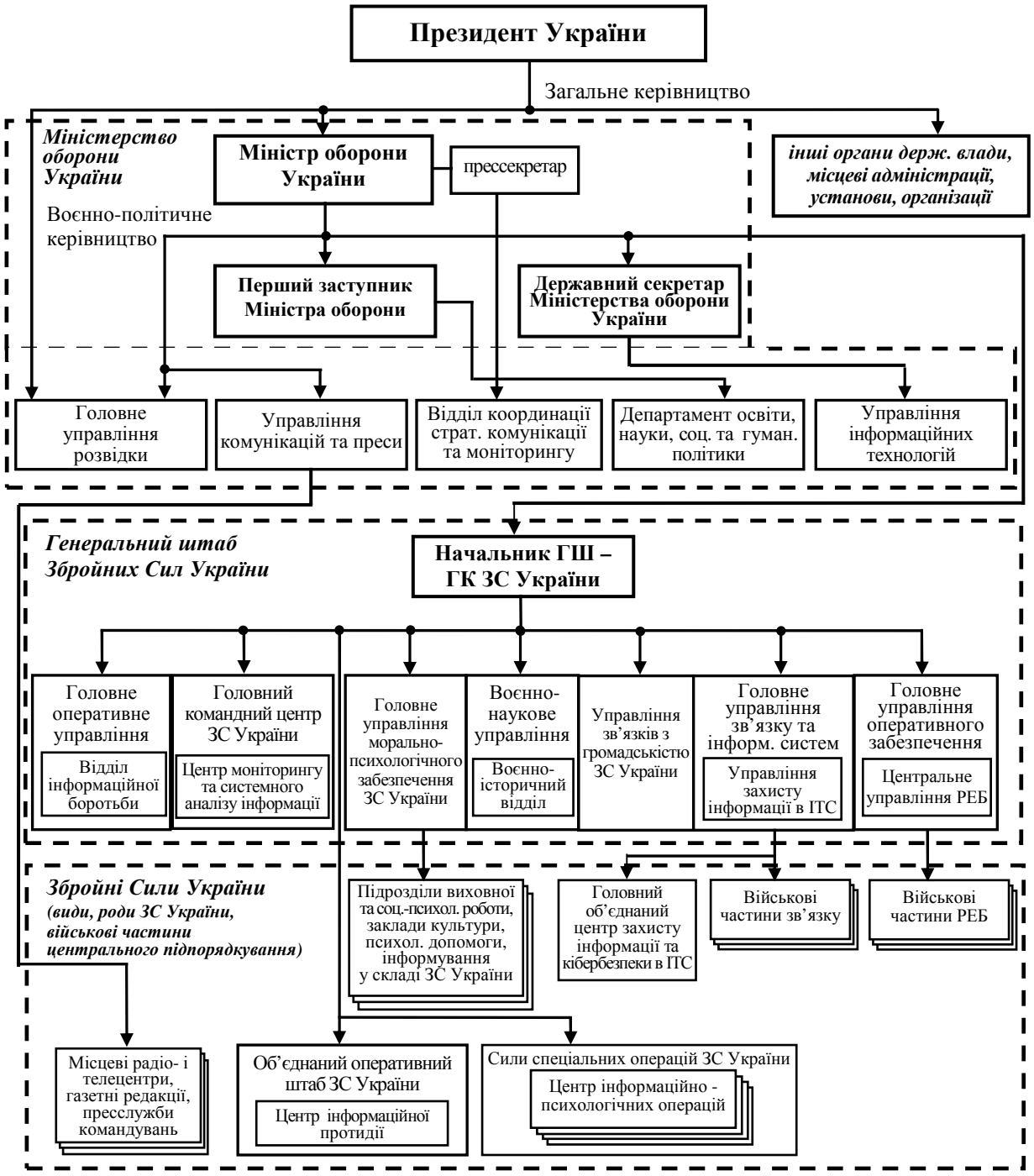


**Рис. 1. Структура існуючої системи протидії негативному інформаційно-психологічному впливу на особовий склад військ (сил) ЗС України**

У підрозділах Головного управління розвідки проводиться відповідна розвідувальна та інформаційно-аналітична робота для моніторингу інформаційного простору, у тому числі масмедійного, для виявлення ознак та джерел інформаційного впливу на соціальні об'єкти сфери оборони держави.

Відповідно до Положення про Управління комунікацій та преси Міністерства оборони України [0] серед основних завдань значиться:

здійснення постійного моніторингу інформаційного середовища, виявлення потенційних та реальних інформаційних загроз в оборонній сфері, проведення попереджувальних інформаційних заходів.

Як правило, ця діяльність цього Управління та підпорядкованих йому установ і організацій є ситуативною з реагуванням на окремі інформаційні події та приводи і здійснюється без засобів автоматизації.

Відділ координації стратегічних комунікацій та моніторингу має широкі повноваження, зокрема, з питань моніторингу інформаційного простору, що може істотно посилити позиції протидії негативному інформаційному впливу на особовий склад ЗС України. До таких повноважень, зокрема, відносяться [0]:

здійснення медіамоніторингу та підготовка щоденних довідок Міністру оборони України щодо висвітлення діяльності МО України та ЗС України, зокрема в іноземних медіа, соціальних мережах і блогах;

розроблення пропозицій щодо вдосконалення системи моніторингу засобів масової інформації структурними підрозділами апарату МО України, Генерального штабу ЗС України, органів військового управління, підпорядкованих МО України та Генеральному штабу ЗС України, установ та організацій МО України та ЗС України, на яких покладена ця функція, організація впровадження новітніх технологій для покращення ефективності моніторингу; здійснення медіааналізу за результатами проведення медійних заходів.

Проте цей відділ на сьогодні знаходиться в стадії становлення, свої функції виконує в неавтоматизованому (ручному) режимі, а тому його можливості обмежені лише ситуативними завданнями прессслужби Міністра оборони України.

У структурі *Генерального штабу ЗС України* до підрозділів, які безпосередньо можуть бути залучені до протидії негативному інформаційному впливу, можна віднести Головне оперативне управління (у його структурі – відділ інформаційної боротьби), Головне управління морально-психологічного забезпечення ЗС України, Головне управління оперативного забезпечення ЗС України (у його структурі – Центральне управління РЕБ), Головне управління зв'язку та інформаційних систем, Воєнно-наукове управління (у його структурі – воєнно-історичний відділ) та Головний командний центр ЗС України.

Серед них завдання моніторингу інформаційного простору в інтересах протидії негативному інформаційному впливу на особовий склад військ (сил) виконує лише Головний командний центр ЗС України, зокрема його структурний підрозділ – центр моніторингу та системного аналізу інформації. Змістом його діяльності є проведення заходів моніторингу інформаційного простору держави для виявлення та оцінювання інформаційного, інформаційно-психологічного і кібернетичного впливу для оцінки ситуації та планування за необхідності відповідної протидії через інформаційне середовище або в інший спосіб.

До сьогодні виконання цього завдання належним чином не автоматизоване, робота ведеться переважно експертним методом і ситуативно.

У складі структур *ЗС України* також є певні сили та засоби, що здатні здійснювати заходи протидії негативному інформаційному впливу на особовий склад військ (сил). Зокрема, завдання моніторингу інформаційного простору для своєчасного виявлення недостовірної, необ'єктивної, упередженої інформації для протидії інформаційному впливу в усіх сферах його розповсюдження виконує центр інформаційної протидії Об'єднаного оперативного штабу ЗС України [0]. Також завдання моніторингу інформаційного простору в інтересах проведення інформаційно-психологічних операцій та протидії негативному інформаційному впливу на особовий склад військ (сил) можуть виконувати центри інформаційно-психологічних операцій у структурі Сил спеціальних операцій ЗС України [0, 0]. Проте виконання цього завдання в обох структурах належним чином не автоматизоване.

Слід зауважити, що оцінювання рівня негативного інформаційно-психологічного впливу на особовий склад ЗС України здійснюється фактично за його наслідками, тобто "постфактум" і опосередковано – через оцінювання рівня морально-психологічного стану, який є індикатором сукупного інформаційного впливу на армійські цільові аудиторії, що вже відбувся. Таке оцінювання має якісний узагальнений бінарний характер ("здатний" чи "не здатний" виконувати завдання за призначенням) [0].

Наведені результати аналізу усіх доступних інформаційних джерел та

національної практики з питань протидії негативному інформаційному впливу, висвітлили низку важливих закономірностей і деталей:

*виявлення та оцінювання інформаційного впливу на соціальне середовище (цільову аудиторію) є невід'ємною складовою систем протидії такому впливу;*

*виявлення та оцінювання негативного інформаційного впливу на особовий склад ЗС України здійснюється в неавтоматизованому (ручному) режимі із застосуванням експертних процедур з недостатнім рівнем автоматизації, що знижує об'єктивність та оперативність прийняття рішень щодо протидії;*

*автоматизація процесу виявлення та оцінювання інформаційного впливу на основі комп'ютерного лінгвістичного аналізу у провідних країнах світу знаходиться в стадії активного розвитку;*

*незважаючи на наявність в МО України та ЗС України структурних підрозділів, причетних до протидії негативному інформаційному впливу на особовий склад військ (сил), їх діяльність є ситуативною та некоординованою, отже незбалансованою та неефективною;*

*оцінювання негативного інформаційного впливу на особовий склад ЗС України та реагування на нього проводиться не інтегрально, а за окремими інформаційними проявами, причому на якісному рівні (без кількісних оцінок), що унеможливлює прогнозування ситуації та випереджувальні системні дії;*

*інтегральне оцінювання негативного інформаційного впливу на особовий склад ЗС України здійснюється за його наслідками через якісну оцінку рівня морально-психологічного стану особового складу ЗС України, що є недостатнім для проведення випереджувальних заходів протидії такому впливу.*

Зазначене свідчить про таке:

висока оперативність та ефективність протидії негативному інформаційному впливу противника потребує впровадження автоматизації усіх фаз цього управлінського процесу, зокрема *виявлення та оцінювання негативного інформаційного впливу на цільову аудиторію;*

існуючий стан системи протидії негативному інформаційному впливу на особовий склад ЗС України, *яка розбалансована, де процеси неавтоматизовані, а оцінювання інформаційних подій здійснюються не за кількісною мірою, а на якісному рівні,* не дає змоги протидії такому впливу як системному управлінському процесу, у якому *об'єктом управління має бути рівень морально-психологічного стану військ (сил), а заходи протидії реалізуються як випереджувальні.*

Це свідчення дало підставу стверджувати про необхідність запровадження в системі протидії, насамперед, принципу реагування на прояви негативного інформаційного впливу на особовий склад ЗС України на основі оцінювання рівня такого впливу та визначення його значимості із використанням кількісної міри.

Для цього розроблено ідею та методику побудови підсистеми виявлення та оцінювання негативного інформаційно-психологічного впливу на особовий склад ЗС України, яка дає змогу визначити його рівень на основі кількісної міри інтенсивності прояву такого впливу [0, 0, 0]. Сутність цієї методики така:

інформаційні процеси відбуваються в інформаційному просторі держави, сприймаються особовим складом військових формувань, залишають певне відображення у свідомості військовослужбовців, змінюють їх морально-психологічний стан. Для кількісного оцінювання рівня негативного інформаційного впливу застосовано показник його інтенсивності $\chi$ як інтегральну характеристику деструктивної дії усієї сукупності інформаційних процесів $M$ (шт.) на особовий склад військ за певний період часу $\Delta T$

$$\chi = \frac{M}{\Delta T}.$$

Зазначене одночасно є інтегральним показником як оцінки рівня негативного інформаційного впливу, так і індикатором виявлення дієвості такого впливу за величиною (значенням) оцінки рівня. Значення показника інтенсивності $\chi$ за деякий період часу $\Delta T$ може приймати певні значення – від мінімальних і вище. Тоді динаміку ескалації інтенсивності загального деструктивного інформаційного процесу в інформаційному просторі держави за час $\Delta T$ стосовно особового складу військ (сил) можна умовно представити ступінчатою функцією рівнів, які слід вважати частковими показниками впливу, як це показано на рис. 2. До того ж, переходу на кожен із рівнів доцільно поставити у відповідність певний критерій за шкалою оцінок $\chi$: $\chi_1, \ldots, \chi_5$.

Через це запропоновано та визначено (характеризовано) шість умовних якісних станів

(часткових показників рівня впливу) загального деструктивного інформаційного процесу в інформаційному просторі держави та відповідні критерії, які можуть бути застосовані для визначення рівня його інтенсивності як міри впливу, зокрема, на особовий склад військ (сил):

інформаційний фон (шум);

виклик (інформаційно-психологічний);

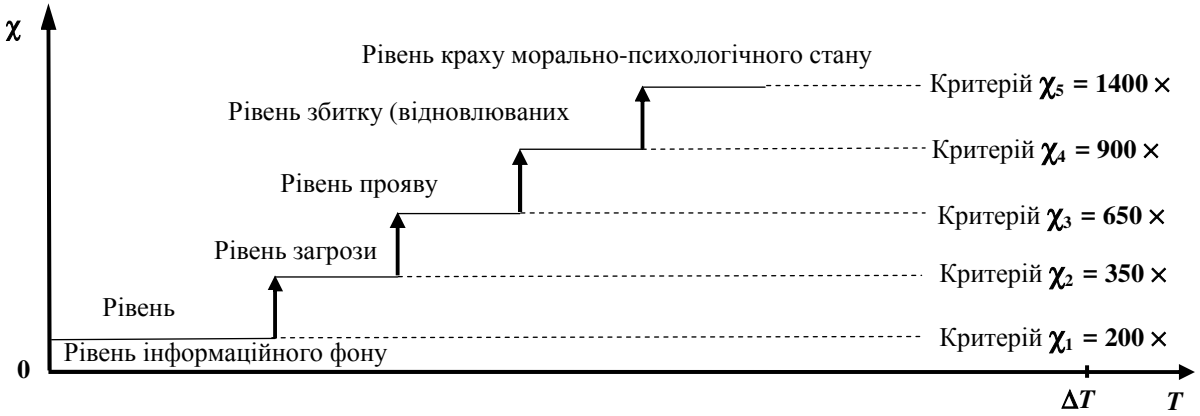


**Рис. 2. Динаміка ескалації інтенсивності загального деструктивного інформаційного процесу (за період $\Delta T$ = 1 рік)**

загроза (інформаційно-психологічна);

прояв інформаційно-психологічного впливу на особовий склад військ;

збиток (відновлювані втрати) в морально-психологічному стані військ;

крах морально-психологічного стану військ.

Експертним методом визначено значення критеріїв для отримання кількісних оцінок рівня інтенсивності інформаційного впливу на цільову аудиторію (особовий склад ЗС України), який покладено в основу розроблення цілісної методики. До того ж за допомогою реалізації процедури експертного опитування фахового середовища України та статистичної обробки отриманих даних визначено 22 класи та 17 підкласів інформаційних процесів (дій, фактів), які можуть негативно впливати на свідомість і, відповідно, морально-психологічний стан особового складу військ (сил), а також "вагу" прояву процесу у кожному з класів (підкласів) на шкалі від 0 до 100.

Застосування такої методики дає змогу в кількісному вимірі оцінити рівень інформаційного впливу на визначену цільову аудиторію за певний період часу за допомогою "вагового" накопичення. Це забезпечує можливість порівняно об'єктивно прогнозувати динаміку цього процесу та можливі наслідки, щоб адекватно та на випередження реагувати (протидіяти) негативним процесам. Методика пропонується невід'ємним елементом підсистеми моніторингу ситуації у загальному контурі управління процесом протидії, який забезпечує підтримку морально-психологічного стану особового складу збройних сил. Це має бути головною метою та об'єктом управління в системі протидії негативному інформаційному впливу на особовий склад військ (сил), яка базується на кібернетичному принципі управління.

Загальна схема кібернетичної моделі системи протидії негативному інформаційному впливу на особовий склад військ (сил), яка запропонована в [0], (рис. 3).

Така модель може найповніше забезпечити активну та адаптивну протидію негативному інформаційному впливу на особовий склад військ (сил). Для її реалізації залучаються структурні підрозділи МО України та ЗС України і вона буде діяти ефективно у тому разі, коли її алгоритм роботи ґрунтуватиметься на чіткій формалізації взаємодії між усіма елементами.

На практиці ця модель в МО України та ЗС України частково реалізується в межах контуру, окресленого штриховою лінією. Але як вже зазначено, діяльність цих структур розбалансована, вони діють поодиноко та не координовано. А виявлення та оцінювання інформаційного впливу на особовий склад військ (сил) сьогодні може бути здійснено лише "ручним" методом, що є трудомістким та тривалим процесом. Це шкодить оперативності управлінського процесу протидії такому впливу та загалом ефективності здійснення випереджувальних стабілізаційних заходів (серед них мають бути заходи впливу як на особовий склад ЗС України, так і на шкідливі інформаційні джерела). Зазначене слід вважати недоліком отриманого на сьогодні методичного рішення, який спричиняє проблемне питання щодо підвищення оперативності усього процесу протидії та потребує зусиль для його розв'язання за допомогою автоматизації

процесів виявлення та оцінювання негативного інформаційного впливу на особовий склад ЗС України, насамперед класифікації інформаційних подій шкідливого характеру.

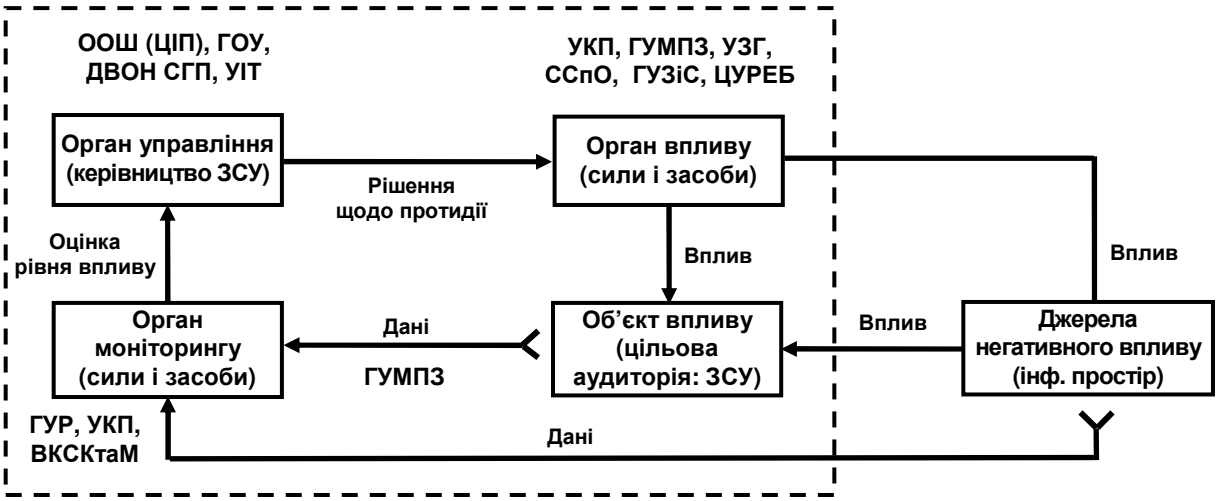


**Рис. 3. Кібернетична модель реалізації системи протидії негативному інформаційному впливу на особовий склад військ (сил)**

**Висновки**

1. Аналіз світового досвіду проведення інформаційних операцій та протидії інформаційному впливу на особовий склад військ (сил) показав, що провідні у воєнній сфері країни світу для досягнення воєнно-політичних цілей обов'язково застосовують сили і засоби інформаційного впливу на війська і населення протидіючої сторони та проводять заходи щодо захисту своїх військовослужбовців.

Найрозвиненішою та потужною є система, яка створена у США, де реалізовано цілісний механізм інформаційного забезпечення діяльності збройних сил, зокрема ефективну систему протидії негативному інформаційному впливу противника.

Країни-члени НАТО мають орієнтацію на колективне вирішення воєнно-політичних питань у складі багатонаціональних сил під егідою НАТО.

Досить чітку та організаційно всеохоплюючу систему інформаційно-психологічних дій у воєнній сфері мають РФ.

Невід'ємною складовою усіх систем протидії негативному інформаційному впливу є підсистема моніторингу інформаційного простору, сили і засоби якої сьогодні активно розвиваються.

2. Аналіз існуючої системи протидії негативному інформаційному впливу на особовий склад військ (сил) ЗС України засвідчив, що в Україні існують основні складові такої системи. Поряд із цим, виявлено, що існуюча система має низку недоліків організаційного, технічного та методичного характеру, що є об'єктивною підставою для її суттєвого удосконалення в інтересах дієвішого забезпечення виконання ЗС України завдань за призначенням.

3. Результати аналізу іноземного, а найважливіше, вітчизняного досвіду, зокрема, свідчать, що виявлення та оцінювання інформаційного впливу на цільову аудиторію здійснюється переважно за допомогою експертних процедур, причому на якісному рівні без кількісних характеристик впливу, що негативно впливає на якість рішення щодо адекватних випереджувальних заходів протидії. Низька ефективність процесу виявлення та оцінювання інформаційного впливу спричинена "ручним" методом вирішення поставленого завдання.

4. Підвищення оперативності вирішення завдання виявлення та оцінювання негативного інформаційного впливу на особовий склад ЗС України, як необхідної умови високої результативності випереджувальних заходів протидії такому впливу, вбачається у реалізації автоматизації визначених процедур оцінювання та класифікації проявів впливу. Наявність потреби вирішення цього завдання як проблемного визначає **напрям подальших досліджень**, зокрема пов'язаних з розробленням моделі автоматизованої класифікації інформаційних подій в системі управління протидією негативному інформаційному впливу на особовий склад ЗС України.

ПЕРЕЛІК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Толубко В. Б. Концептуальні основи інформаційної безпеки України / В. Б. Толубко, С. Я. Жук,

В. О. Косевцов // Наука і оборона. – 2004. – № 2. – С. 19-25.
2. Руснак І. С. Розвиток форм і способів ведення інформаційної боротьби на сучасному етапі / І. С. Руснак, В. М. Телелим // Наука і оборона. – 2000. – № 2. – С. 18-23.
3. Основи стратегії національної безпеки та оборони держави: підруч. / О. П. Дузь-Крятченко, Т. М. Дзюба, А. О. Рось, ін. – 2-ге вид., доп. і випр. – К.: НУОУ, 2010. – 591 с.
4. Інформаційно-психологічна боротьба у воєнній сфері: монографія / Г. В. Пєвцов, А. М. Гордієнко, С. В. Залкін, С. О. Сідченко, А. О. Феклістов, К. І. Хударковський. – Х.: Вид. Рожко С.Г., 2017. – 276 с.
5. Інструкція про порядок оцінки морально-психологічного стану в Міністерстві оборони України та Збройних Силах України (затверджено наказом МО України від 21.05.2013 № 335, зі змінами, внесеними наказом МО України від 17.12.2015 № 728, зареєстровано в Мін'юсті України 11.01.2016 № 29/28159).
6. Військовий стандарт ВСТ 01.004.004. Воєнна політика, безпека та стратегічне планування. Інформаційна безпека держави у воєнній сфері. Терміни та визначення.
7. Горбулін В. П. Проблеми захисту інформаційного простору України: Монографія / В. П. Горбулін, М. М. Биченок // Ін-т пробл. нац. безпеки. – К.: Інтертехнологія, 2009. – 136 с.
8. Інформаційна безпека (соціально-правові аспекти): Підручник / Остроухов В. В., Петрик В. М., Присяжнюк М. М. та ін. // За заг. ред. Є. Д. Скулиша. – К.: КНТ, 2010. – 776 с.
9. Наказ Міністра оборони України від 27 листопада 2007 року № 659 "Про затвердження Концепції кадрової політики в Збройних силах України".
10. Морально-психологічне забезпечення у Збройних Силах України: підручник у 2-х ч. Ч.1. / В. І. Алещенко, В. М. Грицюк, В. Г. Дикун та ін.] за заг. ред. В. В. Стасюка. – К.: НУОУ, 2012. – 464 с.
11. Вооруженные силы зарубежных государств: информационно-аналитический сборник / А. Н. Сидорин, Г. М. Мингатин, В. М. Прищепов, В. П. Акуленко. – М.: Воениздат, 2009. – 528 с.
12. А. Медин. Силы ВВС США, предназначенные для ведения боевых действий в киберпространстве, и взгляды командования на их применение / А.Медин, С.Маринин. // Зарубежное военное обозрение. – 2012. – № 6. – С.54 - 59.
13. С. Тулин. Органы управления ВС США боевыми действиями в кибернетическом пространстве / С. Тулин // Зарубежное военное обозрение. – 2012. – № 2. – С.3 - 10.
14. Давыдов Д. Развитие сил информационных операций США до 2020 года / Д. Давыдов // Зарубежное военное обозрение. – 2014. – №4. – С. 3-10.
15. Димлевич Н. Информационные войны в киберпространстве – Великобритания и Израиль [Электронный ресурс] / Н. Димлевич. – Режим доступа: http://www.fondsk.ru/news/2010/11/08/informacionnye-vojny-v-kiberprostranstve-velikobritanija-i-izrail.html.
16. В. Хопров. 28-й отдельный полк психологических операций "Павиа" сухопутных войск Италии / В. Хопров // Зарубежное военное обозрение. – 2013. – № 7. – С. 42-46.
17. Комплексна система протидії негативному інформаційно-психологічному впливу на особовий склад Збройних Сил України / П. М. Сніцаренко, Ю. О. Саричев, В. А. Ткаченко, Л. В. Хоменко // Наука і оборона. – № 2. – 2018. – С.40-45.
18. Закон України "Про розвідувальні органи України" від 22 лютого 2001 року №2331-III.
19. ГУР МО України [Електронний ресурс]. – Режим доступу: http://uk.wikipedia.org/wiki/Головне_управління_розвідки_Міністерства_оборони_України#cite_note-2.
20. Наказ Міністерства оборони України від 16 березня 2015 року № 117 "Про затвердження Положення про Управління комунікацій та преси Міністерства оборони України".
21. Наказ Міністерства оборони України від 12 червня 2017 року № 317 "Про затвердження Положення про Відділ координації стратегічних комунікацій та моніторингу".
22. Електронний ресурс. Режим доступу: https://www.facebook.com/JointOperational Headquarters/.
23. Електронний ресурс. Режим доступу: https://www.facebook.com/usofcom/
24. Електронний ресурс. Режим доступу: https://www.ukrmilitary.com/p/specially-forces-operations.html.
25. Наказ ГШ ЗС України від 29.04.2017 № 153 "Про затвердження Інструкції з оцінювання морально-психологічного стану особового складу ЗС України" (зі змінами, внесеними наказом ГШ ЗС України від 16.08.2017 № 287).
26. Методичний підхід до виявлення та оцінювання негативного інформаційно-психологічного впливу на особовий склад військ (сил) / П. М. Сніцаренко, Ю. О. Саричев, Ю. І. Міхєєв, М. В. Праута // Наука і оборона. – № 3-4. – 2017. – С.18-25.
27. Підсистема моніторингу інформаційного простору як необхідна складова системи протидії негативному інформаційно-психологічному впливу на особовий склад Збройних Сил України / П. М. Сніцаренко, Ю. О. Саричев, В. А. Ткаченко, О. А. Мотузяник // Наука і оборона. – № 1. – 2018. – С.29-33.

Стаття надійшла до редакційної колегії 05.08.19

**Сницаренко П. Н., д-р техн. наук, ст. науч. сотрудник;**
**Грицюк В. В.**
Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняхівського, Київ

## Анализ обнаружения и оценки негативного информационного воздействия на личный состав Вооруженных Сил Украины в системе противодействия такому влиянию

**Резюме.** В статье рассмотрен опыт армий передовых стран мира и Украины по вопросам построения, задач и функционала систем противодействия негативному информационному воздействию. Проанализировано современное состояние отечественных структур и подразделений, которые могут быть задействованы в процесс мониторинга информационного пространства для выявления и оценки негативного информационного воздействия на личный состав Вооруженных Сил Украины. Определены актуальность и необходимость автоматизации процесса выявления и оценки такого влияния на основе классификации информационных событий.

**Ключевые слова:** информационное воздействие, выявление и оценка, противодействие, морально-психологическое состояние Вооруженных Сил Украины.

**P. Snitsarenko, DsT, senior researcher**
**V. Hrytsiuk**
The Centre for Military and Strategic Studies National Defence University of Ukraine named after Ivan Cherniakhovskyi, Kyiv

## Analysis of the status of detection and evaluation of negative information impact on the personnel of the Armed Forces of Ukraine in the system of counteracting such influence

**Resume.** The article discusses the experience of the armies of the leading countries of the world and Ukraine on the construction, tasks and functionality of systems of counteracting negative information impact. The current state of national structures and units that can be involved in the process of monitoring the information space to detection and evaluate the negative information impact on the personnel of the Armed Forces of Ukraine is analyzed. The relevance and necessity of automating the process of detecting and evaluation such an impact based on the classification of information events is determined.

**Keywords:** information influence, detection and evaluation, counteraction, moral and psychological state of the Armed Forces of Ukraine.