Адміністративне право і процес

УДК 342.9

**Тична Богдана Миколаївна**
*старший науковий співробітник*
*науково-дослідного відділу проблем військового законодавства*
*Центр воєнно-стратегічних досліджень*
*Національного університету оборони України імені Івана Черняховського*
**Тычна Богдана Николаевна**
*старший научный сотрудник*
*научно-исследовательского цента проблем военного законодательства*
*Центр военно-стратегических исследований*
*Национального университета обороны Украины имени Ивана Черняховского*
**Tychna Bohdana**
*Senior Research Fellow of the*
*Research Department Problematic Legislation*
*Center for Military Strategic Issues of*
*National Defense University of Ukraine name after Ivan Chernyakhovsky*
*ORCID: 0000-0002-3948-4570*

# МЕТА ТА ПРИНЦИПИ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ЗБРОЙНИХ СИЛ УКРАЇНИ ТА ЇЇ РОЛЬ У ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ В СУЧАСНИХ УМОВАХ
# ЦЕЛИ И ПРИНЦИПЫ ИНФОРМАЦИОННОЙ ДЕЯТЕЛЬНОСТИ ВООРУЖЕННЫХ СИЛ УКРАИНЫ И ЕЕ РОЛЬ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА В СОВРЕМЕННЫХ УСЛОВИЯХ
# PURPOSE AND PRINCIPLES OF INFORMATION ACTIVITY OF THE ARMED FORCES OF UKRAINE AND ITS ROLE IN PROVIDING THE

# INFORMATION SECURITY OF THE STATE IN MODERN CONDITIONS

***Анотація.*** *Сучасний світ характеризується бурхливим розвитком інформаційних технологій, прогресом інноваційних технологій та комунікативних засобів, розвитком апаратів передачі інформаційних даних що породжують ситуацію необмежених можливостей реалізації інформаційних процесів для досягнення певної мети, виконання великої кількості завдань практичної діяльності. З розвитком технологій змінюються форми і способи збройної боротьби. "Класичні" методи ведення війни доповнюються «нетрадиційними» інформаційними операціями, інформаційно-психологічними, інформаційно-технічними (кібератаки), що свідчить про ведення нових – асиметричних, неформальних, гібридних воєн з застосуванням зброї шостого покоління. Концепцією гібридної війни є використання асиметричних способів ведення бойових дій з метою домінування на певній території, створення зони (території) замороженого конфлікту на території ведення бойових дій з метою ізоляції противника на міжнародному рівні, посилення внутрішньодержавних антиурядових настроїв, деморалізація військ противника, підрив морально-психологічного стану військ. Станом на сьогодні гібридні війни становлять найбільшу загрозу нормальному функціонуванню системи національної безпеки, державної політики, порушення роботи фінансових, транспортних систем, знищення національної ідентичності. Особливого значення, під час протистояння гібридній агресії, набуває інформація.*

*У зв'язку із цим, як на державному рівні, так і на рівні окремих суб'єктів інформаційної діяльності, зростає проблема забезпечення інформаційної безпеки з метою захисту від деструктивного впливу ззовні.*

*Варто зазначити, що сьогодні у нашій державі та її Збройних Силах триває інтенсивний процес формування системи інформаційної безпеки. Тому розробка науково обґрунтованих підходів до створення дієвої системи протидії загрозам національній безпеці держави в інформаційній сфері є актуальним науково-практичним завданням. Саме тому дана стаття присвячена змісту та принципам інформаційної діяльності Збройних Сил України, а також проблемам її вдосконалення.*

***Ключові слова:*** *інформаційна діяльність, Збройні Сили України, інформаційна безпека, принципи діяльності, завдання.*

***Аннотация.*** *Современный мир характеризуется бурным развитием информационных технологий, прогрессом инновационных технологий и коммуникативных средств, развитием аппаратов передачи информационных данных которые порождают ситуацию неограниченных возможностей реализации информационных процессов для достижения некоторой цели, исполнения большого количества задач практической деятельности. С развитием технологий изменяются формы и способы ведения боевых действий. "Классические" методы ведения войны дополняются проведением информационных операций, информационно-психологических, информационно-технических (кибератак) что говорит о ведении новых – асимметрических, неформальных, гибридных воен с использованием оружия шестого поколения. В основе гибридной войны заложено использование асимметрических способов ведения боевых действий с целью доминирования на определенной территории, создания зон (территорий) замороженного конфликта на территории ведения боевых действий с целью изоляции противника на международном уровне, усиление антигосударственных настроев, деморализация войск противника, снижение морально-психологического состояния.*

*На сегодняшний день гибридная война составляет большую опасность функционированию системы национальной безопасности, государственной политики, нарушение роботы финансовой, транспортной систем и уничтожения национальной идентичности.*

*В связи с этим, на государственном уровне и на уровне отдельных субъектов информационной деятельности возрастает проблема обеспечения информационной безопасности во избежание деструктивного влияния из вне.*

*Стоит отметить, что сегодня в нашем государстве и ее Вооруженных Силах продолжается интенсивный процесс формирования системы информационной безопасности. Поэтому разработка научно обоснованных подходов к созданию действенной системы противодействия угрозам национальной безопасности государства в информационной сфере является актуальным научно-практической задачей. Именно поэтому данная статья посвящена содержанию и принципам информационной деятельности Вооруженных Сил Украины, а также проблемам ее совершенствования.*

***Ключевые слова:*** *информационная деятельность, Вооруженные Силы Украины, информационная безопасность, принципы деятельности, задачи.*

***Summary.*** *The modern world, which leaps into information technology, advances innovative technologies and communications technologies, develops devices, transmitting information that creates a situation that does not exist, but it can be used irrevocably for everyone in need of work, and great responsibilities on practical activity. With the development of technological, technologies that are created and created in the process, there are fighting. "Classical" methods, transmitted for the first time, trust information operations, information-psychological, economic operations, information-technology (cyberattacks),*

*keeping up-to-date news - asymmetric, informal, hybrid wars with the use of the sixth weapon on the results. The concept of hybrid war is usually used asymmetric methods of warfare with the use of dominance in the northern space, the creation of roots (forbidden) frozen conflicts to date combat really using unique capabilities of state-level confrontation, taking into account the internal forces of anti-war sentiment, raising the moral and psychological state. The state of hybrid warfare today leaves a large number of yields, a normally functioning national security system, while transport systems reduce the number of national identifiers. When you work with this, how to keep it, you mean that it is true information work, and it is important information about the security of information used by destructive factors. It is worth noting that today there are three long intensive processes of information security system in its own state and its Armed Forces. Therefore, the development of scientific research justified in the creation of existing systems of counteraction to civil security, which is used in the information system, is a relevant scientific and practical reason. At the same time, it became a possible change and fundamental information activity of the Armed Forces of Ukraine, as well as the problem of its improvement.*

***Key words:*** *information work, Armed Forces of Ukraine, information security, basic actions, work.*

**Постановка проблеми.** В умовах розбудови демократичної правової держави та громадянського суспільства в Україні зростає значення і роль інформаційної діяльності всіх без винятку органів держави, підприємств, установ та організацій. З точки зору забезпечення інформаційної безпеки особи, суспільства, держави негативний характер інформаційного впливу викликає потребу всебічного захисту та реабілітації цільової аудиторії, яка зазнає такого впливу, захисту власних інформаційних ресурсів, а також проведення попереджувальних заходів для його унеможливлення або зниження рівня ефективності.

Наукове опрацювання цього питання, зокрема в інтересах Збройних Сил України, є важливим з таких причин. По-перше, в передових у воєнному відношенні державах світу останнім часом накопичено значний науковий, технічний та практичний досвід проведення інформаційно-психологічних операцій, акцій, атак і актів при вирішенні завдань у ході воєнних конфліктів, коли об'єктами інформаційного впливу виступали збройні сили (формування) противника, – такий досвід необхідно вивчати та враховувати в практичній діяльності Збройних Сил України. По-друге, за цілою низкою ознак можна стверджувати, що ключова роль у війні Росії проти України належить інформаційній складовій у формі надпотужної інформаційної кампанії щодо провокування розколу в українському суспільстві та забезпечення встановлення контролю над південно-східними регіонами України. В цих умовах гостро постає проблема захисту національного інформаційного простору від зовнішніх інформаційних загроз. По-третє, наукова дискусія стосовно вирішення проблеми забезпечення інформаційної безпеки, у тому числі з її інформаційно-психологічною складовою, активно продовжується як у міжнародному вимірі, так і загальнодержавному в Україні, починаючи з термінології, – це викликає потребу подальших наукових досліджень цієї проблематики. По-четверте, активне реформування Збройних Сил України потребує адаптації наукових розробок, зокрема з питань протидії незаконному інформаційному впливу.

**Аналіз останніх досліджень та публікацій.** Для досягнення перемоги в збройних конфліктах необхідно одержувати, передавати й обробляти інформацію як найближче до реального часу. Усе це вимагає вдосконалення інформаційної моделі системи управління ЗСУ для забезпечення інформаційної переваги. Побудові інформаційної моделі системи управління збройних сил як сучасному різновиду стратегічного озброєння дотримуються науковці: Банах С.В.[5], Богуш В.М. [6], Жарков Я.М. [8],

В.Г. Дикун [11], Прохоренко М.М. [13]. Проте, малодослідженим залишається питання інформаційної діяльності ЗСУ, її основних засад та напрямків вдосконалення.

Окрім того, аналіз спеціалізованої літератури, показує, що на сьогодні у нашій державі та її Збройних Силах триває інтенсивний процес формування системи інформаційної безпеки, а саме у Міністерстві оборони України розроблені концептуальні документи та плани щодо розгортання такої системи, у Збройних Силах України створюються відповідні підрозділи. Разом з тим, забезпечення інформаційної безпеки держави в особливий період, в умовах якого цільовою аудиторією такого впливу розглядається особовий склад військ (сил) та органи військового управління, а об'єктами інформаційно-технічного впливу – засоби управління військами та зброєю, вивчено недостатньою мірою. Тому розробка науково обґрунтованих підходів до створення дієвої системи протидії загрозам національній безпеці держави в інформаційній сфері в особливий період є актуальним науково-практичним завданням.

**Формулювання цілей статті (постановка завдання).** Аналіз змісту та основних принципів інформаційної діяльності ЗСУ, її ролі у забезпеченні інформаційної безпеки нашої держави в сучасних умовах, а також проблеми її вдосконалення, що сформульовані відповідно до досвіду провідних країн світу.

**Виклад основного матеріалу:** Питання інформаційної діяльності ЗСУ регулюються Конституцією України, Законом України «Про Збройні Сили України» від 06.12.1991 р.№1934-XI [1], Законом України «Про національну безпеку України» від 21.06.2018р. № 2469-VIII [2], «Доктриною інформаційної безпеки України», затвердженою указом Президента України від 8.07.2009р. №514/2009[3],Наказом Міністерства оборони України «Про затвердження Концепції інформатизації Міністерства оборони України» від 17.09.2014 р. №650 [4] та іншими

нормативно-правовими актами. Проте, незважаючи на існуючу нормативну базу, яка регламентує процес інформатизації в Україні, рівень інформатизації у Міністерстві оборони не відповідає сучасним потребам. Основною причиною цього є неналежне науково-теоретичне опрацювання основних процесів інформатизації у Міністерстві оборони України і Збройних Силах України та, як наслідок, – на всіх рівнях системи військового управління недостатній рівень розуміння змісту інформатизації, її ролі та місця як складової формування інформаційного середовища у сфері оборони і держави загалом.

Російська агресія змусила нас переглянути підходи щодо інформаційної політики держави, застосування Збройних Сил України та використання кіберпростору в нових умовах. Виконуючи завдання Президента України – Верховного Головнокомандувача Збройних Сил України щодо нарощування обороноздатності держави, в Україні було затверджено Концепцію розвитку сектору безпеки і оборони України, нові редакції Стратегічного оборонного бюлетеня України та Воєнної доктрини України, а також Державну цільову оборонну програму розвитку озброєння та військової техніки і Державну програму розвитку Збройних Сил України на період до 2020 року, в яких, відповідно до світових тенденцій, базовим є акцент на розвиток сектору безпеки та оборони держави, у тому числі і щодо дій в інформаційному просторі [15, с.79].

За останній період в Україні спостерігається тенденція збільшення випадків використання інформації як інформаційно-психологічної зброї. За її допомогою здійснюється приховане маніпулювання інформацією з метою ураження індивідуальної і масової свідомості цільової аудиторії в інформаційному просторі (наприклад, гібридна війна РФ проти України починаючи з 2014 року). Тому розвиток інформаційно-телекомунікаційних технологій обумовлює підвищення рівня безпеки в кіберпросторі. Інформаційна протидія в кіберпросторі – це лише одна із складових

елементів забезпечення інформаційної безпеки. Одним з важливих напрямів забезпечення обороноздатності країни є підтримання на достатньо високому рівні інформаційної безпеки Збройних Сил України [13, с. 57].

Варто зазначити, що реалізацію державної інформаційної політики в Міноборони та Збройних Силах України, ведення інформаційно-роз'яснювальної роботи з питань підвищення престижу військової служби, формування в українському суспільстві позитивної громадської думки щодо Збройних Сил та висвітлення їх діяльності, виконання завдань в інформаційній сфері, забезпечення ефективної діяльності системи інформування громадськості та взаємодії зі ЗМІ покладено на Управління комунікацій та преси Міністерства оборони України.

Забезпечення інформаційної діяльності Міністерства оборони України та Збройних Сил України здійснюють підпорядковані структури:1 газета — Центральний друкований орган Міністерства оборони України «Народна армія» (м. Київ); 1 журнал — Центральний друкований орган Міністерства оборони України «Військо України» (м. Київ); 1 телерадіоорганізації — Центральна телерадіостудія Міністерства оборони України (м. Київ), Телерадіокомпанія Міністерства оборони України «Бриз» (м. Одеса) [9, с.41].

Метою інформаційної діяльності ЗСУ є нейтралізації існуючих загроз в інформаційній сфері, проведення попереджувальних заходів військових ЗМІ в інформаційній сфері, що зосереджено на використанні всесвітньої мережі Інтернет, а також інформування суспільства про реформування Міністерства оборони України та Збройних Сил України, їх життєдіяльність та виконання ними завдань забезпечення оборони держави, захисту її суверенітету та територіальної цілісності, зокрема, в ході антитерористичної операції на території Донецької та Луганської областей, створення позитивного іміджу ЗС України у суспільстві.

Інформаційна діяльність Міністерства оборони України та ЗСУ спрямована на забезпечення основних принципів:

- своєчасне, об'єктивне та вичерпне інформування особового складу та громадськості про життєдіяльність Збройних Сил України, зокрема, в контексті останніх подій, які відбуваються в державі;
- підтримання на високому рівні морально-психологічного стану особового складу з використанням відпрацьованих форм інформаційної діяльності;
- формування психологічної стійкості, мотивації військовослужбовців до виконання найважливіших завдань щодо підтримання високої обороноздатності держави;
- створення умов для формування у Збройних Силах України розвинутого інформаційного середовища як елемента прозорого, демократичного цивільного контролю над військовими формуваннями;
- оприлюднення офіційної позиції Міністерства оборони України, забезпечення підтримки урядових рішень та вільного доступу до інформації.

Основою інформаційної діяльності Міністерства оборони України є доведення керівництвом Міністерства оборони України, Генерального штабу Збройних Сил України до громадськості відомостей про діяльність Міністерства оборони України як органу виконавчої влади та Збройних Сил України як інституту збройного захисту держави.

Основні форми поширення інформації: брифінги, прес-конференції та інтерв'ю керівного складу Міністерства оборони України та Генерального штабу Збройних Сил України для засобів масової інформації; підготовка публікацій для друкованих та електронних засобів масової інформації та ін.

Найефективнішими шляхами проведення інформаційно-роз'яснювальної роботи стали: постійне інформування суспільства про

життєдіяльність Міністерства оборони України та Збройних Сил України шляхом оприлюднення інформаційних повідомлень на офіційному веб-порталі Міністерства оборони України у мережі Інтернет, підготовки публікацій у друкованих ЗМІ, трансляції відповідної інформації у теле- та радіоефірі; збільшення присутності Міністерства оборони України в мережі Інтернет та популяризація офіційного веб-порталу Міністерства оборони України шляхом розсилки інформаційних повідомлень та відео матеріалів з посиланнями на веб-портал.

З початку року Управлінням підготовлено, направлено до вітчизняних засобів масової інформації та оприлюднено через офіційний веб-портал Міністерства оборони України в мережі Інтернет близько 1600 інформаційних повідомлень і прес-релізів. Матеріали поширювалися серед вітчизняних та іноземних ЗМІ (понад 500 адресатів).

Постійно діє англомовна версія стрічки новин офіційного веб-порталу Міністерства оборони України та офіційної сторінки Міністерства оборони України у соціальної мережі «Facebook».

Постійно здійснюється цілодобовий моніторинг центральних та регіональних ЗМІ. Щоденно готуються огляди новин (тричі на добу на 8.00, 13.00 та 21.00) та дайджести газетних матеріалів з оборонної тематики.

У зв'язку з активним інформуванням громадян України про поточну суспільно-політичну ситуацію на Сході України та пов'язаним з цим надзвичайним ростом престижу військової служби у Збройних Силах України, офіційний веб-портал Міністерства оборони України відвідало понад 350 тисяч користувачів.

На щоденне отримання новин від Міноборони у соціальній мережі «Facebook» підписано182 тисячі 495 осіб. Кількість переглядів відеоматеріалів каналу Міністерства оборони на Інтернет-каналі «Youtube» становить 2 мільйона 887 тисяч 636 осіб. На канал підписано 4 тисячі 675

осіб. Сторінка Міністерства оборони в соціальній мережі мікроблогів Twitter на сьогодні має 25 тисяч 815 читачів [9, с. 42].

З метою інформування суспільства про заходи реформування і розвитку Збройних Сил України Управлінням організовано, проведено та забезпечено інформаційне супроводження наступних найважливіших заходів за участю посадових осіб Міністерства оборони та Генерального штабу ЗС України, за участю керівного складу Міністерства оборони та Збройних Сил України та інших посадових осіб: 5 брифінгів та прес-конференцій; участь у 7 теле-, радіопрограмах; 43 інтерв'ю та коментарів вітчизняним та зарубіжним ЗМІ. Також забезпечено підготовку та інформаційне супроводження участі керівництва Мінооборони у прямій телефонній лінії Кабінету Міністрів України та брифінгу для представників ЗМІ перед початком її проведення [9, с. 44].

На виконання рішення Міністра оборони України, з метою об'єктивного та оперативного висвітлення питань діяльності Міністерства оборони України та Збройних Сил України проводяться: брифінги в Українському кризовому медіа-центрі речників Міністерства оборони України (двічі на тиждень); брифінги речників Міністерства оборони України з питань АТО в Українському кризовому медіа-центрі (щодня); брифінги англомовного речника Міністерства оборони України в Українському кризовому медіа-центрі з питань українсько-російського військового конфлікту для іноземних засобів масової інформації (щопонеділка).

Зазначені заходи дозволили значно знизити стурбованість і напругу в суспільстві щодо нагальних питань діяльності Міністерства оборони України, забезпечення військовослужбовців в зоні АТО необхідним речовим та медичним майном, піклування про них з боку держави. Забезпечено постійне оперативне наповнення достовірною інформацією з

актуальних питань державної політики (в межах компетенції) Українського національного інформаційного агентства «Укрінформ».

Також забезпечено висвітлення у засобах масової інформації заходів міжнародного співробітництва в Україні та за кордоном, участі Міністерства оборони України, Збройних Сил України у загальнодержавних заходах з нагоди державних свят та пам'ятних дат, робочих поїздок Міністра оборони України та начальника Генерального штабу – Головнокомандувача ЗС України у військові гарнізони та райони проведення Антитерористичної операції, участі Збройних Сил України у міжнародних навчаннях, тактичних навчаннях на всій території України.

На сьогоднішній день у Збройних Силах України є актуальними завдання із захисту власного інформаційного простору військових частин та підрозділів, частина з яких може покладатись на командирів підрозділів, які беруть участь у визначенні інформаційно-психологічного впливу (ІПсВ) на підлеглий особовий склад та проведенні окремих заходів протидії ІПсВ [12, с. 118].

Прискорений розвиток технологічних засад інформаційного суспільства (ІС), неконтрольоване поширення новітніх інформаційних технологій та створення глобального інформаційного простору призводить до того, що інформаційні технології стають, по суті, основним джерелом інформації для кожної людини, здійснюють безпосередній вплив на її психічну діяльність, формування її соціальної поведінки. Фактично навкруги людини створюється її індивідуальний "віртуальний інформаційний простір" з можливістю практично безперешкодного доступу, моніторингу та диференційованого ІПсВ на конкретну особистість. Людина в цих умовах може втратити свою незалежну особистість, перетворитись у "віртуальний біоресурс" для рефлексивного управління й інформаційно-психологічних маніпуляцій [11, с. 312].

В інформаційному світі визначальною стає можливість безпосереднього ІПсВ на населення країни, особовий склад її збройних сил, інших військових формувань, що ускладнює ефективне вирішення завдання їх інформаційного захисту з боку відповідних державних структур без усвідомленої допомоги самої людини. Тому є виключно важливим забезпечити безпеку взаємодії людини з інформаційними технологіями (інформаційним середовищем) шляхом отримання певного мінімуму знань про закони розвитку інформаційного суспільства (його окремі негативні чинники і ризики), можливий деструктивний вплив та основи захисту від інформаційних загроз для особистості й суспільства. Це завдання особливо актуальне відносно особового складу збройних сил і, в першу чергу, усього офіцерського складу.

На сьогодні в нашій державі та її Збройних Силах ще не до кінця створено цілісну систему інформаційної безпеки, яка б у повному обсязі забезпечувала гарантований захист і надійну протидію інформаційним загрозам. Разом з тим, триває інтенсивний процес її формування, зокрема в Міністерстві оборони України розроблені концептуальні документи і плани щодо розгортання такої системи, у ЗСУ створюються відповідні підрозділи [14, с. 40].

Однак відсутність власного досвіду формування зазначеної системи та різноплановість поглядів на шляхи підтримання інформаційної безпеки у сфері оборони держави, складність вивчення питань інформаційної безпеки у воєнній сфері, котра полягає в слабко виявлених зв’язках між елементами всієї системи, не дає змоги повною мірою визначити структуру системи інформаційної безпеки цієї сфери, її завдання та функції. Тому розробка науково обґрунтованих підходів до створення дієвої системи гарантування інформаційної безпеки держави у сфері оборони з урахуванням досвіду іноземних держав є актуальним науково-практичним завданням.

Інформаційними загрозами стосовно нашої держави, як визначено в Законі України «Про національну безпеку України» [2], можуть бути: прояви обмеження свободи слова та доступу громадян до інформації;поширення засобами масової інформації культу насильства, жорстокості, порнографії;намагання маніпулювати суспільною свідомістю, зокрема шляхом поширення недостовірної, неповної або упередженої інформації;розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;комп'ютерна злочинність та комп'ютерний тероризм.

Разом з тим, на думку Ю.І. Радковець, сформованими на основі аналізу іноземного впливу на інформаційний медіа та кіберпростір України, існують ознаки реальних загроз для нашої держави. Про це свідчать такі основні тенденції: цілеспрямоване формування окремими іноземними державами негативного міжнародного іміджу України;активізація критики вищого державного керівництва України; здійснення низкою зарубіжних країн потужного інформаційного тиску на Україну з метою спонукання українського керівництва до прийняття вигідних для цих країн рішень у внутрішньо та зовнішньополітичній сферах;посилення інформаційних заходів з перешкоджання реалізації Україною її зовнішньополітичного курсу та спонукання її до участі в проектах, які в сучасних умовах не вигідні нашій державі; дискредитація нашої держави як конкурента у сфері міжнародного військово-технічного співробітництва;зростання для України загроз кібернетичних атак, що зумовлено появою нових, більш досконалих зразків кібернетичної зброї [14, с. 38]. Крім того, новим джерелом загроз інформаційній безпеці України слід вважати соціальні мережі, які можуть використовуватись окремими країнами для просування власної ідеології у світі та впливу на ситуацію в нашій країні.

У збройних силах іноземних держав системи інформаційної безпеки загалом побудовані за подібними підходами, але з урахуванням національних особливостей При цьому країни, які входять до певних воєнно-політичних блоків, будують відомчі системи інформаційної безпеки відповідно до принципу розподіленості зусиль у рамках колективних систем безпеки.

Цей досвід може застосовуватися для побудови системи інформаційної безпеки як нашої держави, так і її Збройних Сил. Але при формуванні системи інформаційної безпеки держави у сфері оборони обов'язково слід ураховувати геополітичне положення нашої країни, її позаблоковий стан та національні особливості.

Для прикладу, у Міністерстві оборони Великобританії питаннями випуску друкованої продукції, а також теле- і радіопрограм займається Комітет міністерства з питань преси, телебачення і радіомовлення. Центральний апарат Міністерства, штаби органів ЗС, великі військові бази і гарнізони мають свої сторінки в Інтернеті. За питання висвітлення діяльності ЗС в телевізійному і радіоефірі відповідає Корпорація радіо- і телемовлення Збройних Сил, яка має статус самостійного органу Міністерства оборони Великобританії. Її очолює цивільна особа (керівник), безпосередньо підкоряється помічнику заступника міністра оборони. Основними завданнями корпорації є забезпечення радіо- і телемовлення на гарнізони Збройних Сил Великобританії, в тому числі на заморських територіях, а також підготовка радіо-, кіно-, відео- і фотографічного матеріалу для військово-навчальних закладів, штабів і військ [15, с. 78].

Крім того, Сполучене Королівство має багато оперативних розвідувальних служб, включаючи оперативний розвідувальний підрозділ 22-го полку SAS, який надає широку інформаційну підтримку підрозділам спеціальних сил. Банах С.В. відзначає: «Серед функцій оперативного розвідувального підрозділу збір даних щодо можливих напрямків майбутніх

військових дій (фізико-географічні умови, історія, культура, релігія тощо), збройних сил імовірного ворога, зокрема наявність протидії – підривні блоки; адміністрування баз даних про терористичні організації та прогнозування терористичних актів. Він також збирає дані та узагальнює досвід бойового застосування спеціальних антитерористичних підрозділів усіх країн. Він активно співпрацює з Комітетом з питань оборони і зовнішньої політики, британською військовою розвідкою і контррозвідкою, іншими розвідувальними службами національних збройних сил, а також зі спеціальними підрозділами країн НАТО» [5, с. 110]. Такий досвід інформаційної співпраці між підрозділами органів внутрішніх справ та збройних сил Великобританії, вважаємо позитивним, та потрібним для України у сучасних умовах.

У Міністерстві оборони Франції відсутні органи, спеціально орієнтовані на інформування зарубіжної громадськості. Разом з тим керівництво Міністерства і командування Збройних Сил надають великого значення реалізації механізму інформування французької та зарубіжної громадськості, що, на їхню думку, сприяє створенню позитивного образу, розвитку відкритості в дусі зміцнення заходів довіри, подолання негативних наслідків скорочення чисельності Збройних Сил та працівників військових галузей промисловості. Завдання інформування зарубіжної громадськості у Франції вирішують особисто представники вищого військового командування, апарати військових аташе (аташе оборони) в країнах перебування під керівництвом управління зовнішніх відносин штабу Збройних Сил, а також служба інформації і громадських зв'язків (SIRPA) Міністерства оборони.

Центр засобів масової інформації ЗС ФРН грає важливу роль в інформаційному забезпеченні військ і освітленні їх повсякденній діяльності. Організаційно Центр підпорядкований центральному управлінню Збройних Сил міністерства оборони ФРН. Основним завданням Центру є

інформаційно-пропагандистська робота у військах і серед цивільного населення [15, с. 79].

Зважаючи на досвід провідних країн світу, основною метою створення Системи гарантування інформаційної безпеки держави у сфері оборони (далі – Системи) є запобігання та нейтралізація інформаційних загроз їх функціонуванню; створення умов для сталого й гарантованого виконання Міністерством оборони України та Збройними Силами України завдань, визначених Конституцією та законами України. Відповідно до зазначеної мети, доцільно визначити основні функції такої Системи:

1) створення й забезпечення діяльності організаційних структур та елементів Системи, зокрема: розроблення адміністративно-правових засад для побудови та функціонування Системи; усебічне забезпечення діяльності елементів Системи;

2) управління Системою, зокрема: розроблення та введення в дію Керівництва із підтримання інформаційної безпеки в Міністерстві оборони та Збройних Силах України, у якому визначаються єдині підходи до запобігання та нейтралізації інформаційних загроз;прогнозування, планування, організація, координація та контроль у межах Системи та окремих її елементів;оцінювання результативності заходів протидії інформаційним загрозам, витрат на їх підготовку та проведення;

3) проведення планової і оперативної діяльності з підтримання інформаційної безпеки та протидії інформаційним загрозам, зокрема: визначення та формування моделі потенційних і реальних інформаційних загроз;визначення об’єктів критичної інфраструктури, які мають важливе значення для національної безпеки та оборони; виявлення інформаційних загроз, джерел їх виникнення, а також прогнозування можливих наслідків у разі їх реалізації з відпрацюванням відповідних превентивних заходів;удосконалення форм, методів і засобів запобігання загрозам інформаційній безпеці та ліквідація наслідків її порушення.

**Висновки.** Підводячи підсумок даного дослідження необхідно наголосити на наступному:

1. Досвід іноземних країн свідчить, що забезпечення надійної протидії сучасним викликам і загрозам національній безпеці України в інформаційній сфері можливе лише за умови формування та проведення єдиної державної інформаційної політики та системного підходу до організації захисту національного інформаційного простору. Виходячи із цього, для гарантування інформаційної безпеки Збройних Сил України доцільно формувати відомчу систему підтримання інформаційної безпеки як складову загальнодержавної системи, яка структурно має складатися із взаємопов'язаних функціональних підсистем: виявлення інформаційних загроз; аналізу і прогнозування загроз та планування заходів інформаційної безпеки; протидії інформаційним загрозам; захисту від інформаційних загроз; наукових досліджень; підготовки спеціалістів з питань інформаційної безпеки. Такий підхід дасть змогу побудувати раціональну систему інформаційної безпеки держави у сфері оборони та забезпечити підвищення загальної ефективності протидії загрозам у інформаційному просторі України.

2. Інформаційна діяльність ЗСУ повинна будуватись на принципах: відкритості інформації для громадськості про діяльність ЗСУ та інших складових частин Воєнної організації держави, що не становить державну таємницю;незалежності від незаконного впливу будь-яких структур, органів чи організацій; відповідальності посадових осіб за повноту, достовірність і своєчасність наданої інформації, та за реагування на звернення громадян, організацій, засобів масової інформації;запровадження новітніх методів в процеси управлінської діяльності відповідно до сучасного рівня розвитку інформаційних технологій у сфері інформатизації та створення умов для надійної взаємодії інформаційних систем

Міністерства оборони України, ЗСУ та органів внутрішніх справ України.

3. Основними завданнями Міністерства оборони мають бути: координація діяльності інформаційних органів Збройних Сил; інформування громадськості з питань військової політики, будівництва, стану і перспектив розвитку Збройних Сил, що плануються і поточних кадрових змінах та найбільш важливих моментах у діяльності структур МО; пропаганда військової служби серед населення, формування сприятливого образу Збройних Сил в громадській думці; інформаційне забезпечення заходів, що проводяться МО (церемонії, конференції, симпозіуми, військові виставки, конкурси для набору добровольців на службу в армію); поширення в Збройних Силах матеріалів з питань військової політики і діяльності Збройних Сил, випуск військових видань і забезпечення військ відповідними матеріалами. Необхідно відзначити, що в даний час в арміях країн НАТО приділяється величезна увага інформаційному забезпеченню населення та збройних сил. А інформаційно-психологічні дії стають самостійним способом застосування засобів в «інформаційній війні».

## Література

1. Про Збройні Сили України: Закон України від 06.12.1991р.№1934-XI // URL: https://zakon.rada.gov.ua/laws/show/1934-12
2. Про національну безпеку України: Закон України від 21.06.2018р. № 2469-VIII // URL:https://zakon.rada.gov.ua/laws/show/2469-19#n355
3. Доктрина інформаційної безпеки України: затверджена Указом Президента України від 8 липня 2009 року № 514/2009. К.: Офіційний вісник України, 2009. № 52.
4. Про затвердження Концепції інформатизації Міністерства оборони України: Наказ Міністерства оборони України від 17.09.2014 р. № 650. URL: https://zakon.rada.gov.ua/rada/show/v0650322-14

5. Банах С. В. Поняття інформаційної діяльності правоохоронних органів // Актуальні проблеми правознавства. 2019. Вип. 3. С. 107-112.
6. Богуш В. М. Інформаційна безпека держави. Київ: МКПрес, 2005. 432 с.
7. Галушко С. О. Протиборство в інформаційному просторі // Оборонний вісник. 2011. № 11. С. 16–19.
8. Жарков Я.М. Напрями зовнішнього інформаційно-психологічного впливу на Україну // Сучасні інформаційні технології у сфері безпеки та оборони. 2009. № 1 (4). С. 42–46.
9. Кондратенко А.В. Досвід інформаційних структур Міністерства оборони України в інформаційному протистоянні в умовах гібридної війни // Інформаційний вимір гібридної війни: досвід України: матеріали міжнародної науково-практичної конференції. Київ: НУОУ, 2017. С. 41-44.
10. Левченко О.В. Концептуальний підхід до комплексної оцінки стану інформаційної безпеки // Наука і техніка Повітряних Сил Збройних Сил України.2015. № 3 (20). С. 47-50.
11. Морально-психологічне забезпечення у Збройних Силах України: підр. у 2-х ч. Ч.1. / ред. В.М. Вілко, В.М. Грицюк, В.Г. Дикун. Київ: НУОУ, 2012. 464 с.
12. Ожеван М.А. Основні напрями зовнішніх інформаційно-маніпулятивних впливів на суспільні трансформації в Україні: засоби протидії // Стратегічні пріоритети. 2011. № 3. С. 118-126.
13. Право національної безпеки та військове право: історія, сучасність і перспективи: збірник матеріалів / заг. ред. М.М. Прохоренка. Київ, 2019. 168 с.
14. Радковець Ю.І. Погляди на створення системи інформаційної безпеки України та її Збройних Сил // Наука і оборона. 2014. № 1. С. 38-41.

15. Синчук Ю. В. Информационные структуры армий ведучих зарубежных государств // Вестник МГЛУ. 2017. Вип. 3. С. 78-96.

**References**

1. Pro Zbroini Syly Ukrainy: Zakon Ukrainyvid 06.12.1991r.№1934-XI // URL: https://zakon.rada.gov.ua/laws/show/1934-12 [in Ukrainian].
2. Pro natsionalnu bezpeku Ukrainy: Zakon Ukrainy vid 21.06.2018r. № 2469-VIII. URL:https://zakon.rada.gov.ua/laws/show/2469-19#n355 [in Ukrainian].
3. Doktryna informatsiinoi bezpeky Ukrainy: zatverdzhena Ukazom Prezydenta Ukrainy vid 8 lypnia 2009 roku № 514/2009. K.: Ofitsiinyi visnyk Ukrainy, 2009. № 52 [in Ukrainian].
4. Pro zatverdzhennia Kontseptsii informatyzatsii Ministerstva oborony Ukrainy: Nakaz Ministerstva oborony Ukrainy vid 17.09.2014 r. № 650. URL: https://zakon.rada.gov.ua/rada/show/v0650322-14 [in Ukrainian].
5. Banakh S. V. Poniattia informatsiinoi diialnosti pravookhoronnykh orhaniv // Aktualni problemy pravoznavstva. 2019. Vyp. 3. S. 107-112. [in Ukrainian].
6. Bohush V. M. Informatsiina bezpeka derzhavy. Kyiv: MKPres, 2005. 432 s.
7. Halushko S. O. Protyborstvo v informatsiinomu prostori // Oboronnyi visnyk. 2011. № 11. S. 16–19 [in Ukrainian].
8. Zharkov Ya.M. Napriamy zovnishnoho informatsiino-psykholohichnoho vplyvu na Ukrainu // Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony. 2009. № 1 (4). S. 42–46 [in Ukrainian].
9. Kondratenko A.V. Dosvid informatsiinykh struktur Ministerstva oborony Ukrainy v informatsiinomu protystoianni v umovakh hibrydnoi viiny // Informatsiinyi vymir hibrydnoi viiny: dosvid Ukrainy: materialy mizhnarodnoi naukovo-praktychnoi konferentsii. Kyiv: NUOU, 2017. S. 41-44 [in Ukrainian].

10. Levchenko O.V. Kontseptualnyi pidkhid do kompleksnoi otsinky stanu informatsiinoi bezpeky // Nauka i tekhnika Povitrianykh Syl Zbroinykh Syl Ukrainy.2015. № 3 (20). S. 47-50 [in Ukrainian].
11. Moralno-psykholohichne zabezpechennia u Zbroinykh Sylakh Ukrainy: pidr. u 2-kh ch. Ch.1./ red. V.M. Vilko, V.M. Hrytsiuk, V.H. Dykun. Kyiv: NUOU, 2012. 464 s. [in Ukrainian].
12. Ozhevan M.A. Osnovni napriamy zovnishnikh informatsiino-manipuliatyvnykh vplyviv na suspilni transformatsii v Ukraini: zasoby protydii // Stratehichni priorytety. 2011. № 3. S. 118–126 [in Ukrainian].
13. Pravo natsionalnoi bezpeky ta viiskove pravo: istoriia, suchasnist i perspektyvy: zbirnyk materialiv / zah. red. M.M. Prokhorenka. Kyiv, 2019. 168 s. [in Ukrainian].
14. Radkovets Yu.I. Pohliady na stvorennia systemy informatsiinoi bezpeky Ukrainy ta yii Zbroinykh Syl // Nauka i oborona. 2014. № 1. S. 38–41 [in Ukrainian].
15. Synchuk Yu. V. Ynformatsyonnye strukturы armyi veduchykh zarubezhnыkh hosudarstv. Vestnyk MHLU. 2017. Vyp. 3. S. 78-96. [in Russian].