УДК 329.09.5(477)
ПОРОНЮК Р.О.
https://orcid.org/0000-0001-5289-9431
ГАПЄЄВА О.Л.
https://orcid.org/0000-0002-3145-7025
https://doi.org/10.33577/2313-5603.38.2022.266-280

ДІЯЛЬНІСТЬ ГРУП МОНІТОРИНГУ ІНФОРМАЦІЙНОГО ПРОСТОРУ ТА ПРОТИДІЇ ЯК СКЛАДОВА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ У ВОЄННІЙ СФЕРІ

У статті розглядається діяльність груп моніторингу інформаційного простору та протидії обласних військових комісаріатів та військових частин безпосереднього підпорядкування оперативних командувань Сухопутних військ Збройних Сил України у 2018 – 2020 рр. Основна увага сконцентрована на історичних передумовах та правничих підставах їх створення, аналізі діяльності щодо протидії негативному інформаційному впливу в українському медіасередовищі з боку російської федерації, узагальненню отриманого досвіду в контексті забезпечення інформаційної безпеки держави у воєнній сфері. Досліджуються досвід та діяльність офіцерів підрозділів інформаційної боротьби за своїм призначенням у складі Командування Сухопутних військ як у зоні проведення операції Об'єднаних сил, так і в пунктах постійної дислокації.

Ключові слова. групи моніторингу інформаційного простору та протидії, Збройні Сили України, інформаційна війна, інформаційна протидія, комунікаційна кампанія.

Постановка проблеми та її актуальність. Через стрімкий розвиток сучасних форм і методів інформаційного впливу на світову спільноту українське суспільство, особовий склад Збройних Сил України та, особливо, мешканці тимчасово окупованих територій потерпають від інформаційних гібридних атак російської федерації. Виникає необхідність пошуку нових та удосконалення існуючих форм і методів протидії негативному інформаційному впливу, виробленні дієвих засобів протидії агресивній інформаційній політиці кремля.

Аналіз останніх досліджень і публікацій. Забезпечення інформаційної безпеки України «…тривалий час залежало від зовнішньополітичного курсу держави й поглядів її керівництва, отже

Поронюк Роман Олександрович, ад'юнкт штатний науково-організаційного відділу, Національна академія сухопутних військ імені гетьмана Петра Сагайдачного, м. Львів.

Гапеєва Ольга Львівна, кандидат історичних наук, старший науковий співробітник, професор кафедри мобілізаційної, організаційно-штатної, кадрової роботи та оборонного планування, Національна академія сухопутних військ імені гетьмана Петра Сагайдачного, м. Львів.

носить ситуативний і амплітудний характер» (*Гапеєва О.Л., 2017:423)*. Від початку російської "гібридної" агресії відбулись відчутні зміни у концептуальному і нормативно-правовому забезпеченні проблематики інформаційної безпеки.

Питання протидії негативному інформаційному впливу розглядали українські дослідники Я. Жарков, Л. Смола, Б. Ратніков, П. Черник, А. Шумка, В. Телелим, В. Горбулін, І. Руснак, Г. Певцов, Г. Почепцов, М. Подибайло та ін.

Діяльність груп моніторингу інформаційного простору та протидії у 2018–2020 рр., враховуючи відносно короткий історичний проміжок часу їх існування, ще не стала предметом дослідження українських науковців. Натомість, створення системи, яка могла б забезпечити своєчасне виявлення негативної (неправдивої інформації) та оперативно протидіяти даним чинникам, було розглянуто у науковій статті П. Сніцаренка, Ю. Саричева, В. Семененка, В. Ткаченка ще до офіційного введення таких структур (*Сніцаренко, 2018*).

Метою наукової розвідки є дослідження та аналіз діяльності груп моніторингу інформаційного простору та протидії, спираючись на розпорядчу документацію (накази, директиви, розпорядження) та досвід особового складу цих підрозділів; визначити доцільність їх створення та ефективність проведеної роботи у контексті протидії агресивному інформаційному впливу російської федерації на українське військо, населення України та мешканців тимчасово окупованих територій.

Виклад основного матеріалу. У лютому 2018 р. при обласних військових комісаріатах та частинах безпосереднього під порядкування оперативним командуванням (далі – ОК), на підставі Наказу командувача Сухопутних військ Збройних Сил України (далі – КСВ ЗС України) № 113 дск від 23.02.2018 "Про затвердження Тимчасової інструкції з організації та проведення заходів забезпечення інформаційної безпеки Сухопутних військ Збройних Сил України" були сформовані групи моніторингу інформаційного простору та протидії (далі – ГРМП), які виконували свої завдання за призначенням понад два роки.

Правовою підставою для створення ГРМП було виконання оперативної цілі 1.7 Стратегічного оборонного бюлетеня, схваленого Указом Президента України від 06.06.2016 року № 240/2016. Зокрема, Оперативна ціль 1.7. передбачає: "…становлення та

розбудову спроможностей сил оборони у сфері стратегічних комунікацій як частини загальнодержавної та міжвідомчої системи стратегічних комунікацій, спрямованих на підтримку формування та реалізації політики у сфері безпеки і оборони України, також досягнення цілей оборони держави. Результативний (індикативний) показник: Створено комунікаційні спроможності на стратегічному, оперативному та тактичному рівнях, що забезпечують інтеграції та підтримки стратегічними комунікаціями на усіх рівнях планування та впровадження політики у сфері безпеки і оборони" (Указ Президента України від 6 червня 2016 року № 240 «Про рішення Ради національної безпеки і оборони України від 20 травня 2016 р. «Про Стратегічний оборонний бюлетень України»).

У перші дні російсько-української війни (2014 р.) проти якісно підготовлених, з потужною матеріально-технічною та методичною базою, гібридно-інформаційних військ збройних сил рф виступили підрозділи Служби безпеки України, Міністерства внутрішніх справ та ІПСО ЗС України. Проте вони мали свої окремі напрямки діяльності та дещо специфічні завдання. Окрім того, невелика чисельність даних підрозділів, їх матеріально-технічне забезпечення не дозволяла охопити всі необхідні ділянки. Тому на даному етапі на допомогу силовому блоку в інформаційній боротьбі повстали поодинокі "блок пости" українських патріотичних сил, цивільних та військових журналістів, блогерів, "інформволонтерів". Серед них найбільш відомими є проєкт Центру військово-політичних досліджень (м. Київ) – "Інформаційний спротив" Дмитра Тимчука; Stopfake.org –випускників та викладацького складу Могилянської школи журналістики та Програми для журналістів і редакторів – DigitalFutureofJournalism; проєкт InformNapalm, діяльність якого за інформативністю порівнюють із публікаціями WikiLeaks; проєкт-сайт "Інформаційні війська України" i-army.org, створений з метою залучення громадян України до інформаційної діяльності проти російської пропаганди і дезінформації (*Гапеєва О.Л., 2017:423*). Діяльність цих громадських організацій заповнила український інформаційний простір, надавши при цьому час для створення штатних підрозділів моніторингу інформаційного простору та протидії у Сухопутних військах ЗС України. Слід додати, що до моменту створення ГРМП значна частина цих обов'язків покладалась на структури

по роботі з особовим складом. Проте із врахуванням кількості додаткових завдань для даних підрозділів роботи з особовим складом, комунікації з громадськістю, проведення службових розслідувань – у них банально не вистачало часу на якісне виконання даних додаткових обов'язків.

Посади у ГРМП комплектувалися виключно особами офіцерського складу. Обов'язковою умовою стали такі якості, як комунікабельність, вміння писати тексти за визначеною тематикою, робота з графічними редакторами, високі навички володіння персональним комп'ютером, наявність професійних зв'язків із представниками ЗМІ та громадськістю. До складу групи увійшли офіцери з числа журналістів, призваних по мобілізації на особливий період, волонтерів, громадських діячів, а також фахівців підрозділів морально-психологічного забезпечення, зв'язківців, програмістів тощо.

Існував певний алгоритм відбору кандидатів до проходження військової служби у ГРМП. Так, кандидатури усіх претендентів підлягали ретельному вивченню: командири структурних підрозділів подавали свої пропозиції; у подальшому інформація узагальнювалась у вищих штабах, вносились певні корективи. Пізніше представники командування КСВ ЗС України ознайомлювались з особовими справами офіцерів, вивчали їхні морально-ділові якості, проводили особисті співбесіди з усіма кандидатами, приймали відповідні рішення щодо призначення на кожну конкретну посаду.

Необхідно зазначити, що у подальшому призначення іншого офіцера на посаду здійснювалось виключно за погодженням КСВ ЗС України, що свідчить про увагу керівництва до вирішення питань інформаційної протидії через якісне комплектування та функціонування новоствореного підрозділу.

Особливе значення приділялось професійній підготовці особового складу ГРМП. Так, за три роки існування цих груп за рішенням вищого командування особовий склад проходив підготовку на курсах та зборах у провідних військових вишах України, серед яких:

- Національна академія сухопутних військ (2018 рік);
- Національний університет оборони України імені Івана Черняховського (2018 рік);

- Військовий інститут телекомунікацій та інформатизації імені Героїв Крут (2019 рік).

Суттєвою та цінною була допомога наших міжнародних партнерів держав–членів НАТО, зокрема США, Польщі, Литви, Великобританії. Для проведення занять залучались фахівці інформаційно-аналітичних структур, зв'язків із громадськістю (РАО), викладачі провідних вищих військових навчальних закладів Альянсу. Такі курси тривали один тиждень на базі Центрального будинку офіцерів Збройних Сил України. Слухачів навчали формам і методам роботи щодо інформування громадськості, комунікації зі своїми громадянами, а головне – алгоритмам пошуку негативної чи "фейкової" новини, яка може завдати шкоди армійському підрозділу, та формам і методам реакції на неї. Важливо, що все навчання зводилося до головного принципу – першим давати інформацію та говорити правду, із урахуванням інтересів військової частини, армії, держави.

Слід зауважити, що ГРМП швидко та органічно зайняли своє місце, яке з об'єктивних та суб'єктивних причин до 2018 року було вакантне як в системі ЗС України, так і національної безпеки держави загалом. У стислі терміни був налагоджений механізм отримання, оброблення та подання інформації, що давало змогу командирам (начальникам) на місцях у найкоротші терміни приймати рішення, реагувати на виклики та загрози у зоні відповідальності.

Особовий склад груп моніторингу інформаційного простору та протидії офіційно заборонялося залучати до будь-якої діяльності, не передбаченої посадовими обов'язками, виключенням була лише робота, пов'язана із співпрацею з громадськими організаціями, журналістами, органами державної влади задля проведення ефективних комунікаційних кампаній Збройних Сил України.

Начальники ГРМП підпорядковувалися безпосередньо командиру підрозділу (військовому комісару, командиру бригади тощо), що дозволяло оперативно реагувати на ті чи інші події та зменшити час прийняття рішення. Методичне керівництво діяльністю ГРМП здійснював відділ інформаційної боротьби оперативного командування, який, у свою чергу, підпорядковувався відповідному відділу у КСВ ЗС України. Розглянемо схему підпорядкування детальніше (рис.1).

Рис.1 **Схема підпорядкування ГРМП**

Завдяки такій структурі ГРМП 24 обласних військових комісаріати та ГРМП військових частин доводили інформацію про зміни в інформаційному полі зони відповідальності щодо проблемних питань територіальної оборони, резонансних подій та інших кризових ситуацій, що стосувались діяльності військового відомства. Відтак, вище командування у максимально стислі терміни отримувало необхідну інформацію та більш оперативно та адекватно приймало рішення щодо подальшого реагування на неї.

У цілому на ГРМП обласних військових комісаріатів покладалися завдання, тотожні завданням забезпечення інформаційної безпеки держави у воєнній сфері:

- оперативне виявлення негативної інформації щодо КСВЗС України в термін до двох годин від часу її публікації;
- моніторинг регіональних ЗМІ та їхньої інтерпретації загальнодержавних подій;
- участь у комунікаційних кампаніях, які проводяться ЗС України, СВ ЗС України, оперативними командуваннями;
- моніторинг акцій протесту, які відбуваються в регіонах, та їх аналіз;
- проведення аналізу та прогнозу розвитку соціально-політичної та соціально-економічної обстановки в регіоні;

- виявлення “рейкової” інформації та інформаційних загроз, які впливають на підготовку, ведення територіальної оборони та проведення заходів призову громадян України на строкову військову службу;

- інформаційна підтримка заходів з підготовки та веденні територіальної оборони, заходів проведення комплектування Збройних Сил України та підготовки військових частин і підрозділів;

- здійснення інформаційної протидії виявленим інформаційним загрозам шляхом поширення інформації у соціальних мережах;

- проведення превентивних інформаційних заходів (комунікаційних кампаній) у регіонах з метою популяризації діяльності Сухопутних військ Збройних Сил України;

- збір бази даних про регіональні інформаційні ресурси, ЗМІ та спільноти в соціальних мережах;

- налагодження контактів та взаємодії з регіональними інформаційними ресурсами та ЗМІ;

- наповнення бази даних про регіональні проросійські громадські об'єднання та партійні осередки;

- збір інформації в регіонах про настрої громадян щодо Збройних Сил України та військового і військово-політичного керівництва;

- збір інформації з мережі Інтернет та з соціальних мереж про суспільно-політичну обстановку у прикордонних з Україною регіонах інших держав та на тимчасово окупованих територіях;

- здійснення інформаційного впливу на громадян країни-агресора в соціальних мережах під час проведення інформаційних операцій (акцій), які сплановані вищим командуванням.

До завдань груп моніторингу інформаційного простору і протидії військових частин додатково включено:

- оперативне виявлення негативної інформації щодо військової частини та інформації, яка негативно впливає на суспільно-політичну обстановку в районах виконання завдань, у термін до двох годин від часу її публікації;

- внесення пропозицій командуванню військової частини щодо реагування на виявленні інформаційні загрози;

- проведення інформаційних акцій у районах проведення ООС при їх координації з підрозділами ІПСО;

- збір інформації в районах проведення ООС про настрої громадян щодо Збройних Сил України та військового та військово-політичного керівництва;

- збір інформації з мережі Інтернет та з соціальних мереж про суспільно-політичну обстановку на тимчасово окупованих територіях;
- проведення моніторингу соціальних мереж противника під час перебування військової частини в районах виконання завдань за призначенням;
- здійснення заходів інформаційної протидії шляхом поширення інформації в соціальних мережах у координації з прес-службою, з підрозділами цивільно-військового співробітництва та з підрозділами розвідки;
- здійснення інформаційного впливу на громадян країни-агресора в соціальних мережах під час проведення інформаційних операцій (акцій), які сплановані вищим командуванням;
- поширення інформації в соціальних мережах в інтересах забезпечення заходів безпеки операцій.

Аналіз діяльності ГРМП дає підстави стверджувати, що найбільша дієвість та ефективність у забезпеченні інформаційної безпеки спостерігалась лише за умови активної співпраці та взаємодії з прес-службами цих підрозділів, представниками відділів цивільно-військового співробітництва та відділом морально-психологічного забезпечення. Так, у зоні проведення ООС у форматі постійного контролю за інформаційним простором було організовано цілодобовий моніторинг. Інформація про всі важливі заходи, резонансні події, новини, пропозиції, які могли впливати на ситуацію, обов'язково доводилась безпосередньо командиру військової частини. Також офіцери ГРМП долучались до випуску газети, підготовки друкованих матеріалів для місцевого населення та розповсюдження їх у прифронтових населених пунктах. Було розроблено та проведено важливе соціологічне опитування мешканців прифронтових містечок щодо прихильності та довіри до ЗМІ України, російської федерації та сепаратистів.

Важливою та постійною ділянкою роботи був моніторинг місцевих сепаратистських груп, зокрема у соціальних мережах "Фейсбук", "Вконтакте", "Одноклассники". Проводився аналіз сторінок бойовиків проросійських військових формувань. Усі отримані дані після обробки та систематизації передавалися відповідним підрозділам, що дозволяло об'єктивно оцінювати обстановку.

Робота ГРМП обласних військових комісаріатів мала дещо іншу специфіку. Вона була спрямована на недопущення зриву

виконання заходів комплектування особовим складом бойових підрозділів, призову на строкову військову службу, реагування на кризові ситуації, що стосувались діяльності структур обласного військового комісаріату та Збройних Сил України. Окрім типових завдань, ГРМП ОВК на постійній основі взаємодіяла зі структурними підрозділами обласної державної адміністрації. Зокрема, була налагоджена дієва співпраця з департаментом комунікацій та внутрішньої політики, відділом оборонної роботи та взаємодії з правоохоронними органами, департаментом освіти і науки обласної адміністрації. Також офіцери груп активно проводили "комунікаційні кампанії" з населенням області, що передбачало створення агітаційних картинок із подальшим поширенням їх у соціальних мережах; розповсюдження офіційних повідомлень у місцевих групах соціальних мереж та через обласні, районні та міські засоби масової інформації. Проте найбільш важливою ділянкою роботи була протидія інформаційним атакам, які постійно відбувались як під час проведення призову, так і при черговому загострені ситуації в зоні проведення ООС.

За період діяльності ГРМП можемо визначити декілька недоліків: ГРМП ОВК та підрозділів безпосереднього під порядкування ОК іноді виконували дублюючі функції, зокрема під час перебування підрозділів у пункті постійної дислокації. Окрім цього, зона відповідальності ГРМП підрозділів безпосереднього підпорядкування ОК була значно вужча (обмежувалася одним або декількома населеними пунктами в районі дислокації частини). Проте їхня робота набувала ваги під час виконання бойових завдань у зоні ООС. Натомість ГРМП ОВК відповідала за майже 30 адміністративних районів і, відповідно, мала більше можливостей, контактів та ресурсів.

Фахівці ГРМП постійно брали участь у підготовки інформації висвітлення діяльності обласного військового комісаріату та інформуванні громадськості щодо призовних кампаній та відбору громадян на контрактну військову службу.

При цьому слід зауважити, що діяльність ГРМП була спрямована не на проведення інформаційних операцій, а на виконання комунікаційних заходів – інформували громадськість про діяльність ЗС України та конкретну військову частину, установу. Це давало можливість виконувати завдання відкрито, публічно, із залученням представників ЗМІ та громадськості, що значно

посилювало авторитет військових, додавало важелі впливу обласному військовому комісаріату.

Підкреслимо, що законодавство України чітко регламентує обов'язки щодо інформаційного захисту України. Так, у Законі України «Про Збройні Сили України» (у зв'язку з ухваленням Закону України «Про внесення змін до деяких законів України щодо Сил спеціальних операцій Збройних Сил України») частини четверта і п'ята статті 1 викладені в наступній редакції: *«З'єднання, військові частини і підрозділи Збройних Сил України відповідно до закону можуть залучатися до здійснення заходів правового режиму воєнного і надзвичайного стану, організації та підтримання дій руху опору, проведення військових інформаційно-психологічних операцій*…»(Закон України «Про внесення змін до деяких законів України щодо Сил спеціальних операцій Збройних Сил України» від 07 липня 2016 року № № 1437-VIII). Тобто функції щодо проведення інформаційних операцій ЗС України покладені виключно на Сили спеціальних операцій ЗС України. Відповідно, інші структурні підрозділи до такої діяльності на професійному рівні не залучалися. Частково ці функції покладалися на структури морально-психологічного забезпечення. Проте враховуючи кількість покладених завдань на дані підрозділи та іншу специфіку діяльності, дані завдання виконувалися на недостатньому рівні. Саме тому силами ГРМП системно проводилися "комунікаційні кампанії".

Комунікаційна кампанія – комплекс заходів, організованих та проведених структурними підрозділами Збройних Сил України задля доведення певної інформації до суспільства з використанням ЗМІ (засобів масової інформації), соціальних мереж, мессенджерів тощо. Головною метою заходу є підвищення іміджу ЗСУ, постійне, позитивне, трансформаційне перебування армійських структур в інформаційному полі держави, набуття у суспільстві довіри, розуміння, взаємодії.

Розглянемо декілька основних прикладів проведення заходів комунікаційної кампанії (далі – КК):

1. КК «Строкова служба: міфи та реальність».(План проведення комунікаційної кампанії, затверджений Командувачем Сухопутних військ Збройних Сил України 10.03.2020 року, № 8303).

Головним завданням комунікаційної кампанії було забезпечення проведення якісного призову на строкову військову службу

військовими комісаріатами. Увага акцентувалася на роз'ясненні чинного законодавства щодо обов'язків призовників, розвінчування міфів щодо "дідівщини", демонстрації умов проходження військової служби. Наголошували на тому, що солдати строкової служби до участі в Антитерористичній операції (операції Об'єднаних сил) не залучаються. Для проведення такого інформування застосовувалися радіо, телебачення, газети, інформаційні агенції. Окремою ділянкою роботи були соціальні мережі. Зокрема, використовуючи місцеві групи та акаунти місцевих лідерів думок, в інформаційний простір додавали наступні картинки, які досить активно поширювалися далі серед місцевого населення (цільової аудиторії) (рис. 2).

Рис.2 **Заставка комунікаційної кампанії «Строкова служба: міфи та реальність».**

1. КК «Обери своє майбутнє» (Розпорядження начальника штабу Командування Сухопутних Військ Збройних Сил України від 27.02.2020 р. № 116/3/2468). Основними завданнями даної КК були:

- популяризація навчання у вищих військових навчальних закладах;

- нарощування зацікавленості серед вступників в отриманні військової освіти, акцентуючи увагу на те, що деякі спеціальності є дуже популярними та користуються попитом і у цивільній сфері.

Такі кампанії проводилися системно, відповідно до планових заходів Командування Сухопутних військ та суспільно-політичної обстановки у регіоні.

Загалом ГРМП продемонстрували ефективну роботу. У 2019 р. КСВ, враховуючи та розуміючи виклики і загрози в інформаційній сфері, ініціювало експеримент із розширення структур ГРМП, створивши за їх рахунок декілька центрів моніторингу інформаційного простору та протидії зі значно більшим штатом та можливостями. Цей експеримент успішно був реалізований і впроваджений на початку 2020 р. І тому з 01 червня 2020 р. ГРМП безпосереднього підпорядкування ОК та обласних військових комісаріатів припинили свою діяльність.

Війна триває, й інформаційні атаки з боку російської федерації лише посилюються. За найскромнішими підрахунками, які наводить Ілля Вітюк, керівник Департаменту кібербезпеки СБУ, «…сьогодні з території Російської Федерації проти України працюють близько 7 000 співробітників спецслужб. У 2021 році Департамент кібербезпеки СБУ заблокував 15 розгалужених мереж антиукраїнських інтернет-агітаторів, припинив діяльність близько 20 ботоферм потужністю понад 150 000 облікових записів. Це – нібито 150 тисяч осіб, які щось коментують, репостять, пишуть та дають оцінку подіям. СБУ було проведено безпрецедентну спецоперацію проти хакерської групи «Армагедон», яка штатно перебувала у ФСБ Росії і діяла з території Криму» (Телепрограма «Свобода слова», від 30.11.2021року).

На нашу думку, ГРМП лише підсилять оперативні командування знанням глибини проблеми, вони реальною картиною процесів і подій. Можлива підготовка кадрів з числа мешканців регіону, які найкраще обізнані з соціально-політичною ситуацією, національно-культурними традиціями тощо.

Висновки. До початку російсько-української війни (2014 р.) у сухопутних військ ЗС України були відсутні підрозділи, які б системно здійснювали діяльність, пов’язану із моніторингом інформаційного простору та протидією інформаційній агресії. Велику роботу зробили громадські організації, журналісти, блогери

та “інфоволонтери”, які з перших днів війни активно протидіяли інформаційній діяльності агресора. Лише у 2018 рр. було проведено експеримент зі створення ГРМП при обласних військових комісаріатах та військових частинах, методичне керівництво якими здійснювали профільні відділи у вищих штабах – ОК, КВС. Наступним кроком стало створення у 2020 році центрів інформаційного моніторингу та протидії. Разом з тим стратегічна ціль 1 Стратегії інформаційної безпеки України передбачає: “…протидію дезінформації та інформаційним операціям, насамперед держави-агресора, спрямованим, серед іншого, на ліквідацію незалежності України, повалення конституційного ладу, порушення суверенітету і територіальної цілісності держави, пропаганду війни, насильства, жорстокості, розпалювання національної, міжетнічної, расової, релігійної ворожнечі та ненависті, вчинення терористичних актів, посягання на права і свободи людини”. Досягнення зазначеної цілі має здійснюватися шляхом виконання таких завдань, як створення системи раннього виявлення, прогнозування та запобігання гібридним загрозам, зокрема, створення системи протидії дезінформації та інформаційним операціям, спрямованої на запобігання, максимально швидке виявлення та реагування держави і суспільства на інформаційні загрози (Указ Президента України № 685/2021 «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»).

Отже, на державному рівні передбачено розширення мережі структур з протидії дезінформації та інформаційним операціям. Відповідно, ГРМП, які добре зарекомендували та ефективно діяли впродовж 2018–2020 років, змогли б бути відновлені та працювати у ланці центрів моніторингу інформаційного простору та протидії КСВ/ОК та протистояти інформаційним викликам та загрозам.

Використані посилання

Виступ керівника Центру кібербезпеки Служби Безпеки України у телепрограм і«Свобода слова», 30.11.2021року. URL: https://www.youtube. com/watch? v=L3kYMt6_tng. (Дата звернення: 02.12.2021).

Гапеєва О. (2017) Міждержавне протиборство в інформаційній сфері на пострадянському просторі(1991-2017). Монографія. Львів. Тріада-Плюс. 423 с.

Закон України «Про внесення змін до деяких законів України щодо Сил спеціальних операцій Збройних Сил України». URL: https://zakon. rada.gov.ua/laws/ show/1437-19#Text (Дата звернення:15.12.2021).

Наказ командувача Сухопутних військ Збройних Сил України №113-ДСК від 23.02.2018 «Про затвердження Тимчасової інструкції з організації та проведення заходів забезпечення інформаційної безпеки Сухопутних військ Збройних Сил України».

План проведення комунікаційної кампанії «Строкова служба: міфи та реальність», затверджений Командувачем Сухопутних військ Збройних Сил України 10.03.2020 року, №8303.

Сніцаренко П., Саричев Ю., Семененко В., Ткаченко В.(2018). Удосконалення чинного інформаційного законодавства України як необхідна умова адекватності заходів щодо забезпечення інформаційної безпеки держави. Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. № 2(63). С. 68–74.

Указ Президента України № 685/2021 «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки». URL:https://www.president.gov.ua/documents/6852021-41069 (Дата звернення: 18.12.2021).

Указ Президента України від 20 травня 2016 року № 240/2016 «Про рішення Ради національної безпеки і оборони України «Про Стратегічний оборонний бюлетень України». URL: https://www.president.gov.ua/documents/ 2402016-20137 (Дата звернення: 21.12.2021).

References

Decree of the President of Ukraine №685/2021 «On the decision of the National Security and Defense Council of Ukraine of October 15, 2021 « On the Information Security Strategy» URL: https://www.president.gov.ua/documents/6852021-41069. (Date of application 18.12.2021).

Decree of the President of Ukraine of May 20, 2016 №240 / 2016 «On the decision of the National Security and Defense Council of Ukraine «On the Strategic Defense Bulletin of Ukraine» URL: https://www.president.gov.ua/ documents/2402016-20137 (Date of application 21.12.2021). Gapeyeva, O. (2017). Interstate confrontatio ninthe informations phere inthepost-Sovietspace (1991-2017). Lviv, Triad-Plus, 423 p. (in Ukrainian).

Order of the Commander of the Land Forces of the Armed Forces of Ukraine №113-DSK dated 23.02.2018 «On approval of the Interim Instruction on the organization and implementation of information security measures of the Land Forces of the Armed Forces of Ukraine».

Law of Ukraine «On Amendments to Certain Laws of Ukraine on the Special Operations Forces of the Armed Forces of Ukraine»URL: https://zakon.rada.gov. ua/laws/show/1437-19#Text

PerformanceofleaderofCenterofCibersecurityofUkrainein a telecast«Freedomofspeech», 30.11.2021року. URL: https://www.youtube. com/watch? v=L3kYMt6_tng.

SnicharenkoP., SarichevY., SemenenkoV., TkachenkoV.(2018) Improvement ofthecurrentin formation legislation of Ukraineas a necessary condition fortheadequacyofmeasurestoensuretheinformationsecurityofthestate.Center for Military andStrategicStudiesoftheNationalDefenceUniversityofUkrainenamedaft erIvan Cherniakhovskyi.№2(63).P.74-68 (in Ukrainian).

The plan of the communication campaign «Urgent Service Myths and Reality», approved by the Commander of the Land Forces of the Armed Forces of Ukraine on March 10, 2020, 308303.

Poronyuk R., Gapeyeva O.

ACTIVITIES OF THE GROUP OF INFORMATION SPACE MONITORING AND COUNTERACTION AS A COMPONENT OF ENSURING INFORMATION SECURITY OF THE STATE IN THE MILITARY SPHERE

The article describes the activity in 2018-2020 of the Information space monitoring and counteraction groups as the detachments of regional military commissariats or military units in direct subordination of Operational Army Commands of the Armed Forces of Ukraine. The article is focused on the historical preconditions and legal grounds for their creation, analysis of the activities to combat negative informational influence in the Ukrainian media environment by the Russian Federation, generalization of the practices of the state information security provision in the military sphere. The work examines the experiences and activities of the information operations units assigned to the Army Command in the area of the Joint forces operation and in the permanent units' locations.

Keyword: information space monitoring and counteraction groups, Armed Forces of Ukraine, information war, information counteraction, communication company.