УДК 340
DOI https://doi.org/10.24144/2788-6018.2023.03.51

УДОСКОНАЛЕННЯ МЕРЕЖІ СИТУАЦІЙНИХ ЦЕНТРІВ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Каптан М.В.,
старший науковий співробітник
науково-дослідного відділу правових проблем у сфері міжнародного співробітництва науково-дослідного управління проблем ресурсного забезпечення у воєнній сфері, сфері оборони та військового будівництва
Центру воєнно-стратегічних досліджень
Національного університету оборони України ім. І. Черняховського
https://orcid.org/0009-0008-3610-4633

Каптан М.В. Удосконалення мережі ситуаційних центрів у сфері інформаційної безпеки.

Досліджено проблематику створення та забезпечення функціонування Ситуаційного центру в системі Міністерства оборони України. Доведено необхідність створення спеціалізованої організаційної структури одним із основних завдань якої визначено реагування на інформаційні загрози безпосередньо за загальною координацією Головного ситуаційного центру при Раді національної безпеки і оборони України (далі – РНБО України) у взаємодії з іншими суб'єктами забезпечення сектору національної безпеки і оборони України в інформаційній сфері.

Проаналізовано шляхи створення та функціонування Ситуаційного центру Міністерства оборони України, визначено перелік загроз за якими повинно здійснюватись реагування, як окремої структури (або його окремих елементів), так і спільного виконання визначених положенням завдань з Ситуаційним центром Збройних Сил України під час реагування Збройними Силами України на кризові (надзвичайні) ситуації в інформаційному просторі України.

Наголошено, що в умовах стрімкого розвитку інформаційних процесів в умовах глобалізації, що зумовлені (посиленням ролі соціальних мереж у національному та світовому інформаційному просторі, їх вплив на внутрішню і зовнішню суспільно-політичну ситуацію, стан додержання прав і свобод людини, зокрема щодо забезпечення принципів рівності прав користувачів соціальних мереж), РНБО України прийнято рішення, щодо розширення та подальший розвиток єдиної мережі Ситуаційних центрів та оснащення їх уніфікованим програмним та апаратним забезпеченням обробки інформації, що дозволить підвищити ефективність та спроможність ухвалень ситуаційних управлінських рішень на всіх рівнях. Причиною такого зростання є саме кризові явища, які стають довготривалими, а процеси управління перетворюються з «попередження кризи» на, переважно, «ліквідацію кризи». За цих умов постає доволі вагома проблема, щодо питань взаємодії мережі Ситуаційних центрів органів державної влади в процесі виконання покладених завдань, підготовки нормативно-правових актів за напрямком діяльності, пов'язаних із забезпеченням реалізації державної політики з питань національної безпеки у воєнній сфері, сферах оборони та інформаційної безпеки в умовах надзвичайного і воєнного стану.

Підсумовано, що В Україні триває процес становлення системи стратегічних комунікацій, органами державної влади України здійснено низку організаційних та практичних заходів зі зміцнення власної інституційної спроможності у сфері стратегічних комунікацій, однак не створено дієвого механізму координації і взаємодії між усіма органами державної влади, залученими до здійснення заходів із протидії загрозам в інформаційній сфері. Зазначене послаблює можливості до розбудови комплексного стратегічного планування інформаційного потоку, здійснення системної комунікативної діяльності Кабінету Міністрів України, об'єднання всіх ключових суб'єктів у сфері інформаційних відносин, суб'єктів формування і реалізації державної політики щодо ефективного захисту національного інформаційного простору, утвердження позитивного іміджу України, реалізації цілей захисту національної безпеки України в інформаційній сфері. У цій ситуації, задля досягнення оперативної сумісності є вкрай важливим систематизувати однотипність в використанні спеціального програмного забезпечення для забезпечення здатності до взаємодії, стійкого функціонування, тестування та відстеження продуктивності у прийнятті рішень і контролю їх виконання. Вочевидь, що у процесі розширення та нарощування потужностей мережі Ситуаційних центрів Головний ситуаційний центр при РНБО України відіграватиме вагому роль. Стає зрозумілим, що такі центри, повинні бути об'єднані в

єдину захищену мережу, з наданням можливості оперативно збирати інформацію, аналізувати її та приймати критично важливі для держави рішення.

Ключові слова: ситуаційний центр, інформаційна безпека, РНБО України, загрози інформаційної небезпеки.

Captan M.V. Improvement of the network of situational centers in the field of information security.

The problems of creating and ensuring the functioning of the Situation Center in the system of the Ministry of Defense of Ukraine were studied. The need to create a specialized organizational structure has been proven, one of the main tasks of which is to respond to information threats directly under the general coordination of the Main Situation Center at the Council of National Security and Defense of Ukraine (hereinafter - NSDC of Ukraine) in cooperation with other subjects of ensuring the national security and defense sector of Ukraine in the information field.

The ways of creation and functioning of the Situation Center of the Ministry of Defense of Ukraine were analyzed, a list of threats to which the response should be carried out, both as a separate structure (or its individual elements), and as a joint performance of the tasks defined by the regulations with the Situation Center of the Armed Forces of Ukraine during the response of the Armed Forces of Ukraine to crisis (emergency) situations in the information space of Ukraine.

It is emphasized that in the conditions of the rapid development of information processes in the conditions of globalization, caused by the strengthening of the role of social networks in the national and global information space, their influence on the internal and external socio-political situation, the state of observance of human rights and freedoms, in particular, in relation to ensuring the principles of equality rights of users of social networks), the NSDC of Ukraine made a decision to expand and further develop a single network of Situation Centers and equip them with unified software and hardware for information processing, which will increase the efficiency and capacity of making situational management decisions at all levels. The reason for this growth is precisely the crisis phenomena, which become long-term, and the management processes are transformed from "crisis prevention" to, mainly, "crisis liquidation". Under these conditions, a rather serious problem arises regarding the issues of interaction of the network of Situation Centers of state authorities in the process of fulfilling assigned tasks, preparing normative legal acts in the field of activity related to ensuring the implementation of state policy on national security issues in the military sphere, defense spheres and information security in conditions of emergency and martial law.

It is summarized that the process of forming a system of strategic communications continues in Ukraine, the state authorities of Ukraine have implemented a number of organizational and practical measures to strengthen their own institutional capacity in the field of strategic communications, but an effective mechanism of coordination and interaction between all state authorities involved in the implementation of measures has not been created from countering threats in the information sphere. This weakens the possibilities for the development of comprehensive strategic planning of the information flow, the implementation of systematic communication activities of the Cabinet of Ministers of Ukraine, the unification of all key subjects in the field of information relations, subjects of the formation and implementation of state policy regarding the effective protection of the national information space, and the establishment of a positive image of Ukraine, implementation of the goals of protection of the national security of Ukraine in the information sphere. In this situation, in order to achieve interoperability, it is extremely important to systematize uniformity in the use of special software to ensure interoperability, stable operation, testing and performance tracking in decision-making and control of their implementation. It is obvious that in the process of expanding and increasing the capacities of the network of Situation Centers, the Main Situation Center of the National Security and Defense Council of Ukraine will play an important role. It becomes clear that such centers should be united in a single protected network, with the possibility of quickly collecting information, analyzing it and making decisions of critical importance to the state.

Key words: situation center, information security, National Security and Defense Council of Ukraine, information security threats.

Постановка проблеми. Враховуючи світовий розвиток інформаційної сфери, актуалізується питання інформаційної безпеки не тільки кожної людини, а й держави у цілому. Саме тому останнім часом проблемним питанням інформаційної безпеки приділяється досить велика увага як зі сторони міжнародних організацій, державних органів, так і науковців різних галузей, у тому числі юридичної.

В сучасних умовах інформаційна безпека являє собою одну із сфер національної безпеки України. І це аргументується законодавчим визначенням поняття «національна безпека», яке закріплено у Законі України «Про національну безпеку України». Так, у зазначеному Законі

вказано, що національна безпека являє собою захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз [1].

В Україні відсутня єдина дієва мережа Ситуаційних центрів, так Міністерство оборони України не є виключенням. Ситуаційні центри органів державної влади в своїй діяльності використовують спеціальне програмне забезпечення з інформаційно-аналітичного супроводження, моніторингу, прогнозування, прийняття рішень та безпеки. Зазначені процеси повинні відбуватись в одному цифровому середовищі, надійно захищеному від зовнішнього несанкціонованого втручання [2].

Одним із основних завдань Ситуаційного центру Міністерства оборони України є завчасне виявлення та аналіз кризових ситуацій, інформування про них керівництва Міністерства оборони України, підготовка проектів відповідних рішень, що загрожують національній безпеці України у воєнній та сфері забезпечення інформаційної безпеки [3].

Тому, усвідомлення необхідності створення відповідної організаційної структури у складі Ситуаційного центру Міністерства оборони України є одним з основних завдань стосовно забезпечення інформаційної безпеки. Як результат, інтеграція зусиль щодо організації вищезазначених завдань потребує додаткових наукових досліджень.

Стан опрацювання. Тематика досліджень використання інформаційних технологій в науковій літературі представлена технологічними і гуманітарним напрямами. Технологічний підхід розглядає програмно-технічну сторону процесу забезпечення інформаційної безпеки. Гуманітарний, на відміну, розглядає інформаційну безпеку в якості міждисциплінарної галузі. Важливе значення для розробки проблеми процесу забезпечення інформаційної безпеки мали праці вчених-правознавців: О.А. Баранової, А.М. Новицького, І.В. Арістової, В.Г. Пилипчука, К.І. Белякової, О.А. Баранова, Б.А. Кормича, І.М. Спілко та ін.

На думку А.В. Бабінської, інформаційну безпеку України слід розглядати як стан захищеності її національних інтересів в інформаційній сфері, які в свою чергу визначаються сукупністю збалансованих інтересів особи, суспільства й держави [4].

Дослідники П.В. Мірошниченко, А.А. Нестеренко визначає інформаційну безпеку станом захисту національних інтересів України, які складаються з збалансованих інтересів особи, суспільства та держави від загроз (внутрішніх і зовнішніх), що відповідає принципам національної безпеки в сучасній інформаційній сфери [5].

Досліджуючи питання інформаційної безпеки Л.О. Кочубей зазначає, що це стан захищеності життєво важливих інтересів, включаючи інформаційну озброєність держави, суспільства, окремої особистості, за якого жодні інформаційні виклики неспроможні спричинити деструктивні думки і дії [6].

Роблячи висновок, можна сказати, що поняття «інформаційна безпека» є складною конструкцією, що зумовлюється комплексною соціально-правовою природою, завдяки різноманітті інформаційних відносин в суспільства; відмінністю суб'єктів інформаційних відносин з власними інтересами, правами та обов'язками залежно від галузі використання. Для дослідження інформаційної безпеки використовується весь накопичений досвід, в тому числі історичний, адже використання інформації як зброї почалось ще задовго до появи сучасних технологій. Однак актуальність та проблематика теми статті потребують подальшого дослідження у даній сфері.

Метою статті є здійснення наукового обґрунтування створення організаційної структури у складі Ситуаційного центру Міністерства оборони України із завданнями реагування на інформаційний простір держави, які виникають в інформаційно-аналітичних системах, впровадження нових систем та інформаційних технологій, об'єднання та використання в одній мережі існуючих інформаційних систем та технічної підтримки функціонування програмно-апаратного комплексу набирає критичного характеру і є доволі виваженим.

Виклад основного матеріалу. Застосування Росією технологій гібридної війни проти України перетворило інформаційну сферу на ключову арену протиборства. Саме проти України Росія використовує найновіші інформаційні технології впливу на свідомість громадян, спрямовані на розпалювання національної і релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України [7].

Комплексний характер актуальних загроз національної безпеки в інформаційній сфері потребує визначення інноваційних підходів до формування системи захисту та розвитку інформаційного простору в умовах глобалізації та вільного обігу інформації.

Принципи, пріоритети та напрями інформаційної безпеки України визначені Стратегією інформаційної безпеки, затвердженою Указом Президента України від 28 грудня 2021 року № 685/2021 «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» [8].

Інформаційна безпека поняття, яке можна розглядати й тлумачити різними способами. Наприклад, мають місце енциклопедичні так і нормативно-правові визначення. Відповідно методологічні підходи, сфери застосування можуть суттєво відрізнятись. Слід розглянути нормативно-правові акти України для визначення інформаційної безпеки з легальної сторони. Стаття 17 Конституції України свідчить: «Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу» [9].

Як зазначає А.Ю. Нашинець-Наумова [10] при дослідженні питання проблематики інформаційної безпеки з точки зору законодавства, то в Законі України «Про інформацію» тематика майже не розкрита. Автор виокремлює поняття інформаційна безпека, і окреме поняття «захист інформації». Де, під захистом розуміється сукупність правових, організаційних, адміністративних та інших заходів націлених на збереження, цілісність та доступ до інформації. Таким чином, автор підсумовує, що з боку закону не враховуються усі можливі ризики нанесення шкоди інформаційній безпеці у сфері державного управління.

Зазвичай законодавство України постійно адаптується під нові обставини, умови та, безумовно, технології, які охоплюють усі сфери зокрема безпекові. Так, відповідно до Указу Президента України «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки"» «інформаційна безпека України - складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом» [8].

Як було зазначено, законодавство України постійно розвивається, особливо в інформаційній сфері. На протязі останніх років низка документів були оновлені або створені, задля покращення законодавчого забезпечення інформаційної сфери, наприклад, Закон України «Про інформацію» [11] або Указ президента «Про Стратегію інформаційної безпеки. Однак, слід зауважити, що в сучасних умовах війни й подальшого післявоєнного відновлення суспільних процесів необхідною є адаптація та якісні зміни існуючих законів та нормативно-правових актів. Адже, навіть з існуючими правками воно є не повністю визначеним і деякі питання залишаються суперечливими й не систематизованими. Крім того, воно не розповсюджене на суспільство. Тобто, суспільство, громадяни, як основні споживачі інформації є не захищеними від інформаційних впливів і атак [8].

Так, одним із прикладів Російської дезінформації є «відмивання наративів», за допомогою якого Росія просуває інформацію через неперевірені джерела у соціальних мережах, яка потім проникає в більш масові або державні засоби масової інформації, маскуючи при цьому свій інтерес. Однак, це розповсюджена ситуація, яка прикладом показує важливість не тільки правового забезпечення безпеки інформації та даних, а й говорить про освітню частину процесу повного забезпечення інформаційної безпеки [12].

Повертаючись до указу Президента «Про Стратегію інформаційної безпеки», є прописаний пункт, що «інформаційні заходи оборони держави - сукупність скоординованих дій, які готуються та здійснюються суб'єктами забезпечення національної безпеки і оборони України в мирний час, в особливий період, умовах воєнного або надзвичайного стану щодо прогнозування та виявлення інформаційних загроз у воєнній сфері, запобігання, стримування та відсічі збройній агресії проти України, протидії інформаційним загрозам з боку держави-агресора, а також здійснення інших необхідних дій в інформаційному протиборстві» [8].

Сьогодні в умовах стрімкого збільшення ролі інформації і знань в житті суспільства, зростання інформатизації та ваги інформаційних технологій у суспільних та господарських відносинах, розвиток глобального інформаційного простору та, як наслідок – обмеженість у часі щодо оперативного прийняття рішення управлінцями є доволі обґрунтованими чинниками реформування різних сфер суспільного життя та самої системи державного управління в цілому.

Зважаючи на військово-політичні реалії в Україні, Міністерство оборони України зацікавлено у трансформації Збройних Сил України, інших складових сектору безпеки та оборони держави щодо набуття спроможностей для ефективних дій в умовах виникнення кризових ситуацій. Так, на виконання Директиви Головнокомандувача Збройних Сил України у 2020 році було створено та розгорнуто Ситуаційний центр Збройних Сил України [13], розроблена автором варіант Ситуаційного управління Збройних Сил України, структура якого змінюється, залежно від покладених завдань, рисунок № 1.

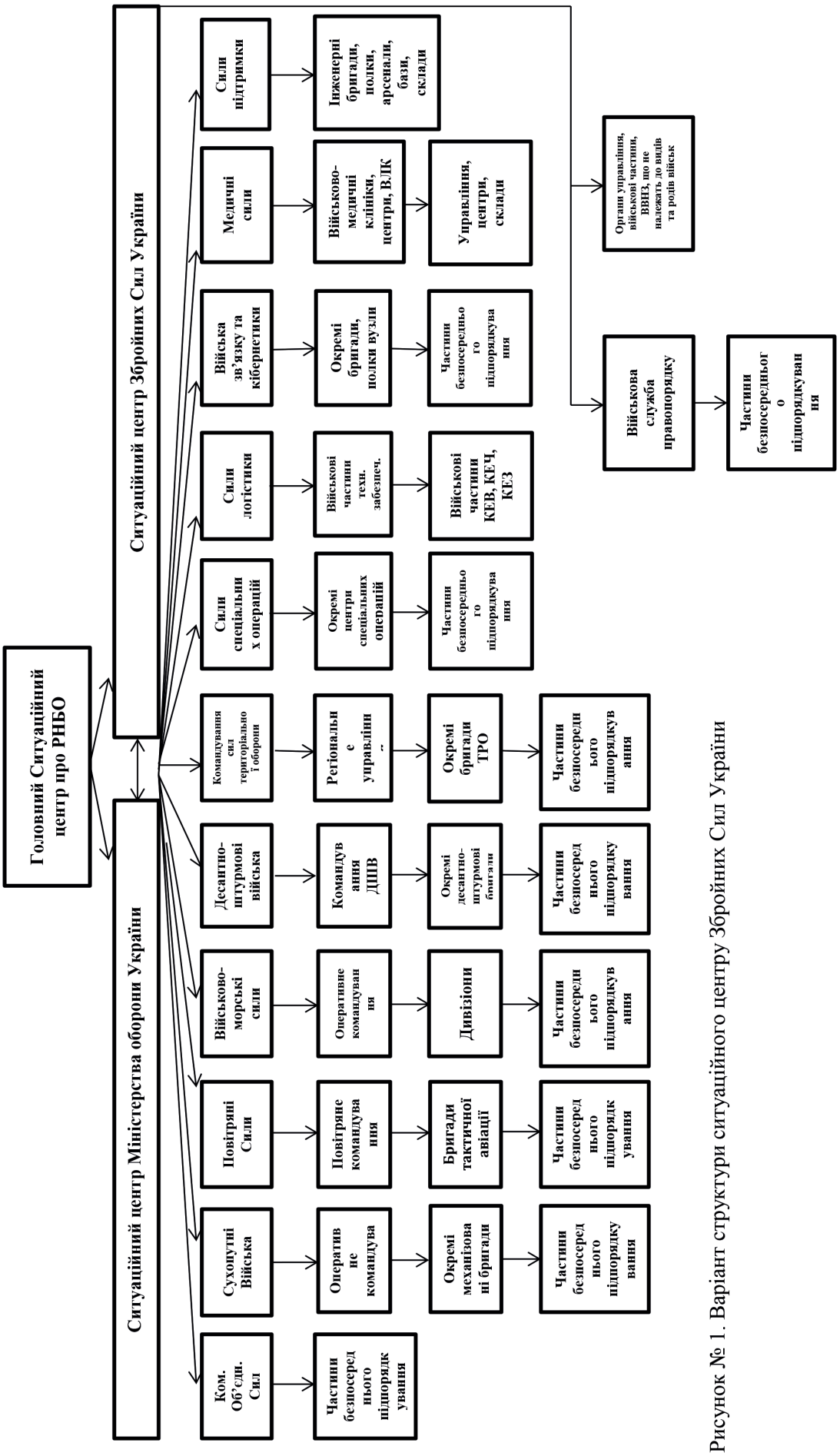

Рисунок № 1. Варіант структури ситуаційного центру Збройних Сил України

Рішенням Ради національної безпеки і оборони України від 4 червня 2021 року «Щодо удосконалення мережі ситуаційних центрів та цифрової трансформації сфери національної безпеки і оборони», введеного в дію Указом Президента України від 18 червня 2021 року № 260/2021 [14], Положення про Міністерство оборони України, затвердженого постановою Кабінету Міністрів України від 26 листопада 2014 року № 671 (у редакції постанови Кабінету Міністрів України від 19 жовтня 2016 року № 730). Так, відповідно до цього нормативно-правового поля, Наказом Міністерства оборони України № 396 від 23 грудня 2021 року було утворено робочу групу з питань створення та забезпечення функціонування Ситуаційного центру в системі Міністерства оборони України [15].

Відповідно до рішення РНБО України від 4 червня 2021 року основним завданням робочої групи з питань створення та забезпечення функціонування Ситуаційного центру в системі Міністерства оборони України є підготовка пропозицій та інформаційних матеріалів щодо:

шляхів створення ситуаційного центру у системі Міністерства оборони та Збройних Сил України;

оцінки та визначення переліку загроз, з якими повинно відбуватися реагування з розгортанням ситуаційного центру Міноборони;

можливостей спільного зі Збройним Силами України реагування на визначені загрози;

розроблення проєкту Положення про ситуаційний центр;

можливостей розгортання резервного ситуаційного центру та ситуаційного центру на рухомих засобах;

оснащення центу уніфікованим (з Головним ситуаційним центром України, Урядовий ситуаційний центр, ситуаційними центрами державних органів та пунктами управління Збройних Сил України) програмними та апаратним забезпеченням.

Створення мережі таких центрів значно підвищить роботу щодо інформаційно-аналітичного забезпечення управління, взаємодії, координації і контролю за діяльністю органів влади, правоохоронних органів та військових формувань у мирний та воєнний час, в умовах надзвичайного стану та під час виникнення кризових ситуацій, що загрожують національній безпеці України.

Слід наголосити, що Наказом Міністерства оборони України № 307 від 5 жовтня 2021 року з метою визначення завдань і функцій, затверджено Положення про управління забезпечення реагування на кризові ситуації. Відповідно до визначених повноважень та виконання покладених завдань положенням про Управління штатним розписом не передбачено відповідальної особи або підрозділ, відповідальний за стан інформаційної безпеки [16].

В умовах сучасного стану розвитку інформаційного простору, питання захисту інформаційної безпеки є нагальним на сьогоднішній день. Існує досить багато варіантів поняття інформаційної безпеки в науковій літературі, а також закріплено на законодавчому рівні.

Так, термін інформаційна безпека України (в редакції Стратегії інформаційної безпеки України, затвердженої Указом Президента України від 28 грудня 2021 року № 685/2021) – складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом [8].

Інформаційна безпека більшістю вчених сприймається як стан, який протистоїть загрозам ззовні та внутрішнім загрозам. Але, за умови, що всі ці загрози направлені всередину держави. Вітчизняні науковці і дослідники пов'язують інформаційну безпеку саме з національною безпекою як частину з цілим. Її визначають як «функціональну сферу національної безпеки», невід'ємну складову національної безпеки, самостійним напрямом національної безпеки [17].

Наприклад, Б.А. Кормич характеризує інформаційну безпеку як інформаційний компонент національної безпеки по співвідношенню «частина-ціле» [18]. Цей дослідник характеризує національну безпеку як стан захищеності держави від внутрішніх і зовнішніх загроз, що забезпечує умови існування людини, держави і суспільства, які гарантовані Конституцією та законами України.

Тобто, будучи складовою частиною національної безпеки, інформаційна безпека повинна сприйматися як стан захищеності держави від зовнішніх і внутрішніх загроз у сфері обігу інформації. Тому інформаційна безпека більшістю вчених сприймається як стан, який протистоїть загрозам як з зовні та внутрішнім загрозам. Але, за умови, що всі ці загрози направлені всередину держави.

Оскільки агресія здебільшого в сучасному світі направляється саме «з середини певних держав і направлена до інших держав або глобального суспільства в цілому, то аналізуючи поняття «національна безпека» під впливом глобальних

процесів, Б.А. Кормич зазначає, що це поняття «втрачає свій державний або блоковий характер, перетворюючись на глобальне явище [19].

Таким чином, з одного боку, стає очевидним, що таке твердження певною мірою відповідає дійсності, але в той же час очевидною також є і можливість застосування терміна «національна» до глобальної (загальносвітової) безпеки.

Цікавий погляд на поняття «інформаційна безпека» має відомий український дослідник Р.А. Калюжний, який вважає, що інформаційна безпека – це вид суспільних інформаційних правовідносин стосовно створення, підтримки, охорони та захисту бажаних для людини, суспільства і держави безпечних умов життєдіяльності, спеціальних правовідносин, які пов'язані зі створенням, зберіганням, поширенням і використанням інформації [20].

Загрози інформаційної небезпеки входять у загальну структуру загроз національної безпеки України так, головними ризиками інформаційної безпеки є:

недосягнення головної мети реалізації Стратегії інформаційної безпеки України щодо посилення спроможностей забезпечення інформаційної безпеки держави, її інформаційного простору, підтримки інформаційними засобами та заходами соціальної та політичної стабільності, оборони держави, захисту державного суверенітету, територіальної цілісності України, демократичного конституційного ладу, забезпечення прав та свобод кожного громадянина;

невиконання заходів щодо стримування та протидії загрозам інформаційній безпеці України та нейтралізації інформаційної агресії, у тому числі спеціальних інформаційних операцій держави-агресора, спрямованих на підрив державного суверенітету, територіальної цілісності України, забезпечення інформаційної стійкості суспільства та держави, створення ефективної системи взаємодії між органами державної влади, органами місцевого самоврядування та суспільством, а також розвиток міжнародної співпраці у сфері інформаційної безпеки на засадах партнерства та взаємної підтримки [21, с. 4].

Національними викликами та загрозами інформаційної безпеки є: інформаційний вплив Росії як держави-агресора на населення України;

інформаційне домінування Росії як держави-агресора на тимчасово окупованих територіях України;

обмежені можливості реагувати на дезінформаційні кампанії; несформованість системи стратегічних комунікацій;

недосконалість регулювання відносин у сфері інформаційної діяльності та захисту професійної діяльності журналістів;

спроби маніпуляції свідомістю громадян України щодо європейської та євроатлантичної інтеграції України;

доступ до інформації на місцевому рівні;

недостатній рівень інформаційної культури та медіаграмотності в суспільстві для протидії маніпулятивним та інформаційним впливам [21, с. 5].

Можемо підсумувати, що поза сумнівом є обґрунтованість нагальність створення організаційної структури у складі Ситуаційного центру Міністерства оборони України із завданнями реагування на інформаційні загрози щодо:

моніторингу інформаційного простору, прогнозування та виявлення інформаційних загроз національній безпеці держави у воєнній сфері;

підготовки та проведення інформаційних заходів оборони держави, координації залучення до них суб'єктів забезпечення національної безпеки держави; розвитку та функціонування системи стратегічних комунікацій сил оборони;

здійснення правових, організаційних, технічних, інформаційних та інших дій щодо забезпечення власної інформаційної безпеки, у тому числі захисту єдиного інформаційного середовища сил оборони, зокрема в місцях дислокації, розгортання та застосування угруповань, військових частин та підрозділів Збройних Сил України, інших військових формувань, утворених відповідно до законів України; звязків з українськими та іноземними засобами масової інформації щодо висвітлення ситуації у районах здійснення заходів із забезпечення національної безпеки і оборони, стримування та відсічі збройної агресії Росії;

протидії інформаційним операціям та іншим заходам інформаційного впливу, спрямованим проти Збройних Сил України та інших військових формувань, утворених відповідно до законів України; донесення достовірної інформації до військовослужбовців Збройних Сил України, інших складових Сил оборони.

Висновки. Отже, враховуючи визначені пріоритети державної політики у сферах національної безпеки і оборони зі створення та функціонування системи Ситуаційного центру Збройних Сил України та Ситуаційного центру Міністерства оборони України, доведено необхідність створення спеціалізованої організаційної структури в системі Міністерства оборони України, яка має завдання щодо реагування на виникаючі інформаційні загрози воєнного характеру безпосередньо за загальною координацією Головного ситуаційного центри при РНБО України у взаємодії з іншими суб'єктами забезпечення сектору національної безпеки і оборони України в інформаційній сфері. Функціонування зазначеної військової організаційної структури дозволить виконувати заходи, щодо стримування, локалізації і відбиття воєнної агресії у сфері інформаційної безпеки, в умовах надзвичайного і воєнного стану.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Про національну безпеку України: Закон України від 21.06.2018 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 20.04.2023).
2. Зеленський увів у дію рішення РНБО щодо удосконалення мережі ситуаційних центрів та цифрової трансформації сфери нацбезпеки: Interfax-Україна. URL: Інформаційне агентство https://interfax.com.ua/news/general/751001.html (дата звернення: 20.04.2023).
3. Міноборони України отримає ситуаційний центр Український міліарний центр – громадська організація однодумців: інтернет-портал Мілітарний. URL: https://mil.in.ua/uk/news/minoborony-ukrayiny-otrymaye-sytuatsijnyj-tsentr/ (дата звернення: 20.04.2023).
4. Бабінська А.В. Інформаційна безпека в доктрині та практиці інформаційного права Адміністративне право і процес. *Юридичний науковий електронний журнал*. 2014. № 2 (8). С. 153–156. URL: http://lsej.org.ua/4_2015/41.pdf (дата звернення: 20.04.2023).
5. Мірошниченко П.В. Суспільна значущість лідера думок під час інформаційного протистояння. Держава та регіони. Сер. Соц. комунікації. 2015. Вип. 4. С. 36–41. URL: http://www.zhu.edu.ua/journal_cpu/index.php/der_sc/issue/viewFile/63/44 (дата звернення: 20.04.2023).
6. Кочубей Л.О. Інформаційна безпека держави: інструменти захисту українського інформаційного поля (на прикладі особливостей інформаційно комунікаційних технологій у сучасному Донбасі. Наукові записки Інституту політичних і етнонаціональних досліджень імені І.Ф. Кураса. 2015. Вип. 3. С. 220–237.
7. Білоус А.О. Логіко-риторичний аналіз інтернет-дискурсу: дис. кан. фйіл. наук: 09.00.06. 2017. Київ, 75-76 с.
8. Стратегія інформаційної безпеки, затвердженою Указом Президента України від 28 грудня 2021 року № 685/2021 «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення: 20.04.2023).
9. Конституція України : основний Закон України від 28.06.1996 р. № 254к/96-ВР. *Верховна Рада України.* URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (дата звернення: 20.04.2023).
10. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ, видавничий дім «Гельветейка», 2017. 168 с.
11. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII. *Верховна Рада України.* URL: https://zakon.rada.gov.ua/laws/show/2657-12#top (дата звернення: 20.04.2023).
12. Одним із компонентів російської дезінформації є «відмивання наративів», – Міноборони Великобританії: LB.ua. Дорослий погляд на світ. Інтернет видавництво.URL: https://lb.ua/society/2023/04/19/552420_iz_komponentiv_rosiyskoi.html (дата звернення: 20.04.2023).
13. Директива Головнокомандувача Збройних Сил України «Про створення Ситуаційного центру Збройних Сил України» від 19.10.2020 № Д.
14. Щодо удосконалення мережі ситуаційних центрів та цифрової трансформації сфери національної безпеки і оборони : Рішення Ради національної безпеки і оборони України від 4 червня 2021 року «Щодо удосконалення мережі ситуаційних центрів та цифрової трансформації сфери національної безпеки і оборони», введеного в дію Указом Президента України від 18.06.2021 р. № 260/2021. URL: https://zakon.rada.gov.ua/laws/show/n0039525-21#n2 (дата звернення: 20.04.2023).
15. Про утворення робочої групи з питань створення та забезпечення функціонування Ситуаційного центру в системі Міністерства оборони України : наказ Міністерства оборони України від 23.11.2021 № 396. URL: https://www.mil.gov.ua/content/mou_orders/mou_2021/396_nm.pdf (дата звернення: 20.04.2023).
16. Положення про управління забезпечення реагування на кризові ситуації наказ Міністерства оборони України від 05.10.2021 № 307. URL: https://www.mil.gov.ua/content/mou_orders/mou_2021/307_nm.pdf (дата звернення: 20.04.2023).
17. Боднар І.Р. Інформаційна безпека як основа національної безпеки. URL: Механізм регулювання економіки. Львів. 2014. № 1. С. 68–75. https://core.ac.uk/download/pdf/141443493.pdf (дата звернення: 20.04.2023).
18. Кормич Б.А. Інформаційна безпека. *Організаційно-правові основи.* навч. посіб. / за заг. ред. Б.А. Кормича. Київ, 2004. 382 с.
19. Кормич Б.А. Організаційно-правові засади політики інформаційної безпеки України: монографія. Одеса: Юридична літератур., 2003. 472 с.

20. Калюжний Р.А. Координація діяльності органів влади у боротьбі з організованою кіберзлочинністю. Боротьба з організованою злочинністю і корупцією. 2002. № 6. 108 с.
21. Щодо заходів наукового супроводження реалізації положень Указу Президента України від 18 червня 2021 року № 260/2021 «Про рішення Ради національної безпеки і оборони України від 4 червня 2021 року "Щодо удосконалення мережі ситуаційних центрів та цифрової трансформації сфери національної безпеки і оборони"» в частині щодо створення Ситуаційного центру Міністерства оборони України: лист начальника Управління забезпечення реагування на кризові ситуації від 08.02.2023 № 420/246. 1–50 с.