

Машталір Вадим Віталійович (доктор історичних наук, професор)

Гудима Олег Петрович (кандидат технічних наук, старший науковий співробітник)

Національний університет оборони України, Київ, Україна

КОНЦЕПТУАЛЬНИЙ ПІДХІД ДО ФОРМУВАННЯ МОДЕЛІ ОРГАНІЗАЦІЙНОЇ СТРУКТУРИ СИТУАЦІЙНОГО ЦЕНТРУ МІНІСТЕРСТВА ОБОРОНИ УКРАЇНИ

Початок агресії російської федерації проти України та хід збройного протистояння формує потребу в якісному інформаційно-аналітичному забезпеченні управлінської діяльності. Аналіз останніх наукових публікацій свідчить, що питання системного (комплексного) підходу до формування моделі організаційної структури Ситуаційного центру Міністерства оборони України, як органу інформаційно-аналітичного забезпечення, не розглядалися. Метою статті є формування концептуального підходу до формування моделі організаційної структури Ситуаційного центру Міністерства оборони України для забезпечення реагування на кризові ситуації. Під час опрацювання статті було застосовано методи аналізу, синтезу, аналогії, декомпозиції, структурного синтезу, моделювання, експертні методи. Опрацьований концептуальний підхід дозволив виокремити та опрацювати орієнтовні завдання і функції Ситуаційного центру Міністерства оборони України. Крім того, запропоновано його організаційну структурну модель, враховуючи категорії «загроза», «кризова ситуація», «ризик» та вимоги чинного законодавства держави. Означене дає підстави для уточнення завдань, функцій і структури Ситуаційного центру Міністерства оборони України. Крім того, запропонований підхід може бути використаний для вироблення завдань, формування функцій та побудови організаційних структур ситуаційних центрів складових сил оборони України й інших центральних органів виконавчої влади. В подальшому дослідження будуть спрямовані на удосконалення алгоритмів роботи та взаємодії Ситуаційного центру Міністерства оборони України з ситуаційними центрами центральних органів виконавчої влади держави.

Ключові слова: кризова ситуація, ситуаційний центр, реагування, концептуальний підхід.

Вступ

Широкомасштабне вторгнення російської федерації в Україну ще раз підтвердило тезу, що характер сучасних конфліктів має гібридний характер, ознаками якого є [1]: «використання воєнних і невоєнних інструментів в інтегрованій кампанії, спрямованій на досягнення раптовості, захоплення ініціативи та отримання психологічних переваг для використання в дипломатичних діях; масштабні і стрімкі інформаційні, електронні і кібернетичні операції; прикриття воєнних і розвідувальних дій у поєднанні з економічним тиском». Означене актуалізує підвищення якості інформаційно-аналітичного забезпечення управлінської діяльності з метою завчасного прогнозування (виявлення) «гібридних» дій.

Для підвищення спроможностей сектору безпеки і оборони України (далі – СБіО) та сил оборони (далі – СО) в зазначеному напрямі видано Указ 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”» [2]. Цим нормативним документом унормовано розширення та

подальший розвиток єдиної мережі ситуаційних центрів (далі – СЦ), до складу якої мають входити Головний СЦ України, Урядовий СЦ, СЦ органів СБіО, СЦ центральних органів виконавчої влади, Ради міністрів Автономної Республіки Крим, обласних, Київської та Севастопольської міських державних адміністрацій, а також резервні та рухомі СЦ. Крім того, Указом визначено відповідні завдання для досягнення необхідного результату.

Реалізація заходів, що передбачені зазначеним Указом, потребує наукового супроводу питань створення (розвитку) СЦ Міністерства оборони України (далі – МО України) та, відповідно, формування моделі його організаційної структури та межі відповідальності (перелік завдань, функцій та готовність реагувати на відповідні кризові ситуації (далі – КС).

Аналіз останніх досліджень і публікацій. Щодо побудови механізмів протидії «гібридним» загрозам: в [3] авторами розглянуто різні підходи щодо визначення змісту «гібридної» агресії й проаналізовані військові та невійськові інструменти в збройному протистоянні; в [4] авторами розглянуто питання розробки нового

інструментарію щодо комплексного використання військових та невійськових сил в умовах протидії сучасним загрозам; в [5] опрацьовано варіант побудови державної системи управління (координації) заходів протидії гібридним загрозам на базі системи СЦ.

Щодо теоретичних і практичних підходів до нового формату стратегічного керівництва СБіО та військового управління СО: в [6], авторами на підставі аналізу зарубіжного досвіду стратегічного керівництва обороною країн-членів НАТО та системи забезпечення воєнної безпеки і оборони України, сформовано потребу в удосконаленні системи державного управління й міжвідомчої координації зусиль під час КС воєнного характеру; в [7] авторами на основі аналізу вітчизняного законодавства сформовано варіант побудови моделі системи оборони України та здійснено її опис; в [8] автором на основі аналізу досвіду країн світу сформовані пропозиції, що стосуються удосконалення системи забезпечення національної безпеки України та системи державного управління СО в КС.

Щодо визначення місця і ролі СЦ в загальній системі аналізу воєнно-політичної обстановки та реагування на КС: в [1] авторами розглянуті питання аналізу воєнно-політичної обстановки та висвітлено питання щодо використання СЦ для її аналізу; в [9] авторами розроблено методику оцінювання впливу загострення воєнно-політичної обстановки на виникнення КС; в [10] автором зроблено аналіз понятійного апарату в сфері кризового реагування, що використовується в багатьох країнах; в [11] автором запропоновано використовувати єдину методику обробки інформаційних потоків для забезпечення процесів ухвалення рішень на державному рівні; в [12] авторами розглянуто СЦ, як елемент механізму стратегічних комунікацій та проаналізовано СЦ ЗС України; в [13] автором проведено комплексний аналіз досвіду створення СЦ (кризових центрів, інформаційно-аналітичних центрів) в Україні; в [14] розглянуто питання, що стосується необхідності створення в межах СЦ МО України спеціалізованої організаційної структури для реагування на кіберзагрози.

Проведений аналіз останніх досліджень і публікацій свідчить, що питання системного (комплексного) підходу до формування організаційної структури СЦ МО України для забезпечення реагування на КС наразі не розглядалося. Отже, можна констатувати наявну потребу в усуненні невизначеностей, що виникають під час формування СЦ МО України для реагування на КС.

Метою статті є формування концептуального підходу до формування моделі організаційної структури Ситуаційного центру Міністерства оборони України для забезпечення реагування на кризові ситуації.

Виклад основного матеріалу дослідження

Загальний перелік нормативно-правових актів

держави [2; 15–18], які формують вимоги щодо інформаційно-аналітичного забезпечення управлінської діяльності представлено на рис. 1.



Рисунок 1 – Перелік національних нормативних документів, які формують вимоги щодо інформаційно-аналітичного забезпечення управлінської діяльності Міністерства оборони України

Розширений перелік завдань в зазначених нормативно-правових актах подано в таблиці 1, де передбачено створення (розширення, розвиток):

- мережі СЦ у державних органах (в межах системи національних стратегічних комунікацій);
- мережі СЦ моніторингу та аналізу ризиків з метою запобігання загрозам для об'єктів критичної інфраструктури;
- системи СЦ СБіО для оперативного прийняття рішень у сфері оборони;
- мережі галузевих СЦ кібербезпеки;
- єдиної мережі СЦ.

З огляду на означене, з метою інформаційно-аналітичного забезпечення виконання функцій управління державою, передбачено створення низки мереж (систем) СЦ в різних сферах діяльності держави, робота яких потребує синхронізації та забезпечення надійного обміну інформацією. Зважаючи на означене, виникає потреба опрацювати підхід до інтеграції відповідних елементів всіх зазначених мереж (систем) СЦ для конкретного СЦ органу державної влади, відповідно до його завдань і функцій.

Завдання щодо створення (розвитку) ситуаційних центрів у нормативно-правових актах України

Назва нормативно-правового документу	Окремі завдання щодо створення (розвитку) ситуаційних центрів
<p>Указ Президента України від 14 вересня 2020 року № 392/2020 «Про Стратегію національної безпеки України»</p>	<p>Україна запровадить національну систему стійкості для забезпечення високого рівня готовності суспільства і держави до реагування на широкий спектр загроз, що передбачатиме: оцінку ризиків, своєчасну ідентифікацію загроз і визначення вразливостей; ефективне стратегічне планування і кризовий менеджмент, зокрема впровадження універсальних протоколів реагування на КС та відновлення з урахуванням рекомендацій НАТО.</p> <p>З метою національної захисту України від загроз національній безпеці необхідним є розвиток СБіО. Для цього Україна: «...створить систему ефективного управління та координації діяльності органів СБіО, удосконалив її архітектуру; ...завершить створення національної системи кібербезпеки, сформує сучасні спроможності суб'єктів забезпечення кібербезпеки і кібероборони та зміцнить систему їх координації;...» та інше.</p>
<p>Указ Президента України від 25 березня 2021 року № 121/2021 «Про Стратегію воєнної безпеки»</p>	<p>Визначено пріоритет досягнення цілей державної політики у воєнній сфері, сфері оборони і військового будівництва – запровадження об'єднаного керівництва з підготовки та ведення всеохоплюючої оборони України, який буде реалізований шляхом виконання таких основних завдань: «створення системи комплексного стратегічного аналізу воєнних загроз національній безпеці України; координація діяльності розвідувальних органів; розвиток об'єднаних розвідувальних спроможностей СО з метою отримання повної та достовірної упереджувальної інформації для своєчасного ухвалення рішень щодо забезпечення воєнної безпеки держави; упровадження сучасних інформаційних та космічних технологій; автоматизація управлінських процесів і цифровізація діяльності в СО України з відповідним рівнем захищеності інформації, що обробляється; розвиток спроможностей щодо забезпечення кібербезпеки, кіберзахисту та кібероборони під час підготовки та ведення всеохоплюючої оборони України» та інші.</p>
<p>Укази Президента України від 26 травня 2020 року № 203/2020 «Про Річну національну програму під егідою Комісії Україна – НАТО на 2020 рік» та від 11 травня 2021 року № 189/2021 «Про Річну національну програму під егідою Комісії Україна – НАТО на 2021 рік»</p>	<p>Визначено завдання (на 2021 рік) стосовно створення: системи національних стратегічних комунікацій: «...створення мережі СЦ державних органів...» та інше;</p> <p>Національної системи стійкості: «...формування єдиної нормативно-правової бази у сфері планування та реагування на КС та загрози з метою забезпечення координації дій державних органів у таких ситуаціях...»;</p> <p>державної системи захисту критичної інфраструктури: «...створення мережі СЦ моніторингу та аналізу ризиків для запобігання загрозам для об'єктів критичної інфраструктури, що досягається виконанням таких пріоритетних завдань: формування нормативно-правової бази для функціонування СЦ; створення ефективної системи обміну інформацією між суб'єктами та об'єктами державної системи захисту критичної інфраструктури для прогнозування можливих загроз та запобігання їм...»;</p> <p>системи управління СО: «...розбудова спільної структури командування, контролю та координації СО на стратегічному, оперативному та тактичному рівнях, сумісну із системами військового керівництва держав – членів НАТО; нарощення можливостей СЦ складових СБіО, що досягається виконанням пріоритетного завдання зі створення системи СЦ СБіО для оперативного прийняття рішень у сфері оборони...»;</p> <p>умови для безпечного функціонування кіберпростору та його використання в інтересах особи, суспільства і держави: «...створення єдиної мережі галузевих СЦ кібербезпеки, що здатна забезпечити оперативне реагування на кіберзагрози на рівні, який відповідає стандартам НАТО...» та інше.</p>
<p>Указ Президента України від 18 червня 2021 року № 260/2021 «Щодо удосконалення мережі СЦ та цифрової трансформації сфери національної безпеки і оборони»</p>	<p>1. Визнати за необхідне розширення та подальший розвиток єдиної мережі СЦ, до складу якої мають входити Головний СЦ України, Урядовий СЦ, СЦ органів СБіО, СЦ центральних органів виконавчої влади, Ради міністрів Автономної Республіки Крим, обласних, Київської та Севастопольської міських державних адміністрацій, а також резервні та рухомі СЦ.</p> <p>2. Забезпечити: подальший розвиток мережі СЦ, використовуючи інформаційно-аналітичну систему Головного СЦ України; можливість розгортання резервних СЦ у запасних резервних (міських, позаміських) пунктах управління, а також рухомих СЦ для забезпечення стійкості та живучості системи управління державою в особливий період, зокрема в умовах воєнного стану, в умовах надзвичайного стану та під час виникнення КС, що загрожують національній безпеці України та інше.</p>

Спираючись на положення теорії організації, загальна схема взаємодії елементів управління має вигляд наведений на рис. 2 [19]:

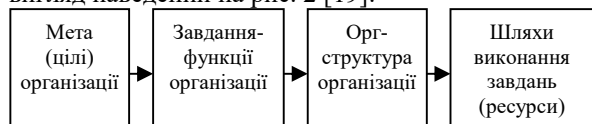


Рисунок 2 – Загальна схема взаємодії елементів управління

На основі розглянутої схеми пропонується концептуальний підхід до формування моделі організаційної структури СЦ МО України для реагування на КС, а саме: визначення мети СЦ, його завдань і функцій та формування моделі організаційної структури СЦ.

Мета (цілі) СЦ органу державного управління – визначаються відповідно до

положення про орган державного управління в інтересах якого буде функціонувати СЦ.

Під час формування завдань і функцій організації СЦ відповідного органу державного управління доцільно врахувати:

- вимоги нормативно-правових документів держави та відомчих документів;
- перелік загроз (реагування на які є сферою відповідальності органу державного управління);
- перелік КС (згідно до сфери відповідальності органу державного управління);
- ризик негативних наслідків від настання КС (сформовані у відповідному органі державного управління).

Варто зазначити, що під час формування завдань і функцій СЦ додатково залучено такі категорії, як «загроза», «кризова ситуація», «ризик», зміст яких наведено в таблиці 2.

Таблиця 2

Зміст категорій «загроза», «кризова ситуація», «ризик»

Визначення категорії «загроза»	Визначення категорії «кризова ситуація»	Визначення категорії «ризик»
<p><i>Загрози національній безпеці України</i> – явища, тенденції і чинники, що унеможливають чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України [20].</p> <p><i>Загрози гібридного типу</i> – різновид загроз національній безпеці, реалізація яких спричиняє синергетичний ефект від одночасного застосування комбінованих методів впливу, які часто мають прихований характер або маскуються під інші процеси у рамках правового поля [21].</p> <p><i>Загроза</i> – можливість або неминучість виникнення чогось небезпечного, прикрого, тяжкого для кого-, чого-небудь [32].</p>	<p><i>Кризова ситуація</i> – крайнє загострення суперечностей, гостра дестабілізація становища в будь-якій сфері діяльності, регіоні, країні [22].</p> <p><i>Кризова ситуація</i> – порушення або загроза порушення штатного режиму функціонування критичної інфраструктури чи окремого її об'єкта, реагування на яке потребує залучення додаткових сил і ресурсів [23].</p> <p><i>Кризова ситуація</i> – стан, що характеризується крайнім загостренням суперечностей, значною дестабілізацією становища в будь-якій сфері діяльності, регіоні, державі, у тому числі значним порушенням умов функціонування основних сфер життєдіяльності суспільства і держави, й потребує вжиття комплексу заходів для стабілізації ситуації та відновлення якості життя населення, умов функціонування суспільства і держави на рівні, не нижчому за докризовий. Однією з передумов розвитку КС може бути виникнення надзвичайної ситуації [21].</p>	<p><i>Ризик</i> – це ймовірність виникнення збитків або недоотримання прибутків порівняно з варіантом, що прогнозується [24, 25].</p> <p><i>Ризик</i> – небезпека несприятливого кінця на одну очікувану подію [24, 26].</p> <p><i>Ризик</i> – це потенційна можливість того, що під час реалізації функцій, процесів та операцій, спрямованих на досягнення встановленої мети (місії), цілей і виконання завдань, можуть виникнути обставини, що призведуть до втрат ресурсу, небезпеки або небажаного результату у майбутньому [27].</p>

Наведені у таблиці 2 категорії дають змогу висвітлити питання реагування на КС, включно з періодом, який передую настанню кризової ситуації та період усунення її наслідків (розмір можливої шкоди від них). Співзв'язок (співвідношення) вищезазначених категорій подано на рис. 3.

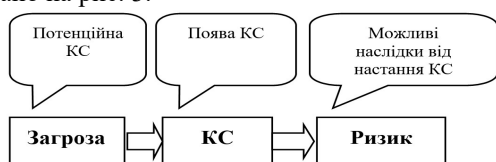


Рисунок 3 – Орієнтовна модель співзв'язку (співвідношення) категорій, як «загроза», «кризова ситуація», «ризик»

Особливої уваги заслуговує розгляд питання щодо класифікації КС. Відповідно до Закону України «Про національну безпеку України» від 21.06.2018 № 2469-VIII «державна політика у сферах національної безпеки і оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, кібербезпеки України тощо» [20].

Водночас, якщо розглянути термін «кризова ситуація», що зазначено в [21] через призму сфер діяльності, які визначені в [20] та враховуючи зміст понять «інформація» та «інформаційний простір» можна припустити, що КС кіберхарактеру є складовою частиною КС інформаційного характеру. Зважаючи на означене,

констатуємо наявність типів кризових ситуацій:

невосного характеру: зовнішньополітичні; державні; економічні; інформаційні (в тому числі і КС кіберхарактеру); екологічні (надзвичайні ситуації (далі – НС));

восного характеру. Розглядаючи систему понять «кризова ситуація» і «надзвичайна ситуація» з погляду послідовності їх настання, то можна припустити, що КС воєнного характеру є кінцевою складовою і їй передують (можуть передувати) КС в усіх вищезазначених напрямках. Варто констатувати, що поява одночасно всіх вищезазначених КС не є обов'язковою умовою настання КС воєнного характеру.

Отже, визначимо призначення СЦ МО України і запропонуємо орієнтовну модель з формування завдань і функцій цього центру. З урахуванням [28] СЦ МО України призначений для здійснення інформаційно-аналітичної підтримки діяльності під час формування та реалізації державної політики з питань національної безпеки у воєнній сфері. Орієнтовну модель з формування завдань і функцій СЦ МО України подано на рис. 4.

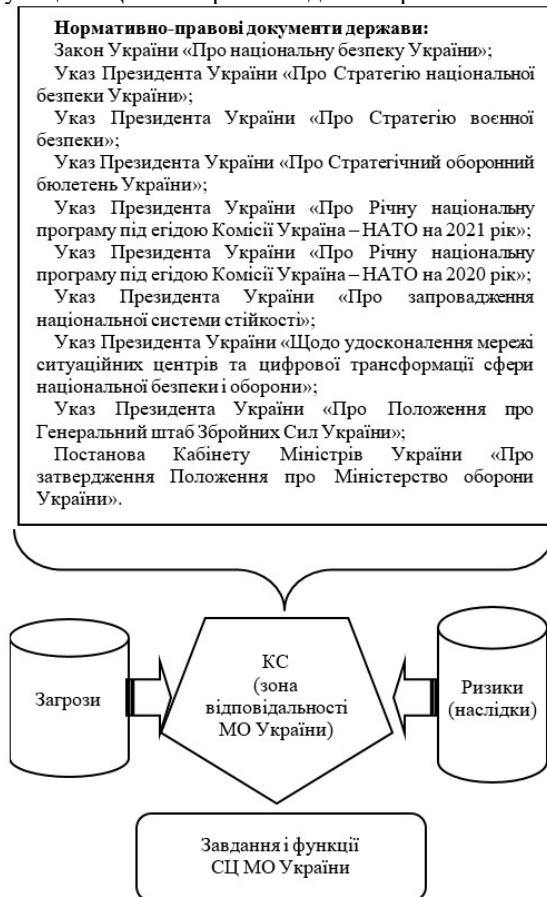


Рисунок 4 – Орієнтовна модель з формування завдань і функцій Ситуаційного центру Міністерства оборони України

Охарактеризуємо елементи орієнтовної моделі з формування завдань і функцій Ситуаційного центру Міністерства оборони України.

Загрози. Відповідно до [16], основними загрозами, на які має реагувати МО України є: стрімке зростання ролі інформаційних

технологій у всіх сферах суспільного життя. Розробляються системи озброєнь на основі нових фізичних принципів, із використанням квантових, інформаційних, космічних, гіперзвукових, біотехнологій, а також технологій у сфері штучного інтелекту, створення нових матеріалів, робототехніки та автономних безпілотних апаратів;

зовнішня і внутрішня деструктивна пропаганда з використанням суперечностей у суспільстві, розпалом ворожнечі, провокуванням конфліктів, підривом суспільної єдності. Крім того, спостерігається відсутність цілісної інформаційної політики держави, а слабкість системи стратегічних комунікацій ускладнюють нейтралізацію цієї загрози;

недостатня ефективність державних органів, що ускладнює вироблення і реалізацію ефективної політики;

загрози для критичної інфраструктури, пов'язані з погіршенням її технічного стану, відсутністю інвестицій в її оновлення та розвиток, несанкціонованим втручанням у її функціонування, зокрема фізичного і кіберхарактеру, триваючими бойовими діями, а також тимчасовою окупацією частини території України;

загострюються змагання між Сполученими Штатами Америки і Китайською Народною республікою за світове лідерство. Посилюється міжнародна конкуренція із застосуванням усіх інструментів національної сили – політико-дипломатичних, воєнних, економічних, інформаційно-психологічних, кіберзасобів. Її наслідки проявляються у Східній Європі, на Близькому Сході і у Північній Африці, Південно-Східній Азії, Арктиці, в інших регіонах;

зростають виклики трансатлантичної та європейській єдності, що може спричинити ескалацію наявних і виникнення нових конфліктів. Ситуацією намагається скористатися російська федерація, яка продовжує збройну агресію проти України;

російська федерація використовує Чорноморсько-Каспійський регіон, окупований Крим як «міст» на Балкани, у Середземномор'я, на Близький Схід і у Північну Африку. Для зміцнення позицій у Європі російська федерація застосовує енергетичну та інформаційну «зброю», намагається впливати на внутрішньополітичну ситуацію у європейських державах, підживлює тривалі конфлікти, збільшує військову присутність у Східній Європі тощо.

Кризові ситуації. До КС, реагування на які є сферою відповідальності МО України можна віднести тільки КС воєнного характеру.

Ризики. Зважаючи на нормативно-правові документи, управління ризиками у сфері воєнної безпеки передбачає прийняття відповідних рішень та здійснення заходів, спрямованих на їх зменшення. Основними ризиками у цій сфері можуть бути [15]:

ухвалення стратегічно помилкових рішень у

воєнній сфері на підставі неякісного аналізу реальних і потенційних воєнних загроз національній безпеці;

недостатні інвестиції в розвиток сил оборони, неефективний розподіл витраток на оборону України і витрачання державних ресурсів на утримання безперспективного озброєння, військової та спеціальної техніки;

недостатній рівень взаємодії і неузгодженість заходів, що здійснюються СО, іншими складовими СБіО, відсутність належної координації їх дій з іноземними партнерами та міжнародними організаціями в ході підготовки до збройного захисту України у разі збройної агресії або збройного конфлікту, а також відбудовного періоду після закінчення воєнних дій;

неспроможність забезпечити відсіч і стримування збройної агресії проти України з боку російської федерації традиційними формами та способами збройної боротьби, зважаючи на незрівнянну різницю у воєнних потенціалах;

недостатні спроможності Збройних сил України (далі – ЗС України) та інших складових СО з охорони повітряного простору та протиповітряного прикриття важливих державних і військових об'єктів, недостатні військово-морські спроможності, у тому числі щодо охорони підводного простору в межах територіального моря України, берегової оборони, а також захисту національних інтересів України в Азовському і Чорному морях.

За результатами проведеного дослідження [2, 15–18, 20, 21, 28–31], можна виокремити такі орієнтовні завдання СЦ МО України:

організація і здійснення моніторингу інформаційного простору, обробка інформації та її узагальнення з метою забезпечення діяльності керівництва МО України, здійснення прогнозування розвитку ситуації у визначених сферах відповідальності МО України;

здійснення (в межах компетенції) аналізу воєнно-політичної обстановки, прогнозуванні, виявленні та визначенні рівня воєнної загрози національній безпеці України;

участь у створенні та функціонуванні системи комплексного стратегічного аналізу воєнних загроз національній безпеці України;

оцінювання наявних (можливих) ризиків у сфері оборони, налагодження взаємодії та обміну інформацією між суб'єктами оцінювання ризиків національної безпеки і стану відповідних спроможностей;

участь у плануванні та здійсненні заходів (у межах компетенції) щодо протидії і нейтралізації воєнно-політичних ризиків, викликів, загроз застосування воєнної сили проти України;

завчасне виявлення та аналіз (в межах компетенції) КС, підготовка проектів відповідних рішень щодо підготовки держави до оборони, реагування на КС;

підтримка достатнього рівня забезпечення готовності до реагування МО України в умовах виникнення загроз і настання КС, підтримання

функціонування базових елементів національної системи стійкості;

забезпечення здатності (в межах компетенції) МО України швидко адаптуватися до змін безпекового середовища, протистояти воєнним загрозам, безперебійно функціонувати до і під час воєнного конфлікту, а також відновлюватися після його завершення;

оперативне інформаційно-аналітичне забезпечення керівництва МО України з прийняття управлінських рішень в НС та КС;

проведення керівництвом МО України службових нарад та інших відповідних заходів з використанням інформаційно-телекомунікаційних систем в режимі реального часу;

організація і підтримання постійної взаємодії з обміну інформацією між Головним СЦ при Апараті Раді національної безпеки і оборони України (далі – РНБО), Національним координаційним центром кібербезпеки РНБО, Урядовим СЦ, СЦ центральних органів виконавчої влади, органів військового управління (стратегічного рівня) та органів місцевої влади, інформаційно-аналітичними групами (центрами);

підтримка інформаційного і програмно-технічного середовища та забезпечення доступу до загальнодержавної системи оперативної, архівної інформації підтримки прийняття рішень органами виконавчої влади всіх рівнів;

забезпечення розвитку спроможностей МО України в сфері стратегічних комунікацій;

забезпечення розвитку спроможностей МО України в сфері кібербезпеки, кіберзахисту і кібероборони під час підготовки та ведення всеохоплюючої оборони України.

Крім того, слід зазначити такі орієнтовні функції СЦ МО України:

забезпечення моніторингу стану МО України; здійснення збору, обробки інформації про стан різних сфер національної безпеки України (складових СО);

здійснення оповіщення керівництва МО України, координація та контроль за виконанням заходів з ліквідації НС і КС;

введення в дію та контролювання механізму реагування на НС і КС, визначеного керівництвом;

здійснення оцінювання ситуації, прогнозування її розвитку та можливих негативних наслідків з допомогою застосування сучасних інформаційних технологій;

здійснення інформаційно-аналітичної підтримки керівництва МО України під час формування рішення та прогнозування наслідків проєктів управлінських рішень за результатами проведеного моделювання їх реалізації;

здійснення експертної оцінки проєктів управлінських рішень та підготовка пропозицій щодо їх оптимізації;

забезпечення проведення керівництвом МО України нарад та інших відповідних заходів з використанням інформаційно-телекомунікаційних систем МО України в режимі реального часу;

підтримання та контролювання, в межах

компетенції, захищеного інформаційного і програмно-технічного середовища та загальнодержавної системи доступу до оперативної й архівної інформації;

організація впровадження до СЦ сучасних інформаційних технологій для прийняття обґрунтованих управлінських рішень;

забезпечення удосконалення методичних підходів до діяльності СЦ, а саме, організування розробки засад оцінювання ризиків національній безпеці й науково-математичного апарату щодо прогнозування, запобігання та реагування на ризики та КС на різних етапах їх розвитку; удосконалення системи забезпечення кібербезпеки для забезпечення гарантованої кіберстійкості інформаційних ресурсів МО України;

забезпечують організацію обміну досвідом з Європейським Центром передового досвіду з протидії гібридним загрозам;

організують впровадження адаптивних алгоритмів узгоджених дій щодо запобігання та реагування на загрози та КС на різних етапах їх розвитку;

забезпечують ефективне стратегічне планування і кризовий менеджмент, зокрема, впровадження універсальних протоколів реагування на КС з урахуванням досвіду НАТО;

здійснюють накопичення інформації про стан та діяльність МО України;

беруть участь в опрацюванні інформаційно-аналітичних матеріалів про стан ЗС України для їх подання керівництву держави;

беруть участь у впровадженні сучасних інформаційних та космічних технологій, автоматизації управлінських процесів і цифровізації діяльності в МО України з відповідним рівнем захищеності інформації, що обробляється;

беруть участь у розгортанні захищеної мережі обміну інформацією між органами управління СО, що відповідає вимогам до захисту інформації;

беруть участь у впровадженні інформаційних технологій (інформаційних систем) в управління військами і зброєю, захисту інформації, розвідки та логістики у війсьній сфері;

беруть участь у впровадженні програмно-проектного управління оборонними ресурсами, планів утримання і розвитку відповідних складових СО, забезпечення виконання державних цільових програм;

беруть участь, в межах повноважень передбачених законом, у міжнародному співробітництві за воєнно-політичним, військово-технічним та іншими напрямками з відповідними органами іноземних держав і міжнародними організаціями.

Означені вище завдання та функції СЦ МО України дають змогу візуалізувати модель організаційної структури СЦ МО України (враховуючи категорії «загроза», «кризові ситуації», «ризик» (наслідки від настання КС) (рис. 5).

Слід зазначити, що загрози, КС і ризики

групуються за напрямками з використанням експертних методів, які в організаційній структурі відображаються відповідними модулями (загрози – модулі 1...L, КС – модулі 2...M, ризики – модулі 3...N).

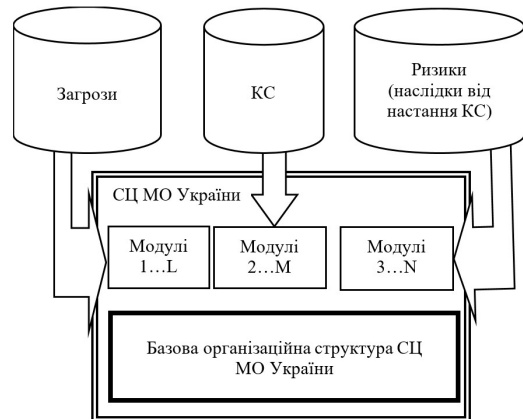


Рисунок 5 – Модель організаційної структури Ситуаційного центру МО України

Під базовою організаційною структурою розуміємо перелік елементів (підрозділів), які забезпечують цілодобове функціонування та попередній аналіз (обробку) інформації, що надходить; штаб реагування на КС, який здійснює формування рішень на реагування; технічний підрозділ.

Представлена на рис. 5 модель з урахуванням вимог нормативно-правових документів [2; 15–18], аналіз яких був проведений вище, приймає вигляд зображений на рис. 6, де додатково введені елементи (модулі) вищезазначених мереж СЦ, а саме: моніторингу об'єктів критичної інфраструктури (модуль Р); стратегічних комунікацій (модуль R); кібербезпеки (модуль S)), які будуть забезпечувати обмін інформацією та координацію з вищезазначеними мережами.

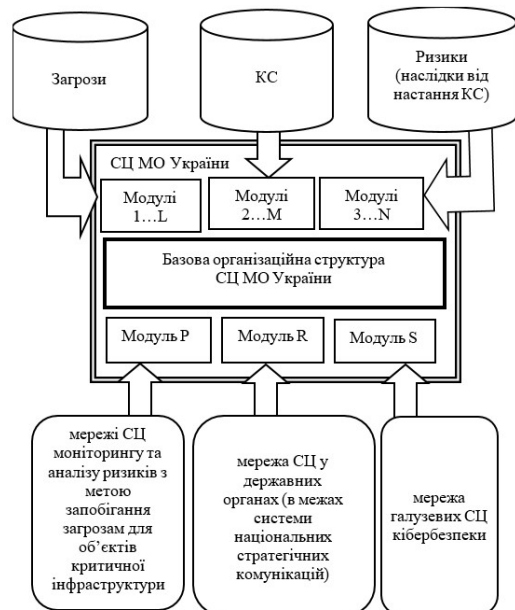


Рисунок 6 – Модель організаційної структури СЦ МО України (враховуючи категорії «загроза», «кризові ситуації», «ризик» (наслідки) та вимоги чинного законодавства держави)

Висновки й перспективи подальших досліджень

В статті опрацьовано концептуальний підхід до формування моделі організаційної структури Ситуаційного центру Міністерства оборони України для забезпечення реагування на кризові ситуації. Такий підхід дав змогу виокремити та опрацювати орієнтовні завдання і функції Ситуаційного центру Міністерства оборони України. А також – запропонувати організаційну структурну модель, враховуючи категорії «загроза», «кризова ситуація», «ризик» та вимоги чинного законодавства держави.

Практичною значущістю отриманих

результатів дослідження є можливість уточнення завдань, функцій і структури Ситуаційного центру Міністерства оборони України, а також вироблення завдань, формування функцій та побудови організаційних структур ситуаційних центрів складових сил оборони України й інших центральних органів виконавчої влади.

У подальшому, дослідження будуть спрямовані на удосконалення алгоритмів роботи та взаємодії Ситуаційного центру Міністерства оборони України з ситуаційними центрами центральних органів виконавчої влади держави.

Список бібліографічних посилань

1. Бочарніков В.П., Свєшніков С.В., Тимошенко Р.І., Павленко В.І. Технологія аналізу воєнно-політичної обстановки: монографія. Київ : НУОУ ім. Івана Черняхівського, 2019. 384 с. 2. Щодо удосконалення мережі ситуаційних центрів та цифрової трансформації сфери національної безпеки і оборони: Указ Президента України від 18.06.2021 № 260/2021. URL: <https://www.president.gov.ua/documents/2602021-39225> (дата звернення: 02.02.2023). 3. Воєнні аспекти протидії «гібридній» агресії: досвід України: монографія / колектив авторів; за заг. ред. А. М. Сиротенка. Київ: НУОУ ім. Івана Черняхівського, 2020. 176 с. 4. Богданович В. Ю. та ін. Методологія комплексного використання військових і невійськових сил та засобів сектору безпеки і оборони для протидії сучасним загрозам воєнній безпеці України: монографія. 2 видання, розш. і доп. Київ : НУОУ ім. Івана Черняхівського, 2021. 364 с. 5. Hudyma O. Situational Center as an element of the state management system in countering hybrid threats. *Current issues of military specialists training in the Security and Defence Sector under conditions of hybrid threats*: monograph / Scientific editors Boguslaw Pacek, Hennadii Pievtsov, Anatolii Syrotenko. Warsaw: Wydawnictwo Instytutu Bezpieczeństwa i Rozwoju Międzynarodowego. 2021. P. 58–65. URL: https://instytutbirm.pl/wp-content/uploads/2021/03/Monografia_mm1.pdf. (Accessed : 02.02.2023). 6. Саганюк Ф. В. та ін. Сектор безпеки і оборони України: стратегічне керівництво та військовое управління: монографія / за ред. д. військ. н., проф. І. С. Руснака. Київ, ЦЗ МО та ГШ ЗС України, 2018. 230 с. 7. Тимошенко Р. І., Павліковський А. К., Лобко М. М. Модель системи оборони України. *Наука і оборона*. 2021. № 1. С. 21–30. DOI: 10.33099/2618-1614-2021-14-1-21-30. 8. Гудима О. П. Міжнародний досвід побудови систем забезпечення національної безпеки. Висновки для України. *Збірник наукових праць Харківського національного університету Повітряних Сил*. 2021. № 3(69). С. 16–25. DOI: 10.30748/zhups.2021.69.02. 9. Загорка О. М., Поліщук С. В., Коваль В. В., Загорка І. О. Оцінка впливу загострення воєнно-політичної обстановки на виникнення кризової ситуації: методичний аспект. *Наука і оборона*. 2021. № 2. С. 61–65. DOI: 10.33099/2618-1614-2021-15-2-61-65. 10. Гудима О. П. Методологічні основи побудови підсистеми антикризового реагування в системі державного управління. *Наукові перспективи*. 2022.

Вип. №2(20). С. 54–67. DOI: 10.52058/2708-7530-2022-2(20)-54-67. 11. Домарєв В. В. Система ситуаційного управління: Теорія, методологія, рекомендації. Київ: Знання України, 2017. 347 с. 12. Сальнікова О. Ф., Посмітєх О. І., Петренко М. І. Ситуаційний центр як ефективний механізм стратегічних комунікацій. *Інвестиції: практика та досвід*. 2021. № 17. С. 62–66. DOI:10.32702/2306_6814.2021.17.62. 13. Гудима О. П. Національний досвід створення ситуаційних центрів в органах державної влади. *Публічне адміністрування та національна безпека*. 2020. № 8(16). С. 104–111. <https://doi.org/10.25313/2617-572X-2020-8-6446>. 14. Живило Є. О. Ситуаційний центр Міністерства оборони України – модель завчасного виявлення та аналізу кризових ситуацій сектору безпеки держави. *Актуальні проблеми державного управління*. 2022. № 1(60). С. 27-41. DOI: <https://doi.org/10.26565/1684-8489-2022-1-02>. 15. Про Стратегію воєнної безпеки: Указ Президента України від 25.03.2021 № 121/2021. 16. Про Стратегію національної безпеки України: Указ Президента України від 14 вересня 2020 р. № 392/2020. 17. Про Річну національну програму під егідою Комісії Україна – НАТО на 2021 рік: Указ Президента України від 11.05.2021 № 189/2021. URL: <https://www.president.gov.ua/documents/1892021-38845> (дата звернення: 02.02.2023). 18. Про Річну національну програму під егідою Комісії Україна – НАТО на 2020 рік: Указ Президента України від 26 травня 2020 р. № 203/2020. URL: <https://www.president.gov.ua/documents/2032020-33861> (дата звернення: 02.02.2023). 19. Городнов В. П., Фьк О. В. Математическое моделирование, оценка эффективности и синтез организационных структур предприятий. Харьков.: изд-во НУА, 2005. 192 с. 20. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2469-19#Text> (дата звернення: 02.02.2023). 21. Про запровадження національної системи стійкості: Указ Президента України від 27.09.2021 N 479/2021. URL: <https://www.president.gov.ua/documents/4792021-40181> (дата звернення: 02.02.2023). 22. Про Раду національної безпеки і оборони України: Закон України від 5.03.1998 № 183/98-ВР. URL: <https://zakon.rada.gov.ua/laws/show/183/98-%D0%B2%D1%80/conv#Text> (дата звернення: 02.02.2023). 23. Про критичну інфраструктуру: Закон України від 16.11.2021 № 1882-IX. URL:

<https://zakon.rada.gov.ua/laws/show/1882-20#Text> (дата звернення: 02.02.2023). **24. Кутащенко М. В.** Сутність ризику і причини його виникнення. *Інвестиції: практика та досвід*. 2009. Вип. № 6. С. 45–48. **25. Шарапов О. Д.** Ризикологія в економіці та підприємстві: *Зб. наук. пр. за матеріалами міжнародної науково-практичної конф.* 27–28 березня 2001 року. Київ: Київський національний економічний ун-т; Академія державної податкової служби України, 2001. С. 452. **26. Фере В. А., Романченко О. В.** Методи оцінки фінансового ризику. *Фінанси України*. 1997. № 2. С. 48–53. **27. Методичний посібник** щодо аспектів управління ризиками, як складової системи внутрішнього контролю у розпорядника бюджетних коштів. Київ: Міністерство фінансів України, 2022. 22 с. **28. Про затвердження Положення** про Міністерство оборони України: Постанова Кабінету Міністрів України від 26.11.2014 № 671. URL:

<https://zakon.rada.gov.ua/laws/show/671-2014-%D0%BF#Text> (дата звернення: 02.02.2023). **29. Про Положення** про Генеральний штаб Збройних Сил України: Указ Президента України від 30.01.2019 № 23/2019. URL: <https://zakon.rada.gov.ua/laws/show/23/2019#Text> (дата звернення: 02.02.2023). **30. Про Стратегічний** оборонний бюлетень України: Указ Президента України від 17.09.2021 № 473/2021. URL: <https://www.president.gov.ua/documents/4732021-40121> (дата звернення: 02.02.2023). **31. Гудима О. П.** Концептуальний підхід до формування змісту типового положення про ситуаційний центр органу сектору безпеки і оборони. *Наукові перспективи*. 2022. випуск № 4(22). С. 11–23. DOI: [https://doi.org/10.52058/2708-7530-2022-4\(22\)-11-23](https://doi.org/10.52058/2708-7530-2022-4(22)-11-23). **32. Академічний** тлумачний словник. Словник української мови. URL: <https://sum.in.ua/s/zagfroza> (дата звернення: 02.02.2023).

CONCEPTUAL APPROACH TO THE FORMATION OF A MODEL OF THE ORGANIZATIONAL STRUCTURE OF THE SITUATION CENTER OF THE MINISTRY OF DEFENSE OF UKRAINE

Mashtalir Vadym (Doctor of Historical Sciences, Professor)
Hudyma Oleh (Candidate of technical sciences, Senior Research Fellow)

National Defence University of Ukraine, Kyiv, Ukraine

The beginning of the russian federation's aggression against Ukraine and the course of the armed conflict creates a need for high-quality information and analytical support for management activities. The analysis of recent scientific publications shows that the issues of a systematic (integrated) approach to the formation of a structural model of the organizational structure of the Situation Center of the Ministry of Defense of Ukraine as an information and analytical support body have not been considered. The purpose of the article is to formulate a conceptual approach to creating a structural model of the organizational structure of the Situation Center of the Ministry of Defense of Ukraine to ensure crisis response. The methods of analysis, synthesis, analogy, decomposition, structural synthesis, modeling, and expert methods were used in the course of elaboration of the article. The developed conceptual approach made it possible to identify and elaborate on the approximate tasks and functions of the Situation Center of the Ministry of Defense of Ukraine. In addition, the author proposes its organizational structural model, taking into account the categories of "threat", "crisis situation", "risk" and the requirements of the current legislation of the State. This gives grounds to clarify the tasks, functions and structure of the Situation Center of the Ministry of Defense of Ukraine. In addition, the proposed approach can be used to develop tasks, formulate functions and build organizational structures of situational centers of the components of the defense forces of Ukraine and other central executive bodies. Further research will be aimed at improving the algorithms of work and interaction of the Situation Center of the Ministry of Defense of Ukraine with the situation centers of the central executive authorities of the state.

Key words: crisis situation, situation center, response, conceptual approach.

References

- 1. Bocharnikov, V. P., Sveshnikov, S.V., Tymoshenko, R. I., Pavlenko, V. I.,** (2019). *The technology of analysis of the military and political situation: a monograph*. Kyiv: NUOU named after Ivan Chernyakhovsky. **2. Regarding** the improvement of the network of situation centers and the digital transformation of the sphere of national security and defense [online], (2021). Decree of the President of Ukraine № 260/2021, June 18. Available at: <https://www.president.gov.ua/documents/2602021-39225> [Accessed 02 February 2023]. **3. Military aspects** of countering «hybrid» aggression: experience of Ukraine: monograph (2020). Collective of authors; in general ed. A. M. Syrotenko. Kyiv: NUOU named after Ivan Chernyakhovsky. **4. Bohdanovych, V.Yu. et al.,** (2021). Methodology of integrated use of military and non-military forces and means of the security and defense sector to counteract modern threats to the military security of Ukraine: monograph; 2nd edition, expanded and supplemented. Kyiv: NUOU named after Ivan Chernyakhovsky. **5. Hudyma, O.,** (2021). Situational Center as an element of the state management system in counteracting hybrid threats. Current issues of military specialists training in the Security and Defense Sector under conditions of hybrid threats: Monograph / Scientific editors Boguslaw Pacek, Hennadii Pievtsov, Anatolii Syrotenko. Warsaw: Wydawnictwo Instytutu Bezpieczeństwa i Rozwoju Międzynarodowego. [online]. Available at: https://instytutbirm.pl/wp-content/uploads/2021/03/Monografia_mml.pdf. [Accessed 02 February 2023]. **6. Saganyuk F.V. and others,** (2018). The security and

- defense sector of Ukraine: strategic leadership and military management: monograph / under the editorship Doctor of Military Sciences, Prof. I.S. Russian Kyiv, Center of the Ministry of Defense and General Staff of the Armed Forces of Ukraine. **7. Tymoshenko, R. I., Pavlikovskyi, A. K., Lobko, M. M.,** (2021). Model of the defense system of Ukraine. *Science and defense*, 1, 21-30. DOI: 10.33099/2618-1614-2021-14-1-21-30. **8. Hudyma, O. P.,** (2021). International experience of building national security systems. Conclusions for Ukraine. *Collection of scientific works of the Kharkiv National University of the Air Force*, 3(69), 16-25. DOI: 10.30748/zhups.2021.69.02. **9. Zagorka, O. M., Polishchuk, S. V., Koval, V. V., Zagorka, I. O.,** (2021). Assessment of the influence of the aggravation of the military and political situation on the emergence of a crisis situation: methodological aspect. *Science and defense*, 2, 61-65. DOI: 10.33099/2618-1614-2021-15-2-61-65. **10. Hudyma, O. P.,** (2022). Methodological foundations of the construction of the anti-crisis response subsystem in the state administration system. *Scientific perspectives*, 2(20), 54-67. DOI: 10.52058/2708-7530-2022-2(20)-54-67. **11. Domarev, V. V.,** (2017). System of situational management: Theory, methodology, recommendations. Kyiv: Knowledge of Ukraine. **12. Salnikova, O. F., Posmityukh, O. I., Petrenko, M. I.,** (2021). The situational center as an effective mechanism of strategic communications. *Investments: practice and experience*, 17, 62-66. DOI:10.32702/2306_6814.2021.17.62. **13. Hudyma, O. P.,** (2020). National experience of creating situational centers in state authorities. *Public administration and national security*, 8(16), 104-111. <https://doi.org/10.25313/2617-572X-2020-8-6446>. **14. Jvilo, E. O.,** (2022). The Situation Center of the Ministry of Defense of Ukraine is a model for early detection and analysis of crisis situations in the state security sector. *Actual problems of public administration*, 1(60), 27-41. DOI: <https://doi.org/10.26565/1684-8489-2022-1-02>. **15. On the Military Security Strategy:** Decree of the President of Ukraine №. 121/2021, March 25, 2021. **16. On the National Security Strategy of Ukraine:** Decree of the President of Ukraine №. 392/2020, September 14, 2020. **17. About the Annual National Program under the auspices of the Ukraine-NATO Commission for 2021:** Decree of the President of Ukraine № 189/2021, May 11, 2021. **18. About the Annual National Program under the auspices of the Ukraine-NATO Commission for 2020:** Decree of the President of Ukraine №. 203/2020, May 26, 2020. **19. Horodnov, V. P., Fyk, O. V.,** (2005). Mathematical modeling, efficiency assessment and synthesis of organizational structures of enterprises. Kharkiv: NUA publishing house. **20. On the national security of Ukraine:** Law of Ukraine № 2469-VIII, June 21, 2018. **21. On the introduction of the national sustainability system:** Decree of the President of Ukraine № 479/2021, September 27, 2021. **22. About the National Security and Defense Council of Ukraine:** Law of Ukraine № 183/98-VR, March 5, 1998. **23. On critical infrastructure:** Law of Ukraine № 1882-IX, November 16, 2021. **24. Kutashenko, M. V.,** (2009). The essence of the risk and its causes. *Investments: practice and experience*, 6, 45-48. **25. Sharapov, O. D.,** (2001). Riskology in economics and entrepreneurship: *Collection of science pr. based on the materials of the international scientific and practical conference*. March 27-28, Kyiv: Kyiv National University of Economics; Academy of the State Tax Service of Ukraine. **26. Fere, V. A., Romanchenko, O. V.,** (1997). Methods of financial risk assessment. *Finances of Ukraine*, 2, 48-53. **27. Methodical manual on aspects of risk management as a component of the internal control system of the manager of budget funds,** (2022). Kyiv: Ministry of Finance of Ukraine, 22. **28. On the approval of the Regulation on the Ministry of Defense of Ukraine:** Resolution of the Cabinet of Ministers of Ukraine №. 671, November 26, 2014. **29. On the Regulations on the General Staff of the Armed Forces of Ukraine:** Decree of the President of Ukraine № 23/2019, January 30, 2019. **30. About the Strategic Defense Bulletin of Ukraine:** Decree of the President of Ukraine № 473/2021, September 17, 2021. **31. Hudyma, O. P.,** (2022). A conceptual approach to the formation of the content of the standard provision on the situational center of the body of the security and defense sector. *Scientific perspectives*, 4(22), 11-23. DOI: [https://doi.org/10.52058/2708-7530-2022-4\(22\)-11-23](https://doi.org/10.52058/2708-7530-2022-4(22)-11-23). **32. Academic explanatory dictionary.** Dictionary of the Ukrainian language [online]. Available at: <https://sum.in.ua/s/zagyroza> [Accessed : 02 February 2023].