Електронний журнал «Державне управління: удосконалення та розвиток» включено до переліку наукових фахових видань України з питань економіки (Категорія «Б», Наказ Міністерства освіти і науки України № 1643 від 28.12.2019). Спеціальність – 281.

Державне управління: удосконалення та розвиток. 2022. № 9.

DOI: http://doi.org/10.32702/2307-2156.2022.9.15
УДК 354/351.861

І. О. Семененко,
аспірант, Київський національний економічний університет імені Вадима Гетьмана, м. Київ
ORCID ID: https://orcid.org/0000-0003-1418-9302

СВІТОВИЙ ДОСВІД ФУНКЦІОНУВАННЯ МЕРЕЖІ СИТУАЦІЙНИХ ЦЕНТРІВ ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ

I. Semenenko,
Postgraduate student, Kyiv National Economic University named after Vadym Hetman

FOREIGN EXPERIENCE OF OPERATION OF STATE AUTHORITIES' SITUATIONAL AWARENESS CENTRES NETWORK

Загострення загроз національної безпеки, з якими стикається Україна від початку російської збройної агресії, зокрема окупація Криму та розгортання війни на Сході України у 2014 році, а також широкомасштабне вторгнення Росії 24 лютого 2022 року, формують для керівництва нашої країни кризові виклики, які потребують не лише ефективного оперативного реагування, але і постійного відстеження ситуації, прогнозування можливого розвитку подій, обміну інформацією та взаємодію для прийняття рішень. У світовій практиці з цією метою напрацьовано досвід створення та функціонування мережі спеціальних ситуаційних центрів оперативного реагування, які оснащують високотехнологічним обладнанням та забезпечуються кваліфікованим персоналом для аналізу ситуацій у критично важливих сферах, де можуть виникати загрози національній безпеці, спричинені різними чинниками. Тому вивчення дієвих та ефективних практик прийняття рішень в мережі ситуаційних центрів є передумовою успішної розбудови в Україні мереж антикризового реагування для органів державної влади. Метою дослідження є обґрунтування на основі дослідження світового досвіду дієвих механізмів формування та

функціонування мережі ситуаційних центрів органів державної влади, а об'єктом – ситуаційні центри органів державної влади. Методологія дослідження ґрунтується на компаративному аналізі світового досвіду формування та функціонування мережі ситуаційних центрів. Авторський підхід полягає в узагальненні ключових засад діяльності ситуаційних центрів в міжнародних міжурядових організаціях та об'єднаннях а також в окремих країнах світу. Дослідження показало, що ситуаційні центри є осередками постійного моніторингу, аналізу даних, моделювання ситуацій та прийняття управлінських рішень в кризових ситуаціях. Вони створюються як в межах однієї країни, так і на міжнародному рівні та забезпечують успішну координацію зусиль органів влади задля протидії загрозам для суспільства військового, техногенного, стихійного чи інших видів. Автором показано, що особлива увага з боку органів влади надається діяльності ситуаційних центрів щодо безпеки критичної та стратегічної інфраструктури, зокрема у військовій та енергетичній сфері, кібербезпеки інформаційного середовища, безпеки повітряного, наземного на морського простору.

The aggravation of national security threats that Ukraine has faced since the beginning of Russian armed aggression, in particular the occupation of Crimea and the outbreak of war in the East of Ukraine in 2014, as well as the large-scale invasion of Russia on February 24, 2022, are creating crisis challenges for the leadership of our country that require not only effective operational response, but also constant monitoring of the situation, forecasting of possible developments, exchange of information and interaction for decision-making. In global practice, for this purpose, experience has been gained in the creation and operation of a network of special situational awareness centres equipped with high-tech equipment and provided with qualified personnel to analyse situations in critical areas, where threats to national security caused by various factors may arise. Therefore, the study of effective and efficient decision-making practices in the network of situational awareness centres is a prerequisite for the successful development of anti-crisis response networks for state authorities in Ukraine. The purpose of the study is to justify, based on the study of world experience, effective mechanisms for the formation and functioning of the network of situational awareness centres of state authorities, and the object is situational awareness centres of state authorities. The research methodology is based on a comparative analysis of the global experience of the formation and functioning of the network

of situational awareness centres. The author's approach consists in summarizing the key principles of the activity of situational awareness centres in international intergovernmental organizations and associations, as well as in individual countries of the world. The study showed that situational awareness centres are centres of constant monitoring, data analysis, modelling of situations and management decision-making in crisis situations. They are created both within the borders of one country and at the international level and ensure the successful coordination of the efforts of authorities to counter threats to society of military, man-made, natural or other types. The author shows that the authorities pay special attention to the activities of situational awareness centres regarding the security of critical and strategic infrastructure, in particular in the military and energy spheres, cyber security, security of air, land and sea space.

Ключові слова: *мережі ситуаційного управління, функціональна структура ситуаційного центру, система ситуаційного моделювання, центри обміну та аналізу інформації, системи підтримки прийняття управлінських рішень*

Keywords: *situation management networks, functional structure of the situation center, situation modeling system, information exchange and analysis centers, management decision support systems.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Ситуаційні центри є ефективним інструментом прийняття рішень в сфері управління ситуаціями, які динамічно розвиваються. Їх застосування дозволяє виявляти на основі послідовного та всебічного аналізу основні тенденції, що визначають динаміку ситуації, а також прогнозувати її подальший розвиток [9]. Діяльність ситуаційних центрів у світовій практиці доволі часто пов’язують з функцією «усвідомлення ситуації» (англ. «situational awareness»), яку визначають як сприйняття елементів навколишнього середовища у

відповідному просторі та часі, розуміння їхнього значення та прогнозування їх стану в найближчому майбутньому [4]. На практиці ситуації є спрощеними представленнями складної системи суб'єктів, організацій, подій і дій, що супроводжуються гіпотезами про можливі їх наслідки. Основним завданням ситуаційних центрів є моделювання ситуацій, які виникають у відповідній предметній області прийняття управлінських рішень.

Створення ситуаційних центрів різного профілю для обміну та аналізу інформації ініціюють органи державної влади у багатьох країнах світу, а також міжнародні та міжурядові організації та об'єднання. Вони виконують роль центрального ресурсу для збору інформації про загрози для критичної інфраструктури окремих країн чи для суспільства в цілому, дозволяють двосторонній обмін інформацією між приватним і державним секторами про основні причини, інциденти та загрози, а також забезпечують поширення досвіду, знань та аналітичних даних. Більше того, в інфраструктурних сферах, які мають високу заінтересованість з боку приватних компаній, зокрема кіберпростір та кібербезпека, на міжнародному рівні сьогодні функціонують недержавні спільноти, що створюють ситуаційні центри, які використовують інформаційні технології та мають спільну прихильність до забезпечення безпеки, уможливлюють співпрацю та обмін актуальною, дієвою інформацією про поточні загрози та сприяють ефективними державним заходам політики державної безпеки. Обмін інформацією між національними зацінтересованими сторонами, навіть у міжнародних випадках, є важливим аспектом безпеки. Відповідні заінтересовані сторони можуть поділитися знаннями про боротьбу з загрозами, реагування на інциденти, заходи пом'якшення наслідків і підготовчий контроль.

Для України, яка сьогодні перебуває в активній фазі європейської інтеграції та просуває поглиблення співпраці з Північноатлантичним альянсом, важливою є адаптація їх практик щодо створення мережі ситуаційних центрів. Зокрема, законодавство ЄС передбачає виконання вимог щодо звітування про інциденти безпекових загроз та створення

галузевих ситуаційних центрів на національному рівні. При цьому, передбачається, що під час транспонування такого європейського законодавства до національного законодавства такі спільноти ситуаційних центрів могли б додатково інформуватися та консультуватися з боку політиків [6].

В умовах розгортання військового конфлікту на Сході України внаслідок російської агресії на початку 2015 року створено Головний ситуаційний центр України при РНБО України, який має сучасне інформаційно-комп'ютерне обладнання, що дозволяє обробляти величезні масиви інформації, яка надходить з усіх державних і недержавних баз даних, зокрема, з супутників, та безпосередньо з місць подій [14]. У червні 2021 року відповідно до рішення Ради національної безпеки і оборони України «Щодо удосконалення мережі ситуаційних центрів та цифрової трансформації сфери національної безпеки і оборони» (введено в дію указом Президента України від 18 червня 2021 року № 260/2021) визначено подальше розширення та розвиток єдиної мережі ситуаційних центрів. Метою розбудови ситуаційних центрів в Україні визначено підвищення ефективності інформаційно-аналітичного забезпечення прийняття управлінських рішень, взаємодії, координації і контролю за діяльністю органів виконавчої влади, правоохоронних органів та військових формувань у сферах національної безпеки і оборони у мирний час, а також в особливий період, у тому числі в умовах воєнного стану, в умовах надзвичайного стану та під час виникнення кризових ситуацій, що загрожують національній безпеці України.

З огляду на такі стратегічні цілі та розгортання широкомасштабної російсько-української війни після 24 лютого 2022 році для України особливої актуальності набуває вивчення світових практик формування та функціонування ситуаційних центрів, їх організаційних засад, ресурсного забезпечення, налагодження взаємодії та співпраці з іншими вітчизняними органами державної влади, іноземними інституціями, міжнародними та

міжурядовими організаціями. Їх узагальнення дозволить Україні не лише здійснити адаптацію до вимог міжнародного законодавства, але і сформувати сучасні механізмі протидії безпековим загрозам та напрацювати інноваційні осередки прийняття рішень в кризових ситуаціях.

Аналіз останніх досліджень і публікацій, в яких започатковано розв'язання даної проблеми, виділення не вирішених раніше частин загальної проблеми, котрим присвячується означена стаття. Дослідженню принципів, механізмів та секторальних особливостей розвитку ситуаційних центрів присвячені численні праці таких іноземних дослідників як М. Амановіч [2], А. Астіакопулос, А. Блум, В. Драгос [3], Р. Лежчина, В. Овенс, Н. Павлов [8], Т. Уолліс [12], С. Ван Бейлен, Г. Пітерс, Х. Брюнінккс, П. Пілоцці, П. Слатс [11] та ін. У своїх публікаціях автори розкривають особливості функціонування ситуаційних центрів, симуляційних систем, платформ, командно-контрольних систем, віртуальних середовищ, баз даних у різних секторах управління об'єктами, таких як прикордонний контроль, морський нагляд, енергетична безпека, кібербезпека, семантичний аналіз, а також міжнародне співробітництво в сфері моніторингу ситуацій та обміну даними. Серед вітчизняних дослідників проблематика розвитку ситуаційних центрів відображена у працях В. Вишневського [13], В. Горбік [15], Г. Кузьменка та А. Морозова [17], В. Пристайка, В. Тютюника [18], М. Циркун та інших. Авторами, зокрема, висвітлено еволюцію процесів автоматизації управління об'єктами в Україні, сутнісні характеристики, організаційні аспекти формування та особливості функціонування ситуаційних центрів на різних стадіях розвитку надзвичайних ситуацій, принцип мережево-центричності у функціонуванні ситуаційних центрів, а також особливості обґрунтування експертами антикризових рішень щодо функціонування органів державної влади.

Метою статті є обґрунтування на основі дослідження світового досвіду дієвих механізмів формування та функціонування мережі ситуаційних центрів органів державної влади.

Виклад основних наукових результатів та їх обґрунтування. Спеціалізовані системи динамічного моделювання ситуацій використовуються для вирішення безпосередніх завдань, зміст яких випливає з вихідних даних з подальшим аналізом ситуацій, що виникають у системах відображення ситуаційної інформації та аналітичних ситуаційних системах. Водночас, адаптивні системи застосовуються для вирішення діаметрально протилежних управлінських завдань, а саме – для опису факторів та передумов виникнення можливих ситуацій за допомогою імітаційного (динамічного) моделювання. Їх завданням є визначення вихідних даних, що відображають умови і фактори виникнення певних ситуацій.

Застосування аналітичних ситуаційних систем здійснюється з врахуванням того, що кількість можливих станів цільової системи є значною, водночас, кількість можливих рішень є обмеженою. Таким чином, поєднання системного підходу, який дає повне уявлення про об’єкт управління та його функціонування в зовнішньому середовищі, із ситуаційним дозволяє ефективно керувати розвитком конкретної управлінської ситуації. При цьому, ефективні управлінські рішення приймаються з врахуванням вихідних умов та характеристик конкретної ситуації.

Як свідчить аналіз світової практики, системи ситуаційного моделювання можна розділити на три основні види [9]:

- спеціалізовані та адаптивні системи моделювання динамічних ситуацій;
- моніторингові ситуаційні системи (центри ситуаційного відображення; розподілені системи відображення ситуаційної інформації);
- аналітичні ситуаційні системи (системи ситуаційного управління; аналітичні ситуаційні центри; експертні системи реального часу).

Окрім того, важливо розрізняти зовнішні ситуаційні центри, чиї функції пов’язані з оцінкою ситуацій взаємодії певної організації із

зовнішнім середовищем, та внутрішні центри, що застосовуються для моделювання, аналізу, оцінки взаємодії та управління внутрішніми структурними підрозділами організації.

Ситуаційні центри використовуються при виробленні стратегічних управлінських рішень на основі аналізу масиву вхідної інформації про ситуацію. Окрім того, вони сприяють формуванню коректного розуміння ситуації з урахуванням динаміки її розвитку, а також є інструментом системного пошуку релевантних управлінських рішень. Ситуаційні центри дають можливість відстежувати хід ситуації, її зміни, а також прогнозувати її ймовірні майбутні стани. Добре організована робота ситуаційного центру дозволяє економити час і ресурси, приймати обґрунтовані рішення, одночасно уникаючи численних управлінських помилок, що є наслідком застосування в практиці менеджменту принципу перевірки рішень з досвіду власних спроб і помилок.

Структура ситуаційних центрів може відрізнятися залежно від їх цільового призначення та предметного поля діяльності. Відтак, структура є одним із найвагоміших критеріїв класифікації ситуаційних центрів. Так, у загальному розумінні ситуаційним центром (пунктом або кімнатою) можна назвати приміщення, призначене для проведення спостереження або аналізу поточної ситуації. Проте така дефініція є надто широкою, оскільки під її кваліфікацію підпадатиме будь-яке приміщення, оснащене телебаченням, радіо, телефонним зв’язком, комп’ютерною технікою та географічними картами. В такому випадку йдеться про персональний ситуаційний центр. При цьому, структура професійних ситуаційних центрів, як правило, є складнішою та охоплює оперативний штаб, ситуаційний зал управління (нагляду), обладнаний потужним обчислювальним середовищем, а також інформаційні моделі складних динамічних ситуацій. Відмінною рисою будь-якого сучасного ситуаційного центру є наявність в ньому геоінформаційної системи.

Обов’язковими компонентами функціональної структури ситуаційного центру є три базові модулі, які відповідають за динамічне (імітаційне) моделювання поведінки зовнішнього, внутрішнього середовища та за оцінку їх взаємодії. Структура ситуаційного центру, як інформаційної системи, окрім функціональної складової включає ще й різні види ресурсного забезпечення – інформаційно-аналітичного, технічного, організаційного, кадрового, лінгвістичного тощо. Велике значення має інформаційна інфраструктура таких центрів, що складається з програмного забезпечення та інформаційних потоків, що у сукупності забезпечують роботу базових модулів і візуалізацію ситуаційного центру. Сюди можна віднести усі вищезгадані типи систем ситуаційного моделювання.

Типовим прикладом з категорії зовнішніх міжнародних ситуаційних центрів є SITCEN НАТО, до функціональних обов’язків якого належить інформування Північноатлантичної ради та Військового комітету НАТО про ситуацію в світі як у мирний час, так і в часи криз та військових конфліктів. Його послуги також використовуються для проведення міжнародних військових навчань північноатлантичного альянсу. SITCEN обробляє та поширює найактуальнішу інформацію, отриману як з внутрішніх, так і з зовнішніх ресурсів як відкритого, так і секретного характеру. SITCEN також виконує функції хабу для зв’язку з подібними установами в країнах північноатлантичного альянсу та міжнародними організаціями.

Зміст діяльності SITCEN полягає в обробці інформації з метою забезпечення ситуаційної обізнаності північноатлантичного альянсу, що дозволяє Північноатлантичній раді (North Atlantic Council, скорочено – NAC) та Військовому комітету (Military Committee, скорочено – MC) приймати обґрунтовані рішення. NAC є вищим органом НАТО, який приймає політичні рішення, водночас, MC є вищим військовим органом НАТО, який надає консультативну підтримку діяльності NAC та Групи ядерного планування НАТО.

Розміщений у штаб-квартирі НАТО в Брюсселі (Бельгія) SITCEN посідає унікальне місце в організаційній структурі НАТО у взаємодії між цивільними та військовими підрозділами персоналу (рис. 1).

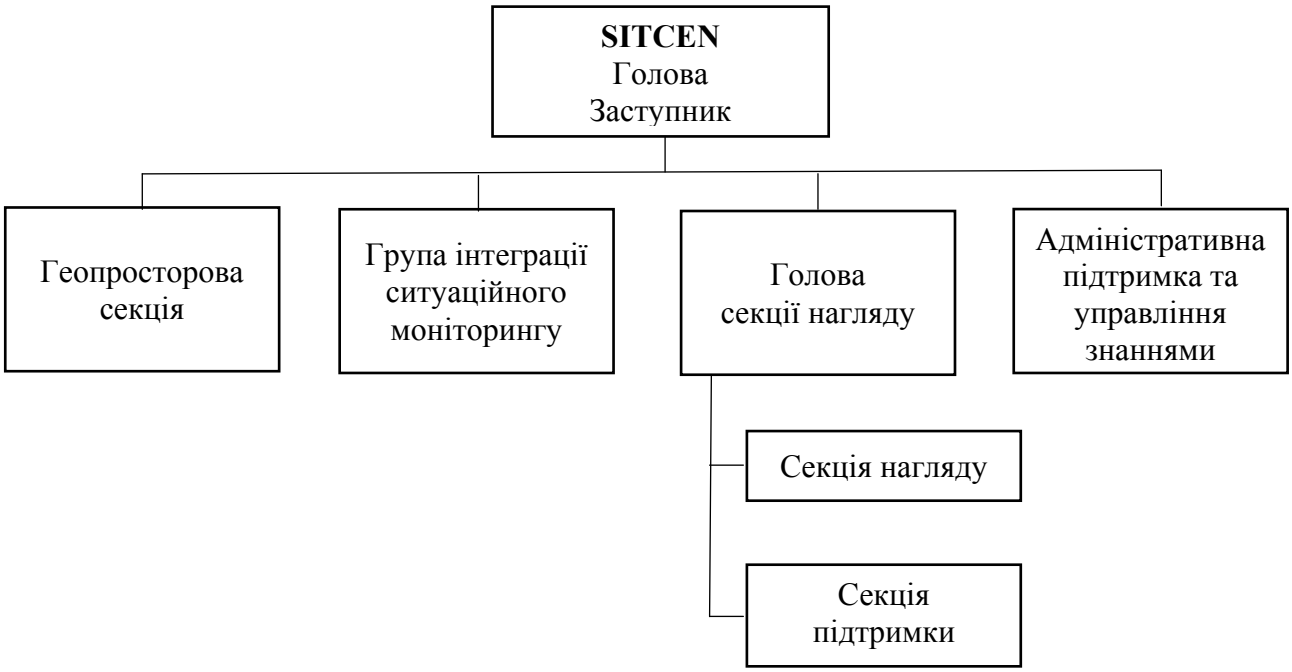

Рис. 1. Структура ситуаційного центру SITCEN НАТО (Брюссель, Бельгія)

Джерело: складено автором за: [10].

Секція нагляду (SITCEN Watch) надає штаб-квартирі НАТО цілодобову ситуаційну інформацію щодо політичних, економічних, військових та терористичних подій у всьому світі. Персонал секції працює цілодобово 24/7 вахтовим методом, змінюючи вахту кожні 12 годин. Перелік функціональних обов'язків секції нагляду включає:

- надання оперативної інформації про події з використанням автоматизованої системи виклику;
- інформаційне забезпечення підготовки нарад та особистих брифінгів керівництва міжнародного військового штабу НАТО;
- моніторинг систем раннього попередження протиповітряної оборони від балістичних ракет;

- співпраця з Відділом громадської дипломатії НАТО з метою безперервного моніторингу інформації у пресі;
- підтримка діяльності організацій та робочих груп з врегулювання криз;
- сприяння Управлінню безпеки НАТО у здійсненні моніторингу за виконанням міжнародних місій персоналу НАТО, що знаходиться за кордоном.

Геопросторова секція SITCEN надає комплексні географічні послуги штаб-квартирі НАТО як у сфері наземного геопросторового спостереження, такі в сфері морського, повітряного та космічного спостереження. Функціональні завдання секції є доволі широкими – від оперативного відображення місцевості до відтворення загальної оперативної ситуації для керівних органів НАТО. Окрім того, секція забезпечує управління геопорталами на різних мережевих доменах, а також займається створенням навчальних географічних сценаріїв для військових навчань. При цьому у кризових умовах геопросторова секція розробляє геопросторові програми та стратегічні інформаційні панелі з геопросторовим контентом з метою забезпечення цілодобового ситуаційного аналізу, а також процесу прийняття управлінських рішень.

Група інтеграції ситуаційного моніторингу (Situational Awareness Integration Team – SAIT), створена в березні 2020 року, є відносно новим підрозділом SITCEN. Вона виконує роль системного інтегратора ситуаційного центру, розробляючи системне бачення глобального та регіонального середовища безпеки та його впливу на союзників і партнерів НАТО. Одним із головних завдань підрозділу є підготовка, координація та проведення нарад керівного персоналу штаб-квартири НАТО. SAIT також проводить якісні та кількісні дослідження ситуацій, а також виконує роль посередника між усіма зацікавленими сторонами в межах НАТО.

У структурі SITCEN також є офіс адміністративної підтримки та управління знаннями (Administrative Support and Knowledge Management –

АКМ), який є центральним пунктом інформаційного контролю та управління, а також професійного навчання та фінансового управління.

Доволі показовим прикладом сучасного етапу еволюції ситуаційних центрів є американський проект SANER (Situational Awareness for Novel Epidemic Response), що є національною мережею медичних ситуаційних центрів, яка має на меті революціонізувати застарілі процеси обміну даними в сфері охорони здоров'я, покращити рівень оперативної обізнаності про пандемічну ситуацію з COVID-19 у режимі реального часу, а також прогнозувати всі майбутні надзвичайні ситуації в сфері охорони здоров'я [7]. До мережі SANER залучено партнерів з державного та приватного секторів з метою автоматизації звітності щодо працездатності лікарень, моніторингу поточної ситуації у сфері охорони здоров'я під час катастроф, надзвичайного стану та інших форс-мажорних обставин.

Головною перевагою проекту SANER є автоматизація процесів звітності з використанням інструментарію прикладного програмування (API) на основі міжнародного стандарту обміну даними HL7® Fast Healthcare Interoperability Resources (FHIR®). Заклади охорони здоров'я, критичної інфраструктури та державні органи можуть використовувати ці стандарти для розкриття даних, які є критичними для контролю поширення хвороб та управління ресурсами системи охорони здоров'я у межах всієї країни. Завдяки такому стандарту обміну даними основні елементи інформації можна автоматично отримувати з цілого ряду джерел (баз даних) лікарень, серед яких: електронні медичні карти (EHR) пацієнтів, система управління ліжко-місцями, система управління активами, інвентаризаційна звітність тощо. При цьому, елементи даних, що підлягають обміну в межах мережі, включають таку критично важливу інформацію, як кількість і статус конкретних типів лікарняних ліжок, забезпеченість персоналом, кількість апаратів штучної вентиляції легень та іншого критично необхідного медичного обладнання. Цими даними можна поділитися з іншими лікарнями,

місцевими, державними та федеральними органами охорони здоров'я та компетентними організаціями.

В Європейському Союзі наразі сформувалася диверсифікована система платформ, проектів та мереж ситуаційного управління з доволі різнобічним функціоналом. Так, наприклад, Datalab — це спеціалізована база даних і знань, розроблена Гаазьким центром стратегічних досліджень (The Hague Centre for Strategic Studies), яка використовується для здійснення геостратегічного аналізу та дослідження країн, які знаходяться в зоні ризику на основі відкритих даних [8, с. 9-10]. При цьому, в центрі уваги проекту перебувають внутрішньодержавні конфлікти та громадянські війни.

В проекті Datalab застосовується система прогнозних економетричних моделей, що базуються на аналізі 50 факторів уразливості, пов'язаних з політичною нестабільністю. Моделі останнього покоління використовують системи штучного інтелекту для створення прогнозів конфліктів на субнаціональному (районному) рівні з часовим горизонтом від 1 до 24 місяців. Моделі нового покоління Datalab визначають причинно-наслідкові зв'язки під час виникнення конфліктів та спрямовані на роз'яснення різних конфліктних патологій і ефектів взаємодії між різними чинниками виникнення конфліктів.

HCSS StratBase Datalab передбачає аналіз більше 11 тисяч змінних із різних відкритих та приватних баз даних, більшість з яких мають кількісну природу (наприклад, економічні, фінансові, військові та інші дані), проте все частіше застосовується аналіз текстів, зображень, аудіо та відео. Набори даних обробляються за допомогою аналітичних алгоритмів, що дають змогу здійснювати картування досліджуваних ситуацій, а також відстеження глобальної геодинаміки, життєвих циклів конфліктів, політичних ризиків та ризиків безпеки як в автономному режимі, так і в кіберпросторі.

Загалом, база даних StratBase та моделі DataLab можуть застосовуватися у політиці Європейського Союзу щодо запобігання конфліктам та забезпечення миру різними способами, а саме:

- застосування портфелю прогнозних моделей для ситуаційного аналізу;
- виявлення конфліктних патологій на основі причинно-наслідкових конфліктних моделей;
- сценарні моделі застосування політичних інструментів для врегулювання конфліктних ситуацій тощо.

Ще більш комплексний підхід в сфері ситуаційного менеджменту, розроблений компанією «4C Strategies», застосовується у Швеції [8, с. 11-12]. Exonaut — це електронна платформа керування ситуаціями, що базується на інтегрованих підходах до управління економічними ризиками та антикризового управління. Пакет програмного забезпечення дозволяє моделювати, оцінювати та відстежувати рівень організаційної готовності до кризових ситуацій. Наразі, платформа Exonaut фактично стала глобальним стандартом програмного забезпечення для проведення військових навчань та спеціалізованої фахової підготовки. Дана платформа дає змогу користувачам оцінювати, візуалізувати та використовувати навчальні дані для прийняття ефективних антикризових рішень. Зокрема, програмний додаток Exonaut Command and Control є комплексною системою управління надзвичайними ситуаціями, що охоплює весь спектр функцій – від диспетчерської до передової. Система дозволяє спостерігати за перебігом інцидентів на основі карти та інформаційних панелей, що дають змогу відстежувати стан та переміщення активів, створювати журнали інцидентів тощо. Система постійно удосконалюється з врахуванням вимог військових, поліцейських, пожежних та служб швидкої медичної допомоги.

Додаток Consular Online 2.0 забезпечує можливість спільного оперативного реагування на кризові ситуації та пройшов апробацію Європейською службою зовнішніх дій (EEAS) для реагування на консульські кризи. Мобільна онлайн система Exonaut Incident and Crisis Manager включає дошки оголошень і сповіщень у режимі реального часу, інтерактивні карти посольств, лікарень, пунктів збору тощо, а також автоматизовані звіти про

інциденти та спеціальні панелі інструментів. Критерії, набори запитань і цілі можуть бути зіставлені в системі з різними видами діяльності, які найбільше підходять для аналізу відповідних гіпотез або завдань. Окрім того, отримані об'єктивні та суб'єктивні дані можуть бути записані в систему майже в режимі реального часу та застосовуватися для інформування про подальший перебіг подій або адля отримання визначених користувачем результатів.

Компанія MASA Group (Франція) розробила «MASA Synergy», що є високорівневою системою підтримки прийняття рішень державними або приватними організаціями в умовах надзвичайних ситуацій, криз і катастроф. MASA Synergy дозволяє моделювати міжвідомчі кризові сценарії забезпечення громадської безпеки та операцій цивільного захисту на місцевому, регіональному та державному рівнях [1]. Перелік моделей «Synergy», зокрема, включає стихійні лиха (землетруси, повені, урагани, зсуви, посухи тощо), техногенні катастрофи (витоки хімікатів, забруднення, пожежі тощо), напади злочинців / терористів, операції з боротьби з натовпом, захист стратегічної інфраструктури, охорону велелюдних заходів тощо. Загалом MASA Synergy застосовується для підготовки персоналу кризових підрозділів, а також осіб, які приймають рішення. Система дозволяє оптимізувати процеси планування ресурсів, перевіряти ефективність планів на випадок надзвичайних ситуацій, а також оцінювати характер впливу катастроф на населення, майно та інфраструктуру.

Центри обміну та аналізу інформації (англ. «Information Sharing and Analysis Centres», абревіатура – ISAC) є об'єднаннями представників зацікавлених сторін з метою здійснення обміну інформацією про загрози та інциденти кібербезпеки в окремих галузях діяльності.

Одним з таких інститутів є заснований в ЄС у 2015 році Європейський центр обміну та аналізу інформації в сфері енергетики (англ. «The European Energy Information Sharing and Analysis Centre», абревіатура – EE-ISAC). Головними завданнями EE-ISAC є секторальні дослідження вздовж всього ланцюжка створення доданої вартості в енергетиці, розширення складу

членів мережі через залучення зацікавлених сторін енергетичного сектора, проактивна та заснована на довірі система обміну інформацією, підвищення організаційної стійкості та готовності членів мережі [5].

З моменту свого створення і до сьогодні EE-ISAC перетворився на міжнародну галузеву мережу взаємної довіри в сфері обміну інформацією, став кібербезпековою платформою, яка об'єднує зацікавлених представників енергетичного сектору у процесі обміну даними про загрози, вразливі елементи, інциденти та можливі рішення у випадку настання порушень безпеки енергетичних систем [5]. В межах мережі EE-ISAC державні органи, комунальні підприємства (постачальники енергії, оператори транспортування та розподільники), охоронні організації, академічні установи, а також спеціалізовані громадські організації обмінюються між собою цінною інформацією про стан кібербезпеки та кіберстійкості в енергетичному секторі країн-учасниць платформи [12]. Обмін інформацією відбувається як під час фізичних зустрічей, так і за допомогою електронних засобів комунікації, включно зі спеціальною системою обміну інформацією. Наразі, система дозволяє обробляти лише вторинну інформацію, тобто таку, яка вже пройшла попередню обробку на національному рівні з відповідних первинних локальних першоджерел. Проте, наразі головним пріоритетом розвитку кіберплатформи є її інтеграція з платформою аналізу загроз, яка дозволить її учасникам отримувати первинну інформацію безпосередньо з місця інциденту, що призведе до більшої ситуаційної обізнаності в режимі реального часу та значно підвищить ефективність і своєчасність прийняття управлінських та адміністративних рішень для реагування на такі інциденти.

Проект EFFECTOR (повна назва англ. «An End to end Interoperability Framework For MaritimE Situational Awareness at StrategiC and TacTical OpeRations») отримав фінансування у розмірі 5 млн євро на 18 місяців у жовтні 2020 року від програми ЄС з досліджень та інновацій «Горизонт 2020» за тематичним пріоритетом «Демонстрація прикладних рішень для посилення прикордонної та зовнішньої безпеки» з підтемою «Нові концепції

підтримки прийняття рішень та інформаційних систем». Реалізація проекту здійснювалася консорціумом із 16 партнерів, що включав великі (NAVAL, THALES, ENG, CLS) та малі компанії (SATWAYS), дослідні організації (KEMEA, ICCS, INOV, IRIT), кінцеві користувачі, якими є державні органи країн-учасниць (Secreteriat General de la Mer; Hellenic Ministry of Maritime Affairs & Insular policy; Hellenic Police; Portuguese Navy; Bulgarian Executive Agency for Maritime Administration; Hellenic Ministry of Defense; Administration for Maritime Safety and Port Management of Montenegro).

Головною метою проекту EFFECTOR є розробка міжнародної системи морського спостереження та безпеки кордонів, що забезпечує моніторинг подій у морі, об'єднання та аналіз даних, а також підтримку прийняття рішень. Крім того, EFFECTOR забезпечує комунікацію та обмін інформацією між керівними органами країн-учасниць проекту на місці подій. Важливим технічним завданням в межах проекту є розробка структури сумісності національних систем моніторингу морської зони, а також надання пов'язаних з нею аналітичних послуг морського спостереження та безпеки кордонів. Складна система проекту включає цілу низку елементів, а саме:

- багаторівневе озеро даних і спільне середовище обміну інформацією для місцевих, регіональних і національних координаційних центрів;
- підсистема об'єднання і аналізу даних для надання послуг ситуаційної обізнаності;
- підсистема гармонізації даних для повної інтеграції систем морського та прикордонного спостереження, датчиків, платформ і джерел даних;
- підсистема звітності;
- підсистема морської семантики;
- підсистема інтеграції з європейськими мережами CISE та EUROSUR для транснаціонального обміну інформацією;
- безпекова підсистема.

Серед основних завдань проекту EFFECTOR варто визначити:

- впровадження багаторівневої платформи «озера даних» для наскрізної взаємодії та використання даних, що сприятиме інтеграції національних систем морського спостереження та взаємодії інформаційних систем на тактичному та стратегічному рівнях;
- здійснення обміну даними про ситуацію на місцевому, регіональному та національному рівнях з наднаціональним Спільним середовищем обміну інформацією в ЄС (CISE) та з Європейською системою нагляду за кордонами (EUROSUR);
- упровадження системи гармонізації даних та розроблення стандартів сумісності даних в середовищі морського спостереження;
- розроблення нових інструментів отримання знань, об'єднання даних, їх семантичного представлення та аналізу;
- перевірка прикладних рішень національними морськими органами, кінцевими користувачами та практиками;
- забезпечення повної відповідності діючій нормативно-правовій базі щодо захисту персональних даних та конфіденційності.

Багаторівневе озеро даних і спільне середовище обміну даними для місцевих, регіональних і національних координаційних центрів в межах проекту EFFECTOR було розгорнуто національних координаційних центрах трьох морських країн ЄС – Франції, Португалії та Греції. Воно підтримує національні та місцеві системи спостереження і складається з кількох взаємопов'язаних технологій з відкритим вихідним кодом великих даних, що забезпечує можливості отримання, перетворення та завантаження даних (Extract, Transform and Load – ETL) з метою:

- отримання, очищення та агрегування неоднорідних даних, зберігання необроблених даних та метаданих;
- забезпечення підтримки більшості існуючих стандартів обміну інформацією у таких сферах, як керування інцидентами, відстеження цілей, планування місій, розвідувальні рейди тощо;

- використання великих даних за допомогою останніх досягнень IT платформ в сфері агрегації великих даних, їх обробки, зберігання та розповсюдження;
- підвищення ефективності прийняття рішень шляхом ідентифікації контекстної інформації, багаторівневого злиття даних та їх семантичної аналітичної обробки.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі. У світовій практиці як на рівні окремих країн світу так і в міжнародному управлінні ситуаційні центри відіграють одну з ключових ролей як осередка оперативного реагування органів влади на кризові виклики. Головною метою їх створення є забезпечення безпеки функціонування країни та/чи міжнародної діяльності в усіх її аспектах, концентруючись на протидії ризикам, пов'язаним як з діяльністю окремих осіб чи їх груп, так і з можливими надзвичайними ситуаціями, спричиненими природними явищами. Зокрема, в світовій практиці мережі ситуаційних центрів створюються для протидії військовим внутнішньодержавним чи міждержавним конфліктам, політичним кризам, кіберзагрозам, пандемічним ситуаціям у випадку поширення хвороб, стихійним лихам, техногенним катастрофам терористичним злочинам, загрозам стратегічної інфраструктури (зокрема, енергетичної, сільськогосподарської та ін.).

Діяльність ситуаційних центрів може передбачати їх спеціалізацію на окремих напрямках чи сферах, або охоплювати широке коли проблем, вирішення яких покладається на спеціально створену мережу. Прийняття рішень при цьому здійснюється на основі постійного моніторингу та збору ситуаційної інформації, яка обробляється спеціальними системами ситуаційного управління. Системи ситуаційного моделювання дозволяють оптимізувати процеси планування, покращити дієвість планів в умовах надзвичайних ситуацій, оцінювати характер впливу катастроф на населення, майно та інфраструктуру.

Організація діяльності мережі ситуаційних центрів потребує широкого ресурсного забезпечення, яке охоплює широке коло матеріальних засобів (приміщення, обладнання) та відповідно підготовлений кваліфікований персонал. Зокрема, ключова увага в світовій практиці приділяється матеріально-технічним засобами високого рівня технологічної спроможності (новітні ІКТ-технології), які б дозволяли максимально швидко відстежувати ситуацію, збирати інформацію та приймати оперативні рішення. Водночас, невід'ємним ресурсним елементом для обґрунтування рішень є достатня та прийнятна база програмного забезпечення, яка дозволяє здійснювати моделювання проблемної ситуації, прогнозувати її наслідки та передбачати можливі варіанти її розвитку з використанням кількісної та якісної інформації.

Подальші дослідження діяльності ситуаційних центрів повинні спрямовуватись на обґрунтування шляхів адаптації та узгодження світового досвіду із вітчизняною практикою в контексті пошуку оптимальних організаційних, фінансово-економічних механізмів їх функціонування, а також на розробку сучасних цифрових інструментів, які б забезпечували оперативну взаємодію органів державної влади та ефективну розробку і реалізацію ними управлінських рішень щодо управління кризовими ситуаціями.

Література

1. A.I. for training military and civilian decision makers. URL: https://masasim.com/en/ (дата звернення: 15.09.2022)

2. Amanowicz M. A Shared cybersecurity awareness Platform. *Journal of telecommunications and informational technology. 2021. N3. Pp. 32-41. DOI:* https://doi.org/10.26636/jtit.2021.154421

3. Dragos V. Semantic frameworks to enhance situation awareness for defence and security applications. Information Retrieval. Université de

Paris, 2021. 100 p. URL: https://hal.archives-ouvertes.fr/tel-03347626/document (дата звернення: 15.09.2022)

4. Endsley M. R. Toward a theory of situation awareness in dynamic systems. Human Factors: *The Journal of the Human Factors and Ergonomics Society*. 1995. Volume 37, Issue 1. DOI: https://doi.org/10.1518/001872095779049543

5. European energy information sharing & analysis centre. URL: https://www.ee-isac.eu/ (дата звернення: 15.09.2022)

6. Information Sharing and Analysis Centers (ISACs). URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing (дата звернення: 15.09.2022)

7. Knieser L. The case for a situational awareness network for emergency response. 2020. URL: https://www.healthitanswers.net/the-case-for-a-situational-awareness-network-for-emergency-response/ (дата звернення: 15.09.2022)

8. Pavlov N. Concept development and experimentation for EU conflict prevention and peace-building (CDE4PEACE). D4.1 Catalogue of available and emerging CD&E tools in the European Union. Vienna: SYNYO GmbH, 2021. URL: https://www.cde4peace.eu/wp-content/uploads/sites/41/2021/07/CDE4Peace-D4.1-Catalogue-of-available-and-emerging-CDE-tools-in-the-EU-1.0.pdf (дата звернення: 15.09.2022)

9. Situation centers. RCI-Consulting Solutions. URL: https://rci-c.com/en/technology/sytuatsijni-tsentry/ (дата звернення: 31.03.2022)

10. Situation Centre (SITCEN). URL: https://www.nato.int/cps/en/natohq/topics_57954.htm (дата звернення: 31.03.2022)

11. Van Baelen S., Peeters G., Bruyninckx H., Pilozzi P. Slaets P. Dynamic semantic world models and increased situational awareness for highly automated inland waterway transport. *Frontiers in Robotics and AI.* 2022. Vol. 8. Pp. 1-26. DOI: 10.3389/frobt.2021.739062

12. Wallis T., Leszczyna R. EE-ISAC□Practical cybersecurity solution for the energy sector. *Energies*. 2022. 15. 2170. DOI: https://doi.org/10.3390/en15062170

13. Вишневський В.В. Мережа ситуаційних центрів органів державної влади України. Організаційні аспекти. URL: https://niss.gov.ua/sites/default/files/2014-05/0515_prez2.pdf

14. Головний ситуаційний центр України функціонує в штатному режимі. URL: https://www.rnbo.gov.ua/ua/Diialnist/3278.html (дата звернення: 15.09.2022)

15. Горбік В. Війна за стандартами НАТО. Як працюють сучасні технології, ситуаційні центри та мережево-центричність на війні в Україні. *Dev Україна.* 2022. URL: https://dev.ua/news/sytuatsiini-tsentry-ta-merezhe-tsentrychnist (дата звернення: 15.09.2022)

16. Морозов А.О., Кузьменко Г.Є. Шлях від АСУП до ситуаційних центрів. *Математичні машини і системи.* 2008. № 3. С82-107.

17. Тютюник В.В., Ященко О.А., Рубан І.В., Тютюник О.О., Особливості функціонування системи ситуаційних центрів на різних стадіях розвитку надзвичайних ситуацій. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2022. Том 43 № 1. С. 41-52. DOI:10.33099/2311-7249/2022-43-1-41-52

References

1. MASA (2022), “A.I. for training military and civilian decision makers”, available at: https://masasim.com/en/ (Accessed: 15.09.2022)

2. Amanowicz, M. A (2021), “Shared cybersecurity awareness Platform”, Journal of telecommunications and informational technology, vol. 3, Pp. 32-41. DOI: https://doi.org/10.26636/jtit.2021.154421

3. Dragos, V. (2021), Semantic frameworks to enhance situation awareness for defence and security applications. Information Retrieval.

Université de Paris, available at: https://hal.archives-ouvertes.fr/tel-03347626/document (Accessed: 15.09.2022)

4. Endsley, M. R. (1995), "Toward a theory of situation awareness in dynamic systems", Human Factors: The Journal of the Human Factors and Ergonomics Society, Vol. 37, Is. 1. https://doi.org/10.1518/001872095779049543

5. EE-ISAC (2022), "European energy information sharing & analysis centre", available at: https://www.ee-isac.eu/ (Accessed: 15.09.2022)

6. ISACs (2022), "Information Sharing and Analysis Centers", available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing (Accessed: 15.09.2022)

7. Knieser, L. (2020), "The case for a situational awareness network for emergency response", available at: https://www.healthitanswers.net/the-case-for-a-situational-awareness-network-for-emergency-response/ (Accessed: 15.09.2022).

8. Pavlov, N. (2021), "Concept development and experimentation for EU conflict prevention and peace-building (CDE4PEACE). D4.1 Catalogue of available and emerging CD&E tools in the European Union", Vienna: SYNYO GmbH, available at: https://www.cde4peace.eu/wp-content/uploads/sites/41/2021/07/CDE4Peace-D4.1-Catalogue-of-available-and-emerging-CDE-tools-in-the-EU-1.0.pdf (Accessed: 15.09.2022).

9. RCI-Consulting (2022), "Situation centers", available at: https://rci-c.com/en/technology/sytuatsijni-tsentry/ (Accessed: 31.03.2022)

10. NATO (2022), "Situation Centre (SITCEN)", available at: https://www.nato.int/cps/en/natohq/topics_57954.htm (Accessed: 31.03.2022)

11. Van Baelen, S., Peeters, G., Bruyninckx, H., Pilozzi, P. and Slaets, P. (2022), "Dynamic semantic world models and increased situational

awareness for highly automated inland waterway transport", Frontiers in Robotics and AI, Vol. 8, Pp. 1-26. DOI: 10.3389/frobt.2021.739062

12. Wallis, T. and Leszczyna, R. (2022), "EE-ISAC−Practical Cybersecurity Solution for the Energy Sector", Energies, Vol. 15. 2170, available at: https://doi.org/10.3390/en15062170 (Accessed: 15.09.2022).

13. Vyshnevskyi, V.V. (2014) "Network of situational centers of state authorities of Ukraine. Organizational aspects", available at: https://niss.gov.ua/sites/default/files/2014-05/0515_prez2.pdf (Accessed: 15.09.2022).

14. PRESS service of the National Security Council of Ukraine (2019), "The Main Situation Center of Ukraine operates in regular mode", available at: https://www.rnbo.gov.ua/ua/Diialnist/3278.html (Accessed: 15.09.2022).

15. Horbik, V. (2022), "War by NATO standards. How modern technologies, situation centers and network-centricity work in the war in Ukraine", available at: https://dev.ua/news/sytuatsiini-tsentry-ta-merezhe-tsentrychnist (Accessed: 15.09.2022).

16. Morozov, A.O. and Kuzmenko, H.Ie. (2008), "The path from ASUP to situational centers", *Matematychni mashyny i systemy*, *Vol.* 3, Pp. 82-107.

17. Tyutyunyk, V.V., Yashchenko, O.A., Ruban, I.V. and Tyutyunyk, O.O. (2022), "Peculiarities of the functioning of the system of situational centers at different stages of the development of emergency situations", *Modern information technologies in the sphere of security and defense*, Vol. 43, no. 1, Pp. 41-52. DOI:10.33099/2311-7249/2022-43-1-41-52

Стаття надійшла до редакції 20.09.2022 р.