

УДК 35:004.05

Світлана Усик

ORCID iD: 0000-0001-7219-3727

E-mail: usicom@ukr.net

Анна Терент'єва

ORCID iD: 0000-0003-3881-5865

E-mail: teren_a@ukr.net

ГЕНЕЗА ЦЕНТРІВ СИТУАЦІЙНОГО УПРАВЛІННЯ В УМОВАХ НАДЗВИЧАЙНИХ СИТУАЦІЙ: ДОСВІД УКРАЇНИ І СВІТОВА ПРАКТИКА

[https://doi.org/10.33269/2618-0065-2022-2\(12\)-53-74](https://doi.org/10.33269/2618-0065-2022-2(12)-53-74)

Анотація. Трансформаційні процеси в Україні набувають ознак певної екстремальності протягом останнього десятиліття, корелюючись із загальносвітовими тенденціями глобального розвитку щодо зміщення безпекової парадигми від практики реагування на надзвичайні та кризові ситуації до запобігання їх виникненню в поєднанні з розвитком інформаційної складової цих процесів і широким застосуванням інформаційно-комунікаційних та цифрових технологій. Визначено, що метою інформаційної безпеки в умовах надзвичайних ситуацій є забезпечення безперервності управлінського процесу і захист інформації, необхідної та достатньої для прийняття управлінських рішень за умов надзвичайної ситуації, від навмисного втручання, а також системи та обладнання, призначені для використання, накопичення та передання цієї інформації. Можемо стверджувати, що за критеріями інформаційної безпеки найбільшого ураження в умовах несанкціонованого інформаційного втручання може зазнати система прийняття рішень з реагування на виникнення надзвичайної ситуації і ліквідації їх наслідків, система прогнозування, моніторингу й обробки інформації про потенційне виникнення надзвичайної ситуації. Відзначено, що вітчизняна практика реагування та запобігання кризам і кризовим явищам є фрагментарними діями навздогін, структурно й функціонально недосконалими і ресурсно витратними, що має ознаки відомчої роз'єднаності, інституційної слабкості, а також бюрократизованість і заполітизованість. Наголошено на позитивній практиці ефективного реагування на кризи та надзвичайні ситуації в діяльності ДСНС України внаслідок застосування методології кризового менеджменту на рівні держави з метою його імплементації в діяльність центральних органів виконавчої влади із удосконаленням їх координації та взаємодії. З огляду на інтеграцію нашої держави в загальноєвропейський безпековий простір як базову функцію ситуаційного центру управління в умовах надзвичайних ситуацій слід розглядати

безпосередню взаємодію з Координаційним центром реагування на надзвичайні ситуації ЄС.

Ключові слова: ситуаційне управління, центр, рішення, надзвичайна ситуація, цивільний захист, безпека.

Постановка проблеми. Можна стверджувати, що трансформаційні процеси в Україні набувають ознак певної екстремальності протягом останніх десяти років, що корелюються із загальносвітовими тенденціями глобального розвитку. Також відбувається зміщення безпекової парадигми від практики реагування на надзвичайні й кризові ситуації до запобігання їх виникненню. Відповідно вектор уваги зміщується на розвиток інформаційної складової технологій запобігання та більш широке застосування інформаційно-комунікаційних і цифрових технологій. Прикладом цього може слугувати сплеск процесів цифровізації в умовах поширення пандемії COVID-19 протягом 2020–2021 років.

З огляду на події новітнього періоду розвитку сучасного світу нині процеси виникнення й поширення надзвичайних ситуацій (далі – НС) не знають кордонів і здатні вражати одну чи декілька країн одночасно, без попередження. Досвід діяльності окремих держав та їх об'єднань беззаперечно доводить, що за таких умов найкраще виявляє себе узгоджена спільна реакція, продумана до найменших деталей і апробована на практиці, адже лише спільний підхід до підготовки, попередження чи ліквідації наслідків НС здатен не лише об'єднати набутий ними досвід функціонування й реагування в подібних випадках, а й може мінімізувати дублювання певних функцій щодо забезпечення й координації надання допомоги, максимально адаптувати її до потреб і запитів постраждалих територій.

Сьогодні відбувається запровадження інформаційно-комунікаційних та цифрових технологій і у сфері цивільного захисту та запобігання виникненню НС через удосконалення роботи оперативного-координаційних центрів і створення ситуаційних центрів управління в умовах НС, а також цифровізація всіх підрозділів служби цивільного захисту.

Управлінська діяльність у кризових ситуаціях і НС значно відрізняється від рутинної поведінки – перед управлінцями та їх підлеглими постають нові та невідомі задачі, змінюються звичні процедури, пріоритети і розподіл обов’язків. Дії за таких умов передбачають тісну співпрацю з різними установами і структурами, які не входять до звичного кола спілкування, у зв’язку з чим ключове значення надається ступеню готовності до дій за подібних обставин. Заздалегідь визначено коло обов’язків і розподіл відповідальності, оперативний обмін інформацією про НС та аналіз для ухвалення обґрунтованих управлінських рішень.

НС із комплексними наслідками, що поширюються на значні території та спричиняють людські втрати серед постраждалого населення, зумовлюють сучасні виклики для системи цивільного захисту та потребують адекватних організаційно-управлінських підходів щодо реагування і мінімізації їх наслідків, а також раціонального використання наявних ресурсів всіх видів в умовах швидкої зміни обстановки.

Нині серйозною проблемою організації ефективного управління за умов НС є реальне ускладнення або відсутність координації дій офіційних урядових, відомчих і неурядових органів управління, незважаючи на наявність низки підзаконних актів, що регламентують взаємодію та інформаційний обмін під час ліквідації наслідків НС.

Аналіз останніх досліджень і публікацій. Потреба дослідження інформаційного супроводу прийняття управлінських рішень під час НС зумовила проведення дослідження значного масиву інформації щодо проблем управління в умовах зі швидкою зміною обстановки, бачення аналізу оперативної інформації. Вивчення питань інформаційного забезпечення управлінських рішень покладалося на фахівців не лише управлінського спрямування, є значна кількість публікацій з проблем збирання, накопичення, оброблення та аналізування інформації в графічному й символічному поданні. Особливу увагу дослідники приділили питанням інформаційної безпеки, зокрема збереженню великих масивів даних і захисту від несанкціонованого доступу.

Важливим є розуміння самої інформаційної безпеки як

складної багатокомпонентної системи. Погоджуємося з думкою К. Соколова [1, с. 4], який розглядає систему інформаційної безпеки як складну розподілену ергатичну інформаційну систему зі статичною структурою із наявним об'єктивним конфліктом між статикою структури системи інформаційної безпеки і вимогою значної динаміки її функціонування за складних умов, розуміючи завдання щодо ефективного вирішення питань збирання, накопичення й обробки інформації та прогнозування як у разі невизначеності, так і значної надмірності інформації про поточну ситуацію.

З початку російсько-українського військового протистояння в 2014 р., як вважає М. Сунгуровський [2, с. 3], система національної безпеки України виявилася неготовою не лише запобігти, а й адекватно відреагувати на деструктивні процеси в оборонній, інформаційній, економічній, соціально-політичній сферах. Дослідником підкреслено, що запізнення щодо утворення міжвідомчих координаційних штабів було реакцією на проблеми, що вже існують, з досить низькою результативністю внаслідок втрати часу на організаційні процедури.

Застосування сучасних інформаційних і телекомунікаційних технологій (технології OLAP-аналізу та просторового аналізу засобами ГІС-технологій) для супроводу прийняття управлінських рішень та отримання своєчасної та адекватної інформації про наслідки НС та обстановку в зоні НС, як зазначає А. Терент'єва у роботі [3, с. 103], дасть можливість адекватно оцінювати обстановку, відстежувати і прогнозувати динаміку розвитку подій та оптимально використовувати наявні ресурси для реагування. Відповідно може значно ускладнити прийняття правильного управлінського рішення в умовах НС [3, с. 116] відсутність або викривлення інформації із зони НС через нехтування часового і людського фактору.

Інформаційно-аналітичне забезпечення органів публічної влади всебічно було досліджено Т. Ганцюк у роботі [4, с. 4], а також визначено вимоги до управлінської інформації з наголосом на тому, що діяльність центральних та місцевих органів виконавчої влади, виконавчих органів рад у цій сфері є гласною і відкритою, якщо інше не передбачено законом.

В. Котковський докладно дослідив функціональну структуру інформаційно-аналітичної системи органу публічної влади [5, с. 135] та виокремив підсистеми збору і подання інформації та аналізу й прогнозування, наголошуючи на адекватності та достовірності інформації для ухвалення управлінських рішень.

О. Барило в публікаціях [6, с. 392; 2, с. 78] дослідила процес прийняття органами державного управління обґрунтованого рішення щодо застосування сил і засобів цивільного захисту внаслідок удосконалення інформаційного забезпечення.

Незважаючи на численні дослідження проблем інформаційної безпеки та інформаційного супроводу, прийняття управлінських рішень функціонування ситуаційних центрів управління в умовах НС дослідники комплексно не висвітлювали в наукових працях.

Мета статті полягає у дослідженні підтримки прийняття та формування рішень щодо попередження, реагування та ліквідації наслідків НС техногенного, природного та соціального характеру, а зокрема генези ситуаційних центрів управління за складних умов у разі швидкоплинної зміни обстановки.

Методи дослідження. З метою реалізації визначеної мети використано комплекс загальнонаукових і спеціальних методів дослідження, зокрема: системний метод для дослідження підтримки прийняття та формування рішень щодо попередження, реагування та ліквідації наслідків НС; метод аналізу застосовується на всіх етапах дослідження з метою комплексного вивчення порушеного питання; метод узагальнення та аналогії – на всіх етапах дослідження під час зіставлення теорії та практики з урахуванням практичного досвіду європейських країн.

Виклад основного матеріалу. За своїм характером і природою походження НС мають досить невисокий ступінь передбачуваності: до моменту отримання інформації, достатньої для опрацювання ефективних дій у відповідь, утворюється дефіцит часу для їх реалізації. Це призводить до очевидного парадоксу за умов НС: очікуючи отримання

достовірної і достатньої для прийняття рішень інформації, система несе збитки від непередбачуваних змін, а маючи невизначену інформацію, не може вживати продумані заходи з метою вирішення проблем, що виникають. Тому на ранніх стадіях потенційної небезпеки НС дії у відповідь повинні бути загального характеру, спрямовані на збільшення стратегічної гнучкості організації. У міру надходження деталізованої інформації повинні бути конкретизовані дії у відповідь, кінцевою метою яких є або усунення загрози НС або використання можливостей для ліквідації НС та її наслідків. Завчасне накопичення запасу гнучкості та адаптивності системи дає змогу зменшити небезпеку катастрофічних втрат на ранніх стадіях виникнення НС. Зауважимо, що невизначена на перших етапах інформація про можливості виникнення НС та альтернативи її розвитку може бути корисною і змістовною. Відповідно заходи інформаційної безпеки не обмежуються безпекою технічних інформаційних систем чи безпекою інформації у чисельному чи електронному вигляді, а стосуються усіх аспектів захисту даних чи інформації незалежно від форми, у якій вони перебувають.

Важливо розуміти, що мета інформаційної безпеки в умовах НС – забезпечення безперервності управлінського процесу і захист інформації, необхідної та достатньої для прийняття управлінських рішень за умов НС, від навмисного втручання, а також, зокрема, системи та обладнання, призначених для використання, заощадження та передання цієї інформації. Тобто це набір технологій, стандартів і методів управління, які необхідні для захисту інформаційної безпеки.

Грунтуючись на аналізі досліджень [2; 4–6] можемо стверджувати, що за критеріями інформаційної безпеки найбільшого ураження в умовах несанкціонованого інформаційного втручання може зазнати система прийняття рішень з реагування на виникнення НС і ліквідації їх наслідків, система прогнозування, моніторингу й обробки інформації про потенційне виникнення НС.

Важливо розуміти, що приховування, затримка надходження, перекручування та зниження актуальних даних, несанкціонований доступ до них окремих осіб чи груп осіб

можуть призвести як до людських жертв, так і до виникнення різних ускладнень під час ліквідації наслідків НС, пов'язаних з особливостями інформаційного впливу за цих умов. Критичним несанкціоноване інформаційне втручання може бути в умовах, якщо є ознаки паніки чи психоемоційного стресу під час переміщення значних людських контингентів та випадки поширення чуток і неправдивої інформації про перебіг НС і процес ліквідації її наслідків.

Швидкість, з якою загострюється соціально-політична ситуація, що склалася на Сході України, та масштаби можливих негативних наслідків потребують створення нових, адекватних рівню загроз, нормативно-правових та організаційних механізмів підтримки прийняття та формування рішень щодо попередження, реагування та ліквідації наслідків НС техногенного, природного та соціального характеру. Вочевидь напружена воєнно-політична ситуація, в якій нині Українська держава відстоює свою цілісність, тільки загострила необхідність створення спеціалізованої організаційної структури в системі забезпечення національної безпеки – Ситуаційного центру, із завданням забезпечення підтримки прийняття рішень щодо здійснення заходів на всіх етапах управління надзвичайними ситуаціями.

Згідно з Указом Президента України від 28.02.2015 № 115 «Про рішення Ради національної безпеки і оборони України від 25 січня 2015 року «Про створення та забезпечення діяльності Головного ситуаційного центру України» було створено Головний ситуаційний центр (ГСЦ) при Раді національної безпеки і оборони (РНБО) у форматі програмно-апаратного комплексу зі збору, накопичення і обробки інформації, необхідної для підготовки та прийняття рішень у сфері національної безпеки і оборони, супроводження діяльності РНБО з координації та контролю за діяльністю органів виконавчої влади, правоохоронних органів і військових формувань. За надання інформації до ГСЦ були визначені відповідальними Міністерство оборони України, МВС України, МЗС України, Державна фіскальна служба України, Державна служба України з надзвичайних ситуацій, Адміністрація Державної прикордонної служби України, Державне космічне

агентство України, Служба безпеки України, розвідувальні органи.

Про створення Ситуаційного центру при Президентові України було проголошено в 1992 р., був затверджений склад науково-технічної ради з його створення та схвалена Концепція відповідним розпорядженням Президента України від 14.07.1992 № 128/92-рп. На той час Ситуаційний центр при Президентові України бачили як багаторівневу ієрархічну систему, «яка поєднує людський інтелект, інформаційні технології, сучасні програмно-технічні засоби і засоби моделювання в процесі прийняття Президентом України рішень стосовно комплексних проблем в усіх сферах державної діяльності з метою захисту національних інтересів і забезпечення національної безпеки». По своїй суті Концепція зазначеного центру була продуктом вітчизняної школи кібернетики, вбачала залучення її найкращих досягнень. Проте донині весь потенціал вітчизняної наукової школи залишається на цьому напрямі нереалізованим.

У період 1994–1996 рр. функції замовника Ситуаційного центру були покладені на Секретаріат Ради національної безпеки при Президентові України [8].

З метою підготовки України до набуття членства в НАТО у річній національній програмі на 2010 рік, затвердженій Указом Президента України від 03.02.2010 № 92 [9], було обґрунтовано створення Ситуаційного центру РНБО України. Необхідність оперативного реагування на загрози національній безпеці шляхом швидкого формування обґрунтованих рішень на найвищому рівні державного управління було підтверджене рішенням про створення Інформаційно-аналітичного центру – робочого органу РНБО України [10], завдання якого пов'язані із забезпеченням інформаційної безпеки нашої держави.

На початку 2015 року розпочав функціонувати Головний ситуаційний центр (далі – ГСЦ) при РНБО України, оснащений відповідно до кращих аналогічних центрів провідних країн світу інформаційно-комп'ютерним обладнанням, що дає змогу обробляти величезні масиви інформації, яка надходить з усіх державних і недержавних баз даних, а також із супутників та безпосередньо з місць подій. Прикладом роботи цього центру є

інформаційне забезпечення управлінських рішень протягом 2020–2022 рр. стосовно реагування на пандемію COVID-19 щодо готовності медичних закладів, загальної кількості ліжок-місць у них для хворих на цю хворобу та їх заповнення тощо.

Оснащений ГСЦ інформаційно-аналітичною системою «СОТА» (далі – ІАС «СОТА»), що працює з метою ефективної координації діяльності державних органів, використовує програмні засоби для Big Data Analytics, забезпечує зберігання, поєднання та аналіз даних з різних джерел задля підвищення достовірності, ефективного моніторингу стану національної безпеки більш ніж за 20 напрямками, серед яких соціальна, внутрішня та зовнішньополітична безпека, поширення захворюваності на небезпечні інфекційні хвороби у світі та в Україні, просторова та функціональна трансформації, самоврядування у контексті децентралізації, місцеві бюджети та спроможність громад, користування надрами, економічна безпека, фінансові ринки, загрози на внутрішніх та зовнішніх ринках тощо.

У системі відбувається повна синхронізація всього масиву інформації із зовнішніх джерел із геопросторовими даними. За своїми параметрами ІАС «СОТА» є складною багатовартовою інформаційно-аналітичною системою найвищого рівня захисту інформації з гнучкою відкритою архітектурою з можливістю агрегувати нові функціональні модулі відповідно до завдань і викликів, що виникають у сфері національної безпеки, з трьома рівнями обробки інформації: загальнодоступний, для службового користування та таємний. Атестатом відповідності на комплексну систему захисту інформації, виданим за результатами державної експертизи, підтверджено безпеку обробки даних у системі. Наразі триває виконання рішень Указу Президента України від 18.06.2021 № 260 щодо імплементації програмного забезпечення ІАС «СОТА» у єдину мережу ситуаційних центрів держави задля удосконалення мережі ситуаційних центрів та цифрової трансформації сфери національної безпеки і оборони.

Необхідно зауважити, що в Україні функціонують постійно діючі органи, що виконують функції, характерні для

ситуаційних центрів в окремих галузях забезпечення національної безпеки і оборони. Такими є Антитерористичний центр при Службі безпеки України, що здійснює координацію діяльності суб'єктів боротьби з тероризмом щодо запобігання, попередження та припинення терористичних актів (у тому числі на об'єктах підвищеної небезпеки) [11], а також Ситуаційний центр Головного командного центру Збройних Сил України (далі – ГКЦ ЗСУ), до функцій якого належать, зокрема, здійснення аналізу та узагальнення інформації про НС, організація накопичення інформації про потенційно небезпечні об'єкти Міністерства оборони України.

Принагідно варто згадати наказ Міністра оборони України щодо утворення робочої групи для організації виконання заходів зі створення Ситуаційного центру МО України, що мало підвищити ефективність системи управління силами та засобами Збройних сил України під час виконання заходів Міністерства оборони з антитерористичного забезпечення Євро-2012 [12].

Ще один проєкт створення ситуаційного центру стратегічного рівня був розроблений в 2012 р. у Державному космічному агентстві України. Він передбачає створення Інформаційно-аналітичного (ситуаційного) центру при Кабінеті Міністрів України з використанням космічних технологій. Такий центр мав би стати основою урядової інформаційно-аналітичної системи для підтримки прийняття рішень із використанням геопросторових інформаційних технологій та дистанційного зондування Землі. Потрібно також зауважити, що питання про створення ситуаційних центрів не залишилося поза увагою і в Стратегії розвитку інформаційного суспільства в Україні [13], де в пункті про розвиток інформаційної інфраструктури підкреслюється необхідність залучення до виконання цього завдання українських виробників та врахування результатів вітчизняних наукових досліджень.

Окремо потрібно відзначити Урядову інформаційно-аналітичну систему з питань НС (далі – УІАСНС). В 1996 р. була ухвалена Програма її створення [14], а через три роки вона була затверджена на період 2000–2002 рр. [15], тобто передбачалось створення Кризового центру у складі Центру

інформаційних ресурсів у Кабінеті Міністрів України. В результаті для Управління експертизи та аналізу розвитку техногенної, екологічної, ядерної безпеки та природокористування Секретаріату Кабінету Міністрів України була створена Центральна підсистема УІАСНС. Безумовно, впровадження УІАСНС потребувало узгодження численних питань міжвідомчої взаємодії, тому, зважаючи на складність та важливість завдань щодо створення та функціонування УІАСНС, протягом 2001–2007 рр. працювала окрема координаційна рада з цих питань (під головуванням першого заступника Міністра НС і за участю представників Секретаріату Кабінету Міністрів України та низки центральних органів виконавчої влади) [16].

Хоча з моменту ухвалення першої програми створення УІАСНС пройшло багато років, процес створення цієї системи ще й досі не завершений. Про поступовий розвиток УІАСНС доповідалося в Національних доповідях про стан техногенної та природної безпеки в Україні (пункт «Інформаційне забезпечення» – п. 5.3 в 2004–2010 р.р. та п. 6.4 в 2011–2012 р.р.), але на сьогодні далеко не всі заплановані елементи цієї системи впроваджені у життя. Крім того, як свідчать дані ДСНС України (лист ДСНС від 13.02.2014 р. № 03-2024/162), в 2013 р. через брак фінансування не виконувалися заходи Загальнодержавної цільової програми захисту населення і територій від НС техногенного та природного характеру [17] щодо забезпечення функціонування та розвитку УІАСНС (п. 30 цільової Програми).

Не можна стверджувати, що функції, які зазвичай належать до ситуаційного центру, були упущені у процесі розгляду під час затвердження в 2012 р. Кодексу цивільного захисту України. На державний центр управління в НС, згаданий у ст. 73. п. 1 Кодексу цивільного захисту [18], покладені функції щодо здійснення «цілодобового чергування та забезпечення функціонування системи збору, оброблення, узагальнення та аналізу інформації про обстановку в районах надзвичайних ситуацій». Тобто передбачалося, що функціонування окремих підсистем єдиної державної системи запобігання і реагування на НС техногенного та природного

характеру мало здійснюватися із залученням відомчих структурних підрозділів, що виконують частину функцій, притаманних ситуаційному центру.

Зауважимо, що вітчизняна практика реагування та запобігання кризам і кризовим явищам є фрагментарними діями навздогін, структурно й функціонально недосконалими і ресурсно витратними. Ця практика має ознаки відомчої роз'єднаності, інституційної слабкості, а також забюрократизованість і заполітизованість. Водночас дослідники [1–3] відзначають позитивну практику ефективного реагування на кризи і НС в діяльності ДСНС України. З метою підвищення ефективності кризового менеджменту на рівні держави необхідно його імплементувати в діяльність з реалізації і захисту національних інтересів, а саме – в діяльність центральних органів виконавчої влади із удосконаленням їх координації та взаємодії.

Наприклад, у структурі Держатомрегулювання функціонує Інформаційно-кризовий центр, який є ключовим елементом підсистеми «Безпека об'єктів ядерної енергетики», необхідність створення та підтримки функціонування окремих, в деяких випадках «корпоративних», ситуаційних центрів підтверджує досвід галузі ядерної енергетики. Так, НАЕК «Енергоатом» запроваджує нову систему радіаційного моніторингу РОДОС (RODOS – Real-time On-line Decision Support System), яка діє в ряді країн-членів ЄС, створює Центр прогнозування наслідків радіаційних аварій (містить у собі математичні моделі і бази даних для прогнозування й оцінки наслідків можливих радіаційних аварій, а також планування невідкладних і довгострокових контрзаходів з використанням даних систем радіаційного моніторингу), автоматичну метеорологічну станцію і обчислювальний центр у місті Нікополі, поблизу Запорізької АЕС.

Зважаючи на поступову інтеграцію нашої держави в загальноєвропейський безпековий простір, слід звернути увагу й на останні кроки, що здійснює ЄС та окремі країни-члени ЄС у сфері управління надзвичайними ситуаціями, і більш конкретно – на розвиток нормативних та організаційних основ функціонування ситуаційних центрів з питань надзвичайних

ситуацій. В грудні 2013 р. Європейська Комісія опублікувала офіційний документ щодо нових законодавчих актів, які «зміцнюють» загальноєвропейську політику в сфері управління НС [19], в якому вказується на те, що потрібні добре скоординовані дії країн-членів ЄС як під час реагування на НС, так і у разі підготовки до них та їх попередження.

Досягти цього намагаються через проведення більшої кількості навчань для персоналу служб цивільного захисту за межами їх територіального розміщення (міжнаціональні навчання), навчань аварійно-рятувальних служб, рятувально-пошукових служб, медичних служб (у тому числі мобільних госпіталів), а також обміну експертами та більш тісної взаємодії між службами цивільного захисту сусідніх країн в межах ЄС. Передбачається створення країнами-членами ЄС спільного «волонтерського пулу», доступного для негайного спільного реагування на НС (сили та засоби аварійно-рятувальних служб, окремі спеціалісти та експерти, прилади та устаткування, транспортні засоби тощо).

Особливу роль в організації спільного реагування на теренах ЄС відіграє Координаційний центр реагування на НС (Emergency Response Coordination Centre), який був відкритий в травні 2013 р., до функцій якого належать: неперервний (цілодобовий – 24/7) моніторинг ситуації щодо НС в усьому світі, надання інформації країнам-членам ЄС, управління реєстром сил та засобів реагування, які можуть бути розгорнуті негайно під час великомасштабної НС. У разі таких НС центр має підготувати план реагування із зазначенням необхідних сил та засобів, що рекомендується надавати кожній з країн-членів ЄС (остаточне рішення щодо надання допомоги та її розмірів залишається за країнами-членами ЄС). Крім того, зазначений центр виконує функції «кризової кімнати» для управління операціями з надання гуманітарної допомоги. В європейських країнах усвідомлення необхідності створення організаційних структур, що підтримують прийняття рішень в умовах НС різного походження, реалізується через здійснення конкретних кроків.

Наприклад, у Німеччині в 2002 р. на базі Федерального управління цивільного захисту та допомоги під час стихійних

лих (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe) був створений Спільний інформаційний та ситуаційний центр (Gemeinsames Melde- und Lagezentrum – GMLZ), до завдань якого належать: надання оперативної інформації (цілодобово) у разі настання великомасштабної НС, зокрема надання інформації для ЗМІ; формування та регулярне оновлення матеріалів щодо загальної ситуації із захисту населення від НС, які надаються федеральним міністерствам та органам влади земель; аналіз і прогнозування загроз та можливих наслідків, пов'язаних із НС, визначення необхідних розмірів ресурсів тощо; участь в управлінні спільними операціями з реагування на НС, що здійснюють країни-члени ЄС в рамках загальноєвропейського Механізму цивільного захисту.

Подібну увагу до цих питань демонструє і Швейцарія, де в структурі органу виконавчої влади (Federal Office for Civil Protection), що реалізує державну політику в сфері цивільного захисту, функціонує Національний центр з НС (National Emergency Operations Centre), який є федеральним центром експертної підтримки прийняття рішень під час НС. Цей центр може функціонувати як в режимі цілодобового моніторингу, так і в режимі мобілізації всіх ресурсів (як власник, так і залучення ресурсів інших відомств). До основних завдань центру належить координація заходів з реагування на НС, пов'язаних із радіоактивними матеріалами, аваріями на підприємствах хімічної промисловості, проривами дамб, масштабними надзвичайними ситуаціями природного характеру. Отже, до завдань такого центру належать: постійний моніторинг і комплексний аналіз наявних загроз; прогнозування їх динаміки й виявлення нових загроз; прогнозування кризових ситуацій і НС; координація дій залучених відомств у передкризових та кризових ситуаціях і НС; вироблення рішень щодо попередження, подолання та мінімізації наслідків кризових ситуацій та НС.

Зауважимо, що на сьогодні в системі забезпечення національної безпеки України немає дієвого механізму моніторингу та формування рішень щодо попередження можливих кризових ситуацій. Це питання залишилося невирішеним як в організаційному, так і в нормативно-

правовому аспектах. Так, на відміну від термінів «надзвичайний стан» та «надзвичайна ситуація», для яких у чинному законодавстві чітко прописані механізми введення режиму надзвичайного стану та оголошення НС (державного, регіонального чи місцевого рівнів), термін «кризова ситуація» визначений лише у вузькопрофільних нормативних документах (цивільна авіація, фінансовий ринок, фізичний захист ядерних матеріалів та установок тощо). Крім того, за винятком економічної та продовольчої безпеки, відсутні індикатори та їх порогові значення, за якими можна було б визначати перехід системи забезпечення національної безпеки у стан «кризової ситуації», чи наближення до нього за окремими складовими. Потрібно згадати, що в Україні на загальнонаціональному рівні створювалися системи моніторингу, які мали б забезпечувати органи державної влади даними щодо стану безпеки за окремими складовими національної безпеки, в тому числі для визначення подібних індикаторів та наближення до «кризової ситуації».

Зокрема, джерелом даних щодо стану навколишнього середовища могла б стати Державна система моніторингу довкілля (далі – ДСМД) [20] через інформаційно-аналітичний центр ДСМД або безпосередньо від суб'єктів цієї системи. Очевидно, що такий ситуаційний центр має стати основним отримувачем інформації, про яку йдеться в проєкті постанови Кабінету Міністрів України «Про затвердження Порядку функціонування системи моніторингу і прогнозування надзвичайних ситуацій» (підготовлений ДСНС, нині йдеться про територіальні складові цієї системи), а прогнозування НС має здійснюватися із врахуванням положень Концепції управління ризиками виникнення НС техногенного та природного характеру [21].

Відповідно до ст. 73 Кодексу цивільного захисту з метою забезпечення ефективного управління та координації дій органів управління і підрозділів ДСНС України, інших центральних і місцевих органів влади у разі загрози або виникнення небезпечних подій та НС функціонує державний центр управління в НС і на регіональному рівні функціонують центри управління в НС, що створюються для управління у

режимі повсякденного функціонування суб'єктами забезпечення цивільного захисту, координації дій органів управління та сил цивільного захисту, здійснення цілодобового чергування та забезпечення функціонування системи збору, оброблення, узагальнення та аналізу інформації про обстановку в районах НС у системі ДСНС України.

У разі виникнення НС до роботи центрів управління в НС залучаються представники заінтересованих органів державної влади, що безпосередньо взаємодіють із штабом з ліквідації наслідків НС у разі його утворення і забезпечують його роботу. Важливим є те, що розпорядження і вказівки керівника робіт з ліквідації наслідків НС для персоналу центрів управління в НС обов'язкові для виконання.

Ключовою ланкою системи управління є пункти управління (стаціонарні та пересувні) – спеціально обладнані та оснащені технічними засобами місця, з яких керівник робіт з ліквідації НС через штаб з ліквідації НС здійснює управління залученими силами і засобами. Стаціонарний пункт управління обладнується в приміщеннях будівель і споруд за місцем розташування органу управління для забезпечення функціонування підпорядкованих формувань у повсякденному режимі та організації заходів з ліквідації наслідків НС. Пересувний пункт управління – це спеціально обладнані транспортні засоби (тимчасові приміщення, намети), оснащені технічним обладнанням для забезпечення роботи органу управління в польових умовах безпосередньо у районі НС. Він розгортається на відстані, яка забезпечує безперерйне управління залученими силами і може обладнуватися в наметах, на спеціальних командно-штабних автомобілях, або інших транспортних засобах. На пункті управління розміщуються і працюють органи управління – члени спеціальної комісії з ліквідації наслідків НС, керівник робіт з ліквідації НС, чергові зміни штабу з ліквідації наслідків НС та пересувного вузла зв'язку.

Висновки та напрями подальших досліджень. Подолання напруженої воєнно-політичної ситуації, в умовах якої наша держава відстоює власну цілісність та суверенітет, потребує подальшого вдосконалення системи забезпечення

національної безпеки, зокрема підвищення ефективності механізмів формування та підтримки прийняття рішень у сфері попередження, реагування та ліквідації наслідків НС різного характеру (техногенного, природного та соціального). Розв'язання таких завдань потребує створення ситуаційного центру управління як постійно діючого органу в системі забезпечення національної безпеки, на який буде покладено виконання функцій як щоденного моніторингу ситуації в усіх сферах національної безпеки, так і забезпечення підтримки прийняття рішень у НС.

Аналіз здійснених в Україні кроків щодо створення ситуаційного центру стратегічного рівня з питань НС показує, що сформульовані ще в середині 1990-х років задачі донині залишаються повністю невирішеними. Попри певні досягнення у створенні окремих елементів відомчих ситуаційних центрів управління, досі не вирішено в достатній мірі (адекватній нинішньому безпековому середовищу) завдання моніторингу та формування обґрунтованих рішень щодо попередження загроз національній безпеці, інформаційної підтримки для формування аналітичних матеріалів та своєчасного донесення інформації про ситуацію на найвищий рівень державного управління.

З урахуванням практичного досвіду європейських країн, можна визначити такі режими роботи ситуаційного центру: моніторинг, планування, координація дій з реагування та мінімізації наслідків НС. Окремо слід відзначити те, що такий центр може виконувати функції ситуаційної кімнати для вищого керівництва держави в умовах надзвичайного стану. Також з огляду на поступову інтеграцію нашої держави в загальноєвропейський безпековий простір слід розглядати як майбутню функцію ситуаційного центру безпосередню взаємодію з Координаційним центром реагування на надзвичайні ситуації ЄС.

Список використаних джерел

1. Соколов К.О. Аналіз загальних підходів до синтезу систем інформаційної безпеки. *Збірник наукових праць Житомирського військового інституту* : електр. наук. фах. вид. 2018. URL : https://zvir.zt.ua/images /stories/ ZbirnikNP/30_08_18/3.pdf (дата звернення : 14.10.2021).
2. Сунгуровський М. Перспективи кризового менеджменту в Україні.

- Центр Разумкова* : вебсайт. 2017. URL : https://razumkov.org.ua/upload/14346989_94_file.pdf (дата звернення : 20.10.2020).
3. Терент'єва А. В. Управління надзвичайними ситуаціями : монографія. Київ : ІДУЦЗ, УНПЦ ЕМД та МК, 2009. 332 с.
 4. Ганцюк Т. Д. Інформаційне аналітичне забезпечення діяльності органів публічної влади в Україні : джерелознавчий аналіз дискурсійного поля. *Державне управління : удосконалення та розвиток* : електр. наук. фах. вид. 2018. № 8. URL : http://www.dy.nauka.com.ua/pdf/8_2018/102.pdf (дата звернення : 04.11.2020).
 5. Котковський В. Інформаційно-аналітичне забезпечення прийняття управлінських рішень у діяльності органів державної влади. *Теорія та практика державного управління* : зб. наук. пр. 2015. Вип. 4. С. 132–138.
 6. Барило О. Г. Зарубіжний досвід створення інформаційно-аналітичної системи цивільного захисту. *Вісник Національного університету цивільного захисту України. Серія : Державне управління*. 2017. Вип. 2. С. 387–395
 7. Барило О. Г. Інформація як складова системи державного управління у надзвичайних ситуаціях. *Інвестиції: практика та досвід* : міжнар. наук.-практ. журн. 2011. № 2. С. 76–78.
 8. Про Ситуаційний центр при Президентіві України : розпорядження Президента України від 10.12.1994 р. № 185/94-рп. Верховна Рада України : вебсайт. URL : <http://zakon.rada.gov.ua/laws/show/185/94-%D1%80%D0%BF> (дата звернення : 03.11.2021).
 9. Про затвердження Річної національної програми на 2010 рік з підготовки України до набуття членства в Організації Північноатлантичного договору : Указ Президента України від 03.02.2010 р. №92/2010. Офіційне інтернет-представництво : Президент України. URL : <http://www.president.gov.ua/documents/10395.html> (дата звернення : 13.10. 2021).
 10. Про Інформаційно-аналітичний центр : Указ Президента України від 12.04.2014 р. № 398. Верховна Рада України : вебсайт. URL : <https://zakon.rada.gov.ua/laws/show/398/2014#Text> (дата звернення : 26.10.2021).
 11. Про Положення про Антитерористичний центр та його координаційні групи при регіональних органах Служби безпеки України : Указ Президента України від 14.04.1999 р. № 379/99. Верховна Рада України : вебсайт. URL : <http://zakon2.rada.gov.ua/laws/show/379/99> (дата звернення : 22.06.2022).
 12. Про призначення робочої групи зі створення Ситуаційного центру Міністерства оборони України» : наказ Міністра оборони України від 20.01.2012 р. № 32. Міністерство оборони України : вебсайт. URL : <http://www.mil.gov.ua/index.php?lang=ua&part=news&sub=read&id=23058> (дата звернення : 22.06.2022).
 13. Про схвалення Стратегії розвитку інформаційного суспільства в Україні : розпорядження Кабінету Міністрів України від 15.05.2013 р. № 386-р. Верховна Рада України : вебсайт. URL : <http://zakon2.rada.gov.ua/laws/>

- show/386-2013-%D1%80 (дата звернення : 05.07.2022).
14. Про Програму створення Урядової інформаційно-аналітичної системи з питань надзвичайних ситуацій на 1996 рік : постанова Кабінету Міністрів України від 16.01.1996 р. № 96. Верховна Рада України : вебсайт. URL : <http://zakon1.rada.gov.ua/laws/show/96-96-п> (дата звернення : 22.06.2022).
 15. Про створення Урядової інформаційно-аналітичної системи з питань надзвичайних ситуацій : постанова Кабінету Міністрів України від 16.12.1999 р. № 2303. Верховна Рада України : вебсайт. URL : <http://zakon0.rada.gov.ua/laws/show/2303-99-%D0%BF> (дата звернення : 15.06.2022).
 16. Про утворення Координаційної ради із створення та функціонування Урядової інформаційно-аналітичної системи з надзвичайних ситуацій : постанова Кабінету Міністрів України від 07.03.2001 р. № 215. Верховна Рада України : вебсайт. URL : <http://zakon1.rada.gov.ua/laws/show/215-2001-%D0%BF> (дата звернення : 17.07.2022).
 17. Про Загальнодержавну цільову програму захисту населення і територій від надзвичайних ситуацій техногенного та природного характеру на 2013-2017 роки : Закон України від 07.06.2012 р. № 4909-VI. Верховна Рада України : вебсайт. URL : <http://zakon3.rada.gov.ua/laws/show/4909-17> (дата звернення: 29.06.2022).
 18. Кодекс цивільного захисту України : Закон України від 02.10.2012 р. № 5403-VI. Верховна Рада України : вебсайт. URL : <http://zakon1.rada.gov.ua/laws/show/5403-17> (дата звернення: 10.07.2022).
 19. New legislation to strengthen European policy on disaster management. European Commission - MEMO/13/1120. 10.12. 2013. *European Commission* : websait. URL : http://europa.eu /rapid/press-release_MEMO-13-1120_en.htm (last accessed : 10.04.2022).
 20. Про затвердження Положення про державну систему моніторингу довкілля : постанова Кабінету Міністрів України від 30.03.1998 р. № 391. Верховна Рада України : вебсайт. URL : <http://zakon1.rada.gov.ua/laws/show/391-98-п> (дата звернення : 23.06.2022).
 21. Про схвалення Концепції управління ризиками виникнення надзвичайних ситуацій техногенного та природного характеру : розпорядження Кабінету Міністрів України від 22.01.2014 р. № 37-р. Верховна Рада України : вебсайт. URL : <http://zakon2.rada.gov.ua/laws/show/37-2014-%D1%80#n8> (дата звернення : 30.06.2022).

References

1. Sokolov, K. O. (2018). Analiz zahalnykh pidkhodiv do syntezy system informatsiinoi bezpeky [Analysis of general approaches to the synthesis of information security systems]. *Zbirnyk naukovykh prats Zhytomyrskoho viiskovoho instytutu – Collection of scientific papers of the Zhytomyr Military Institute*. Retrieved from https://zvир.zt.ua/images/stories/ZbirnikNP/30_08_18/3.pdf [in Ukrainian].
2. Sunhurovskiy, M. (2017). *Perspektyvy kryzovoho menedzhmentu v Ukraini*

- [Perspectives of crisis management in Ukraine]. *Ofitsiyni sait Tsentrazumkova*. Retrieved from https://razumkov.org.ua/upload/1434698994_file.pdf [in Ukrainian].
3. Terentieva, A. V. (2009). *Upravlinnia nadzvychnymy sytuatsiamy [Emergency management]*. Kyiv: IPASCP, USPCEMADM [in Ukrainian].
 4. Hantsiuk, T. D. (2018). Informatsiine analitychne zabezpechennia diialnosti orhaniv publichnoi vlady v Ukraini: dzhereloznavchyi analiz dyskursiinoho polia [Informational analytical support for the activities of public authorities in Ukraine: a source-based analysis of the discourse field]. *Derzhavne upravlinnya: udoskonalennya ta rozvytok*, 8. Retrieved from http://www.dy.nayka.com.ua/pdf/8_2018/102.pdf [in Ukrainian].
 5. Kotkovskiy, V. (2015). Informatsiino-analitchne zabezpechennia pryiniattia upravlinskykh rishen u diialnosti orhaniv derzhavnoi vlady [Informational and analytical support for management decision-making in the activities of state authorities]. *Teoriia ta praktyka derzhavnoho upravlinnia*, 4, 132–138 [in Ukrainian].
 6. Barylo, O. H. (2017). Zarubizhnyi dosvid stvorennya informatsiyno-analitchnoyi systemy tsyvilnoho zakhystu [Foreign experience of creating an information and analytical system of civil protection]. *Visnyk Natsionalnoho universytetu tsyvilnoho zakhystu Ukrainy. Seriya: Derzhavne upravlinnia*, 2, 387–395 [in Ukrainian].
 7. Barylo, O. H. (2011). Informatsiia yak skladova systemy derzhavnoho upravlinnia u nadzvychnykh sytuatsiakh [Information as a component of the state management system in emergencies]. *Investytsiyi: praktyka ta dosvid – Investments: practice and experience*, 2, 76–78 [in Ukrainian].
 8. Order of the President of Ukraine: About the Situation Center under the President of Ukraine from December 10 1994, № 185/94. Official site of the Verkhovna Rada of Ukraine. Retrieved from <http://zakon2.rada.gov.ua/laws/show/185/94-%D1%80%D0%BF> [in Ukrainian].
 9. Decree of the President of Ukraine: On the approval of the Annual National Program for 2010 to prepare Ukraine for membership in the North Atlantic Treaty Organization from February 3 2010, № 92/2010. Official online representation of the President of Ukraine. Retrieved from www.president.gov.ua/documents/10395.html [in Ukrainian].
 10. Decree of the President of Ukraine: About the Information and Analytical Center from April 12 2014, № 398. Official site of the Verkhovna Rada of Ukraine. Retrieved from [//zakon.rada.gov.ua/laws/show/398/2014#Text](http://zakon.rada.gov.ua/laws/show/398/2014#Text) [in Ukrainian].
 11. Decree of the President of Ukraine: On the Regulation on the Anti-Terrorist Center and its coordination groups under the regional bodies of the Security Service of Ukraine from April 14+ 1999, № 379/99. Retrieved from <https://zakon.rada.gov.ua/laws/show/379/99#Text> [in Ukrainian].
 12. Order of the Minister of Defense of Ukraine: On the appointment of a working group on the creation of the Situation Center of the Ministry of Defense of Ukraine from January 20 2012, № 32. Official site of the Verkhovna Rada of

- Ukraine. Retrieved from <http://www.mil.gov.ua/index.php?lang=ua&part=news&sub=read&id=23058> [in Ukrainian].
13. Order of the Cabinet of Ministers of Ukraine: On the approval of the Information Society Development Strategy in Ukraine from May 15 2013, № 386-р. Official site of the Verkhovna Rada of Ukraine. Retrieved from <http://zakon2.rada.gov.ua/laws/show/386-2013-%D1%80> [in Ukrainian].
 14. About the Program for the Creation of the Governmental Information and Analytical System on Emergency Situations for 1996: Resolution of the Cabinet of Ministers of Ukraine dated 16.01.1996, № 96. Official site of the Verkhovna Rada of Ukraine. Retrieved from <http://zakon1.rada.gov.ua/laws/show/96-96-п> [in Ukrainian].
 15. Resolution of the Cabinet of Ministers of Ukraine: On the creation of the Governmental Information and Analytical System on Emergencies from December 16 1999, № 2303. Official site of the Verkhovna Rada of Ukraine. Retrieved from <http://zakon0.rada.gov.ua/laws/show/2303-99-%D0%BF> [in Ukrainian].
 16. Resolution of the Cabinet of Ministers of Ukraine: On the formation of the Coordination Council for the creation and operation of the Governmental Information and Analytical System for Emergencies from March 7 2001, № 215. Official site of the Verkhovna Rada of Ukraine. Retrieved from <http://zakon1.rada.gov.ua/laws/show/215-2001-%D0%BF> [in Ukrainian].
 17. Law of Ukraine: On the National Targeted Program for the Protection of the Population and Territories from Man-made and Natural Emergencies for 2013-2017 from June 7 2012, № 4909-VI. Official site of the Verkhovna Rada of Ukraine. Retrieved from <http://zakon3.rada.gov.ua/laws/show/4909-17> [in Ukrainian].
 18. Code of Civil Protection of Ukraine from October 2 2012, № 5403-VI. Official site of the Verkhovna Rada of Ukraine. Retrieved from <http://zakon1.rada.gov.ua/laws/show/5403-17> (2020, July 24) [in Ukrainian].
 19. New legislation to strengthen European policy on disaster management. European Commission - MEMO/13/1120 10/12/2013. European Commission: websait. Retrieved from http://europa.eu/rapid/press-release_MEMO-13-1120_en.htm [in Ukrainian].
 20. Resolution of the Cabinet of Ministers of Ukraine: On the approval of the Regulation on the state environmental monitoring system from March 30 1998, № 391. Official site of the Verkhovna Rada of Ukraine. Retrieved from <http://zakon1.rada.gov.ua/laws/show/391-98-п> [in Ukrainian].
 21. Order of the Cabinet of Ministers of Ukraine: On the approval of the Concept of risk management of man-made and natural emergencies from January 22 2014, № 37-р. Official site of the Verkhovna Rada of Ukraine. Retrieved from <http://zakon2.rada.gov.ua/laws/show/37-2014-%D1%80#n8> [in Ukrainian].

GENESIS OF SITUATION MANAGEMENT CENTERS IN EMERGENCY CONDITIONS: EXPERIENCE OF UKRAINE AND GLOBAL PRACTICE

Svitlana Usyk, Anna Terentieva

Abstract. Transformational processes in Ukraine have acquired signs of a certain extremity during the last ten years, which are correlated with the global trends of global development with a shift in the security paradigm from the practice of responding to emergencies and crisis situations to preventing their occurrence in combination with the development of the information component of prevention technologies and the wide application of information, communication and digital technologies. It was determined that the purpose of information security in the conditions of an emergency is to ensure the continuity of the management process and the protection of information necessary and sufficient for making management decisions under emergency conditions from intentional interference, as well as including systems and equipment intended for use, saving and transfer of this information. We can say that according to the criteria of information security, the system of decision-making for responding to the occurrence of emergencies and the elimination of their consequences, the system of forecasting, monitoring and processing of information about the potential occurrence of an emergency can suffer the greatest damage in conditions of unauthorized information intervention. It was noted that the domestic practice of responding to and preventing emergencies and crisis phenomena is a fragmented, one-on-one, structurally and functionally imperfect and resource-consuming practice, which has signs of departmental disunity, institutional weakness, over-bureaucratization and politicization. We also note the positive practice of effective response to crises and emergencies in the activities of the State Emergency Service of Ukraine due to the application of the crisis management methodology at the state level with the aim of its implementation in the activities of central executive bodies with the improvement of their coordination and cooperation. Given the integration of our state into the pan-European security space as a base function of the situational control center in emergencies, direct interaction with the EU Emergency Response Coordination Center should be considered.

Keywords: situation management, center, decision, emergency, civil protection security.