УДК 321.015+321.02+323.21

КОНЦЕПТУАЛЬНІ ПІДХОДИ ДО РОЗРОБКИ СИСТЕМИ РАННЬОГО ПОПЕРЕДЖЕННЯ ЯК МЕХАНІЗМУ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ СТІЙКОСТІ

Ольга Резнікова
Національний інститут стратегічних досліджень
вул. Пирогова 7а, 01030, м. Київ, Україна

У статті досліджено принципи та особливості розробки системи раннього попередження як механізму забезпечення національної стійкості. Встановлено, що ефективними інструментами у роботі щодо виявлення загроз і визначення заходів реагування є створення єдиної мережі ситуаційних центрів, а також паспортів загроз. Визначено, що найбільш проблематичним питанням у роботі такої системи є ідентифікація і виявлення на ранньому етапі гібридних загроз, які мають прихований характер і проявляються не одразу.

Ключові слова: національна стійкість, національна безпека, загрози, безпекове середовище, сектор безпеки та оборони.

Запровадження механізмів забезпечення національної стійкості має на меті адаптування держави, її національних систем, політичних інститутів і населення до дії загроз руйнівного, постійного або динамічного і тривалого характеру, а також швидких і непередбачуваних змін безпекового середовища. Розробка таких механізмів повинна спиратися на чітке розуміння концепту стійкості (передусім, її критеріїв і принципів забезпечення), особливостей його запровадження у різних сферах національної безпеки, а також історичних, географічних, культурних, соціально-економічних та інших характеристик формування й розвитку держави [1].

У світі не існує універсальної моделі забезпечення національної стійкості. Країни використовують різні практики у цій сфері, а міжнародні організації, як і науковці, що спеціалізуються на цій тематиці, пропонують неоднакові рекомендації щодо розбудови національної стійкості. Це залежить, передусім, від основної сфери їх діяльності, досвіду тощо.

Найбільш характерною є розбіжність у поглядах щодо того, на що саме має бути орієнтована модель забезпечення національної стійкості – на залучення під час кризи механізмів, що дозволять пом'якшити вплив загрози та забезпечать безперервність життєво важливих функцій держави та суспільства на прийнятному у цей період рівні, *або* на швидке відновлення після кризи, виходячи з того, що більшість із загроз, із якими має справу система забезпечення національної стійкості, є неминучими й складно прогнозованими. На це, зокрема, звертає увагу Л. Франкар, характеризуючи особливості британської та французької моделей [2]. Крім того, зазначений автор акцентує, що забезпечення стійкості не є тотожним кризовому менеджменту, який є традиційним елементом державного управління. Скоріше, кризовий менеджмент слід розглядати як одним з механізмів, що дозволяють державним інститутам і суспільству протидіяти загрозам.

Інша дискусія стосується питання, як має бути організована система забезпечення національної стійкості – як окрема складова державного управління або шляхом удосконалення наявних систем і взаємозв'язків між ними. Автором цієї статті раніше було доведено, що немає потреби у розробці та запровадженні окремої системи забезпечення національної

стійкості, яка буде функціонувати паралельно з чинною системою забезпечення національної безпеки [3]. Більш доцільним є впровадження принципів стійкості при забезпеченні національної безпеки, а також формування механізмів забезпечення стійкості у комплексі із традиційними безпековими заходами. У такий спосіб буде забезпечено синергетичний ефект від взаємодії двох систем, а також доцільну економію ресурсів держави та суспільства.

Загалом механізми забезпечення національної стійкості, які застосовуються на практиці у різних країнах, можна розділити на дві основні групи. Ті з них, що відносяться до *першої групи,* мають на меті реагування на певні загрози національній безпеці (наприклад, стійкість держави та суспільства до терористичної загрози, до природних катастроф та інші), а *друга група* передбачає комплексне реагування на широкий спектр загроз (all hazards approach) на рівні певних суб'єктів (держави, громади, родини тощо).

Отже, наявність актуальних або потенційних загроз є визначальною умовою існування системи забезпечення національної стійкості. При цьому визначення ключових загроз національній безпеці, а також виявлення «слабких місць» системи забезпечення національної безпеки у контексті протидії їм сприятиме чіткому розумінню характеру механізмів забезпечення національної стійкості, яких потребує держава.

Проблема своєчасного виявлення, ідентифікації та оцінки загроз набуває все більшого значення в умовах розгортання гібридної агресії, оскільки гібридні загрози часто мають прихований характер або реалізуються через маніпулювання демократичними цінностями й правовими механізмами, що можна спостерігати на прикладі агресивної політики РФ щодо України.

Метою цієї статті є визначення принципів та особливостей формування системи раннього попередження як механізму забезпечення національної стійкості та розробка відповідних рекомендації для органів державної влади України.

Досліджуючи особливості ведення гібридної війни, у тому числі на прикладі Російської Федерації (далі – РФ), А. Рац виділив такі її основні операційні етапи: підготовка, атака, стабілізація. При цьому автор зазначає, що на першому етапі супротивник формує «мапу» стратегічних, політичних, економічних, соціальних, інфраструктурних слабкостей і вразливостей країни-жертви та створює необхідні механізми їх капіталізації з метою подальшого використання. На прикладі агресії РФ проти України А. Рац робить висновок, що на початковому етапі було практично неможливо визначити, чи були дії РФ, у тому числі у рамках традиційної дипломатії, застосування заходів м'якої сили, зовнішнього впливу тощо, підготовкою до гібридної війни, допоки не розпочалася активна фаза (атака). Основними операційними причинами ефективності гібридної агресії РФ проти України А. Рац називає такі: неочікуваність; відмова від визнання втручання на офіційному рівні; маскування загарбників під цивільне населення. Крім того, цьому сприяла тривала спільна історія двох держав, тісні економічні зв'язки, а також пов'язаність політичних, бізнесових і безпекових еліт [4].

Наведене підкреслює проблематичність виявлення, ідентифікації та оцінки загроз у сучасних умовах. Так, поширення спотвореної інформації, яка має на меті розгортання деструктивних процесів у суспільстві, може трактуватися агресором як забезпечення свободи слова і плюралізму думок. Організація міжнародних конференцій або інших публічних дискусійних майданчиків, на яких «науково обґрунтовується» нова історична ретроспектива країни-жертви та надаються пояснення певних політичних подій у вигідному для агресора ракурсі, може мати вигляд «поглиблення наукової та культурної співпраці» між країнами. Намагання безпосередньо впливати на громадську думку, поширюючи пропаганду агресора і виправдовуючи його, подається під гаслом свободи засоби масової

інформації (далі – ЗМІ). Як бачимо, для такої діяльності використовуються цілком легальні механізми, які спираються на традиційні демократичні цінності. А «зелені чоловічки», які з'явилися спочатку в Криму, а потім на Донбасі, довго залишилася предметом для дискусій у більшості країн світу – чи є це загрозою для національної та регіональної безпеки і як на неї реагувати?

В умовах гібридної війни складно не лише ідентифікувати ті або інші події або тенденції як загрозу, але й побачити за ними загальну картину, що може свідчити про підготовку супротивника до більш масштабних дій, переходу до активної фази. Адже гібридна війна характеризується одночасним масштабним скоординованим застосуванням комплексу заходів у різних сферах. Виявлення перших ознак гібридної агресії потребує певного часу і координації зусиль різних органів державної влади.

У цілому, функціонування системи раннього попередження відповідає основним принципам забезпечення національної стійкості, до яких, зокрема, відносяться такі: широка взаємодія, обізнаність, готовність, безперервність, комплексний підхід. Метою її є ідентифікація загроз і створення умов для пом'якшення їх негативного впливу на подальших етапах (під час і після кризи). Таким чином, можна стверджувати, що система раннього попередження є механізмом забезпечення національної стійкості.

Для розбудови системи раннього попередження необхідно чітко усвідомлювати, які процеси вона має охоплювати. Проаналізуємо їх у контексті реалізації принципів забезпечення стійкості.

Широка взаємодія і комплексний підхід. До компетенції різних органів державної влади відноситься своєчасне виявлення загроз у визначеній сфері відповідальності. Для цього використовуються організаційні, аналітичні, технічні, оперативні та інші спроможності відповідного органу. Ефективним інструментом у роботі щодо виявлення загроз і визначення заходів реагування є ситуаційні центри, які можуть утворюватися при міністерствах та відомствах.

За висновками Я.В. Чернятевич, ситуаційні центри покликані вирішувати такі основні завдання: передбачення кризових ситуацій, підготовка управлінських рішень щодо їх попередження (подолання), прогнозування розвитку ситуації, моніторинг ситуації за визначеними критеріями, проектування можливих сценаріїв розвитку ситуації та необхідних заходів реагування, оцінка можливостей щодо виконання управлінських рішень та інше. Для реалізації цих завдань ситуаційний центр має забезпечити виконання таких ключових функцій: збір інформації стосовно певної сфери діяльності; визначення критеріїв її оцінки; обробка даних з метою виявлення факторів впливу; побудова моделей аналізу; проектування управлінських рішень та їх реалізації; моніторинг і оцінка результатів реалізації рішень [5, с. 362–363].

Одним із важливих шляхів забезпечення взаємодії органів державної влади на етапі раннього попередження є створення єдиної мережі ситуаційних центрів, об'єднаної Головним ситуаційним центром.

В Україні рішення про створення та забезпечення діяльності Головного ситуаційного центру України було прийнято Радою національної безпеки та оборони України (далі – РНБОУ) 25 січня 2015 р. (введене у дію Указом Президента України від 28 лютого 2015 р. № 115/2015) на виконання Стратегії національної безпеки України, затвердженої Указом Президента України від 26 травня 2015 р. № 287/2015. Відповідно до прийнятого рішення Головний ситуаційний центр України має отримувати інформацію від Міністерства оборони України, Міністерства внутрішніх справ України, Міністерства закордонних справ України, Державної фіскальної служби України, Державної служби України з надзвичай-

них ситуацій, Адміністрації Державної прикордонної служби України, інших центральних органів виконавчої влади, Служби безпеки України, розвідувальних органів України з метою її накопичення та обробки для підготовки та прийняття рішень у сфері національної безпеки та оборони.

Наразі у відкритому доступі відсутня інформація щодо ефективності діяльності Головного ситуаційного центру України. Слід зазначити, що на етапі його створення відчувалися певні проблеми стосовно визначення критеріїв оцінки інформації, методів її аналітичної обробки і побудови моделей аналізу. На це, зокрема, звертає увагу В.В. Домарєв [6]. Значною мірою така ситуація обумовлена дещо некоректним правовим визначенням Головного ситуаційного центру України як «програмно-апаратного комплексу зі збору, накопичення та обробки інформації, необхідної для підготовки та прийняття рішень у сфері національної безпеки та оборони» [7]. При цьому фактично утворився розрив між забезпеченням технічної складової діяльності Головного ситуаційного центру України, яке покладене на Апарат РНБОУ, і аналітичним забезпеченням його діяльності, адже штат експертів, який мав би при цьому займатися аналізом інформації, її оцінками, прогнозуванням і моделюванням ситуацій, створено не було.

Іншою особливістю зазначеного рішення РНБОУ від 25 січня 2015 р. є те, що у ньому простежується комплексний підхід, притаманний забезпеченню національної стійкості, адже Головний ситуаційний центр України має забезпечити координацію діяльності органів державної влади на різних етапах: у мирний час, в особливий період, у тому числі в умовах військового стану, в умовах надзвичайного стану та при виникненні кризових ситуацій, що загрожують національній безпеці України [7]. Проте, з незрозумілих причин у цьому ланцюгу випущений важливий етап післякризового врегулювання.

Формування мережі ситуаційних центрів є важливим, але не єдиним елементом у системі раннього попередження. Принцип широкої взаємодії у забезпеченні національної стійкості передбачає також активне залучення на всіх етапах громадянського суспільства, а також створення постійно діючих двосторонніх каналів комунікацій.

У цьому контексті для України цікавим є досвід таких країн як Велика Британія – щодо функціонування мережі місцевих форумів стійкості та формування Національного реєстру загроз; США і Ізраїль – щодо залучення населення до протидії терористичній діяльності та формування суспільної стійкості до цієї загрози; Естонія – щодо ролі громадянського суспільства у виявленні та протидії загрозам в інформаційній та кібернетичній сферах тощо.

Ефективна взаємодія державних органів та громадянського суспільства на етапі раннього запобігання загроз національній безпеці потребує належної організації та координації, а також налагодження стійких двосторонніх каналів комунікацій. У світовій практиці таку функцію, як правило, виконує орган виконавчої влади або спеціально утворена у його складі служба. Так, у Великій Британії – це Офіс Кабінету Міністрів (Cabinet Office), у США – Федеральне агентство кризового регулювання у складі Міністерства внутрішньої безпеки (Department of Homeland Security (DHS) Federal Emergency Management Agency (FEMA)).

В Україні таку функцію може виконувати спеціальна служба у складі Апарату Ради національної безпеки та оборони України. Адже згідно зі статтею 3 Закону України «Про Раду національної безпеки та оборони України» РНБОУ здійснює координацію та контроль за діяльністю органів виконавчої влади у сфері національної безпеки та оборони у мирний час, а також в умовах воєнного або надзвичайного стану та при виникненні кризових ситуацій, що загрожують національній безпеці України [8]. Це виглядає цілком логічним ще

і з огляду на те, що Головний ситуаційний центр як важливий інструмент у системі стратегічного управління утворений саме Апаратом РНБОУ.

Відповідні повноваження Кабінету Міністрів України виглядають дещо звуженими. Так, відповідно до статті 2 Закону України «Про Кабінет Міністрів України» КМУ здійснює спрямування і координацію роботи міністерств, інших органів виконавчої влади та контроль за їх діяльністю [9]. Як відомо, не всі суб'єкти сектору безпеки та оборони є органами виконавчої влади. Отже, певна частина діяльності щодо раннього запобігання загрозам може залишитися не охопленою, якщо це не знайде належного правового врегулювання.

Обізнаність. При створенні системи раннього запобігання важливе значення має забезпечення єдиного для всіх розуміння природи загрози, її проявів, оцінок, рівня, який потребує негайного реагування. Розбіжності у поглядах різних органів державної влади та суспільства щодо зазначених питань можуть стати на перешкоді злагодженій діяльності стосовно запобігання і протидії загрозам, а також своєчасного застосування інших механізмів забезпечення національної стійкості.

Розвязання цієї проблеми потребує, зокрема, вжиття таких заходів: розробки єдиних методологічних засад щодо визначення актуальних загроз, ознак їх ідентифікації та методів оцінки; доведення такої інформації до всіх суб'єктів; виготовлення і поширення відповідних інформаційних, демонстраційних матеріалів; проведення роз'яснювальної роботи. До такої діяльності мають залучатися наукові установи, аналітичні центри.

На етапі раннього попередження найскладнішим є виявлення, ідентифікація та оцінка гібридних загроз. Як вже зазначалося, вони мають прихований характер, можуть виявлятися з часом, а чіткі критерії їх ідентифікації та оцінки відсутні. З огляду на це, важливе значення має рівень професійної підготовки й досвід експертів, які залучаються до аналітичної роботи з виявлення загроз.

На прикладі організації роботи ситуаційних центрів Я.В. Чернятевич зазначає, що чим точніше «інтуїція» аналітика вихоплює реальні, об'єктивні процеси, тим ефективнішими будуть його висновки та рекомендації, отримані за допомогою формальних (математичних) висновків [5, с. 363].

Для виявлення й ідентифікації загроз на ранньому етапі необхідно, перш за все, визначити основні сфери, щодо яких буде здійснюватися моніторинг ситуації. Зокрема, можна орієнтуватися на традиційні сфери забезпечення національної безпеки: воєнна, державна, громадська, зовнішньополітична, інформаційна, кібернетична, економічна, соціальна, екологічна, техногенна безпека. Далі доцільно визначити ймовірні загрози у кожній сфері, серед яких можуть бути такі: надзвичайні ситуації природного походження, надзвичайні ситуації техногенного характеру, поширення небезпечних хвороб, зовнішні впливи, розвідувально-підривна діяльність на території країни, тероризм, економічні кризи, дестабілізація політичної ситуації та інші.

По суті, для забезпечення ефективної діяльності системи раннього попередження спочатку доцільно розробити паспорти загроз, у яких мають бути визначені характерні події, явища, процеси, які дозволяють ідентифікувати загрозу (ранні сигнали), об'єкти загрози, фактори, що впливають на появу і розвиток кризової ситуації, джерело небезпеки, можливі наслідки для національної безпеки та інше [10].

Визначення сигналів раннього попередження є складним і достатньо творчим процесом, у ході якого мають використовуватися як традиційні методи аналізу, так і неформальні, такі як інтуїтивно-логічний, формально-логічний, операційно-прикладний, аналітико-прогностичний та інші методи.

У світовій практиці достатньо опрацьованими є, зокрема, ранні прояви терористичної, воєнної загрози, економічних криз, надзвичайних ситуацій природного походження. Подальшого дослідження потребують питання щодо виявлення і раннього попередження негативних зовнішніх впливів, ризиків виникнення конфліктів у суспільстві, інформаційних атак та інше.

Готовність. Система раннього попередження як механізм забезпечення національної стійкості може працювати ефективно лише у разі, якщо вже створені й функціонують інші необхідні механізми, які мають починати діяти, коли отримають від зазначеної системи сигнали про підвищення рівня загрози. Для цього завчасно мають бути розроблені альтернативні плани дій на випадок кризи, проведені навчання і тренування як для уповноважених органів державної влади, так і для населення щодо їх дій до, під час і після настання кризи.

Готовність самої системи раннього попередження забезпечується, зокрема, шляхом розвитку технічних спроможностей мережі ситуаційних центрів, періодичного підвищення кваліфікації експертів-аналітиків і технічного персоналу, наявності альтернативних методик обробки інформації, розробки сценарних прогнозів розвитку ситуації тощо.

Безперервність роботи системи раннього попередження забезпечується шляхом своєчасного запровадження комплексу заходів забезпечення кібербезпеки та захисту інформації у мережі ситуаційних центрів та в уповноважених органах державної влади, а також залучення достатньої кількості спеціалістів необхідної кваліфікації.

Крім того, враховуючи, що сучасні загрози мають складний і динамічний характер, засоби та методи обробки інформації у системі раннього попередження повинні періодично оновлюватися.

Підсумовуючи викладене, можна дійти таких висновків:

Система раннього попередження є ефективним механізмом ідентифікації загроз і створення умов для пом‘якшення їх негативного впливу на подальших етапах, що має використовуватися у комплексі з іншими необхідними механізмами забезпечення національної безпеки та стійкості. Її формування доцільно здійснювати на основі таких принципів, як широка взаємодія, обізнаність, готовність, безперервність, комплексний підхід. Ефективними інструментами у роботі щодо виявлення загроз і визначення заходів реагування є створення єдиної мережі ситуаційних центрів, а також паспортів загроз. Найбільш проблематичним питанням на даний час є ідентифікація і виявлення на ранньому етапі гібридних загроз, які мають прихований характер і проявляються не одразу.

Список використаної літератури

1. Резнікова О.О. Концептуальні підходи до вибору моделі забезпечення національної стійкості. *Стратегічні пріоритети*. 2019. № 1. С. 7–14.
2. Francart L. What does resilience really mean? URL: https://www.diploweb.com/What-does-resilience-really-mean.html (09.01.2019).
3. Резнікова О.О. Забезпечення національної безпеки і національної стійкості : спільні риси та відмінності. *Вісник Львівського університету. Серія «Філософсько-політологічні студії»*. 2018. № 19. С. 170–175.
4. Rácz A. Russia’s Hybrid War in Ukraine. *Breaking the Enemy’s Ability to Resist*. URL: https://stratcomcoe.org/andras-racz-russias-hybrid-war-ukraine-breaking-enemys-ability-resist (14.05.2019).
5. Государственное управление в сфере национальной безопасности : словарь-справочник / В.И. Абрамов и др. ; под общ. ред. Г.П. Сытника. Киев : НАДУ, 2012. 496 с.

6. Домарєв ВВ. Система ситуаційного управління : теорія, методологія, рекомендації. Київ : Знання України, 2017. 347 с.
7. Про створення та забезпечення діяльності Головного ситуаційного центру України : Рішення Ради національної безпеки і оборони України від 25 січня 2015 р. URL: https://zakon.rada.gov.ua/laws/show/n0002525-15 (дата звернення 14.05.2019)
8. Про Раду національної безпеки та оборони України : Закон України від 05 березня 1998 р. № 183/98–ВР. *Відомості Верховної Ради України*. 1998. № 35. Ст.237.
9. Про Кабінет Міністрів України : Закон України від 27 лютого 2014 р. № 794–VII. *Відомості Верховної Ради України*. 2014. № 13. Ст. 222.
10. Резнікова О.О. Паспорт сепаратистської загрози в Україні. *Стратегічні пріоритети*. 2018. № 2. С. 12–24.

CONCEPTUAL APPROACHES TO DEVELOP AN EARLY WARNING SIGNAL SYSTEM AS A MECHANISM FOR BUILDING NATIONAL RESILIENCE

Olha Reznikova
National Institute for Strategic Studies
Pyrogova Str., 7a, 01030, Kyiv, Ukraine

The article explores the principles and peculiarities of building early warning signal system as a mechanism for ensuring national resilience. It proves that effective tools in detecting threats and determining response measures are development a network of situational centers, as well as passports of threats. The article argues that the most problematic issues in the performance of such a system is the identification and detection of hybrid threats at an early stage, because they have a latent nature and do not come to light immediately.

Key words: national resilience, national security, threats, security environment, national security and defense sector.