УДК 351.746

ТИКВА В.Л. старший викладач кафедри інформаційної безпеки держави Навчально-наукового інституту інформаційної безпеки і стратегічних комунікацій Національної академії Служби безпеки України
ORCID: https://orcid.org/0000-0002-2129-6125

ДЕРЖАВНА СТІЙКІСТЬ В УМОВАХ ІНФОРМАЦІЙНИХ ВИКЛИКІВ ТА ПРОТИСТОЯНЬ

DOI: https://doi.org/10.37750/2616-6798.2025.2(53).334232

Анотація. *З початком повномасштабної війни російської федерації проти України, 24 лютого 2022 року, інформаційний та кіберпростори України перетворилися на повноцінні театри воєнних дій в яких країна-агресор намагається реалізувати свою загарбницьку політику, шляхом поєднання деструктивних дій у інфопросторі з інформаційно-психологічними операціями різних рівнів.*

За таких умов, коли агресія росії в інформаційному і кіберпросторі є однією з основних складових повномасштабної війни проти нашої держави, а численні кібератаки на інформаційні ресурси та інформаційно-психологічні операції– невід'ємною її компонентою, перед Україною з новою актуальністю постало питання пошуку шляхів та механізмів забезпечення інформаційної та кібернетичної безпеки від сучасних викликів та загроз, які виникають.

При цьому варто акцентувати увагу, що загрози і ризики інформаційної та кібербезпеки не обмежуються територією однієї лише нашої держави, а мають транскордонний характер, що значно ускладнює можливості їх оцінки й нейтралізації та актуалізує питання міжнародної взаємодії та співробітництва світової спільноти. Зазначене потребує активних та скоординованих заходів реагування суб'єктів міжнародної системи забезпечення інформаційної та кібербезпеки.

Для розробки та реалізації заходів нейтралізації загроз у сфері інформаційної та кібербезпеки України необхідно володіти цілісною картиною суспільних відносин у визначених сферах та особливостями їх правового регулювання. Саме тому, на сьогодні нагальною і вкрай актуальною є проблема аналізу організаційно-правових засад управління інформаційною та кібернетичною безпекою як складовими національної безпеки в Україні.

В запропонованому матеріалі автор розглядає поняття стійкості держави як поєднання внутрішніх і зовнішніх факторів здатності держави як системи виконувати основні функції в умовах інформаційних загроз, викликів і агресій з боку інших держав.

Ключові слова: *стійкість країни, непохитність держави, стійкість системи, критична інфраструктура, безпека держави, системи і підсистеми, інформаційний вплив, шкідливий наратив, сили і засоби інформаційного протиборства.*

Summary. *With the beginning of the full-scale war of the russian federation against Ukraine, on February 24, 2022, the information and cyber spaces of the Ukrainian state have become full-fledged theaters of military operations in which the aggressor country is trying to implement its aggressive policy by combining destructive actions in cyberspace with information and psychological operations of various levels.*

Under such conditions, when russia's aggression in information and cyberspace is one of the main components of a full-scale war against our state, and numerous cyberattacks on information resources and information and psychological operations are its integral components, Ukraine has faced with the issue of finding ways and mechanisms to ensure information and cyber security from modern challenges and emerging threats.

At the same time, it is worth emphasizing that the threats and risks of information and cyber security are not limited to the territory of our state alone, but are of a cross-border nature, which significantly complicates the possibilities of their assessment and neutralization and actualizes the issue of international interaction and cooperation of the world community. This requires the adoption of active and coordinated response measures by the subjects of the international system of ensuring information and cyber security.

To develop and implement measures to neutralize threats in the field of information and cyber security of Ukraine, it is necessary to have a holistic picture of social relations in certain areas and the features of their legal regulation. That is why, today, the problem of analyzing the organizational and legal principles of managing information and cyber security as components of national security in Ukraine is urgent and extremely relevant.

In this article the author considers the concept of state resilience as a combination of internal and external factors of the ability of the state as a system to perform its main functions in the conditions of threats, challenges and aggression from other states.

***Keywords**: country resilience, state stability, system resilience, critical infrastructure, state security, systems and subsystems, information influence, harmful narrative, forces and features of information confrontation.*

Постановка проблеми. Важливою характеристикою міждержавних стосунків у XXI столітті є протиборство різних країн. Враховуючи глобалізацію, котру розуміємо як перманентну взаємодію країн між собою у різних визначальних сферах їх життєдіяльності – економічній, фінансовій, політичній, військовій та ін., держави, з одного боку, мають шукати можливості для співпраці, взаємного розвитку, врахування інтересів партнерів, проте, з іншого боку, нікуди не зникли суперечності, відмінності в концептах розвитку, потенціях, ресурсах для задоволення власних потреб та інтересів. Слід також зважати на наявність у низки країн зброї масового знищення, що накладає додаткові обмеження стосовно розв‘язання конфліктів, у тому числі й силових.

Зрозуміло, що досвід Першої та Другої світових воєн показав жахливу ціну силового протистояння – мільйони загиблих, руйнація держав та територій, падіння моралі та психологічні травми націй. Усе це не могло не зумовити потребу пошуку нових концептуальних засад розв’язання прямих і латентних конфліктів між державами та їх військово-політичними блоками.

Поразка Радянського Союзу у холодній війні без прямих військових дій, без розв’язування третьої світової війни у гарячій фазі продемонструвала можливість вирішення конфліктів зі значним руйнівним потенціалом у відносно мирний спосіб. Такий приклад та набутий досвід спонукав до розробки нових моделей, заснованих на так званій “м‘якій силі”, або “смарт-війні”. Поняття смарт-війни включає концепцію вирішення конфліктів без силової фази або максимально коротке силове протистояння на завершальному етапі, коли потрібен лише один останній поштовх, і противник впаде, виснажений іншими зовні неагресивними діями, які не пов’язані із безпосереднім застосуванням сили.

Метою представленої статті є спроба аналізу зміни поняття стійкості держави в нових умовах глобальної світової безпеки другої чверті XXI століття.

Аналіз останніх досліджень і публікацій. Першим висловом нового підходу у вирішенні конфліктів між державами на основі протистояння систем як основного засобу вирішення конфлікту слід визначити промову Уінстона Черчиля 5 березня 1946 року у місті Фултон, штат Місурі, Сполучені Штати Америки [1]. У своїй промові У. Черчиль у відповідь на посилення протиріч між західними країнами та СРСР наголошував на неминучості силового протистояння між ними. Виокремимо головну

тезу, на наш погляд ключову – ця промова поклала початок системному протистоянню, де одна сторона була представлена низкою країн, об'єднаних єдиною метою – політичною перемогою. Таким чином відбулося проголошення утворення системи із чітко визначеною метою. Отже, світ отримав протистояння об'єднаних країн (у майбутньому блок НАТО) із країнами блоку СРСР (у майбутньому Варшавський договір). Розпочалося формування двополюсної системи колективної безпеки. Одним центром об'єднання стали США, іншим центром став СРСР. За цим підходом всі інші країни світу мали б пристати до одного чи до іншого блоку у тій чи інші формі залучення. За теорією так мало би статися, але країни так званого третього світу не увійшли до цих блоків або ввійшли у якості "слабкого учасника".

Подальший розвиток відносин протистояння неодноразово, із стійким повтором, призводив до збільшення вірогідності ядерної війни і знищення цивілізації. Серед найсерйозніших слід назвати: війна у Кореї, яка призвела до силового втручання військ США, Кубинська криза, Берлінське протистояння, події у В'єтнамі тощо. Політичне керівництво країн-супротивників розуміло наслідки ядерної війни, тому силові акції перенеслися на територію третіх країн, де була можливість застосувати силові акції, але це не призводило до ядерної війни.

Розпад Радянського Союзу призвів до формування однополюсного світу та змінив форми протистояння та силових акцій.

Такий розвиток відносин протистояння об'єднань держав між собою вимагав від політиків, управлінців, науковців осмислення подій та генерації нових підходів до вирішення конфліктів. Наприклад, теракти у США у 2001 році, подальше протистояння із терористичними організаціями наочно довело розширення форм протистояння та географічних місць їх прояву. Західні науковці з цього приводу проводили системні наукові дослідження [2; 3]. Зміна форм, наприклад - терор та залучення третіх сил у протистояння із наданням їм сучасної зброї та тактики ведення малих війн та разових акцій призводило до масштабних змін у політичній, економічній картах світу. Разом з тим, переосмислення практичного досвіду та аналіз отриманих результатів, технічний прогрес та інше приводив до усвідомлення нових реалій: асиметричність відповіді на агресію, декомпозицію своїх дій із дотриманням поставленої загальної мети, тощо

Системний та принципово-послідовний противник США в особі рф постійно шукав нові концепції протистояння вже на основі системного та динамічного підходів.

Як основний елемент гібридного протистояння з обох сторін був обраний інформаційний вплив. Основу даного процесу складав наявний досвід Радянського Союзу у проведенні пропагандистських кампаній. Тому, інформаційна війна набувала рис системного протиборства, а інформаційна сфера стала середовищем, у якому цілком можливою була реалізація загроз безпеці та стабільності країн, що змусила змінити підходи до інформаційного протиборства і діяльності "силових блоків".

Початок військової агресії з боку російської федерації поставив перед нашою країною безліч викликів і загроз, серед яких на перший план виступає посилення захисту в інформаційній сфері. При цьому відсутність жорсткої територіальної прив'язки ключових інформаційних ресурсів дозволяє інформаційно-комунікаційним лідерам опановувати і використовувати будь-яке втручання. Ефективне освоєння чужих територій стає можливим шляхом використання інформаційної локалізації. Небезпеки, що створюються даними загрозами, часто змушують залишати осторонь вирішення гострих соціальних проблем в середині України, формують умови фінансово-економічної нестабільності і створюють передумови соціальної та політичної деструкції [4].

Водночас питанням стійкості держави в сучасних інформаційних викликах і протистояннях в своїх багаточисельних публікаціях приділяв увагу Володимир Горбулін. На його думку, способи ведення сучасної війни рф проти України роблять надзвичайно важливим забезпечення інформаційної безпеки нашої держави і особливо її Збройних Сил, що є запорукою успішної оборони та збереження національної державності. На зміну війні гарячого типу, яка зосереджується на прямому військовому зіткненні, приходить війна гібридного характеру, метою якої є розгортання громадянських воєн та створення керованого інформаційного хаосу на території противника. Для цього використовуються всі можливості – від хакерських атак на найважливіші системи життєзабезпечення держави до цілеспрямованої роботи засобів масової інформації. Якщо раніше світ навколо нас здавався безпечним, то сьогодні виклики несуть у собі набагато більшу небезпеку, ніж у мирний час [5].

Також для нашого розгляду цікавим є розвиток та використання загальної теорії систем, яка дозволила визначити поняття критичної інфраструктури щодо практичної реалізації стратегій, концепцій та доктрин національної безпеки різних країн. Введення поняття критичної інфраструктури дозволило зосередитися на практичній реалізації безпекових роздумів та практичних намірів. У свою чергу для безпеки критичної інфраструктури у основних документах стали використовувати поняття стійкості, яке розуміється як здатність критичної інфраструктури витримати негативний вплив та продовжувати виконувати позитивну функцію системи, основою якої вона є [6]. Звісно, що підхід до розгортання розуміння стійкості критичної інфраструктури виходив із концепції глобальної непохитності однополісного світу.

В останні роки аналітики-прогнозисти почали говорити про сходження США з позиції світових лідерів, що проявляється через так званий закон “перенавантаження системи” на певному рівні розвитку. Зокрема, про поступовий відхід США із лідерських позицій у світовій ієрархії зазначив у своїй публікації Нейл Фергюсон [7].

Погоджуючись із автором, визнаємо, що зараз відбувається формування багатополюсного політичного світу, визнаючи при цьому місце США, рф, Китаю, Індії та регіональних лідерів Туреччини, Ірану, Австралії тощо.

У нових умовах, на нашу думку, є необхідність розглянути поняття стійкості системи, а в нашому питанні — держави, та особливості його розуміння у нових реаліях.

Виклад основного матеріалу. Одна з найбільш поширених та простих сучасних тактик, які спостерігаються в міждержавних стосунках – це порушення стійкості інших країн шляхом випробування функціональності державної системи через виклики у різних сферах або вузлів критичної інфраструктури.

Таким чином, об’єкт нападу виснажується через неефективне використання його сил та засобів, ресурсів. Відбувається своєрідне розхитування у концентрації сил, оперативного реагування тощо, як, наприклад, під час тенісної партії, коли один спортсмен постійно посилає м’ячик у різні кути корту, що швидко виснажує суперника, котрий врешті-решт програє, хоча б і мав ліпшу підготовку.

Ця тактика дій агресора може бути втілена лише за умови поділу основного задуму на сукупність задумів нижчого рівня, реалізація яких дає змогу досягти основної мети. При цьому йдеться про заглиблення не тільки на перший рівень фрагментації, а й на подальші. Даний підхід проводиться й далі, сягаючи глибших рівнів. Слід також зазначити, що при його реалізації можливо активувати дії з різних гілок (сфер) фрагментації, які, на перший погляд, не поєднуються, але за результатом наближають досягнення основної мети. Такий своєрідний оксиморон розглядається як гібридне застосування, гібридні загрози й гібридні війни.

Саме у цьому, на нашу думку, полягає зміст концепту “гібридна війна”, яка проводиться російською федерацією останніми роками проти України та інших країн, що їх рф включає до кола своїх геополітичних інтересів.

Звісно, підґрунтям доктрини “гібридна війна” є теорія й відповідна практика державного управління, без якого проведення гібридних акцій нездійсненне. Розробка необхідного для успіху механізму державного управління можлива в суспільстві, інтегрованому усвідомленням єдиної мети існування країни та потребою захисту цінностей, інтересів держави, суспільства й людини. В умовах же нерозвинутої самоорганізації суспільства це призводить до формування авторитарного режиму [8].

Виникають запитання. А що ж може протистояти такій політиці та методам досягнення поставленої мети, на які працює весь державний механізм? Що слід покласти у фундамент системи захисту, розрахованої на певні загрози, які досить швидко виникають, породжені комбінаціями декомпільованих раніше чинників загроз?

Концепція захисту на конкретний виклик, загрозу, в цьому разі не може забезпечити вирішення вказаної проблеми. Причина полягає у самому розумінні поняття захисту, який завжди орієнтований на конкретні загрози, які в нашому випадку мають динамічний характер та відтворюються доволі просто і швидко агресивною стороною.

Розв’язання цієї проблеми, як вже показано вище, має, на наш погляд, ґрунтуватися на стійкості – показнику системи, під яким розуміємо її спроможність виконувати свою основну функцію під впливом негативних чинників. Стійкість системи включає також відновлення підсистем, зруйнованих унаслідок зловмисних атак, реалізації загроз, інцидентів тощо.

Стійкість як атрибутивна характеристика будь-якої системи дозволяє підходити до забезпечення результативного та ефективного функціонування із конкретикою розуміння відбиття атак (викликів, загроз), у тому числі й гібридних. Розгляд у цьому контексті суспільних і державних інститутів дає змогу визначати й безпекову політику системи державної безпеки. Основу такої політики становитиме критерій стійкості та надійності функціонування, що підвищить життєздатність держави, котра стала об’єктом нападу, застосування гібридних акцій, спрямованих на завдання шкоди.

Цільова функція з орієнтацією на забезпечення стійкості дозволить оцінити рівень політики забезпечення державної безпеки та розглядати акції підриву не лінійно, а комплексно, відповідно до можливої шкоди. Цю тезу слід розуміти так, що відповідь на шкідливі інформаційні операції може полягати у протидії в інших сферах, приміром: реальне зниження напруженості у власній країні, виведення з ладу серверів розповсюджувачів негативної інформації, оперативного спростування фейків. Природно, що належить створювати нові, надвідомчі механізми управління, дієвої координації дій, взаємодії та обміну інформацією між наявними в країні системами забезпечення безпеки та кризового реагування.

Світовий досвід реагування держав на пандемію COVID-19 доводить неефективність існуючих систем забезпечення національної (державної) безпеки через непередбачуваність подібної загрози. Наслідком такої раптовості стало застосування середньовічних засобів боротьби із інфекціями, падінням рівня економіки, численні людські жертви.

Більшість науковців під розумінням поняття стійкості зосереджують свої зусилля суто на внутрішньому стані самої системи, залишаючи поза увагою те, що сама система входить як підсистема до більшої системи.

Отже, стійкість системи залежить від стійкості більшої системи, до якої входить наша держава, надійності зв’язків та підтримки. Тут мова йде про те, що країна, що

входить до союзів, блоків тощо може розраховувати на підтримку союзників, що значно посилює її спроможність протистояння викликам та загрозам завдяки поєднанню зусиль та потенціалів країн блоку. Таким чином, стійкість держави посилюється за рахунок загальної стійкості політичної, військової, економічної системи, до якої вона входить.

Так, країни, що входять до Європейського Союзу, отримують економічну підтримку у разі економічної кризи або природних катастроф тощо. Країни НАТО дістають військову допомогу шляхом отримання озброєння або передислокації військових інших країн на територію країни, що може зазнати агресії іншої держави. Наприклад, на території України під час неодноразових загострень у відносинах із країною-агресором проводилися військові навчання із залученням військових сил країни НАТО. Також, війська США провели передислокацію військових підрозділів до Польщі з метою зменшення вірогідності агресії та захисту території держави. Під час останньої кризи із залученням мігрантів до дестабілізації ситуації у Польщі у листопаді 2021 року за участю влади Білорусі, Польща отримала підтримку від країн Європейського Союзу та міжнародних структур щодо цивілізованого вирішення конфлікту, у якому Білорусь використала мігрантів для вирішення своїх політичних цілей та силового протистояння.

Стійкість системного об’єднання країн допоможе наочно представити фізична модель впливу зовнішніх факторів на стабільність нашого об’єкту розгляду.

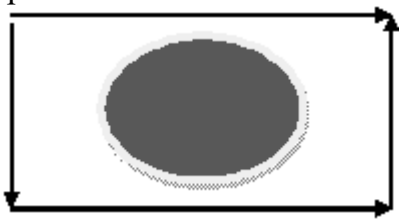

Рис 1. Стабільність об’єкта.

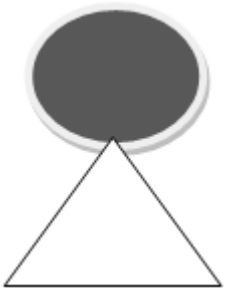

Рис 2. Нестабільність об’єкта

Рисунок 1 – показує, що знаходження нашого об’єкта всередині контуру його захищає та не дає можливості його руйнації. Натомість, рисунок 2 показує, що знаходження об’єкта у такій позиції робить його вкрай нестійким і слабкий поштовх призведе до падіння.

Наведена модель наочно доводить вплив зовнішніх умов на стійкість системи. Мова звісно йде про входження або ні до державних об’єднань, стан стабільності у регіоні, який розглядається, оскільки нестабільність ситуації на зовнішніх кордонах суттєво впливає на ситуацію у країні. Так, довгий кордон між Україною та рф призвів до військової агресії росії, утворення окупованих територій тощо.

Саме тому, усвідомлюючи силу колективного протистояння, агресор російська федерація постійно шукає прогалини в позиціях західних союзників для ослаблення

зв'язків та нав'язування позиції невтручання у події, які вона нав'язує об'єкту своєї агресії.

Висновки.

Варто зазначити, що орієнтація у безпековій політиці на поняття стійкості дозволить започаткувати новий етап реформування системи забезпечення національної безпеки України.

Розгляд поняття стійкості держави як системи слід розглядати у двох аспектах. Перший полягає у визначенні стійкості як суто властивості самої системи. Другий полягає у впливі зовнішніх чинників на забезпечення стійкості держави.

Поняття стійкості держави повинно розглядатися із застосуванням ризиків та вірогідності настання тих чи інших викликів та загроз.

Саме у розгляді ризико-орієнтованих підходів, формування стратегій поведінки під час зниження стійкості системи, до якої входить наша система- держава, і полягають перспективи подальших наукових розвідок.

Використана література

1. The Times, 1946, N 18.
2. Colin B. Burke. America's information wars. The untold story of information systems in America's conflicts and politics from World War II to the Internet age. 2018, 389 p.
3. Senator Bob Grahan, Jeff Nussbaum Intelligence matters. Intelligence matters. The CIA, the FBI, Saudi Arabia, and the Failure of America's War on Terror. Random House Website address: www.atrandom.com. 2004.
4. Подорожна Т. Забезпечення інформаційної безпеки України в умовах сучасних виклилів та загроз з боку рф. *Електронне наукове видання «Аналітично-порівняльне правознавство».* 2023. № 6. С.491-497
5. Горбулін В.П. Як перемогти росію у війні майбутнього / В.Горбулін. Київ: Брайт Букс, 2021. 248 с.
6. Кондратов С.І., Суходоля О.М. Державна система захисту критичної інфраструктури у системі забезпечення національної безпеки: аналітична доповідь. Київ., 2020. 36 с.
7. Nail Ferguson On why the end of America's empire wont be peaceful. *The Economist.* Aug 20th. 2021.
8. Деструктивні впливи та негативні наративи: інструменти виявлення та протидії: метод.мат. / Д.В. Дубов, А.В. Баровська, Ю.К. Каздобіна. Київ: УФБС, 2020. 60 с.

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~