# Узагальнена математична модель функціонування сектору безпеки і оборони в умовах невизначеності та ризиків, притаманних впливу гібридних засобів противника

# A generalized mathematical model for security and defense sector functioning under uncertainty and risks inherent to hybrid adversary impact

**Максим Троцько** [A]

**Corresponding author**: к.т.н., начальник відділу стратегічного і середньострокового планування та сумісності з військовими структурами НАТО, e-mail: maxx.troublesome@gmail.com, ORCID: 0000-0003-1136-0370

**Віктор Гудима** [B]

к.т.н., доцент кафедри технічного забезпечення, e-mail: viktor.gud77@gmail.com, ORCID: 0000-0003-4722-0601

**Андрій Дядечко** [B]

доктор філософії, начальник науково-дослідного відділу проблем супроводження експлуатації інформаційних систем, e-mail: andrewvvs@gmail.com, ORCID: 0000-0003-0191-8326

**Микола Шилан** [B]

науковий співробітник науково-дослідного відділу інституту інформаційно-комунікаційних технологій та кібероборони, e-mail: andrewvvs@gmail.com, ORCID: 0000-0002-8801-4364

**Maksym Trotsko** [A]

**Corresponding author**: Candidate in Technical Sciences, Head of the Strategic and Medium-Term Planning and NATO Military Structures Compatibility Department, e-mail: maxx.troublesome@gmail.com, ORCID: 0000-0003-1136-0370

**Viktor Hudyma** [B]

Candidate in Technical Sciences, Associate Professor of the Technical Support Department, e-mail: viktor.gud77@gmail.com, ORCID: 0000-0003-4722-0601

**Andrii Diadechko** [B]

PhD, Head of the Research Department on Information Systems Operation Support Issues, e-mail: andrewvvs@gmail.com, ORCID: 0000-0003-0191-8326

**Mykola Shylan** [B]

Researcher at the Research Department of the Institute of Information and Communication Technologies and Cyber Defence, e-mail: andrewvvs@gmail.com, ORCID: 0000-0002-8801-4364

[A] Головне управління Національної гвардії України, м. Київ, Україна
[B] Національний університет оборони України, м. Київ, Україна

[A] Main Directorate of the National Guard of Ukraine, Kyiv, Ukraine
[B] National Defence University of Ukraine, Kyiv, Ukraine

**Received:** December 06, 2024 | Revised: December 19, 2024 | Accepted: December 31, 2024

**DOI:** 10.33445/sds.2024.14.6.2

**Мета роботи:** розробити узагальнену математичну модель функціонування сектору безпеки і оборони України в умовах невизначеності та ризиків, притаманних впливу гібридних засобів противника, а також дослідити синергетичний ефект впливу взаємосумісності на спроможності сектору безпеки і оборони протидіяти стратегії застосування гібридної боротьби.

**Метод дослідження:** методи комплексного аналізу та синтезу, метод нелінійного математичного моделювання.

**Результати дослідження:** визначено, що існує взаємозв'язок між невизначеністю та ризиками гібридних загроз, а також доведене існування компенсуючого впливу з боку сектору безпеки та оборони держави на застосування противником заходів гібридного впливу.

**Теоретична цінність дослідження:** теоретичні положення, висновки та рекомендації, викладені в роботі, можуть стати основою для подальших наукових досліджень й дискусій з питань підвищення можливостей сектору безпеки та оборони України протидіяти гібридним засобам противника.

**Практична цінність дослідження:** реалізація рекомендацій і пропозицій, обґрунтованих у роботі, які спрямовані, на основі процесів військової стандартизації, на забезпечення взаємосумісності складових сектору безпеки і оборони України, а також міжнародних партнерів, дозволить протидіяти стратегії противника щодо застосування заходів гібридної боротьби.

**Цінність дослідження:** в даному дослідженні моделювання процесів функціонування сектору безпеки та оборони України в умовах невизначеності та ризиків, притаманних впливу

**Purpose:** to develop a generalized mathematical model for Ukraine's security and defense sector functioning under uncertainty and risks tied to hybrid adversary tools, and to investigate the synergistic effect of interoperability on sector capabilities to counter hybrid warfare strategies.

**Method:** methods of comprehensive analysis and synthesis, nonlinear mathematical modeling methods.

**Findings:** it has been determined that there is a relationship between uncertainty and the risks of hybrid threats, and the existence of a compensating influence from the state's security and defense sector on the adversary's use of hybrid influence measures has been proven.

**Theoretical implications:** the theoretical provisions, conclusions, and recommendations presented in the paper can become the basis for further scientific research and discussions on increasing the capabilities of the security and defense sector of Ukraine to counter the enemy's hybrid means.

**Practical implications**: the implementation of recommendations and proposals substantiated in the work, which are aimed, based on military standardization processes, at ensuring interoperability of the components of the security and defense sector of Ukraine, as well as international partners, will allow countering the enemy's strategy of using hybrid warfare measures.

**Value**: in this study, modeling the processes of functioning of the security and defense sector of Ukraine in conditions of uncertainty and risks inherent in the influence of the enemy's hybrid means has not yet been the subject of comprehensive scientific research.

гібридних засобів противника ще не були предметом комплексного наукового дослідження.

**Тип статті:** теоретичний з практичними рекомендаціями.

***Papertype:*** theoretical with practical recommendations.

***Ключові слова:*** невизначеність, ризики, гібридні загрози, взаємосумісність.

***Key words:*** uncertainty, risks, hybrid threats, interoperability.

## *Вступ*

В дослідженнях історії війни зазначається, що ворогуючі сторони споконвічно використовували іррегулярні сили, а також регулярні сили використовували непряму тактику дій для створення несподіванки та обману разом із прямим застосуванням сили [1]. Коріння гібридної війни бере початок з часів Пелопоннеських війн у п’ятому столітті до нашої ери. Тоді спартанці використовували повстанців проти афінян, щоб змусити їх до миру.

Дискусії про гібридну війну посилилися після війни Ізраїлю та Хезболли в 2006 році, російської інтервенції в Грузію в 2008 році і початку російсько-української війни у 2014 році. Проте гібридна війна не була концептуалізована на рівні інших концепцій ведення бойових дій чи збройного протистояння. Так, наприклад, Міністерство оборони США офіційно не використовує концепцію гібридної війни, а в НАТО, хоча й термін “гібридна загроза” і застосовується, але формальної концепції, узгодженої усіма державами-членами Альянсу немає.

## *Теоретичні основи дослідження*

Дослідники визначають деякі відмінності між термінами “гібридна загроза”, “гібридний конфлікт” і “гібридна війна”, хоча вони часто використовуються як синоніми для позначення взаємопов'язаного характеру таких викликів національній безпеці держав, як етнічні конфлікти, тероризм, міграційні кризи, протизаконна активність недержавних організацій, ведення диверсійної діяльності як регулярних (спеціальних) та нерегулярних (приватні воєнні компанії, найманці тощо) сил, активність кримінальних груп та організованої злочинності, а також багато інших засобів, включаючи військові, дипломатичні, технологічні тощо [1, 2].

У цьому контексті гібридна загроза знаходиться на найнижчому рівні шкали інтенсивності та є результатом взаємодії різних елементів, які разом утворюють більш складну і багатовимірну загрозу. НАТО визначає гібридні загрози як такі, що створюються супротивниками з можливістю адаптивного одночасного використання звичайних і нетрадиційних засобів досягнення своїх цілей [3].

Перш ніж переходити до гібридної війни, необхідно розглянути поняття «гібридного конфлікту». Гібридний конфлікт – це ситуація, в якій сторони утримуються від відкритого використання збройних сил одна проти одної, натомість застосовують залякування демонстрацією військового потенціалу, сконцентрованого поблизу державних кордонів чи географічних центрів тяжіння опонента. Такі дії знаходиться нижче порогу збройного нападу, а їх вплив підсилюється поєднанням використання економічних, політичних, дипломатичних чи інфраструктурних вразливостей держави-опонента [1-3].

У збройному конфлікті високої інтенсивності або звичайному збройному конфлікті перераховані вище засоби та методи впливу на противника також застосовуються. Виникає питання: що насправді нового в ідеї гібридного конфлікту. Новим аспектом стає використання кіберпотужностей для здійснення інформаційно-технічних впливів на об’єкти критичної інфраструктури чи інформаційно-психологічних впливів на визначену цільову аудиторію. При цьому відповідні кіберзагрози настільки нові, що вони ще не включені в правове поле міжнародного гуманітарного права, а вплив на відповідні центри тяжіння як в когнітивній та моральній сферах, так і результати втручання в функціонування об’єктів критичної інфраструктури створюють вагомий кумулятивний ефект на державу-опонента [3, 4].

Гібридні війни поєднують низку різних способів ведення війни, включаючи звичайні способи та засоби ведення бойових дій, тактики застосовування нерегулярних формувань та найманців, терористичні акти, включаючи невибіркове насильство та примус, а також масові заворушення, інспіровані іззовні. Гібридна війна – це ситуація, за якої держава вдається до відкритого використання збройних сил проти іншої держави або недержавного утворення у поєднанні з іншими засобами, такими як економічні, політичні та дипломатичні, а також застосовує приховані (спеціальні) операції, в тому числі і в кіберпросторі [1-4].

Концепція гібридної війни застосовує кілька положень вчення Сунь Цзи [5]. Для неї очевидна важливість зміни форми впливів на противника та їх відповідної адаптації до зміни операційного середовища шляхом використання різних типів і розмірів сил. Вчення Сунь Цзи підтримує використання як регулярних, так і нерегулярних сил для перемоги над противником. Крім того, він також пропонує послаблювати противника шляхом застосування асиметричних (нетрадиційних) підходів щодо виявлених вразливостей, що є основою концепції гібридної війни. Що стосується загальновизнаних дев'яти принципів війни, таких як зосередження, об'єктивність, наступ, раптовість, економія сил, маневр, єдиноначальність, безпека та простота, то в цілому їх також можливо застосувати до гібридної війни. Крім того, гібридна війна представляє дослідникам ще два нових принципи: швидкість і управління сприйняттям [5].

Концепція гібридної війни має потенціал застосування на всіх рівнях війни, від тактичного до стратегічного та стає одним із чинників, що формує безпекове та операційне середовище [1-5]. На стратегічному рівні підтримка повстанських рухів та незаконних збройних формувань регулярними силами значно послаблює державу-опонента, на оперативному рівні зазначені нерегулярні формування можуть застосовуватися для порушення логістичного забезпечення та зриву перегрупувань військ (сил), а на тактичному рівні потенційний ефект від їх застосування може досягти стратегічного рівня завдяки швидкому розповсюдження інформації. Необхідно зазначити, що коли справа стосується таких сфер війни, як когнітивна, моральна та фізична, головним чином засоби гібридної війни мають найвищу ефективність у першій та другій сферах. У фізичний сфері використовуються створені ефекти в когнітивній та моральній сферах для досягнення істотної переваги над дезорієнтованим і деморалізованим спротивом.

## *Постановка проблеми*

Потенціал застосування засобів гібридної боротьби створює нові та модифікує існуючі виклики та загрози національній безпеці держави в цілому та її складовим окремо і вимагає створення ефективної та дієвої системи виявлення, попередження, реагування та протидії, побудованої на спільному розумінні факторів впливу гібридних загроз на безпекове середовище України.

Стаття присвячена розробленню узагальненої математичної моделі функціонування сектору безпеки і оборони в умовах невизначеності та ризиків, притаманних впливу гібридних засобів противника, а також дослідженню синергетичного ефекту впливу взаємосумісності на спроможності сектору безпеки і оборони протидіяти стратегії застосування гібридної боротьби.

## *Методологія дослідження*

Концептуальний підхід гібридного протистояння обіцяє успіх, якщо вразливі місця противника (політичні суперечки чи критичний стан об’єктів інфраструктури) відкривають вікна можливостей для застосування гібридних стратегій і тактик. Вікна можливостей пов’язані з потенційною варіативністю результатів підривної діяльності, що виражається в термінах невизначеності [6-7].

Невизначеність уособлює множину ймовірних станів у будь який момент часу в майбутньому. Чим більше невизначеність, ти більшою є кількість ймовірних результатів діяльності, як позитивних, так і негативних. Це створює певні незручності для здійснення прогнозування потенційного результату, але й становиться джерелом потенційної цінності майбутніх станів операційного (безпекового) середовища.

Західна теорія воєнного мистецтва та економіка й менеджмент систематично обмінюються інноваційними підходами та концепціями. Театр воєнних дій іноді мало відрізняється від протистоянь мегакорпорацій на економічних ринках. Стратегія застосування засобів гібридної боротьби не є виключенням із процесів обміну та запозичень воєнною наукою передових досягнень бізнесу (рис. 1).

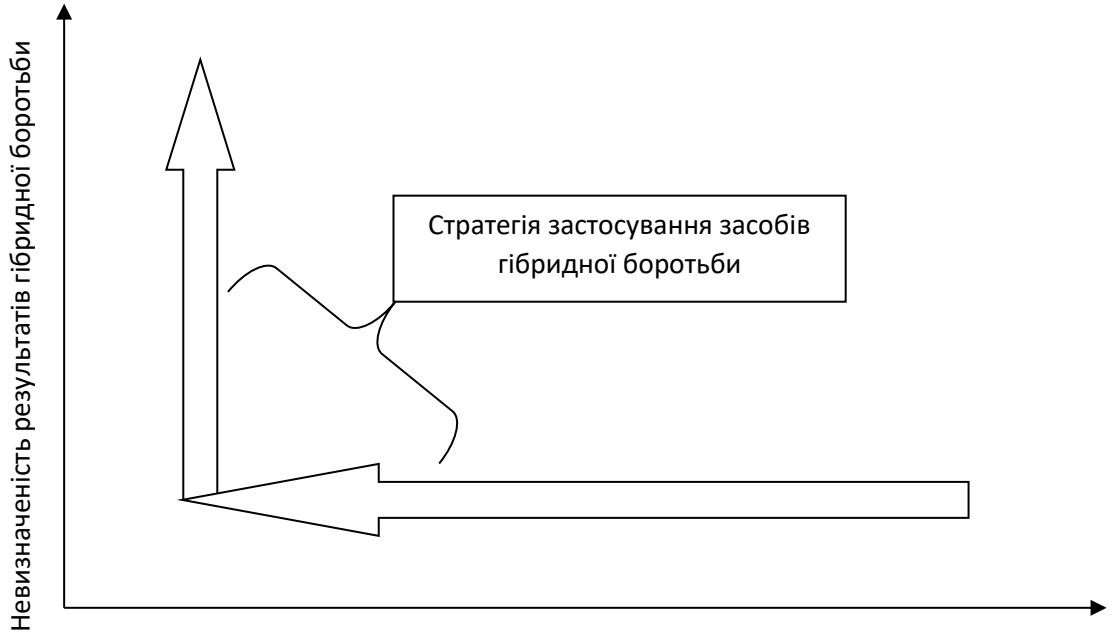


Рисунок 1 – Сутність стратегії застосування засобів гібридної боротьби

Підприємці та новатори вбачають цінність у невизначеності, оскільки вони створюють ймовірність отримання прибутку в умовах, коли виграш істотно перевищує загальні очікування. Для вигідного використання невизначеності необхідно максимально знижувати ризики, функціонуючи в області високого потенціалу станів майбутнього середовища, зменшуючи до мінімуму ймовірність власних витрат. Досвідчені підприємці застосовують цю парадигму, створюючи “мінімально життєздатні продукти” для перевірки ринків та технологій, знижуючи таким чином свої власні ризики під час досліджень невизначеності ринків. Вони продають свої комерційні пропозиції клієнтам до того, як вони будуть створені фізично, і якщо хоча б один з численних пробних варіантів себе виправдає, то прибутки можуть бути набагато більше інвестицій, зроблених для їх ініціювання [6].

Як і підприємець, сторона, що веде гібридну боротьбу, робить наголос на дії з високим рівнем невизначеності та низьким ризиком матеріальних втрат. Результати гібридного протистояння можуть бути як позитивними, так і негативними, але до їх отримання відсутня можливість їх ідентифікації лише на основі історичного досвіду. При цьому, за позитивного варіанту розвитку подій, результат набуває сприятливих рис для агресора, у протилежному випадку програш не є значним, адже агресор не мав високого ризику втрат через низьку ймовірність його ідентифікації, як відповідального за нанесення шкоди.

Сторони, що ведуть гібридну боротьбу, ретельно намагаються знизити ризики власної причетності за рахунок залучення недержавних утворень, застосування спеціальних підрозділів малої чисельності, витратних ресурсів персоналу (приватні військові компанії, найманці тощо), застосування низько затратних технічних засобів (цивільні комерційні БПЛА тощо), прихованих дій, тих що важко ідентифікуються, (інфільтрація диверсійних сил чи когнітивна боротьба). Усі ці заходи проводяться за принципом: “Орел – виграш, рішка – відсутність великого програшу” [6-7].

Один із способів протидії нетрадиційним методам ведення боротьби полягає у створення умов, що є несприятливими для агресора – тобто зниженні рівня невизначеності за рахунок зменшення варіативності станів майбутнього середовища та збільшенні ризиків інвестиціям противника в операції гібридного протистояння. Для цього необхідно дослідити динаміку внутрішніх взаємозв’язків, тобто здійснити аналіз сутності процесів гібридної війни, та застосовувати всеохоплюючий підхід під час синтезу комплексу заходів виявлення та протидії у максимально ефективний та дієвий спосіб в умовах невизначеності та ризиків, притаманних впливу гібридних засобів противника.

Для вирішення цієї задачі розробимо узагальнену математичну модель функціонування сектору безпеки і оборони в умовах невизначеності та ризиків, притаманних впливу гібридних засобів противника. Під час моделювання застосуємо наступні припущення:

- сектор безпеки і оборони України являє собою відкриту нелінійну динамічну систему, яка є невід’ємною частиною системи державного устрою;

- реагування сектору безпеки і оборони на наявні та потенційні виклики й загрози громадській безпеці і порядку, державній та воєнній безпеці відбувається в умовах невизначеності багатовимірного динамічного безпекового середовища та впливу пов’язаних з цією невизначеністю ризиків як матеріального, так і репутаційного характеру;

- складний ієрархічний характер внутрішніх взаємозв’язків складових сектору безпеки і оборони обумовлює часткову відсутність спостережуваності впливів внутрішніх та зовнішніх процесів, що характеризується терміном “поєднання зусиль” та фактично вимагає застосовувати досить формалізовані математичні моделі його функціонування.

Застосування фахівцями НАТО визначеного в аналізі сутності гібридного протистояння підходу, що пов’язує у одній стратегії використання невизначеності та відповідних ризиків створює можливість розглянути процеси функціонування сектору безпеки і оборони України в умовах впливу гібридних загроз як функціонування системи управління, метою якої є компенсація впливу невизначеності та збільшення відповідних ризиків для противника [6].

## *Результати*

Представимо процеси функціонування сектору безпеки і оборони держави в умовах гібридних загроз у вигляді системи нелінійних диференційних рівнянь [8, 9]:

$$\begin{cases} \dot{x}_1 = a_{11} \cdot x_1 + a_1 \cdot x_2 + a_2 \cdot x_2^2 + a_3 \cdot x_2^3 + b_1 \cdot u; \\ \dot{x}_2 = a_{21} \cdot x_1 + a_{22} \cdot x_2 + b_2 \cdot u, \end{cases} \quad (1)$$

де $x_1$ – вплив невизначеності гібридних загроз;

$a_{11}, a_{21}$ – вектори коефіцієнтів, що відображають початкове положення системи у просторі станів (фазовому просторі);

$a_1, a_2, a_3$ – коефіцієнти поліному, що відображає нелінійний характер внутрішніх зв’язків невизначеності та супутніх ризиків;

$b_1, b_2$ – вектори коефіцієнтів підсилення управляючого впливу;

$u$ – управляючий вплив;

$x_2$ – рівень ризиків, пов’язаних із невизначеністю гібридних загроз.

Поліном третього ступеня $a_1 \cdot x_2 + a_2 \cdot x_2^2 + a_3 \cdot x_2^3$ у першому рівнянні системи (1) приведено для наочності наявності нелінійного зв'язку невизначеності та ризиків, при цьому вид функціональної залежності (значення коефіцієнтів поліному) цих параметрів підлягає більш детальному дослідженню та є предметом майбутніх досліджень.

Застосуємо у подальшому припущення, що змінні стану системи є доступними для спостереження та оцінювання. Таке припущення ґрунтується на існуванні методики оцінювання та управління ризиками, яка пов'язує відповідний рівень ризику з невизначеністю отримання результату діяльності [6].

Для визначення наявності впливу заходів протидії гібридним загрозам притаманним невизначеності та ризикам необхідною та достатньою умовою будемо вважати формулювання у загальному вигляді закону управління нелінійною динамічною системою, а комп'ютерне моделювання залишимо для подальших, більш детальних досліджень.

Отже, метою досліджень є визначення закону управління, для якого система буде асимптотично сталою відносно початку координат фазового простору (простору станів). Для цього представимо систему в канонічному вигляді [9]:

$$\begin{cases} \dot{x}_1 = f_1(x_1) + G_1(x_1) \cdot x_2; \\ \dot{x}_2 = f_2(x) + G_2(x) \cdot u, \end{cases} \quad (2)$$

де $x = (x_1, x_2)$ – вектор станів системи, при цьому $x_1 \in R^k, x_1 \in R^m, x \in R^n, n = k + m; n > m$;

$f_1(x_1), f_2(x)$ – функції підсилення впливу параметрів системи;

$G_1(x_1) = [g_{11}(x_1), \dots g_{1m}(x_1)]$ – функція корекції положення зображуючої точки системи, що характеризує ієрархічний характер взаємодії параметрів системи;

$G_2(x) = [g_{21}(x), \dots g_{2m}(x)]$ – функція корекції положення зображуючої точки системи за допомогою управляючого впливу;

функції $f_1$, $f_2$, $g_{11}$, $\dots g_{1m}$, $g_{21}$,$\dots g_{2m}$ є такими, що диференціюються;

$u$ – вектор управляючих впливів, $u \in R^m$.

Необхідно зазначити, що права частина обох диференційних рівнянь залежить від сигналу управління $u$, що ускладнює виділення в цих рівняннях внутрішньої підсистеми [9].

Застосуємо заміну координат:

$$p_1 = x_1 - b_1 \cdot b_2^{-1} x_2;\ p_2 = x_2, \quad (3)$$

та приведемо модель до вигляду (2)

$$\begin{cases} \dot{p}_1 = (a_{11} - b_1 \cdot b_2^{-1} \cdot a_{21})(p_1 + b_1 \cdot b_2^{-1} \cdot p_2) + (a_1 - b_1 \cdot b_2^{-1} \cdot a_{22}) \cdot p_2 + a_2 \cdot p_2^2 + a_3 \cdot p_2^3; \\ \dot{p}_2 = a_{21} \cdot (p_1 + b_1 \cdot b_2^{-1} \cdot p_2) + a_{22} \cdot p_2 + b_2 \cdot u, \end{cases} \quad (4)$$

де від управління залежить тільки права частина останнього диференційного рівняння. Таким чином вираз (4) визначає динаміку поведінки внутрішньої підсистеми, що характеризує взаємозв'язки невизначеності та ризиків. В якості внутрішнього управління виступає координата $p_2 = x_2$, що відповідає впливу невизначеності.

Оберемо в якості внутрішнього управління функцію у вигляді [9]:

$$p_2 = 0, \quad (5)$$

Застосування цієї функції внутрішнього управління в системі рівнянь (4) перетворює її до вигляду:

$$\dot{p}_1 = -\hat{a} \cdot x_1, \text{ де } \hat{a} = b_1 \cdot b_2^{-1} \cdot a_{21} - a_{11}, \quad (6)$$

Система (6) є лінійною асимптотично сталою підсистемою. Тоді функція виходу, чи функція агрегованої макрозмінної матиме вигляд [9]:

$$y = \Psi(p) = p_2, \quad (7)$$

Вибір супроводжуючого функціоналу у вигляді [9]

$$J = \int_0^\infty \Psi(t)^T \Psi(t) + \phi[\Psi(t)]^T \phi[\Psi(t)] dt, \quad (8)$$

визначає, що досягнення його мінімуму буде відповідати перехідним процесам по агрегованій макрозмінній (7), що характеризує якість системи стабілізації впливу невизначеності

$$J = \int_0^\infty \dot{y}(t)^2 + \phi[y(t)]^2 dt, \quad (9)$$

Оберемо функцію $\varphi$ в класі лінійних:

$$\phi(y) = y, \quad (10)$$

тоді рівняння екстремалі супроводжуючого функціонала матиме вигляд:

$$T\Psi(t) + \phi[\Psi(t)] = 0, \text{ для } \forall t \geq 0, T^T = T > 0, \quad (11)$$

що можна записати у вигляді:

$$T \cdot \dot{y} + y = 0, \text{ де } T > 0, \quad (12)$$

Константа $T$ в даному випадку задає час асимптотичного затухання процесів по агрегованій макрозмінній $y$.

Застосовуючи (12) в системі (3), отримаємо:

$$T \cdot [a_{21} \cdot (p_1 + b_1 \cdot b_2^{-1} \cdot p_2) + a_{22} \cdot p_2 + b_2 \cdot u] + p_2 = 0 \quad (13)$$

Розв’язавши це рівняння відносно управляючого впливу, отримаємо закон управління у загальному вигляді:

$$u = -G_2^{-1}(x) \cdot \left[T^{-1} \cdot \phi\left(x_2 - \alpha(x_1) + f_2(x) - \frac{\partial \alpha}{\partial x_1} \cdot [f_1(x_1) + G_1(x_1) \cdot x_2]\right)\right] \quad (14)$$

при цьому

$$u = -b_2^{-1}(x) \cdot (a_{21} \cdot x_1 + (a_{21} \cdot b_1 \cdot b_2^{-1} + a_{22} + T^{-1}) \cdot x_2) \quad (15)$$

Здійснивши перехід до фізично значимих змінних простору станів, запишемо закон управління у вигляді:

$$u = -b_2^{-1}(a_{21}x_1 + (a_{22} + T^{-1}) \cdot x_2) \quad (16)$$

Отже управляючий вплив (16) формується в каналі від'ємного зворотного зв'язку по вектору станів моделі сектору безпеки і оборони. Система (1), (16) має властивості асимптотичної сталості $\Psi(t) \to 0$ при $t \to +\infty$ та має наступну інтерпретацію: невизначеність, притаманна потенційним гібридним загрозам, відіграє роль так званого "параметру порядку" [8, 9], координати, що визначають динаміку поведінки системи, до якої підлаштовуються параметри ризиків, пов'язані із гібридними загрозами. В умовах максимальної компенсації невизначеності ризики гібридних впливів асимптотично затухають, що відповідає досяганню мети управління системи.

## *Обговорення*

Таким чином здійснення комплексу заходів, спрямованих, на основі процесів військової стандартизації, на забезпечення взаємосумісності складових сектору безпеки і оборони України, а також міжнародних партнерів дозволить протидіяти стратегії противника щодо застосування заходів гібридної боротьби.

Слід зазначити, що отриманий вираз (16) в явному вигляді залежить від параметру , значення якого недовизначене, отже система управління має набути властивостей адаптивності стабілізації моделі (1). Це означає, що існує взаємозв'язок між невизначеністю та ризиками гібридних загроз, а також доведене існування компенсуючого впливу з боку сектору безпеки та оборони держави, при цьому завершення певного комплексу заходів по досягненню взаємосумісності не дозволить завершити процеси військової стандартизації (розроблення військових стандартів, запровадження стандартів НАТО у керівних, розпорядчих та нормативних документах). Появи нових загроз, зміни засобів, методів та сфер протистояння вимагає безперервності, ефективності, дієвості, всеохоплюючого підходу до поєднання зусиль усіх складових сектору безпеки і оборони держави в усіх процесах військової стандартизації України.

## *Висновки*

Сутність гібридної боротьби полягає у застосуванні противником впливів на різноманітні сфери життєдіяльності держави у такий спосіб, що ускладнює чи унеможливлює ідентифікацію загроз. Участь у гібридній війні означає для держави та її сектору безпеки і оборони зіткнення з асиметричними діями противника, якого складно ідентифікувати, який адаптивно застосовує комбінації конвенційних та неконвенційних методів боротьби та підсилює ефект отриманих результатів підривної діяльності через інформаційну сферу. Подальше використання результатів аналізу взаємозв'язків невизначеності та ризиків, притаманних впливу гібридних засобів представляє можливість синтезувати такий управляючий вплив, який забезпечить компенсацію (протидію) застосованим противником заходів гібридної боротьби.

Реагування сектору безпеки і оборони на виклики і загрози гібридного характеру має відбуватися у форматі компенсації впливів невизначеності та збільшення ризиків матеріальних втрат для противника. Максимального ефекту в напрямку компенсації невизначеності сектор безпеки і оборони може досягти шляхом розвитку взаємосумісності доктринальної (нормативної) бази, запровадження найкращих практик, методів, принципів та стандартів НАТО.

### *Фінансування*

Це дослідження не отримало конкретної фінансової підтримки.

### *Конкуруючі інтереси*

Автори заявляють, що у них немає конкуруючих інтересів.

### *Список використаних джерел*

1. Hoffman, F. G. (2007). Conflict in the 21st century: the rise of hybrid wars. Potomac Institute for Policy Studies, Arlington, Virginia. URL : https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf.
2. Hoffman, F. G. (2009). Hybrid Warfare and Challenges. *Joint Forces Quarterly*. Issue 52, 1st quarter. URL : https://ndupress.ndu.edu/portals/68/Documents/jfq/jfq-52.pdf.
3. Otaiku, A. A. (2018). A Framework for Hybrid Warfare: Threats, Challenges and Solutions. *Journal of Defense Management*. Volume 8, Issue 3. URL : https://www.longdom.org/open-access/a-framework-for-hybrid-warfare-threats-challenges-and-solutions-25432.html.
4. Евгений Дикий (2016). Гибридная война России: опыт Украины для стран Балтии. Литовская военная академия им. генерала Йонаса Жямайтиса, 126 с.
5. Piscitelli, A. J. (2019). “Generational Warfare” White Paper 2.0, Revised The Pittsfield C5 Congress. Pittsfield, Maine, 23-26 July 2019. https://www.academia.edu/40032381/_Generational_Warfare_White_Paper_2_0_REVISED.
6. Ризик, невизначеність і новаторство – [Електронний ресурс] – URL : https://nato.int/docu/review/ru/articles/2022/04/14/risk-neopredelennost-i-novatorstvo/index.html.
7. Гібридна війна: нові загрози, складнощі та “довіра” як антидот – [Електронний ресурс] – URL : https://nato.int/docu/review/ru/articles/2021/11/30/gibridnaya-voina-novye-ugrozy-sloyonosti-i-doverie-kak-antidot/index.html.
8. Хром’як Й.Я., Слюсарчук Ю.М., Цимбал Л.Л., Цимбал В.М. (2012). Синергетична модель управління економічною системою. Збірник наукових праць Національного університету “Львівська політехніка”. Львів, № 3, С. 233-238.
9. Никифоров О. В., Путятін В. Г. (2023). Нейромережеві моделі управління процесом функціонування систем захисту інформації. Математичні машини і системи. Харків, № 2, С. 34-43.

### *References*

1. Hoffman, F. G. (2007). Conflict in the 21st century: the rise of hybrid wars. Potomac Institute for Policy Studies, Arlington, Virginia. Available from : https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf.
2. Hoffman, F. G. (2009). Hybrid Warfare and Challenges. Joint Forces Quarterly. Issue 52, 1st quarter. Available from : https://ndupress.ndu.edu/portals/68/Documents/jfq/jfq-52.pdf.
3. Otaiku, A. A. (2018). A Framework for Hybrid Warfare: Threats, Challenges and Solutions. Journal of Defense Management. Volume 8, Issue 3. Available from : https://www.longdom.org/open-access/a-framework-for-hybrid-warfare-threats-challenges-and-solutions-25432.html.

4. Evgeniy Diky (2016). Russia's Hybrid War: Ukraine's Experience for the Baltic States. General Jonas Žemaitis Lithuanian Military Academy, 126 p.
5. Piscitelli, A. J. (2019). "Generational Warfare" White Paper 2.0, Revised The Pittsfield C5 Congress. Pittsfield, Maine, 23-26 July 2019. Available from : https://www.academia.edu/40032381/_Generational_Warfare_White_Paper_2_0_REVISED.
6. Risk, Uncertainty and Innovation – [Electronic resource] – Available from : https://nato.int/docu/review/ru/articles/2022/04/14/risk-neopredelennost-i-novatorstvo/index.html.
7. Hybrid warfare: new threats, challenges and "trust" as an antidote – [Electronic resource] – Available from : https://nato.int/docu/review/ru/articles/2021/11/30/gibridnaya-voina-novye-ugrozy-sloyonosti-i-doverie-kak-antidot/index.html.
8. Khrom'yak Y.Ya., Slyusarchuk Y.M., Tsymbal L.L., Tsymbal V.M. (2012). Synergetic model of economic system management. *Collection of scientific papers of the National University "Lviv Polytechnic"*. Lviv, No. 3, Pp. 233-238.
9. Nikiforov O.V., Putyatin V.G. (2023). Neural network models of control of the process of functioning of information protection systems. *Mathematical machines and systems*. Kharkiv, No. 2, Pp. 34-43.