DOI: 10.46299/ISG.2023.MONO.TECH.3.2.6

2.6 Методологічні засади інтелектуального управління системою національної безпеки в умовах асиметричного конфлікту

Вступ

Як слідує з результатів моделювання, характер застосування державами ресурсів у конкурентній боротьбі за контроль над ключовими точками (регіонами) буде комплексним (гібридним). Це важлива, але не єдина характеристика воєнних конфліктів. Воєнні конфлікти мають інші риси, наприклад, характер цілей, склад діючих суб'єктів, акценти в застосуванні ресурсів тощо [82-90].

Зміни у світовій економіці, фінансах, засобах комунікацій визначальним чином відображаються на природі воєнно-політичних відносин та, відповідно, сучасних воєнних конфліктів. Останнім часом багато дослідників констатували, що сучасні воєнні конфлікти набули якихось нових властивостей у порівнянні з минулими конфліктами, в яких ставка робилась на силове домінування. Акцент на певних характерних рисах конфліктів призвів до появи нових термінів, таких як "проксі-війна" [83], "гібридна війна"[84], "мережева війна"[85]. Безумовно, дослідження такого складного явища, як воєнний конфлікт, є можливим з точки зору багатьох аспектів.

За усіх часів головною рушійною силою воєнно-політичних відносин були базові довгострокові цілі воєнно-політичних сил, які знаходилися і сьогодні продовжують знаходитись переважно в економічній площині. Досягнення цих цілей здійснюється через геополітичне домінування, тобто через підпорядкування політики більш слабких держав шляхом певних компромісів або за допомогою воєнної сили.

Класичні війни. До винаходження ядерної зброї воєнні конфлікти відбувалися між державами (коаліціями держав) з рішучими політичними цілями за допомогою великих військових формувань (армій). Політичні цілі війни формулювалися державою, зокрема правлячою елітою, яка уособлювала

державу. В класичній війні держава здійснювала дії в усіх сферах, хоча головний акцент робився на військових діях.

Проксі-війни. Термін "проксі" означає замінник. Згідно цій концепції, впливові світові держави (держави-домінанти) протистоять не прямо, а через проектування воєнних конфліктів між сателітами. В якості сателітів може виступати й політично підпорядковані держави, й різнорідні внутрішні збройні формування, тобто сили, які мають політичні цілі і засоби збройного насильства. У проксі-війні саме сателіти здійснюють воєнні дії і застосовують звичайні, неядерні засоби збройного насильства. Держави-домінанти можуть брати участь у воєнному конфлікті, але обмежену, забезпечуючи сателітам економічну допомогу, поставки зброї, інформації, навчання тощо. Зазначимо, що такий тип воєнного конфлікту вимагає від держави-домінанта значних економічних і фінансових витрат, оскільки сателітами виступають як правило слабкі, нерозвинуті держави, яким важко вести війну.

Переваги проксі-війн для держав-домінантів є очевидними. Це знижений ризик ядерної війни і відвідних ударів, відсутність безпосередніх втрат серед свого населення, інфраструктури та інші. У разі програшу держава-домінант, безумовно, несе збитки, але не критичні для свого існування.

Гібридні війни. На певному етапі розвиток технологій і засобів збройної боротьби припинив надавати провідним державам можливість домінування в озброєннях. Природно, що за таких умов воєнні дії почали відсуватись на другій план, а воєнні конфлікти почали називати гібридними війнами.

В гібридних війнах держава, зокрема її правляча еліта, продовжили формулювати цілі воєнних конфліктів, але у воєнних діях стали переважати спеціальні операції, тобто дії з обмеженими локальними цілями. Головна роль у "поразці" противника була покладена на інші інструменти. Зазнали змін й політичні цілі війни. Якщо раніше "класичною" ціллю була анексія, захоплення територій або зміна уряду, то сьогодні ціллю стало примушення противника до підпорядкування або постановка під контроль його правлячої еліти.

Термін “гібридна війна” робить наголос на поєднанні широкого спектру воєнних та невоєнних інструментів. За великим рахунком, усі воєнні конфлікти є гібридними, оскільки протиборство здійснюється застосуванням усього спектру наявних інструментів.

Мережеві війни. Застосування інструментарію мережевих війн націлене на населення противника, насамперед на його дезорієнтацію і зміну світосприйняття – населення не змушують до підпорядкування, а воно само підпорядковується. Перевага надається інформаційним інструментам, зокрема інформаційно-психологічним. Винахідники нової війни виділили два її типи.

Перший тип (не насильницький) – це боротьба за права людини з метою переходу від авторитаризму до демократії, відкритого суспільства, середовище якого найбільш придатне для зовнішнього впливу.

Другий тип (насильницький) – боротьба кримінальних, терористичних, етнічних, націоналістичних формувань проти контролю з боку держави, тобто підрив державної влади як такої. У мережевій війні державою-агресором залучаються переважно внутрішні суб’єкти (партії, недержавні організації, кримінальні угруповання тощо), але не відкидаються і зовнішні (держави-сателіти, міжнародні терористичні організації).

Приватизована війна. Як й і у проксі-війні, впливові держави намагаються не вступати у безпосереднє протиборство, а використовувати інші підпорядковані сили (сателіти, замінники або прокладки). Як у мережевій війні, розмивається суб’єкт впливу на противника, використовуються внутрішні суб’єкти. Але сьогодні все ж можна виділити кілька нових моментів:

через світову фінансово-економічну кризу фінансування підпорядкованих сателітів в значних обсягах стало проблематичним;

поширилася практика застосування тероризму як головного інструменту досягнення воєнно-політичних цілей (при цьому здійснюються не окремі терористичні акти, а цілі терористичні кампанії і створюються терористичні держави як стійкі соціально-політичні утворення з ідеологією держави);

майже повністю заблоковано міжнародні інститути, які призначені для стримування агресії і вирішення конфліктів, їх перетворено на один з політико-дипломатичних інструментів;

у провідних світових державах поширилася практика формування політичної еліти держави за рахунок делегування представників великих корпорацій (економічна могутність багатьох з них може перевищувати могутність держави з населенням кілька десятків мільйонів чоловік), що призводить до витіснення національних інтересів транскордонними інтересами великого бізнесу (при цьому бізнес-групи часто залишаються невидимими для покарання);

поширилася практика залучення до участі у воєнних конфліктах суб'єктів, які важко ототожнити з державою – приватних військових компаній, незаконних збройних формувань, які керуються приховано і зовсім не обмежуються у власних діях міжнародним гуманітарним правом.

Характер війни сьогодні змінюється у напрямі приватизованих війн, які поєднують елементи усіх інших типів війн. Сучасні війни в комплексі використовують усі інструменти: політичні, економічні, інформаційні, воєнні тощо. Воєнні інструменти відходять на другій план, але не виключаються з протиборства (гібридні війни). Сучасні війни ведуться через підпорядкованих сателітів (проксі-війни) з акцентом на дезорієнтацію населення противника за рахунок множини узгоджених впливів різної природи (мережеві війни). “Приватизація війни” змінила характер суб’єкта-агресора і певним чином зміст воєнно-політичних відносин (дій). Головні зміни торкнулися витіснення держави як суб’єкта війни і заміна її інтересів інтересами великого транснаціонального бізнесу. В якості одного з головних суб’єктів впливу стали активніше використовуватись внутрішні і міжнародні терористичні формування, рівень організації, сила і стійкість яких значно підвищилися.

Враховуючи обмеженість та спрямованість нашого дослідження, автори зупиняться лише на розгляді окремої складової сучасних війн, а саме гібридних війн.

Гібридна війна є наслідком змін форм та способів збройної агресії по причині зміни принципів геополітичного устрою, розвитком наукової думки ведення збройної боротьби [91-96].

Зміни форм і способів збройної боротьби досить наглядно висвітлено з застосуванням гібридних дій в Україні, які поділялися на наступні етапи:

прихований початок війни (1 етап) в ході якої сформована опозиція діючій владі, проведена інформаційно-психологічна операція в результаті чого було здійснено перегляд цінностей військовослужбовців Збройних Сил України, які як наслідок зрадили присязі, решта військовослужбовців були деморалізовані;

ескалація (2 етап) - політичних і військових лідерів у регіонах проінформовано про конфлікт, що розвивається. РФ чинила та чинить політичний, дипломатичний чи економічний тиск на режим чи неполітичні суб'єкти;

початок конфлікту, а саме третій етап почався з більш ворожих дій сил-опонентів – демонстрацій, протестів, диверсій, саботажів, вбивств, втручання воєнізованих угруповань тощо. На цій стадії РФ почала стратегічний запуск її сил у регіони конфлікту у разі наявності стратегічного інтересу або інтересу національної безпеки;

початок військових операцій (4 етап), яким акомпанувала сильна дипломатична та економічна підтримка, разом із постійним потоком інформації, який має на меті змінити публічну думку у бік російської інтервенції.

За таких умов виникла потреба у зміні підходів до стратегічного управління системою національної безпеки. Це в свою чергу потребує використанням сучасного та апробованого математичного апарату, що здатний за короткий проміжок часу провести обробку великого масиву різнотипних даних з заданою достовірністю прийняття управлінських рішень [97-111].

Існуючі підходи з ідентифікації гібридних викликів та загроз національній безпеці держави є вузькоспрямованими та направленими на дослідження лише окремих питань і не дозволяють [97–111]:

комплексно та за короткий час ідентифікувати та оцінити гібридні виклики та загрози національній безпеці;

проводити обробку різнотипних даних з різними одиницями виміру, різних за походженнями та джерелами добування інформації;

виявити нові та не типові гібридні виклики та загрози національній безпеці, а також провести оцінку ступеню їх деструктивного впливу.

Все це потребує перегляду підходів до ідентифікації викликів і загроз національній безпеці держави із застосуванням гібридних дій та пошуку нових підходів до-управління системою національної безпеки.

Враховуючи зазначене, ***метою даного дослідження*** є розробка методологічних засад інтелектуального управління системою національної безпеки в умовах асиметричного конфлікту.

Структурно та логічно зазначене дослідження складається з наступних частин:

методики ідентифікації викликів і загроз національній безпеці держави на основі штучної імунної системи;

методики комплексного аналізу та багатовимірного прогнозування стану системи національної безпеки;

методики пошуку рішень на основі алгоритму зозулі;

синтезу інтелектуальної системи управління національною безпекою;

архітектури інформаційної системи з застосуванням запропонованої методології.

Виклад основного матеріалу дослідження

2.6.1 Методика ідентифікації викликів і загроз національній безпеці держави на основі штучної імунної системи

Методи штучного інтелекту активно застосовується в багатьох сферах людської діяльності. Системи управління національною безпекою держави не стали цьому виключенням. Разом з тим, враховуючи велику кількість викликів та загроз національній безпеці держави, постійний та стрімкий розвиток інформаційних технологій виникають проблемні питання, що пов’язані з

ідентифікацією деструктивного впливу на систему національної безпеки держави, якими є гібридні виклики та загрози [112–121].

Використання систем штучного інтелекту в інтересах забезпечення національної безпеки держави дозволить особам, які їх приймають рішення, підвищити оперативність та достовірність. Виявити та ідентифікувати деструктивний вплив в умовах гібридних викликів та загроз національній безпеці держави є досить складним питаннями. В зазначеному дослідженні під навмисним деструктивним впливом на систему національної безпеки будемо розуміти:

інформаційні повідомлення, направлені на дискредитацію керівництва держави;

кібернетичні атаки, спрямовані на відмову від обслуговування;

заходи не прямого деструктивного впливу на систему національної безпеки;

кібернетична розвідка, спрямована на збір інформації про керівництво держави та сектору безпеки і оборони.

Застосування методів штучного інтелекту в готовому вигляді для виявлення та ідентифікації деструктивного впливу на систему управління національною безпекою не є ефективним. Це не дозволяє виявити нові виклики та загрози національній безпеці держави, провести їх ідентифікацію і, як наслідок, оперативно прийняти рішення відповідними особами що їх приймають.

Для ідентифікації викликів і загроз національній безпеці гібридного впливу пропонується провести розробку методики ідентифікації викликів і загроз національній безпеці держави на основі штучної імунної системи.

Дія 1. Введення вихідних даних про систему національної безпеки.

Дія 2. Ініціалізації математичної моделі виявлення та ідентифікації гібридних викликів і загроз національній безпеці, яка описується:

$$AISEA = \langle D_\tau, D_M, S_A, S_N, G, R, \Psi \rangle, \quad (1)$$

де $D_\tau \subset D$ – сукупність детекторів для ідентифікації гібридних викликів та загроз національній безпеці;

D_M – набір детекторів пам'яті, в які здійснюється запис гібридних викликів та загроз національній безпеці;

$S_A \subset S$ – навчальна вибірка, що складається з набору відомих викликів і загроз національній безпеці держави;

$S_N \subset S$ – тестова множина, що складається з сукупності нормальних параметрів функціонування системи національної безпеки держави;

$D = D_\tau \bigcup D_M$ – набір детекторів, які використовуються для виявлення та ідентифікації викликів і загроз гібридного характеру національній безпеці держави;

$G = \{G_1, ..., G_K\}$ – стратегії оптимізації детекторів виявлення та ідентифікації загроз національній безпеці;

$R: D \times 2^{S_A} \times 2^{S_N} \times G \to D$ – правила навчання детекторів виявлення та ідентифікації викликів і загроз національній безпеці держави;

S – набор можливих вхідних подій, $\Psi: D \times S \to \square_+$ – функція обчислення правила відповідності між детектором $d \in D$ та тестовим показником $s \in S$, де $\square_+ = \square \bigcap [0, +\infty)$.

Кожен детектор для виявлення та ідентифікації гібридних викликів і загроз національній безпеці держави із множини $d \in D$ описується як кортеж наступного виду:

$$d = \langle representation, threshold, life\_time, state \rangle, \quad (2)$$

де $representation \in \{BitString, RealVector, NeuralNetwork, PetrNet..., \}$ –внутрішня структура детектора *d* для виявлення та ідентифікації гібридних викликів і загроз національній безпеці держави;

$threshold \in \square_+$ – поріг активації детектора *d* для виявлення та ідентифікації гібридних викликів і загроз національній безпеці держави;

$life\_time \in \square_+$ – термін дії детектора *d* для виявлення та ідентифікації гібридних викликів і загроз національній безпеці держави;

$state \in \{immature, semimature, mature, memory\}$ – поточний стан детектора.

Дія 3. Визначення корегувального коефіцієнту на ступінь інформованості про сили та засоби деструктивного впливу на систему національної безпеки держави. Ступінь інформованості може бути: повна невизначеність, часткова невизначеність, повна обізнаність.

Дія 4. Вибір внутрішньої структури кожного детектора $d \in D : representation$. Розрахунок для кожного детектора $d \in D$ значення його активації $a_d = \Psi(d, s) - threshold$, тобто переходу з неактивного стану в активний. Вважається, що якщо $a_d \geq 0$, то детектор d є активованим, інакше відповідний детектор не реагує на вхідні дані.

Дія 5. Формування навчального набору даних S_A, що містить заздалегідь відібрані гідридні виклики і загрози національній безпеці держави.

Дія 6. Формування тестового набору даних S_N, що містить заздалегідь відібрані гідридні виклики і загрози національній безпеці держави, які вдалося ідентифікувати та є в пам'яті детектора.

Дія 7. Вибір стратегії генетичної оптимізації імунних детекторів.

Дія 8. Навчання R імунних детекторів D.

Дія 9. Вибір правила відповідності Ψ між імунним детектором та вхідним об'єктом.

Кінець алгоритму.

2.6.2 Розробка методики комплексного аналізу та багатовимірного прогнозування стану системи національної безпеки

Методика комплексного аналізу та багатовимірного прогнозування стану системи національної безпеки складається з такої послідовності дій (рис. 1).

1. Введення вихідних даних (дія 1 на рис. 1). На даному етапі вводяться наявні вихідні дані про систему національної безпеки, що підлягає аналізу. Також відбувається ініціалізація базової моделі стану системи національної безпеки.

2. Оброблення вихідних даних з урахуванням невизначеності

(дія 2 на рис. 1).

На даному етапі відбувається врахування типу невизначеності про стан системи національної безпеки та проводиться ініціалізація базової моделі стану системи [121-131]. При цьому ступінь невизначеності може бути: повна інформованість; часткова невизначеність та повна невизначеність.

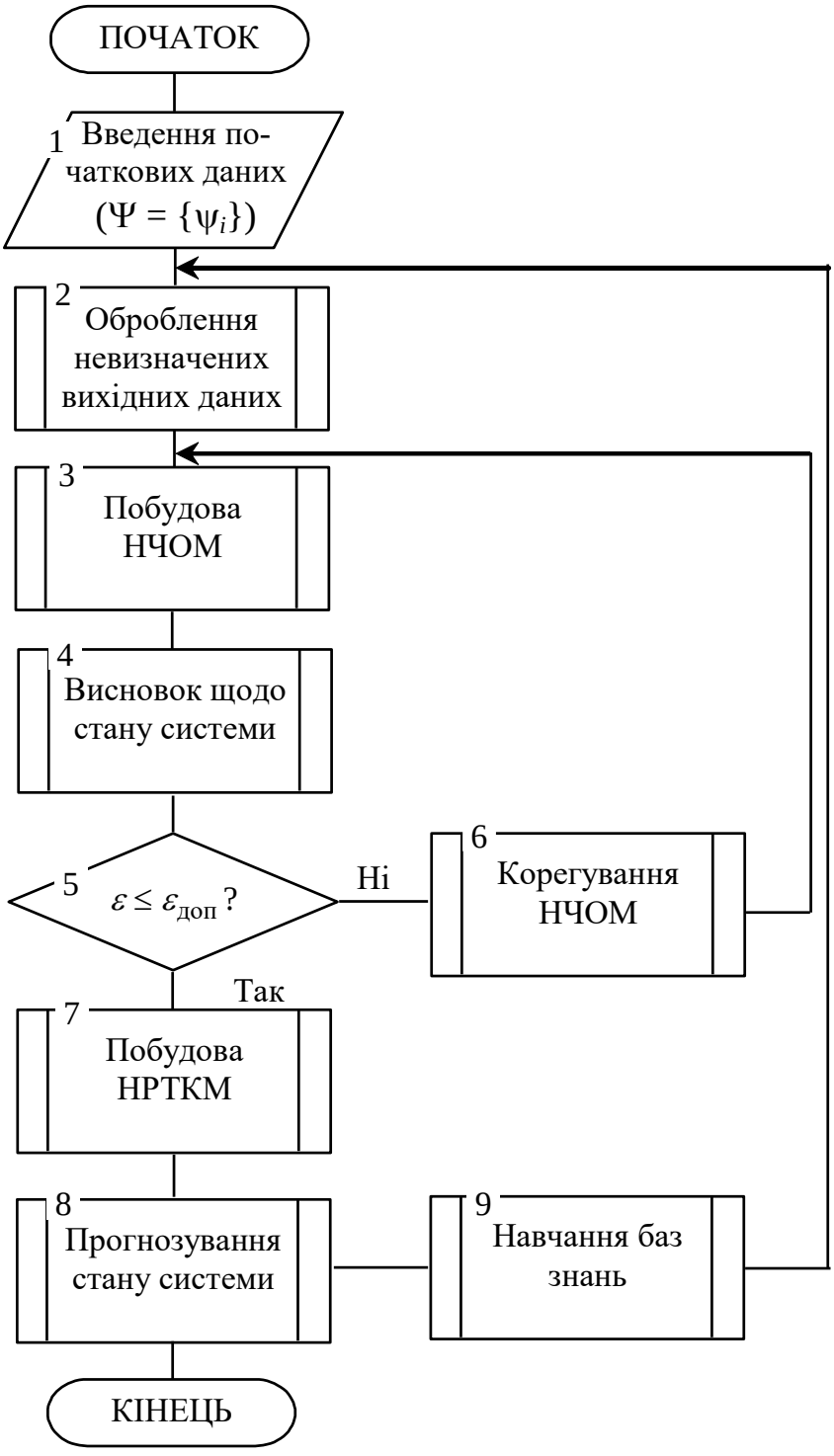

Рис. 1. Алгоритм реалізації методики аналізу стану системи управління системою національної безпеки

3. Побудова нечіткої темпоральної онтологічної моделі стану системи національної безпеки (дія 3 на рис. 1).

При поданні слабоструктурованих інформаційних ресурсів про стан складних систем використовуються методи нечіткого онтологічного моделювання з можливістю відображення динаміки зміни атрибутів [132−135]. Водночас застосовувані методи не враховують можливості завдання та фіксації взаємовпливу атрибутів між собою з різними часовими лагами (інтервалами затримки).

Для представлення, комплексного аналізу та відображення динаміки зміни стану системи національної безпеки пропонується процедура побудови нечіткої темпоральної онтологічної моделі.

Особливістю запропонованої процедури є те, що атрибути, що відповідають параметрам її векторного простору, а також показникам стану, характеризуються часовими рядами відповідних чітких/нечітких значень, отриманих вимірювань/оцінок, і на основі їх багатовимірного прогнозування.

При цьому нечітка грануляція онтологічної моделі стану системи національної безпеки виконується на рівні нечітких значень часових рядів цих атрибутів. Крім того зазначена дія виконується на рівні нечітких значень бінарних відносин взаємовпливу між атрибутами цієї моделі з різними часовими лагами.

Атрибутами онтологічної моделі стану системи національної безпеки, які є носіями діагностичної інформації про стан системи національної безпеки, служать нормовані параметри матриць Гріна:

$$G = \begin{vmatrix} C_1 & C_4 & C_3 \\ C_1 & C_2 & C_5 \\ C_6 & C_2 & C_3 \end{vmatrix}, \qquad (3)$$

де C_1, C_2, C_3 – параметри, що характеризують реакцію системи національної безпеки на впливи за трьома симетрично розташованими осями робочої ділянки векторного простору системи національної безпеки;

C_4, C_5, C_6 – параметри, що характеризують реакцію системи національної безпеки та ті ж самі впливи по осі ортогональної робочої ділянки системи національної безпеки.

У запропонованій нечіткій темпоральній онтологічній моделі передбачено подання динаміки зміни параметрів, що розглядаються, у вигляді значень компонентних часових рядів, що утворюють багатовимірний часовий ряд:

$$C = \left\{ C_i \middle| i = 1,...,I \right\},$$

$$C_i = \left\{ \tilde{c}_i(t) \middle| t = 1,...,T,... \right\}, i = 1,...,I,$$

$$\forall t \in \{1,...,T,...\}$$

$$\tilde{C}(t) = \left\{ \begin{array}{l} \tilde{c}_1(t) = F_1\left(\phi_{1,1}\left(\tilde{c}_1(t-1),...,\tilde{c}_1\left(t-L_1^1\right)\right),...,\phi_{1,I}\left(\tilde{c}_I(t),...,\tilde{c}_I\left(t-L_1^I\right)\right)\right), \\ \tilde{c}_i(t) = F_i\left(\phi_{i,1}\left(\tilde{c}_1(t-1),...,\tilde{c}_1\left(t-L_i^1\right)\right),...,\phi_{i,I}\left(\tilde{c}_I(t),...,\tilde{c}_I\left(t-L_i^I\right)\right)\right), \\ \tilde{c}_I(t) = F_I\left(\phi_{I,1}\left(\tilde{c}_1(t-1),...,\tilde{c}_1\left(t-L_I^1\right)\right),...,\phi_{I,I}\left(\tilde{c}_I(t),...,\tilde{c}_I\left(t-L_I^I\right)\right)\right), \end{array} \right\}, \quad (4)$$

де C – багатовимірний часовий ряд, що характеризує векторний простір стану системи національної безпеки;

C_i – компонентний (одномірний) часовий ряд багатовимірного часового ряду стану системи національної безпеки;

I – число врахованих компонентів багатовимірного часового ряду (аналізованих атрибутів онтологічної моделі стану системи національної безпеки);

$\tilde{C}(t) = \left\{ \tilde{c}_1(t),...,\tilde{c}_I(t) \right\}$ – "часовий зріз" нечітких значень багатовимірного часового ряду в t-й момент часу;

$\tilde{c}_i(t)$ – нечітке значення C_i у момент часу t; L_j^i – максимальний часовий лаг, що враховується (інтервал затримки) $\tilde{c}_j(t)$ щодо $\tilde{c}_i(t)$; ϕ_{ij} – оператор для врахування впливу $\left\{ \tilde{c}_j(t-1),...,\tilde{c}_j\left(t-L_j^i\right) \right\}$ на $\tilde{c}_i(t)$; F_i – перетворення для обчислення $\tilde{c}_i(t)$.

4. Висновок щодо стану системи національної безпеки (дія 4 на рис. 1).

На підставі побудові нечітких темпоральних онтологічних виразів робиться висновок щодо стану системи національної безпеки.

Крім розглянутого вище подання та відображення динаміки стану системи національної безпеки з використанням процедури в дії 3 на рис. 1, потрібно вирішити наступні завдання:

– розробити модель та провести моделювання та прогнозування багатовимірного часового ряду, компоненти якого відповідають параметрам векторного простору стану системи національної безпеки;

– здійснити прогнозну оцінку стану на основі результатів прогнозування багатовимірного часового ряду, що відповідає багатовимірному векторному простору стану системи національної безпеки;

– виконувати моніторинг та адаптацію моделі прогнозування багатовимірного часового ряду з урахуванням змін фактичних даних у ході застосування стану системи національної безпеки.

5. Корегування НЧОМ (дії 5,6 на рис. 1).

Адаптація НЧОМ полягає в структурно-параметричному налаштуванні (часових лагів та значень нечітких відносин взаємовпливу концептів) з метою забезпечення необхідної точності моделювання та багатовимірного прогнозування параметрів векторного простору стану системи національної безпеки з урахуванням накопичуваних даних про їх при зміні зовнішніх факторів. В якості методу налаштування використовуються удосконалений алгоритм кошачої зграї. Перевагами еволюційного коригування параметрів НЧОМ є такі:

– незалежність від топології НЧОМ;

– можливість визначення, чи показує дана особина низьку пристосованість через невдало сформовану топологію або неправильно підібраних ваг;

– вибіркова оптимізація параметрів нещодавно змінених або доданих зв’язків в НЧОМ без зміни вже модифікованої на попередні ітераціях роботи алгоритму структури.

6. Побудова нечіткої реляційної темпоральної когнітивної моделі стану системи національної безпеки та прогнозування її стану (дії 7, 8 на рис. 1).

У даному дослідженні для багатовимірного прогнозування параметрів векторного простору стану системи національної безпеки пропонується вдосконалена нечітка реляційна темпоральна когнітивна модель що дозволяє типізувати налаштування операторів ϕ_{ij} та перетворень $F(i,j=1,\ldots I)$ за рахунок:

–по-перше, "персоніфікації" моделей системної динаміки (для кожної пари безпосередньо взаємодіючих концептів – параметрів векторного простору системи);

–по-друге, налаштування нечітких відносин впливу між концептами на основі алгоритмів навчання з використанням сформованих навчальних вибірок для компонентних рядів часових багатовимірного часового ряду;

–по-третє, обчислення залежностей між нечітко заданими параметрами у векторно-матричному вигляді.

Запропонований різновид нечіткої реляційної темпоральної когнітивної моделі (НРТКМ) представляється в наступному вигляді:

$$FRTCM = \langle C, R \rangle,$$

$$C = \left\{ C_i \middle| i = 1,...,I \right\},$$

$$R = \left\{ R_i \middle| i = 1,...,I \right\},$$

$$R_i = \left\{ \tilde{r}_{ij}(t-l) \middle| l = 0,...,L_j^i,\ j = 1,...,J^i \right\},$$

$$c_i : \tilde{c}_i(t) = \tilde{F}_i \left(\begin{array}{c} \left\{ \tilde{c}_i(t-k), \tilde{r}_{ii}(t-k) \middle| k = 1,...,L_i^i \right\}, \\ \left\{ \tilde{c}_j(t-l), \tilde{r}_{ii}(t-l) \middle| j = 1,...,J^i, l = 1,...,L_j^i \right\} \end{array} \right), i = 1,...,I. \qquad (5)$$

де C – множина концептів НРТКМ; I – число концептів НРТКМ; R – множина нечітких відносин впливу концептів один на одного;

R_i – підмножина нечітких бінарних відносин впливу концептів, що безпосередньо впливають на концепт c_i; J^i – число концептів, безпосередньо впливають на концепт c_i;

$\tilde{r}_{ij}(t-k)$ – нечітке відношення впливу концепту c_i на себе у момент часу (t–k); L_i^i – максимальне значення часового значення лага (інтервалу затримки) при впливі концепту c_i на себе; $\tilde{r}_{ij}(t-l)$ – нечітке відношення впливу концепту c_j на концепт c_i у момент часу (t–l);

L_j^i – максимальне значення часового лага (інтервалу затримки), що враховується при впливі концепту c_j на концепт c_i; $\tilde{c}_i(t), \tilde{c}_i(t-k), \tilde{c}_j(t-l)$ – нечіткі значення ня концептів c_i і c_j у відповідні моменти часу.

При багатовимірному прогнозуванні параметрів векторного простору стану системи національної безпеки кращим є використання нечітких композиційних правил передачі впливу між концептами НРТКМ, відповідно до яких моделі системної динаміки набудуть наступного вигляду:

$$\tilde{c}_i(t) = \bigoplus_{j=1}^{J^i}\left(\bigoplus_{l=1}^{L_j^i}\left(\tilde{c}_j(t-l)\circ\tilde{r}_{ij}(t-l)\right)\right),$$

$$\tilde{c}_i(t) = \left(\bigoplus_{k=1}^{L_j^i}\left(\tilde{c}_i(t-k)\circ\tilde{r}_{ij}(t-k)\right)\right)\oplus\left(\bigoplus_{j=1}^{J^i}\left(\bigoplus_{l=1}^{L_j^i}\left(\tilde{c}_j(t-l)\circ\tilde{r}_{ij}(t-l)\right)\right)\right), \quad (6)$$

$$\tilde{c}_i(t) = \left(\bigoplus_{k=1}^{L_j^i}\left(\Delta\tilde{c}_i(t-k)\circ\tilde{r}_{ij}(t-k)\right)\right)\oplus\left(\bigoplus_{j=1}^{J^i}\left(\bigoplus_{l=1}^{L_j^i}\left(\Delta\tilde{c}_j(t-l)\circ\tilde{r}_{ij}(t-l)\right)\right)\right),$$

де $\Delta\tilde{c}_i(t-k)$ – нечітке збільшення значення концепту C_i у момент часу (t–k); $\Delta\tilde{c}_j(t-l)$ – нечітке збільшення значення концепту C_i у момент часу (t–l); $\circ$ – операція нечіткої композиції; $\bigoplus_{k=1}^{L_j^i}$ – операція нечіткого агрегування окремих впливів концепту c_i на самого себе в діапазоні, часового лага, які враховуються $\left(k=1,...,L_i^i\right)$; $\bigoplus_{l=1}^{L_j^i}$ – операція нечіткого агрегування окремих впливів концепту c_i на концепт c_j в діапазоні часового лага, який враховується $\left(l=1,...,L_j^i\right)$; $\bigoplus_{j=1}^{J^i}$ – операція нечіткого агрегування окремих впливів концептів c_j (j=1,…, J^i), безпосередньо впливають на концепт c_i; $\oplus$ – операція нечіткого агрегування сукупних впливів.

Для визначення діапазонів часових лагів L_i^i та L_j^i при взаємовпливі концептів, при впливі нечітких відносин взаємовпливу $\tilde{r}_{ii}(t-k)$, $\tilde{r}_{ij}(t-l)$ з підмножин R_i (i=1,…, I) є значущим, а також для налаштування цих відносин використовуються статистичні (експертні) методи. Так, за наявності навчальних вибірок у компонентів багатовимірного часового ряду для визначення нечітких відносин взаємовпливу застосуємо метод нечіткої множинної лінійної регресії:

$$\tilde{c}_i(t) = \sum_{j=1}^{J^i} \sum_{l}^{L_j^i} \left(\tilde{a}_{ij}(t-l)\tilde{c}_j(t-l) + \tilde{b}_{ij}(t-l) \right), i = 1,..., I. \quad (7)$$

де $\tilde{a}_{ij}(t-l)$ – нечіткі регресійні коефіцієнти; $\tilde{b}_{ij}(t-l)$ – нечіткі вільні члени (як правило, рівні 0).

Отримані значення нечітких регресійних коефіцієнтів $\tilde{a}_{ij}(t-l)$ нормуються $\tilde{a}_{ij}^{`}(t-l)$ у діапазоні [81, 82]. І таким чином, на їх основі задаються підмножини $R_i = \left\{ \tilde{r}_{ij}(t-l) = \tilde{a}_{ij}^{`}(t-l) \middle| l = 0,..., L_j^i, j = 1,..., J^i \right\}$ нечітких відносин взаємовпливу концептів НРТКМ. Потім виключаються ті відносини, модальні значення яких менші за заданий поріг (наприклад, менше 0,1).

Результати моделювання та багатовимірного прогнозування параметрів векторного простору стану системи національної безпеки з використанням НРТКМ є підставою для прогнозної оцінки стану системи національної безпеки.

9. Навчання баз знань (дія 9 на рис.1).

В зазначеному дослідженні для навчання баз знань використовується розроблений у дослідженні [83] метод навчання на основі штучних нейронних мереж, що еволюціонують.

Кінець алгоритму.

2.6.3 Удосконалена методика пошуку рішень на основі алгоритму зозулі

2.6.3.1 Опис базового алгоритму зозулі

В якості базового алгоритму зозулі розглянуто отриманий в роботі [104] алгоритм зозулі.

У загальній постановці розглядаємо детерміноване безперервне завдання глобальної умовної мінімізації:

$$\min_{X \in D \subseteq R^{|X|}} f(X) = f(X^*) = f^*, \quad (8)$$

де $f(X)$ – скалярна цільова функція (критерій оптимальності);

$f(X^*)=f^*$ – мінімальне значення цільової функції;

$X=(x_1, x_2, \ldots, x_{|X|})$ – $|X|$-мірний вектор параметрів, що змінюються, яке необхідно знайти;

D – множина допустимих значень цього вектору;

$R^{|X|}$ – $|X|$-мірний арифметичний простір.

Алгоритм зозулі орієнтований для вирішення завдання безумовної оптимізації, коли $D = R^{|X|}$. Кожне яйце в гнізді є рішенням, а яйце зозулі представляє собою нове рішення. Мета полягає у використанні нового і потенційно кращого рішення (імітація поведінки зозулі), щоб замінити не? неприйнятні рішення в гніздах. У найпростішій формі у кожному гнізді знаходиться по одному яйці. Алгоритм може бути розширений на більш складний випадок, коли в кожному з гнізд знаходиться кілька яєць, що представляють деяку сукупність потенційних рішень.

Алгоритм зозулі ґрунтується на трьох наступних правилах:

1. Кожна зозуля відкладає одне яйце за один раз і підкладає його в гніздо, яке вибирається випадковим чином.

2. Найкращі гнізда з яйцями високої якості переходять у наступне покоління.

3. Число доступних гнізд фіксоване і яйце зозулі може бути виявлено господарем із ймовірністю $p_a \epsilon (0,1)$. Виявлення впливає на деякий набір найгірших гнізд, і виявлені рішення виключаються з подальших обчислень, а замість випадково створюється відповідне число нових рішень.

Схема канонічного алгоритму зозулі має такий вигляд:

1. Ініціалізація популяції $S(=s_i, i \epsilon [1:|S|]$ з $|S|$ гнізд, які належать господарю гнізда, тобто визначається початкові значення компонентів векторів X_i, $i \epsilon [1:|S|]$.

2. Виконуються випадкові переміщення зозулі у просторі пошуку за допомогою польотів Леві (Lévy Flights) [114] і знаходимо її нове положення X'.

3. Випадковим чином обирається гніздо s_i,iє[1:|S|] і якщо $f(X') \langle f(X_i)$, то замінюємо яйце в цьому гнізді на яйце зозулі, тобто $X_i' = X'$.

4. З ймовірністю p_a видаляємо з популяції кілька випадково вибраних гнізд і за правилами кроку 1 будуємо таку ж кількість нових гнізд.

5. Якщо умова закінчення ітерації не виконана, переходимо до кроку 2.

При створенні нового рішення X' польоти Леві здійснюємо по формулі:

$$X' = X + A \otimes L_{|X|}(\lambda), \tag{9}$$

де $L_{|X|}(\lambda)$ – |X|-мірний вектор незалежних дійсних випадкових чисел, розподілених за законом Леві:

$$\xi(x) = x^{-\lambda}, \lambda \in (1;3), \tag{10}$$

де $\otimes$ – символ покомпонентного добутку векторів;

A=(a_1, a_2, …, $a_{|X|}$) – вектор розміру кроків; $a_j \rangle 0, j \in \left[1:|X|\right]$.

Як правило всі компоненти останнього вектору вважають однаковими та рівними a, де величина a має бути пов’язана з масштабами ділянки пошуку.

Більшість популяційних алгоритмів глобальної оптимізації використовують міграційний оператор виду (9), але рівномірний чи нормальний розподіл величини кроку.

Польоти Леві є одним із варіантів випадкових блукань, коли для визначення випадкової довжини кроку використовується розподіл Леві (10), що має довгий, повільно спадаючий “хвіст”. Різні дослідження показують, що багато птахів і комах у процесі польоту демонструють типові характеристики польотів Леві. Поведінка людини, наприклад, мисливця-збирача, також показує риси польотів Леві. Одним із найефективніших алгоритмів чисельної генерації псевдовипадкових чисел, розподілених за законом Леві, є алгоритм Мантенья *(Mantegna)* [89].

В канонічному алгоритмі зозулі при ініалізації встановлюють фіксовані значення параметрів p_a та a, що не змінюються зі зростанням числа поколінь. Однак, якщо значення p_a мале, а значення a велике, то може бути повільна збіжність алгоритму. Навпаки, якщо значення p_a велике, а значення a мале, то

швидкість збіжності алгоритму, як правило, висока, але низька можливість локалізації глобального мінімуму цільової функції (алгоритм може “застрягти” в локальному мінімумі).

2.6.3.2 Алгоритм реалізації удосконаленої методики пошуку рішень на основі алгоритму зозулі

Методика пошуку рішень на основі удосконаленого алгоритму зозулі складається з такої послідовності дій (рис. 2).

1. Введення вихідних даних. На даному етапі вводяться вихідні дані, про стан системи національної безпеки, що підлягає аналізу, відбувається ініціалізація популяції $S(=s_i, i\in[1:|S|]$ з $|S|$ гнізд, які належать господарю гнізда, тобто визначається початкові значення компонентів векторів X_i, $i\in[1:|S|]$.

2. Оброблення вихідних даних з урахуванням невизначеності (додаткова процедура).

На даному етапі відбувається врахування типу невизначеності про стан системи національної безпеки та проводиться ініціалізація базової моделі стану системи національної безпеки [83, 100, 102]. При цьому ступінь невизначеності може бути: повна інформованість; часткова невизначеність та повна невизначеність. Це передбачає різну можливість виявлення “хороших” і “поганих” гнізд.

Якщо рішення в гнізді “хороше”, то ймовірність руйнування цього гнізда має бути низькою. Навпаки, можливість руйнування гнізд з “поганими” рішеннями слід підвищувати. Для реалізації зазначеної ідеї на ітерації n здійснюється сортування гнізд по зростанню відповідних значень цільової функції (зменшення якості рішень) та присвоюємо їм номери від 1 до $|S|$. Ймовірності виявлення гнізда з номером i надаємо значення $p_a(i) = p_a^{best}, p_a^{worst}$ – вільні параметри модифікації.

3. Врахування типу зашумленості даних про стан системи національної безпеки (додаткова процедура).

На даному етапі відбувається врахування типу зашумленості даних про стан системи національної безпеки. При цьому ступінь замумленості може бути: повна; часткова та повна зашумленість. Коригувальні коефіцієнти наведені в роботі [83].

4.Коригування моделі стану системи національної безпеки (додаткова процедура).

Коригування значень вільних параметрів p_a та a в процесі ітерації за формулами:

$$p_a(t) = p_a^{\max} - \frac{t}{\hat{t}}\left(p_a^{\max} - p_a^{\min}\right), \tag{11}$$

$$\alpha(t) = \alpha^{\max} \exp\left(c^t\right), \tag{12}$$

де t – номер покоління, $p_a^{\min}, p_a^{\max}, a^{\min}, a^{\max}$ – задані постійні значення, $\hat{t}$ – максимально допустима кількість поколінь:

$$c = \frac{1}{\hat{t}} 1n\left(\frac{a^{\min}}{a^{\max}}\right). \tag{13}$$

Ймовірність p_a видалення з популяції найгірших гнізд зі зростанням номера покоління спадає від величини $p_a^{\max}$ до величини $p_a^{\min}$, а довжина кроку α експоненційно убуває від $a^{\max}$ до $a^{\min}$.

5. Зменшення ймовірності виявлення гнізд та зменшення довжини кроку (оптимізована процедура канонічного алгоритму зозулі).

$$\alpha = \alpha^{\min} + \left(\alpha^{\max} - \alpha^{\min}\right)\eta^t, \tag{14}$$

де $\eta\epsilon(0,1)$ – коефіцієнт згасання, який дозволить дослідити межі мінімуму і тим самим підвищити точність його локалізації.

Суть цієї процедури полягає в тому, що за формулою, аналогічній формулі (14), з ростом номеру покоління t зменшується ймовірність виявлення гнізд:

$$p_a = p_a^{\min} + \left(p_a^{\max} - p_a^{\min}\right)\zeta^t, \zeta \in (0;1). \tag{15}$$

6. Корекція довжини кроку пошуку маршруту (додаткова процедура)

$$\alpha = \beta_b \alpha, \beta_b \in (0;1); \tag{16}$$

в іншому випадку збільшується крок за формулою:

$$\alpha = \beta_g \alpha, \beta_g \rangle 1. \tag{17}$$

7. Навчання баз знань.

З ймовірністю p_a видаляємо з популяції кілька випадково вибраних гнізд і за правилами кроку 1 будуємо таку ж кількість нових гнізд з урахуванням даних в базах знань та методу навчання. В зазначеному дослідженні для навчання баз знань використовується розроблений у дослідженні [83] метод навчання на основі штучних нейронних мереж, що еволюціонують.

Кінець роботи алгоритму.

Результати оперативності оцінювання стану системи національної безпеки наведені в табл. 1.

Таблиця 1

Результати розв’язання задачі

№ ітерації	Метод гілок та границь	Генетичний алгоритм	Гармонійний пошук	Удосконалений алгоритм зозулі
N	*T*, с	*T*, с	*T*, с	*T*, с
5	1,125	1,125	1,125	1,114
10	0,625	0,625	0,625	0,600
15	48,97	58,20	58,28	57,71
20	106,72	44,29	43,75	46,95
30	–0,1790	–0,0018	–0,0002	–0,0001
40	–0,158	–0,070	–0,069	–0,049
50	97,76	–974,30	–3,72	–334,11
100	–133,28	–195,71	–196,24	–193,04
200	**7980,89**	**7207,49**	**7198,43**	**7036,48**

Як видно з табл. 1, виграш зазначеної методики пошуку рішень складає від 11 до 15 % по критерію оперативності обробки даних.

Перевага зазначеної методики в порівнянні з відомими полягає в зменшенні обчислювальної складності, що в свою чергу підвищує оперативність прийняття рішень відносно стану системи національної безпеки.

У табл. 2 представлені порівняльні результати оцінки оперативності навчання штучних нейронних мереж, що еволюціонують, що використовуються на 7 кроці роботи алгоритму зозулі.

Таблиця 2

Порівняльні результати оцінки оперативності навчання штучних нейронних мереж, що еволюціонують

Система	Параметри алгоритму	XB (Індекс Ксі-Бені)	Час, сек
FCM (Fuzzy C-Means)	–	0.2104	3.15
EFCM	Dthr=0.30	0.1218	0.175
EFCM	Dthr=0.23	0.1262	0.21
Запропонована система (пакетний режим)	delta=0.1	0.1	0.32
Запропонована система (online режим)	delta=0.1	0.098	0.2

Перед навчанням ознаки спостережень були нормалізовані на інтервалі [81, 82].

Дослідження показало, що зазначена процедура навчання забезпечує в середньому на 10–18 % більшу високу ефективність навчання штучних нейронних мереж та не накопичує помилок в ході навчання (табл. 2).

Зазначені результати видно з результатів в останніх строках табл. 2, як різниця індексу Ксі-Бені. Разом з тим, як вже було зазначено, в ході роботи відомі методи накопичують похибки, саме тому в запропонованій методиці запропоновано використання штучних нейронних мереж, що еволюціонують.

Результати проведеного оцінювання збігаються в окремих випадках з результатами досліджень [83-88, 104-107, 119]

За результатами порівняльної оцінки (табл. 1, 2) можна зробити висновок що сумарний виграш удосконаленої методики складає від 21 до 28 % по критерію оперативності прийняття рішення за рахунок використання додаткових та удосконалених процедур:

навчання баз знань;

зменшення ймовірності виявлення гнізд та зменшення довжини кроку (оптимізована процедура канонічного алгоритму зозулі);

оброблення вихідних даних з урахуванням невизначеності (додаткова процедура);

врахування типу зашумленості даних про стан системи (додаткова процедура);

коригування моделі стану системи (додаткова процедура);

корекція довжини кроку пошуку маршруту (додаткова процедура).

2.6.4 Синтез інтелектуальної системи стратегічного управління національною безпекою

Досягнення потрібного рівня національної безпеки обов’язково передує створенню максимально ефективної системи, бо вони є “обмеженнями” для подальшого коректного вирішення задачі її оптимального параметричного синтезу. Оцінка рівня національної безпеки є просто її констатацією; для висновку щодо можливості протидіяти гібридним загрозам та викликам сьогодення необхідно, по-перше, провести порівняння наявного стану з потрібним, який попередньо треба визначити, і, по-друге, наявні можливості системи національної безпеки не будуть точно відповідати потрібним, що призводить до зниження рівня національної безпеки Зрозуміло, що при цьому про максимальну ефективність функціонування системи національної безпеки взагалі не йдеться.

Процес “застосування” складної системи (одна з основних її ознак) є максимально ефективною реалізацією її системного “потенціалу здатності” для досягнення системної мети. Обраний варіант застосування рівня системи національної безпеки є також обмеженням для оптимізаційної задачі оптимального параметричного синтезу максимально ефективної системи національної безпеки.

Максимально ефективне застосування системи національної безпеки за призначенням пов’язане, як то доведене, з доцільним використанням “внутрішнього” ресурсу системи.

З іншого боку, створення та вдосконалення складних “систем” (особливо – “великої” системи національної безпеки) пов’язані з використанням величезних різнорідних ресурсів (фінансові, трудові, матеріальні і ресурси спеціального і загального призначення, інформаційні ресурси, тощо). Максимальна доцільність (ефективність) використання “зовнішніх” ресурсів для системи національної безпеки також може бути досягнута тільки оптимальним розподілом витрат ресурсів по заходах створення і вдосконалення.

Діяльність у сфері національної безпеки на науковій основі, коли методологічним підґрунтям є “системний” підхід, об’єктивно визначає теоретичні основи державного управління, дослідження операцій та кібернетику передбачає необхідний фах керівника і науковця. Взагалі основи теорії оптимальних рішень є обов’язковою умовою потрібного сучасного рівня фаху як науковців, так і осіб, що займають керівні посади державного управління. Така вимога, нарешті, повинна бути забезпечена відповідною підготовкою керівних та наукових кадрів в державі і стати реальністю.

Метою системного аналізу є всебічне вивчення системи національної безпеки, а саме:

з’ясування системних ознак системи (визначення змісту їх “фреймів”);

виявлення і оцінка властивостей системи;

визначення характеристик системи для оцінки його фактичних можливостей.

Загальна концепція системного аналізу системи національної безпеки надана на рис.2.

Рис.2. Загальна концепція системного аналізу системи національної безпеки

Системний аналіз дозволяє визначити закони функціонування об’єктів “складної системи” та закономірності, через які вони проявляються у загальносистемних характеристиках. Це дозволяє формалізувати задачі синтезу “оптимальних” систем.

Метою системного синтезу є створення “потрібного” об’єкту (в нашому випадку системи національної безпеки), а саме (рис.2 – 4):

визначення потрібного змісту системних ознак;

забезпечення і оцінка потрібних властивостей;

забезпечення значень характеристик об’єкту для досягнення його потрібних можливостей.

Системний синтез дозволяє формалізувати і коректно вирішити задачі побудови “оптимальних” систем національної безпеки з потрібними загальносистемними характеристиками.

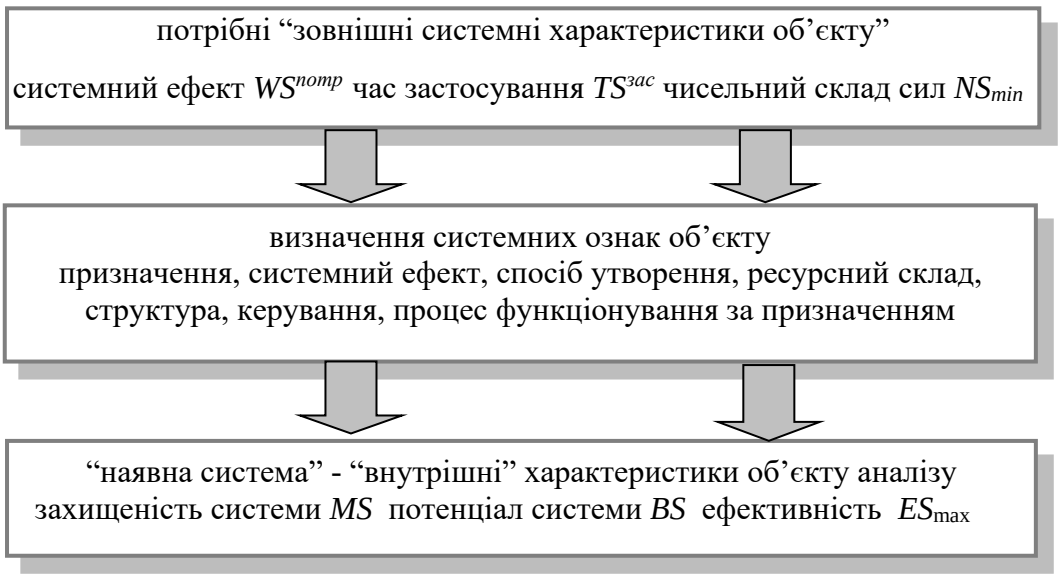

Рис.3. Загальна концепція системного синтезу системи національної безпеки

Метод операційного дослідження містить наступні етапи (рис.3):

Рис.4. Загальна концепція "операційного дослідження" системи національної безпеки

визначення мети і змістова постановка задачі дослідження системи національної безпеки;

визначення характеристик об'єкту дослідження (залежностей "ефекту" і "витрат" від системних параметрів ефективності);

визначення цільової функції і функцій обмежень, формальна постановка задачі дослідження (розробка математичної моделі системи національної безпеки);

вибір методу та вирішення задачі оптимізації системних параметрів, які максимізують ефективність об’єкта дослідження (в ношу випадку системи національної безпеки);

коригування моделі системи національної безпеки по результатах реалізації рішення.

Як було зазначено в попередній частині дослідження та враховуючи постійну появу нових видів та типів викликів і загроз національній безпеці постає необхідність проводити їх виявлення та ідентифікацію в режимі реального часу. З огляду на вищезазначене і необхідність роботи з великими масивами різнотипних даних, найбільш доцільним є використання методів теорії штучного інтелекту. Зазначене дозволить:

описати взаємозв’язки між викликами та загрозами національній безпеці держави;

провести оновлення бази даних викликів та загроз національній безпеці за рахунок процедур навчання;

виявити, ідентифікувати та оцінити ступінь викликів та загроз національній безпеці та величину їх деструктивного впливу в режимі реального часу;

вирішити проблему попадання в глобальний та локальний оптимуми та ін.

Функціонування інтелектуальної системи управління національною безпекою можна описати як постійне прийняття рішень на основі аналізу поточних ситуацій для досягнення певної мети (з урахуванням рис. 2−4).

Пропонуються наступні етапи функціонування інтелектуальних систем для управління національною безпекою держави:

1. Комплексний аналіз зовнішніх та внутрішніх викликів (загроз) національній безпеці. Результатом комплексного аналізу є створення описової моделі (сукупності моделей, комплексної моделі) рівня національної безпеки держави.

2. Порівняння отриманого комплексного опису викликів та загроз національної безпеки з наявними в базі даних викликів та загроз і поповнення цього опису.

3. Обґрунтування можливих заходів протидії викликам та загрозам національній безпеці держави.

4. Імплементація алгоритму протидії викликам та загрозам національній безпеці для реагування інтелектуальної системи управління національною безпекою на виклики і загрози національній безпеці.

5. Реалізація реакції інтелектуальної системи управління національною безпекою.

Ці дії є умовними та концептуально описують основні етапи функціонування інтелектуальних систем для протидії гібридним викликам та загрозам національної безпеки держави.

2.6.5 Архітектура інформаційної системи з використанням методологічних засад інтелектуального управління системою національної безпеки в умовах асиметричного конфлікту

Інформаційна система з використанням методологічних засад інтелектуального управління системою національної безпеки в умовах асиметричного конфлікту наведена рис. 5.

У її основі є система управління базою даних (СУБД) MySQL, підсистема серверу та підсистема клієнта.

Фізично даний комплекс програм може бути розміщений на сервері під управління будь-якої серверної операційної системи, наприклад Windows 2016 Server, Ubuntu 18.04 Server тощо.

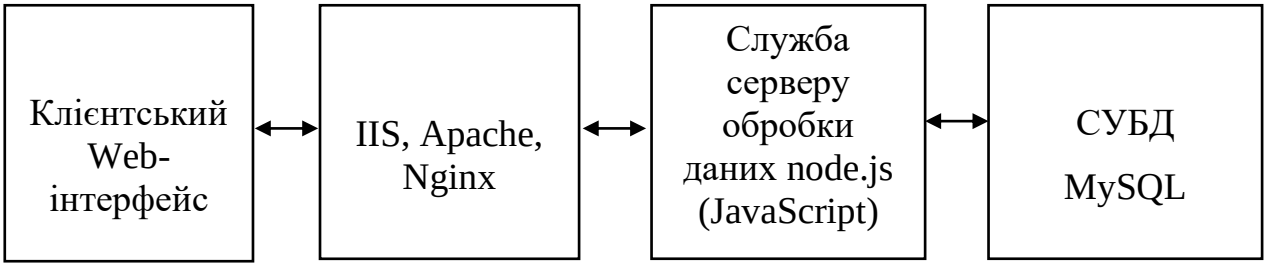

Рис. 5. Функціональна схема комплексу програм інформаційної системи управління національною безпекою

Основу системи зберігання та накопичення даних в “Озері даних” у фізичному вигляді складає СУБД MySQL. Структура таблиць СУБД MySQL цивільного контролю над сектором безпеки і оборони України складається з наступних таблиць:

– таблиця **table1** містить у собі інформацію, що отримана з відкритих джерел інформації. Крім цього у таблиці є поля для ідентифікації оператора, що ввів дані до “Озера даних” та можливі висновки, що формуються користувачем даних.

– таблиця **source1** містить у собі інформацію про кількість, та тип інформації про ресурси, які задіяні в інтересах сектору безпеки і оборони.

– таблиця **pidrozd** містить у собі поля, що дозволяють розкривати належність того чи іншого підрозділу до угруповання, а також вказувати його географічні координати за наявності.

– таблиця **order** містить у собі поля, що дозволяють аналізувати накази вищого керівництва Збройних Сил України та інших складових сектору безпеки і оборони.

– у таблиці **radmer** розміщуються різнорідні дані про інформаційну складову навколо сектору безпеки та оборони.

– таблиці **user** та **owner** створені для розділення користувачів та надання для них прав доступу до системи та моніторингу визначеної групи повідомлень.

Висновки

1. Розглянуті особливості сучасних війн визначальним чином змінюють склад елементів воєнно-політичної обстановки – розвідувальних ознак, які мають бути проаналізовані в рамках аналізу ВПО з метою оцінки можливості початку війни. Одним з головних висновків, який має бути зроблений з аналізу характеру можливих воєнних конфліктів, є те, що сучасна держава не має єдиного органу, який би мав повний спектр інструментів, достатніх для протиборства у сучасних воєнних конфліктах. Це значно підвищує важливість адекватної оцінки ВПО, своєчасного виявлення воєнних загроз, а також висуває підвищені вимоги до якості державного управління і координації дій держаних органів.

Оскільки сучасні воєнні конфлікти набувають нового характеру, аналіз ВПО також має змінювати свій зміст і методи. Зміна характерних рис сучасних воєнних конфліктів і воєнно-політичних відносин висуває нові акценти, на які потрібно звернути увагу під час аналізу ВПО, визначає нові елементи ВПО, які потрібно проаналізувати, щоб забезпечити адекватність результатів аналізу.

2. В ході зазначеного дослідження авторами запропоновані методологічні засади інтелектуального управління системою національної безпеки в умовах асиметричного конфлікту, що складається з наступних взаєпов’язаних складових:

методика ідентифікації викликів і загроз національній безпеці держави на основі штучної імунної системи;

методика комплексного аналізу та багатовимірного прогнозування стану системи національною безпеки;

методика пошуку рішень на основі алгоритму зозулі;

підхід до синтезу інтелектуальної системи управління національною безпекою;

архітектура інформаційної системи з застосуванням запропонованої методології.

3. У цьому дослідженні проведено розробку методики виявлення та ідентифікації гібридних викликів та загроз в системі управління національною безпекою.

Результати дослідження стануть у нагоді при:

– розробці нових алгоритмів управління системою національної безпеки на етапі виявлення та ідентифікації викликів та загроз національній безпеці держави в умовах гібридного деструктивного впливу;

– обґрунтуванні рекомендацій щодо підвищення ефективності оперативного управління системою національної безпеки на етапі виявлення та ідентифікації викликів і загроз національній безпеці держави в умовах гібридного деструктивного впливу;

– при створенні перспективних технологій підвищення ефективності оперативного управління системою національної безпеки на етапі виявлення та ідентифікації викликів та загроз національній безпеці держави в умовах гібридного деструктивного впливу;

– розробці нових та удосконаленні існуючих моделей, методів (методик) управління системою національної безпеки.

4. Визначено алгоритм реалізації методики комплексного аналізу та багатовимірного прогнозування стану системи управління національною безпеки, що дозволяє:

– врахувати тип невизначеності даних та наявні обчислювальні ресурси системи управління національною безпеки;

– врахувати пріоритетність пошуку особинами з кошачої зграї;

– провести початкове виставлення особин кошачої зграї;

– провести точне навчання особин котячої зграї з використанням виразів, що розроблені в роботі [83];

– врахувати тип невизначеності та зашумленості даних;

– провести при коригуванні нечітких когнітивних моделей за допомогою генетичного алгоритму;

– провести навчання баз знань, що здійснюється шляхом навчання

синаптичних ваг штучної нейронної мережі, типу та параметрів функції належності, а також архітектури окремих елементів і архітектури штучної нейронної мережі в цілому;

– застосовувати як універсальний інструмент вирішення завдання аналізу стану системи національної безпеки за рахунок ієрархічності опису системи національної безпеки;

– перевірити адекватність отриманих результатів;

– уникнути проблеми локального екстремуму.

Методика дозволяє підвищити оперативність обробки даних на рівні 18–25 % за рахунок використання додаткових удосконалених процедур.

5. Проведено аналіз канонічного алгоритму зозулі для пошуку рішень щодо стану системи національної безпеки. В ході аналізу визначені недоліки канонічного алгоритму зозулі:

– побудова вихідної ділянки пошуку рішення відбувається без врахування типу невизначеності та зашумленості вихідних даних;

– модель стану системи національної безпеки є статичною та не враховує наявні обчислювальні ресурси системи;

– процедури ймовірності виявлення гнізд та довжини кроку зозулі описуються випадковим законом і потребують великих обчислювальних затрат;

– навчання особин в канонічному алгоритмі зозулі не передбачено.

Запропоновано алгоритм реалізації методики, що дозволяє:

– враховувати тип невизначеності даних;

– врахувати ступінь невизначеності про стан системи національною безпеки;

– врахувати наявні обчислювальні ресурси системи аналізу системи управління національною безпеки;

– врахувати пріоритетність пошуку гнізд;

– зменшити довжину маршруту;

– провести точне навчання особин зозуль;

– застосовувати як універсальний інструмент вирішення завдання аналізу стану системи національної безпеки за рахунок ієрархічності її опису;

– перевірити адекватність отриманих результатів;

– уникнути проблеми локального екстремуму.

Методика дозволяє підвищити оперативність обробки даних на рівні 21–28 % за рахунок використання додаткових удосконалених процедур.

6. В дослідженні підхід до синтезу інтелектуальної системи управління національною безпекою.

Новизна запропонованого підходу полягає у:

– врахуванні оперативності при обранні того чи іншого методу при дослідженні стану системи національної безпеки;

– розрахунку достовірності при обранні того чи іншого методу при дослідженні стану системи національної безпеки;

– врахуванні оперативності прийнятих рішень щодо дослідження стану системи національної безпеки при вборі одного або іншого методу дослідження;

– адаптації до нових викликів і загроз національній безпеці;

– обґрунтованості управлінських рішень при управлінні системою національної безпеки;

– врахуванні різних вихідних даних, що є різні за походженням та одиницями виміру;

– проведенні аналізу великих масивів даних.

Зазначену методологію доцільно реалізувати в алгоритмічному та програмному забезпеченні при дослідженні стану системи національної безпеки.

7. Запропонована архітектура інформаційної системи з застосуванням запропонованої методології. Архітектура інформаційної системи дозволяє здійснити імплементацію теоретичних досліджень наведених вище у програмно-апаратне забезпечення.