УДК 614.8.084:351.865:323.28 **DOI: 10.33042/2522-1809-2024-3-184-196-203**

О.В. Азаренко[1], Ю.Ю. Гончаренко[2], М.М. Дівізінюк[3], Р.І. Шевченко[4], О.С. Шевченко[4]

[1]Науково-дослідний лабораторно-експериментальний центр «БРАНД ТРЕЙД», Харків, Україна
[2]Європейський університет, Київ, Україна
[3]Центр інформаційно-аналітичного та технічного забезпечення моніторингу об'єктів атомної енергетики НАН України, Київ, Україна
[4]Національний університет цивільного захисту України, Харків, Україна

АЛГОРИТМ КЕРУВАННЯ РЕАЛІЗАЦІЇ МАТЕМАТИЧНОЇ МОДЕЛІ СЦЕНАРНОГО УПРАВЛІННЯ ЯК ІНСТРУМЕНТА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ СТРАТЕГІЧНОГО ОБ'ЄКТА

У роботі спочатку розглядається математична модель сценарного управління як інструмента безпеки стратегічного об'єкта. Потім розробляється структура алгоритму керування реалізації цієї математичної моделі. Робиться висновок про структуру алгоритму та необхідність розробки основних процедур щодо його застосування.

Ключові слова: *об'єкт критичної інфраструктури, сценарне управління, алгоритм, математична модель, надзвичайна ситуація.*

Постановка проблеми

Під час війни перед Україною постає широкий спектр завдань із захисту держави, зокрема забезпечення безпеки об'єктів критичної інфраструктури (ОКІ) [1]. Для забезпечення безпеки ОКІ та інших стратегічних об'єктів використовується безліч методів, серед яких і методи сценарного аналізу. На підставі цих методів розроблено математичну модель сценарного управління як інструмента забезпечення безпеки стратегічного об'єкта. Проблема полягає у практичному використанні розробленої математичної моделі для забезпечення безпеки конкретного об'єкта критичної інфраструктури.

Аналіз останніх досліджень і публікацій

Наприкінці XX століття провідні країни світу стали виділяти у державній інфраструктурі особливий вид – критичну інфраструктуру [2]. У термінологічній сфері України поряд із терміном «ОКІ» [3] продовжують використовувати термін «стратегічний об'єкт» [4]. Ці поняття використовуються різними фахівцями та є тотожними. Водночас з позицій теорії управління та теорії систем [5] кожен стратегічний об'єкт, або ОКІ, є розподіленою системою. Математична модель сценарного управління як інструмента безпеки стратегічного об'єкта [6] розроблена на основі математичного апарату теорії ліпшицевої глобальної оптимізації [7] для отримання математичних закономірностей впливу на розподілену систему.

Мета та завдання статті

З огляду на вищевикладене, метою цієї статті є розробка алгоритму керування реалізації математичної моделі сценарного управління як інструмента забезпечення безпеки стратегічного об'єкта.

Для досягнення поставленої мети необхідно вирішити такі завдання:

– розглянути математичну модель сценарного управління як інструмент забезпечення безпеки стратегічного об'єкта;

– розробити структуру алгоритму керування реалізації цієї математичної моделі;

– проаналізувати та зробити висновок про структуру алгоритму та необхідність розробки основних процедур щодо його застосування.

Виклад основного матеріалу

Характеристика математичної моделі сценарного управління як інструмента забезпечення безпеки стратегічного об'єкта.

Нині під управлінням або керівництвом, адмініструванням або менеджментом розуміють домінувальний вплив, який здійснюється на учасників процесу з метою покращення характеристик процесу та досягнення певних результатів [8]. Управління безпекою стратегічних об'єктів є багатогранним процесом, який називають розподіленим управлінням розподіленими системами.

Під розподіленою системою розуміють систему, в якій розташування елемента (або групи елементів)

відіграє важливу роль у функціональних аспектах системи [9]. Прийнято розрізняти розподілені інформаційні системи [10], розподілені інформаційно-аналітичні системи [11], розподілені інтелектуальні системи [12], розподілені системи підтримки прийняття рішень [13], розподілені бази даних (розподілені системи зберігання інформації) [14] та асинхронні розподілені системи [15].

Згідно з детальним аналізом, управлінські інформаційні системи, зокрема управління безпекою, є розподіленими системами. Крім того, сценарій вторгнення на об'єкт, що захищається, також є розподіленою системою, оскільки як розгортання сценарію, так і стан захищеності об'єкта, що захищається, залежать від послідовності подій [7].

У цьому випадку, використовуючи математичний апарат теорії глобальної оптимізації Ліпшиця [12], можна отримати математичну закономірність впливу на розподілену систему, стан якої може бути описаний одним з величезної кількості сценаріїв посягання на стратегічний об'єкт захисту [12].

При розробці математичної моделі за припущення були прийняті наступні основні положення.

По-перше, під управлінням розуміється вплив на учасників процесу з метою покращення характеристик процесу та досягнення запланованих результатів, а під сценарним управлінням – вплив на систему безпеки, що захищається (систему фізичного захисту), з метою запобігання терористичному впливу.

По-друге, сценарій вторгнення – це передбачуваний варіант дій зловмисників щодо терористичного впливу на об'єкт, що охороняється, на підставі якого розробляються і плануються заходи щодо протидії терористичним впливам.

По-третє, система безпеки або система фізичного захисту – це комплексна організаційно-технічна система, що складається з трьох складових частин, а саме: технічних засобів, персоналу та фактичного поточного стану безпеки об'єкта, що охороняється.

По-четверте, вважатимемо, що сценарне управління здійснюється з використанням трьох складових: технічні засоби фізичного захисту, що знаходяться в цей момент на озброєнні стратегічного об'єкта, як стаціонарні, так і мобільні та переносні; персонал служби фізичного захисту стратегічного об'єкта, що охороняється; сценарний стан, що формується навколо стратегічного об'єкта, що охороняється, який визначається як наявністю достовірної (або недостовірної) інформації про терористичні наміри, так і її відсутністю.

По-п'яте, кожен співробітник об'єкта, що охороняється, працює на забезпечення його безпеки та запобігання терористичному впливу.

Розроблена на основі цих постулатів математична модель сценарного управління як інструмента безпеки стратегічного об'єкта є системою (1).

$$
\left\{
\begin{array}{l}
\left\{
\begin{array}{l}
\Phi(v)=\int\limits_M\left(\sum\limits_{i,j=1}^{n}k_{ij}\dfrac{\partial v}{\partial x_j}\dfrac{\partial v}{\partial x_i}+qv^2\right)dx+\int\limits_\gamma \beta y^2 d\gamma-\int\limits_M fv dx+2\int\limits_\gamma uv d\gamma \\
\int\limits_M\left(\sum\limits_{i,j=1}^{n}k_{ij}\dfrac{\partial y}{\partial x_j}\dfrac{\partial v}{\partial v_i}+qyv\right)dx+\int\limits_\gamma \beta yv d\gamma=\int\limits_M fv dx+\int\limits_\gamma uv d\gamma
\end{array}
\right. \\
\left\{
\begin{array}{l}
\Phi(v)=\int\limits_M\left(\sum\limits_{i,j=1}^{n}k_{ij}\dfrac{\partial v}{\partial x_j}\dfrac{\partial v}{\partial x_i}+qv^2\right)dx+\int\limits_\gamma \beta v^2 d\gamma-2\int\limits_M fv dx-2\int\limits_\Gamma gv d\Gamma+\int\limits_\Gamma uv d\Gamma \\
\int\limits_M\left(\sum\limits_{i,j=1}^{n}k_{ij}\dfrac{\partial v}{\partial x_j}\dfrac{\partial v}{\partial x_i}+qyv\right)dx+\int\limits_\gamma \beta yv d\gamma=\int\limits_M fv dx-\int\limits_\Gamma gv d\Gamma+\int\limits_\Gamma uv d\Gamma
\end{array}
\right. \\
\left\{
\begin{array}{l}
\Phi(v)=\int\limits_M\left(\sum\limits_{i,j=1}^{n}k_{ij}\dfrac{\partial v}{\partial x_j}\dfrac{\partial v}{\partial x_i}+qv^2\right)dx+\int\limits_\lambda \dfrac{[v]^2}{R_1+R_2}d\gamma+\int\limits_\gamma \beta\left(vv^+ +\chi v^-\right)d\gamma \\
\qquad -2(f,v)-2(u,v)-2\int\limits_\gamma \dfrac{R_2 a-\delta}{R_1+R_2}[v]d\gamma+2\int\limits_\gamma av^+ d\gamma \\
\int\limits_M\left(\sum\limits_{i,j=1}^{n}k_{ij}\dfrac{\partial v}{\partial x_j}\dfrac{\partial v}{\partial x_i}+qyv\right)dx+\int\limits_\gamma \dfrac{[y][v]}{R_1+R_2}d\gamma+\int\limits_\gamma \beta\left(vy^+ +\chi y^-\right)\left(vv^+ +\chi v^-\right)d\gamma= \\
\qquad =(f,v)+(u,v)+\int\limits_\gamma \dfrac{R_2 a-\delta}{R_1+R_2}[v]d\gamma-\int\limits_\gamma av^+ d\gamma
\end{array}
\right.
\end{array}
\right. , \qquad (1)
$$

де M – безліч технічних засобів фізичного захисту, що знаходяться в цей момент на озброєнні стратегічного об'єкта, що складається з підгруп (підмножин, частин);

$\Phi(v)$ – функціонал вартості керувальних впливів (результат просування сценарію забезпечення найбільшої безпеки);

k_{ij} – нормувальні коефіцієнти;

β – довільна наявна функція та її значення;

Γ – межа аналізованої області, причому $x \in \Gamma$;

U – простір управлінь (гільбертовий простір), заданий у вигляді $U = L_2(M)$;

$u \in U$ – одиничне управління (вибір засобу фізичного захисту стратегічного об'єкта);

$y = y(u)$ – одиничний стан розподіленої системи (поточний стан засобів фізичного захисту стратегічного об'єкта), причому $y \in V$;

B – відображення заданого гільбертового простору U, задане у вигляді $B \in J(U; V^!)$;

$V^!$ – простір, подвійний до гільбертового простору V;

q – проєкція елемента f на L, причому $0 < q_0 \le q = q(x) \le q_1 < \infty$;

f – функція співвідношень;

v – ортогональ нормалі до γ, спрямована в M_i (M_1, M_2, $M_i \in R^n$), $v = \frac{R_1}{R_1 + R_2}$, а $\chi = \frac{R_2}{R_1 + R_2}$, причому $R_1, R_2, \beta, \delta \in L_2(\gamma)$, $R_1 + R_2 \ge R_0 > 0$, і $R_0 = const$;

γ – розріз області M;

v^+, y^+ – найбільші та v^-, y^- – найменші значення аргументів;

$[v]$ – округлення числа до найближчого цілого до нього;

a – білінійна форма, причому $0 < a_0 \le \bar{a}(x) \le a_1 < \infty$.

Вона об'єднує три групи залежностей, перша з яких описує управління засобами фізичного захисту, що знаходяться в експлуатації на стратегічному об'єкті, як управління розподіленими системами, що описується задачею Діріхле. Друга – як управління розподіленими системами, що описується задачею Неймана, – це управління персоналом служби фізичного захисту стратегічного об'єкта, що охороняється. А третя – як управління розподіленими системами, описує управління поточним станом сценаріїв, що формуються навколо стратегічного об'єкта, що охороняється.

Кожна група, що описує її складові частини, містить два елементи. Перший – функція витрат, що мінімізує вартість керувальних впливів (для забезпечення протидії тероризму); другий – інтегральне рівняння, що визначає оптимальний оператор впливу на керовану частину системи фізичного захисту стратегічного об'єкта, що охороняється.

Структура алгоритму керування реалізації розробленої математичної моделі.

Структурно він складається із тринадцяти модулів, розташованих на дванадцяти ієрархічних рівнях, як показано на рис. 1. Послідовно розглянемо ці модулі.

На першому ієрархічному рівні знаходиться модуль «Аналіз ситуації» (або поточного сценарію). У цьому модулі обробляється інформація, що надходить від зовнішніх та внутрішніх джерел інформації. Зовнішні джерела, зазвичай структури, здійснюють керівництво об'єктом критичної інфраструктури чи безпосереднє управління його безпекою. Від них надходить інформація про можливі або очікувані в певні періоди часу терористичні атаки. Інформація про технічні характеристики засобів терористичного нападу, можливу тактику їх застосування та способи протидії їм. Внутрішні джерела – це ОКІ, об'єднані в одну сукупність, конгломерацію або адміністративний район і – це ключовий момент – підпорядковані тому самому військово-адміністративному керівництву.

На другому ієрархічному рівні знаходиться блок формування приватних завдань забезпечення безпеки. Він призначений для з'ясування суті розв'язуваного завдання щодо забезпечення безпеки стратегічного об'єкта, що охороняється, або ОКІ, пов'язаної зі сценаріями, що розвиваються (обстановкою, тактичним, оперативно-тактичним або оперативним тлом, подіями або факторами, які називаються різними термінами на різних аудиторіях фахівцями різних областей знань) у різних просторово-тимчасових масштабах. А саме: на поточний проміжок часу, який обчислюється десятками хвилин (до години); добовий – проміжок часу, який обчислюється десятками годин. Наступні масштаби сценаріїв – це одно-, дво-, тритижневий чи місячний проміжок часу, який обчислюється десятками діб. Квартальний чи сезонний сценарії, що визначаються кількома місяцями чи сезонами, наприклад, перший, другий, третій квартали чи весна, літо, осінь та інші.

Прикладами приватних завдань із безпеки можуть бути такі. На поточний момент часу – мобілізувати всі сили та ресурси для безперебійного функціонування об'єкта, що охороняється, відбити атаку ударних «Шахедів» (безпілотних літальних апаратів – БПЛА), у найкоротший термін ліквідувати загоряння та пожежі, спричинені потраплянням та падінням БПЛА. Також необхідно розділяти завдання на три складові: технічні засоби, персонал і сама ситуація, що складається довкола та всередині ОКІ.

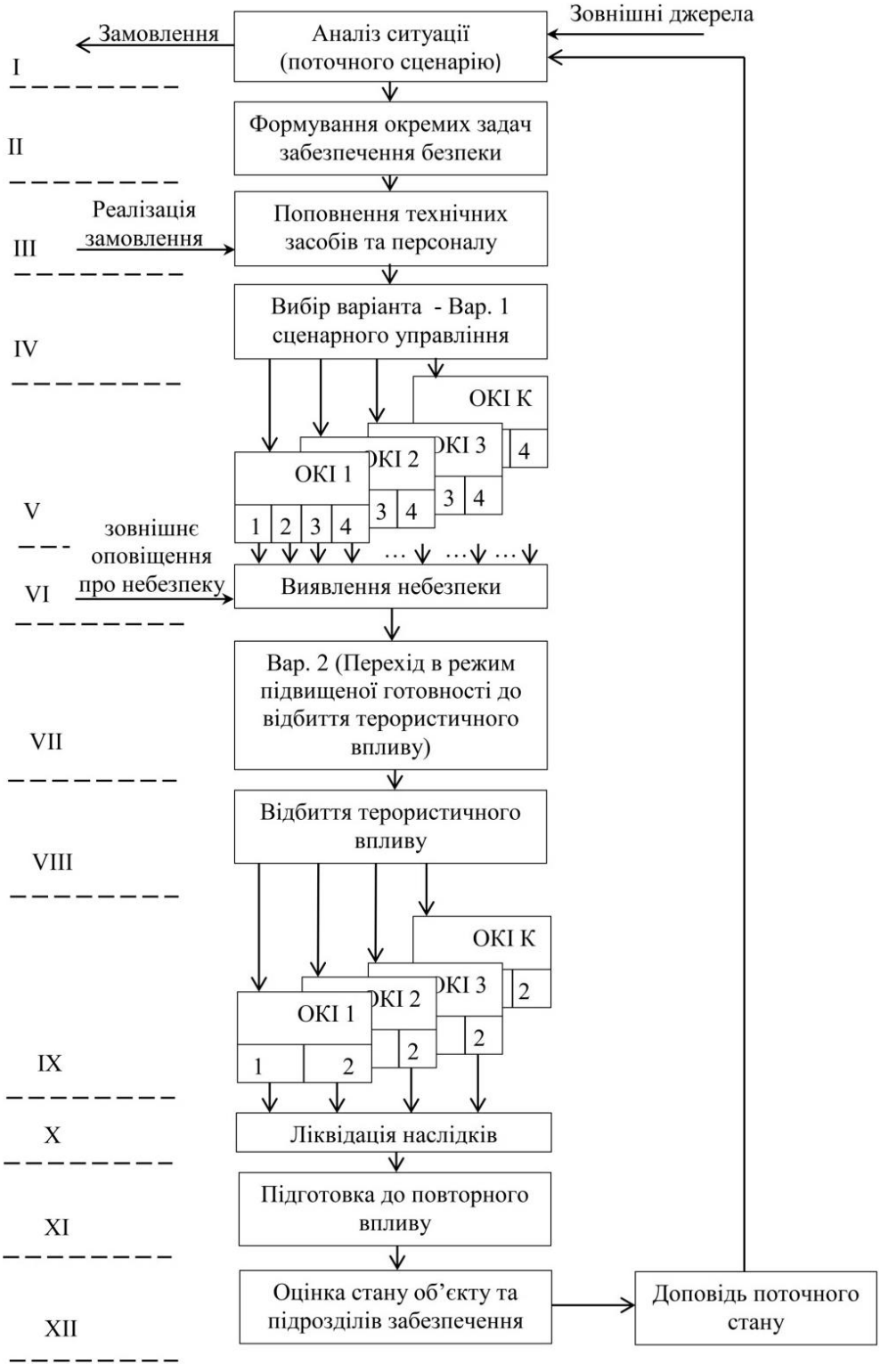

Рис. 1. Структурна схема алгоритму керування

Прикладом добових завдань із безпеки можуть бути наступні. Для технічних засобів: відновлення готовності вогневих засобів (поповнення боєкомплекту, спорядження кулеметних стрічок, усунення несправностей та інше), заправлення пожежних машин водою, ремонт провідних ліній зв'язку та передачі телекомунікаційної інформації. Для персоналу: евакуація або тимчасова ізоляція постраждалих, оптимізація складу та порядку заступлення чергових змін на бойові пости, визначення потреби у поповненні персоналу в майбутньому. Для поточного стану: визначення термінів відновлення бойової готовності підрозділів забезпечення безпеки ОКІ, виявлення недоліків та нових вразливих місць за результатами терористичної атаки, визначення конкретних дій щодо усунення виявлених недоліків.

Приклад тижневих приватних завдань – це підготовка майданчиків та місць для розміщення нових технічних та вогневих засобів, прийом та розподіл нового персоналу за підрозділами та бойовими постами, підготовка нових людей (інструктаж та навчання) з подальшим допуском їх до самостійного виконання обов'язків. Квартальними приватними завданнями можуть бути, наприклад, підготовка до зимового періоду (отримання теплого одягу, підготовка пунктів обігріву та надання першої допомоги та інше).

На третьому ієрархічному рівні – блок поповнення технічних засобів та персоналу. Він виконує функцію реалізації заявок, поданих раніше. Тут відбувається розподіл технічних засобів, витратних матеріалів, матеріальних засобів, необхідних для функціонування об'єкта та персоналу (продуктів та питної води, медикаментів та перев'язувального матеріалу, запасних частин та боєкомплектів та інше). Крім технічних засобів, тут розподіляються нові люди, які прийшли на ОКІ, за структурними підрозділами.

На четвертому ієрархічному рівні розташовується блок вибору варіанта сценарного управління – «Варіант № 1». Перший варіант – це варіант повсякденного функціонування, як окремого ОКІ, так і конгломерації об'єктів, об'єднаних одним військово-адміністративним керівництвом.

Тому на п'ятому ієрархічному рівні розташовується «К» субблоків чи об'єктів, кожному з яких керівник визначає порядок функціонування свого об'єкта [14]. У першому варіанті сценарного управління або повсякденної ситуації існує чотири варіанти функціонування систем забезпечення безпеки ОКІ. Перший – удень, із використанням чергових засобів. У цій ситуації використовуються радіолокаційні та панорамні оптоелектронні засоби. Це продиктовано тим, що вдень дальність візуального спостереження значно перевищує дальність виявлення повітряних засобів терористичного впливу іншими радіоелектронними засобами. Другий – уночі та в умовах обмеженої видимості, з використанням чергових засобів. У таких умовах основними засобами виявлення повітряних цілей є засоби інфрачервоного і акустичного виявлення. Тут дальності виявлення повітряних засобів терористичного впливу можуть бути набагато більшими, ніж дальності виявлення радіолокаційними засобами. Третій – при використанні всіх засобів об'єкта, що охороняється. Така ситуація зазвичай виникає при надходженні інформації про повітряний напад, що готується, наприклад, при оголошенні повітряної тривоги в регіоні, де розташовується об'єкт критичної інфраструктури, що охороняється. Четвертий – оптимальне використання засобів об'єкта, що охороняється, і зовнішніх засобів. Цей варіант характерний для ситуацій, коли в регіоні, де знаходиться об'єкт критичної інфраструктури, що охороняється, відбій повітряної тривоги, але терористична атака не відбулася, і її загроза зберігається. Звідси інформація надходить на наступний ієрархічний рівень.

На шостому ієрархічному рівні – блок виявлення небезпеки. Тут реалізується передача оповіщення про виявлену небезпеку. Вона може бути виявлена як засобами виявлення одного або декількох ОКІ конгломерації, так і надійти у формі зовнішнього оповіщення про небезпеку. Ця інформація відразу запускає блок, розташований на наступному ієрархічному рівні.

На сьомому ієрархічному рівні – блок «Варіант № 2» сценарного управління, а саме: переведення в режим найвищої готовності до відбиття терористичного впливу. Це комплекс заходів, який розробляється стосовно кожного ОКІ. Виконавши їх, об'єкт перебуває у стані, що забезпечує максимальне відбиття терористичної атаки.

На восьмому ієрархічному рівні розташовується блок відбиття терористичного впливу. Тут здійснюються дії військового керівника щодо розподілу вогневих засобів на знищення ударних БПЛА, крилатих або балістичних ракет. У кожній конкретній ситуації військовий керівник приймає рішення та віддає команди на їх виконання, з огляду на свій досвід та задум на відбиття терористичного впливу.

На дев'ятому ієрархічному рівні розташовується «К» об'єктів, на кожному з яких можливі два варіанти [15]. Перший – коли інтенсивність терористичного впливу зростає за експонентним законом протягом обмеженого проміжку часу. Подібна ситуація розвивається, коли спочатку з'являються розвідувальні БПЛА, які виявляють уразливі місця в системі забезпечення безпеки об'єкта, що охороняється. У ці вразливі місця і прямують ударні БПЛА та крилаті ракети. Це призводить до експоненційного зростання інтенсивності терористичного впливу протягом обмеженого проміжку часу. Другий варіант характеризується тим, що інтенсивність терористичного впливу максимальна та зберігається протягом обмеженого проміжку часу. Подібна ситуація розвивається, коли терористичний вплив зосереджується на одному напрямку, і в цю точку спрямовуються всі ударні БПЛА та атакувальні крилаті ракети. Зі свого боку, це призводить до того, що інтенсивність терористичного впливу залишається максимальною протягом обмеженого проміжку часу, але за цей проміжок часу один або кілька ударних засобів проходять систему захисту і пошкоджують об'єкт, що охороняється.

На десятому ієрархічному рівні – блок «Ліквідація наслідків». Він призначений для вироблення управлінських рішень для усунення пошкоджень на об'єкті в найкоротший термін. Крім усунення пош-

коджень, що впливають на функціонування ОКІ за прямим призначенням, відбувається відновлення допоміжних (периферійних) агрегатів та вузлів.

На одинадцятому ієрархічному рівні знаходиться блок підготовки до повторного впливу. Тут виконуються формалізовані протоколи щодо відновлення бойової готовності всіх систем забезпечення безпеки у найкоротші терміни. При цьому об'єкт може бути у найвищій мірі своєї готовності до відбиття терористичного впливу. Цей модуль передбачає обов'язкову наявність резервів: як засобів відбиття терористичних впливів (боєзапасу зенітних вогневих засобів), так і сил ліквідації наслідків (аварійно-рятувальних підрозділів). Це забезпечує можливість маневру при повторній терористичній атаці, яка може повторитись через 30–40 хвилин або через 1,5–2 години.

На дванадцятому ієрархічному рівні розташовуються два блоки. Перший – це блок оцінки стану у підрозділах та на об'єктах. Цей блок призначений для оцінки стану технічних засобів, персоналу та інших обставин, що визначають як функціонування ОКІ за прямим призначенням, так і стан систем безпеки. Другий блок – доповідь про поточний стан, призначена для забезпечення зворотного зв'язку з блоком, розташованим на першому ієрархічному рівні. Через нього здійснюється передача формалізованої інформації, зокрема і заявок на поповнення, які надходять на перший ієрархічний рівень – модуль аналізу ситуації.

Цими зв'язками замикається контур управління із забезпечення безпеки як одиночного ОКІ, так і конгломерації об'єктів критичної інфраструктури.

Висновки

Отже, алгоритм керування реалізації математичної моделі сценарного управління як інструмента забезпечення безпеки стратегічного об'єкта є ієрархічною структурою з тринадцяти блоків (або модулів), розташованих на дванадцяти ієрархічних рівнях, пов'язаних прямими і зворотними зв'язками. Він забезпечує формування приватних завдань забезпечення безпеки стратегічного об'єкта, вибір варіанта сценарного управління, відображення терористичного впливу, ліквідації наслідків, підготовки до повторного впливу, оцінки стану на об'єкті та уточнення приватних завдань забезпечення безпеки.

Для коректного практичного використання цього алгоритму керування при вирішенні завдань щодо забезпечення безпеки стратегічних об'єктів і об'єктів критичної інфраструктури необхідно детально розробити процедури його застосування.

Література

1. Ключове завдання нашої держави / Промови та звернення / Доступ: https://www.president.gov.ua/news/speeches

2. Linhart, P., Richter, R. (2003): Ochrana kritické infrastruktury. Input: http.//www.mvcr.cz/casopisy/112/3_2003/linhart.html

3. Presidential Decision Directive 63 (1998), https://www.fas.org/irp/offdocs/pdd/pdd-63.htm

4. The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, http://www.whitehouse.gov/pcipb/physical.html

5. Указ Президента України №8/2017. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури». Доступ: https://www.president.gov.ua/documents/82017-21058

6. Закон України «Про критичну інфраструктуру» {Із змінами, внесеними згідно із Законом № 2684-IX від 18.10.2022}. Доступ: https://zakon.rada.gov.ua/laws/show/1882-20#Text

7. Дівізінюк М.М. Теоретичні засади парадигми «цивільний захист» / М.М. Дівізінюк, С.А. Єременко, О.А. Лєфтєров, А.В. Пруський, В.В. Стрілец, В.М. Стрілец, Р.І. Шевченко // Монографія. Київ.: ТОВ «АЗИМУТ-ПРІНТ». 2022. 335 с. (ISBN 978-617-8015-20-6).

8. Постанова КМУ від 04.03.2015 р. № 83 «Про затвердження переліку об'єктів державної власності, що мають стратегічне значення для економіки і безпеки держави». Доступ: https://document.vobu.ua/doc/7863

9. Papalou, A., Baros, K., (2019). Assessing Structural Damage after a Severe Wildfire: A Case Study Department of Civil Engineering, University of Peloponnese; 26334 Patras, Greece. Buildings, 9(7), 171 DOI: http://doi.org/10.3390/buildings9070171

10. Jakubowski, K., Paś, J., Duer, S., & Bugaj, J., (2021). Operational Analysis of Fire Alarm Systems with a Focused, Dispersed and Mixed Structure in Critical Infrastructure Buildings, Energies 14(23), 7893; DOI: http://doi.org/10.3390/en14237893

11. Aliş, B., Yazici, C., & Özkal, F.M., (2022). Investigation of Fire Effects on Reinforced Concrete Members via Finite Element Analysis ACS Omega 2022, 7(30), 26881–26893 DOI: http://doi.org/10.1021/acsomega.2c03414

12. Азаренко О.В., Гончаренко Ю.Ю., Дівізінюк М.М., Шевченко О.С., Шевченко Р.І. 1. Азаренко О.В., Гончаренко Ю.Ю., Дівізінюк М.М., Шевченко О.С., Шевченко Р.І. Характеристика об'єктів критичної інфраструктури держави (особливості ядерних та інших стратегічних об'єктів) // Комунальне господарство міст, 2023, том 1, випуск 175. С.160- 168 ISSN 2522-1809(Print); ISSN2522-1817 (Online) DOI 10.33042/2522-1809-2023-1-175-160-168

13. Азаренко О.В., Гончаренко Ю.Ю., Дівізінюк М.М., Шевченко О.С., Шевченко Р.І. Поняття загрози та ризику, їх загальні риси та принципіальні відмінності (стосовно ядерних та інших стратегічних об'єктів) // Комунальне господарство міст, 2023, том 3, випуск 177. С.153- 158 ISSN 2522-1809(Print); ISSN2522-1817 (Online) DOI 10.33042/2522-1809-2023-3-177-153-158

14. О.В. Азаренко, Ю.Ю. Гончаренко, М.М. Дівізінюк, О.С. Шевченко, Р.І. Шевченко Методи дослідження загроз і ризиків // Комунальне господарство міст, 2023, том 4, випуск 178. С.269- 279 ISSN 2522-1809(Print); ISSN2522-1817 (Online) DOI https://doi.org/10.33042/2522-1809-2023-4-178-172-178

15. Азаренко О.В., Гончаренко Ю.Ю., Дівізінюк М.М., Шевченко О.С., Шевченко Р.І. Методи оцінки терористичних загроз стосовно стратегічних об'єктів держави // Комунальне господарство міст, 2023, том 6, випуск 180. С. 187-195 ISSN 2522-1809(Print); ISSN2522-1817 (Online) DOI: https://doi.org/10.33042/2522-1809-2023-6-180-187-195

References

1. Kliuchove zavdannia nashoi derzhavy / Promovy ta zvernennia / Dostup: https://www.president.gov.ua/news/speeches
2. Linhart, P., Richter, R. (2003): Ochrana kritické infrastruktury. http.//www.mvcr.cz/casopisy/112/3_2003/linhart.html
3. Presidential Decision Directive 63 (1998), https://www.fas.org/ irp/offdocs/pdd/pdd-63.htm
4. The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, http://www.whitehouse.gov/pcipb/physical.html
5. Ukaz Prezydenta Ukrainy №8/2017. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 29 hrudnia 2016 roku «Pro udoskonalennia zakhodiv zabezpechennia zakhystu obiektiv krytychnoi infrastruktury». Dostup: https://www.president.gov.ua/documents/82017-21058
6. Zakon Ukrainy «Pro krytychnu infrastrukturu» {Iz zminamy, vnesenymy zghidno iz Zakonom № 2684-IX vid 18.10.2022}. Dostup: https://zakon.rada.gov.ua/laws/show/1882-20#Text
7. Diviziniuk M.M. Teoretychny zasady paradyhmy «tsyvilnyi zakhyst» / M.M. Diviziniuk, S.A. Yeremenko, O.A. Lieftierov, A.V. Pruskyi, V.V. Strilets, V.M. Strilets, R.I. Shevchenko // Monohrafiia. Kyiv.: TOV «AZYMUT-PRINT». 2022. 335 s. (ISBN 978-617-8015-20-6).
8. Postanova KMU vid 04.03.2015 r. № 83 «Pro zatverdzhennia pereliku obiektiv derzhavnoi vlasnosti, shcho maiut stratehichne znachennia dlia ekonomiky i bezpeky derzhavy». Dostup: https://document.vobu.ua/doc/7863
9. Papalou, A., Baros, K., (2019). Assessing Structural Damage after a Severe Wildfire: A Case Study Department of Civil Engineering, University of Peloponnese; 26334 Patras, Greece. Buildings, 9(7), 171 DOI: http://doi.org/10.3390/buildings9070171
10. Jakubowski, K., Paś, J., Duer, S., & Bugaj, J., (2021). Operational Analysis of Fire Alarm Systems with a Focused, Dispersed and Mixed Structure in Critical Infrastructure Buildings, Energies 14(23), 7893; DOI: http://doi.org/10.3390/en14237893
11. Aliş, B., Yazici, C., & Özkal, F.M., (2022). Investigation of Fire Effects on Reinforced Concrete Members via Finite Ele-ment Analysis ACS Omega 2022, 7(30), 26881–26893 DOI: http://doi.org/10.1021/acsomega.2c03414
12. Azarenko O.V., Honcharenko Yu.Iu., Diviziniuk M.M., Shevchenko O.S., Shevchenko R.I. 1. Azarenko O.V., Honcha-renko Yu.Iu., Diviziniuk M.M., Shevchenko O.S., Shevchenko R.I. Kharakterystyka obiektiv krytychnoi infrastruktury derzhavy (osoblyvosti yadernykh ta inshykh stratehichnykh obiektiv) // Komunalne hospodarstvo mist, 2023, tom 1, vypusk 175. S.160-168 ISSN 2522-1809(Print); ISSN2522-1817 (Online) DOI 10.33042/2522-1809-2023-1-175-160-168
13. Azarenko O.V., Honcharenko Yu.Iu., Diviziniuk M.M., Shevchenko O.S., Shevchenko R.I. Poniattia zahrozy ta ryzyku, yikh zahalni rysy ta pryntsypialni vidminnosti (stosovno yadernykh ta inshykh stratehichnykh obiektiv) // Komunalne hospodarstvo mist, 2023, tom 3, vypusk 177. S.153- 158 ISSN 2522-1809(Print); ISSN2522-1817 (Online) DOI 10.33042/2522-1809-2023-3-177-153-158
14. O.V. Azarenko , Yu.Iu. Honcharenko, M.M. Diviziniuk , O.S. Shevchenko, R.I. Shevchenko Metody doslidzhennia zahroz i ryzykiv // Komunalne hospodarstvo mist, 2023, tom 4, vypusk 178. S.269- 279 ISSN 2522-1809(Print); ISSN2522-1817 (Online) DOI https://doi.org/10.33042/2522-1809-2023-4-178-172-178
15. Azarenko O.V., Honcharenko Yu.Iu., Diviziniuk M.M., Shevchenko O.S., Shevchenko R.I. Metody otsinky terorystychnykh zahroz stosovno stratehichnykh obiektiv derzhavy // Komunalne hospodarstvo mist, 2023, tom 6, vypusk 180. S. 187-195 ISSN 2522-1809(Print); ISSN2522-1817 (Online) DOI: https://doi.org/10.33042/2522-1809-2023-6-180-187-195

Рецензент: д-р техн. наук, проф., заступник начальника з навчальної та наукової роботи О.М. Мирошник, Черкаський інститут пожежної безпеки імені Героїв Чорнобиля Національного університету цивільного захисту України, Україна.

Автор: АЗАРЕНКО Олена Василівна
доктор фізико-математичних наук, професор, заступник керівника
Науково-дослідний лабораторно-експериментальний центр «БРАНД ТРЕЙД»
E-mail – azarenko_ev@ukr.net
ID ORCID: http://orcid.org/0000-0003-2927-5545

Автор: ГОНЧАРЕНКО Юлія Юріївна
доктор технічних наук, доцент, професор кафедри кібербезпеки та захисту інформації
Європейський університет
E-mail – vup@e-u.in.ua
ID ORCID: http://orcid.org/0000-0003-2045-0263

Автор: ДІВІЗІНЮК Михайло Михайлович
доктор фізико-математичних наук, професор, головний науковий співробітник
Центр інформаційно-аналітичного та технічного забезпечення моніторингу об'єктів атомної енергетики НАН України
E-mail – divizinyuk@ukr.net
ID ORCID: http://orcid.org/0000-0002-5657-2302

Автор: ШЕВЧЕНКО Роман Іванович
доктор технічних наук, професор, начальник кафедри автоматичних систем безпеки та інформаційних технологій
Національний університет цивільного захисту України
E-mail – shevchenko605@i.ua
ID ORCID: http://orcid.org/0000-0001-9634-6943

Автор: ШЕВЧЕНКО Ольга Станіславівна
кандидат технічних наук, провідний фахівець
Національний університет цивільного захисту України
E-mail – shevchenkoolga2008@gmail.com
ID ORCID: http://orcid.org/0000-0003-2106-5009

CONTROL ALGORITHM FOR IMPLEMENTING THE MATHEMATICAL MODEL OF SCENARIO MANAGEMENT AS A TOOL FOR ENSURING SECURITY OF A STRATEGIC FACILITY

O. Azarenko[1], Yu. Honcharenko[2], M. Diviziniuk[3], R. Shevchenko[4], O. Shevchenko[4]
[1]Scientific Research Laboratory and Experimental Center "BRAND TRADE", Kharkiv, Ukraine
[2]European University, Kyiv, Ukraine
[3]Center for Information-Analytical and Technical Support of Nuclear Power Facilities Monitoring of the National Academy of Sciences of Ukraine, Kyiv, Ukraine
[4]National University of Civil Defence of Ukraine, Kharkiv, Ukraine

The article first considers the mathematical model of scenario management as a security tool for a strategic object. Then, it develops the structure of the control algorithm for implementing this mathematical model. The study concludes with the structure of the algorithm and the need to establish basic procedures for its application.

Ukraine at war faces a wide range of tasks to protect the state, including ensuring the safety of critical infrastructure objects (CIO). Many methods, namely scenario analysis methods, can be applied to ensure the security of the CIO and other strategic objects. Based on these methods, the authors develop a mathematical model of scenario management as a security tool for a strategic object. The problem lies in the practical use of the developed mathematical model to ensure the safety of a specific CIO.

Based on the above, the article aims to create a control algorithm for the implementation of a mathematical model of scenario management as a tool for ensuring the security of a strategic object.

For this purpose, the study sets such objectives as considering the mathematical model of scenario management as a tool for ensuring the security of a strategic object, developing the structure of the control algorithm for implementing this mathematical model, analysing it, and drawing a conclusion about the structure of the algorithm and the need to establish basic procedures for its application.

Thus, the control algorithm for implementing the mathematical model of scenario management as a tool for ensuring the security of a strategic object is a hierarchical structure of thirteen blocks (or modules) located on twelve hierarchical levels, connected by direct and feedback links. It ensures the formation of private tasks of securing a strategic object, choosing a scenario management option, countering terrorist influence, eliminating consequences, preparing for a repeated attack, assessing the object's state, and clarifying private tasks of ensuring security.

For the correct practical use of this control algorithm when solving tasks related to the protection of strategic objects and critical infrastructure facilities, it is necessary to develop detailed procedures for its application.

Keywords: *critical infrastructure object, scenario management, algorithm, mathematical model, emergency*.