

## МЕТОДИЧНИЙ ПІДХІД ДО ПОБУДОВИ МОДЕЛІ ПРОЦЕСУ ПІДВИЩЕННЯ РІВНЯ БЕЗПЕКИ ОБ'ЄКТА ПІДВИЩЕНОЇ НЕБЕЗПЕКИ

**Abstract:** The article is devoted to the methodical questions for the support of making management decisions at the prevention and solving conflict situation process. The netting model for the estimation of level security of the potential hazard object of was used. The methodical approach to the selection of the rational strategy for the level security advancement of the potential hazard object was set.

**Key words:** security, model, security level, prognosis, identification, normative, strategy.

**Анотація:** Статтю присвячено методичним питанням підтримки прийняття управлінських рішень щодо запобігання і вирішення конфліктних ситуацій. Було використано мережеву модель для оцінки рівня безпеки потенційно небезпечних об'єктів. Запропоновано методичний підхід і відповідні алгоритми для вибору раціональної стратегії підвищення рівня безпеки потенційно небезпечних об'єктів.

**Ключові слова:** безпека, модель, рівень безпеки, прогнозування, ідентифікація, нормативи, стратегія.

**Аннотация:** Статья посвящена методическим вопросам поддержки принятия управленческих решений в области предупреждения и разрешения чрезвычайных ситуаций. Использована сетевая модель для оценки уровня безопасности потенциально опасных объектов. Предложены методический подход и соответствующие алгоритмы к выбору рациональной стратегии повышения уровня безопасности потенциально опасных объектов.

**Ключевые слова:** безопасность, модель, уровень безопасности, прогнозирование, идентификация, нормативы, стратегия.

### 1. Вступ

Проблема безпеки функціонування об'єктів підвищеної небезпеки (ОПН) на сьогодні є гостро актуальною насамперед стосовно арсеналів, баз, складів Збройних сил України, на яких зберігається велика кількість застарілих боєприпасів колишніх Збройних сил Радянського Союзу. Темпи старіння ракет і боєприпасів випереджають темпи утилізації їх надлишкових запасів, велика частина яких зберігається на відкритих майданчиках і зазнає безперервного руйнівного атмосферного впливу. Ряд керівних нормативних документів, що регламентують порядок і умови зберігання ракет і боєприпасів, а також вимоги до забезпечення живучості, вибухопожежобезпеки та інших аспектів безпеки військових об'єктів підвищеної небезпеки (ВОПН) не відповідають реаліям сьогодення, не враховують сучасний рівень розвитку технічних засобів, інформаційних та телекомунікаційних технологій. Особливо це стосується систем управління функціонуванням ВОПН, у тому числі й управління їх безпекою [1].

Ситуація, яка склалася у галузі безпеки функціонування ВОПН, характеризується, з одного боку, складністю і високим рівнем небезпечності, з іншого, – потребою поглибленого аналізу та пошуку шляхів раціонального вирішення пов'язаних з цим проблем в умовах обмежених матеріальних і фінансових ресурсів, які на сьогодні може виділити для цього держава. На прикладі ВОПН, на якому зберігаються ракети і боєприпаси, авторами розглянуто один із можливих методичних підходів до вирішення цього завдання.

До основних напрямів функціонування ВОПН, які у тій чи іншій мірі впливають на його рівень безпеки, слід віднести:

- безпечне розміщення ракет та боєприпасів на території ВОПН;
- вибухопожежобезпеку;
- охорону і оборону;
- технічну підготовку й організацію виробничих процесів;

- організацію життєзабезпечення персоналу;
- матеріально-технічне забезпечення;
- облік та фінансову діяльність;
- планування діяльності ВОПН та управління ним.

Цілком справедливо припустити, що за кожним з цих та інших напрямів існують певні нормативні вимоги, неухильне виконання яких дає змогу підтримувати рівень безпеки ВОПН на задовільному рівні. Однак, на жаль, на сьогодні не існує системних інтегральних вимог щодо забезпечення безпеки функціонування ВОПН у цілому [1, 2]. Більше того, допускаються порушення навіть елементарних вимог до безпечного функціонування ВОПН, наприклад:

- фактична завантаженість місць зберігання ракет і боєприпасів значно перевищує проектну;
- велика кількість боєприпасів зберігається на відкритих майданчиках і не захищена від атмосферного впливу;
- місця зберігання обладнані застарілою пожежною сигналізацією;
- інженерні мережі тепло- та водопостачання застарілі і ненадійні;
- відсутні або не відповідають технічним умовам блискавкозахисні споруди;
- охоронні периметри у ряді випадків не оснащені сучасними технічними приладами охорони;
- контрольно-пропускні пункти не оснащені відповідними технічними засобами;
- системи управління ВОПН побудовані без використання сучасних інформаційних технологій.

Для повного й ефективного вирішення питань безпеки ВОПН потрібні великі матеріальні і фінансові ресурси, яких в Україні хронічно не вистачає. У той же час очевидно, що ліквідація наслідків надзвичайних ситуацій (НС) на ВОПН, наприклад, під час широко відомих подій у Новобогданівці, Лозовій та ін., потребує значно більших зусиль і коштів, ніж своєчасне і повне дотримання вимог щодо їх безпечного функціонування.

Тому існує нагальна потреба пошуку способів оптимізації витрат на забезпечення безпеки ВОПН, які надавали б адміністрації баз, арсеналів складів, керівництву Збройних сил України можливість об'єктивно оцінювати заходи щодо підвищення рівня безпеки ВОПН за критерієм "ефективність – витрати" та приймати найбільш раціональні рішення. У цій статті розглядаються питання методичного підходу до вирішення таких завдань з використанням мережевих моделей рівня безпеки ВОПН.

## **2. Постановка задачі**

Виходячи із зазначеного та з урахуванням результатів інших досліджень і керівних настанов з проблем безпеки ВОПН [3–12], можна зробити такі висновки:

- будь-який ВОПН становить собою взаємодіючу сукупність структурних елементів, безпека функціонування кожного з яких забезпечується певною мірою автономно;
- рівень безпеки ВОПН у цілому залежить від рівня безпеки кожного із його структурних елементів;

– існують керівні документи, згідно з якими кожний ВОПН має пройти ідентифікацію – процедуру виявлення джерел та чинників небезпеки, на підставі яких об'єкт визнається потенційно небезпечним і встановлюються певні нормативні вимоги до рівня безпеки його структурних елементів;

– нормативний рівень безпеки структурних елементів ВОПН в реальності не завжди забезпечується, що негативно впливає на рівень безпеки ВОПН у цілому;

– рівень безпеки ВОПН суттєво залежить від якості системи управління ним, оскільки саме вона забезпечує синергетичний ефект заходів безпеки по окремих структурних елементах об'єкта.

Як правило, адміністрація ВОПН постійно дбає про підвищення його рівня безпеки. Однак в умовах жорстких фінансових і матеріальних обмежень та з урахуванням існуючого стану ВОПН прийняття рішень щодо тих чи інших запобіжних заходів по кожному виду небезпеки перетворюється на складну проблему. Тому автори статті поставили перед собою задачу розробити методичний підхід до обґрунтування таких рішень за допомогою моделювання процесу підвищення рівня безпеки ВОПН, виходячи з наведених нижче міркувань.

### **3. Базові положення методичного підходу до моделювання процесу підвищення рівня безпеки ВОПН**

Підвищення рівня безпеки ВОПН пропонується розглядати як постійний дискретний процес з певними інтервалами часу  $t$ , величина яких визначається розміром наявних коштів для виконання відповідних заходів безпеки. Загальна послідовність дій у цьому процесі включає такі складові:

- групою експертів-аналітиків з питань безпеки ВОПН встановлюється шкала рівнів безпеки ВОПН, яка враховує:

- зовнішні фактори впливу на ВОПН, які можуть призвести до виникнення надзвичайної ситуації;

- рівень безпеки структурних елементів ВОПН, які призначені для нейтралізації зовнішніх факторів впливу та недопущення виникнення надзвичайної ситуації, ступінь їх готовності до виконання своїх функцій;

- ступінь впливу рівнів безпеки структурних елементів ВОПН на безпеку об'єкта в цілому;

- внутрішні загрози, які можуть призвести до виникнення на ВОПН надзвичайної ситуації;

- формується множина можливих стратегій підвищення рівня безпеки ВОПН через підвищення рівня безпеки його структурних елементів;

- визначаються періоди впровадження стратегій підвищення рівня безпеки ВОПН (часові інтервали  $t$ );

- визначаються плани заходів щодо реалізації кожної із сформованих стратегій по періодах;

- прогнозуються рівні безпеки ВОПН, які будуть досягнуті в результаті реалізації запланованих заходів за кожний період, з урахуванням існуючих нормативів безпеки як структурних елементів ВОПН, так і об'єкта в цілому;

- проводиться експертна оцінка вартісних показників заходів кожної стратегії по визначених періодах;

- здійснюється вибір стратегії підвищення рівня безпеки ВОПН за критерієм досягнення максимального (або заданого) результату з мінімальними матеріальними і фінансовими витратами.

Суттєво, що потрібний рівень безпеки ВОПН у цілому визначає також потрібні рівні безпеки його структурних елементів (підрозділів).

#### 4. Порядок побудови моделі підвищення рівня безпеки ВОПН

Порядок побудови моделі процесу підвищення рівня безпеки окремого ВОПН включає три етапи.

**На першому етапі** групою експертів-фахівців з проблеми безпеки ВОПН формується шкала рівнів безпеки об'єкта та визначаються декілька стратегій підвищення рівня його безпеки за визначені періоди часу. Прогнозуються рівні безпеки, які можуть бути досягнуті за ці періоди за кожною з визначених стратегій.

**На другому етапі** розробляється мережева модель процесу підвищення рівня безпеки ВОПН, яка містить знання предметної області, у тому числі шкалу рівнів безпеки. Для опису такої моделі в [13] пропонується сукупність п'яти множин:

$$M = \langle M_1, M_2, M_3, M_4, M_5 \rangle, \quad (1)$$

де  $M_1$  – множина вершин;

$M_2$  – множина імен вершин, яка характеризує рівні безпеки згідно з нормативною шкалою рівнів безпеки;

$M_3$  – множина дуг, що поєднують пари вершин;

$M_4$  – множина дуг, які характеризують конкретні причинно-наслідкові зв'язки між вершинами у конкретній ситуації, тобто вплив одних факторів безпеки на інші;

$M_5$  – множина імен дуг, довжинам яких відповідають конкретні числові характеристики (часові, фінансові тощо).

На думку авторів, для визначення стратегії підвищення рівня безпеки ВОПН можна обмежитися трійкою множин  $\langle M_2, M_4, M_5 \rangle$ , яка характеризує найбільш суттєві відношення в середині мережевої моделі.

Під час побудови графічної частини моделі використаємо такі позначення:

$n$  – кількість окремих структурних елементів ВОПН;

$i$  – нормативний рівень безпеки окремого структурного елемента;

$L$  – кількість нормативних рівнів безпеки;

$i = \overline{1, L}$ .

Кожному  $i$  відповідають певні дискретні рівні безпеки відповідного структурного елемента ВОПН, які можна контролювати.

Нехай початковий рівень безпеки ВОПН дорівнює  $R_1$ . Треба побудувати модель процесу підвищення рівня безпеки ВОПН за  $T$  періодів часу до бажаної величини  $R_T$ , якої можна досягнути

шляхом реалізації однієї із можливих стратегій. При цьому  $R_1$  і  $R_4$  належать до нормативної шкали безпеки.

Для вирішення поставленої задачі визначимо мережу, яку характеризують:

$X_1$  – початкова вершина;

$X_T$  – кінцева вершина;

$T$  – кількість періодів часу;

$(T - 1)$  – кількість шарів рівнів безпеки, кожний з шарів містить  $L$ -вершин;

$(i, t)$  – вершина з  $i$ -м нормативним рівнем безпеки для  $t$ -го інтервалу часу;

$(i, j)^t$  – дуга, яка єднає вершину  $(i, t - 1)$  з вершиною  $(j, t)$ ;

$S^t ij$  – довжина дуги  $(i, j)^t$ .

Початкова вершина з'єднується дугами з усіма вершинами першого шару безпеки. Кінцева вершина з'єднується дугами з усіма вершинами останнього шару безпеки. Отже, з кожної вершини  $(i, t)$  йдуть дуги до відповідних  $L$  вершин  $(t + 1)$  шару безпеки. При цьому рівень безпеки ВОПН від періоду до періоду має або зростати, або залишатися незмінним.

Кожний шлях у мережі, який поєднує початкову вершину з кінцевою, характеризує одну з можливих стратегій підвищення рівня безпеки ВОПН. Тобто шляху  $[X_1, \dots, X_T]$  відповідає стратегія  $\{1, \dots, T\}$ . І навпаки, кожній стратегії відповідає деякий шлях у мережі, який поєднує початкову вершину з кінцевою.

Загальна кількість стратегій підвищення рівня безпеки  $N_s$  визначається рівнянням

$$N_s = (T - 1)^L - (L - 1)(T - 1). \quad (2)$$

Наведемо приклад мережевої моделі, в якому ВОПН розглядається як єдиний неподільний об'єкт, який пройшов ідентифікацію і для якого визначено рівень безпеки згідно з певною нормативною шкалою. Як шкалу оберемо нормативні рівні безпеки  $\{1, 2, 3, 4\}$ , що визначаються фактичною завантаженістю ВОПН боєприпасами:

- 1-й рівень  $R_1$  – ВОПН завантажено на  $(30 \pm 5)$  % більше норми;
- 2-й рівень  $R_2$  – ВОПН завантажено на  $(20 \pm 5)$  % більше норми;
- 3-й рівень  $R_3$  – ВОПН завантажено на  $(10 \pm 5)$  % більше норми;
- 4-й рівень  $R_4$  – завантаження ВОПН відповідає нормі.

Потрібно обрати й спланувати дії, час і кошти для того, щоб за три періоди часу ( $T = 3$ ) підвищити рівень безпеки ВОПН з  $R_1$  до  $R_4$  за умови, що витрати коштів на це будуть мінімальними. Це типова задача вибору варіанта рішення в залежності від вартості його реалізації.

Мережева модель процесу підвищення рівня безпеки ВОПН для зазначених умов наведена на рис. 1. Мережа складається з початкової вершини  $X_1$ , кінцевої вершини  $X_4$ , трьох періодів та двох шарів безпеки, кожний з яких має чотири вершини.

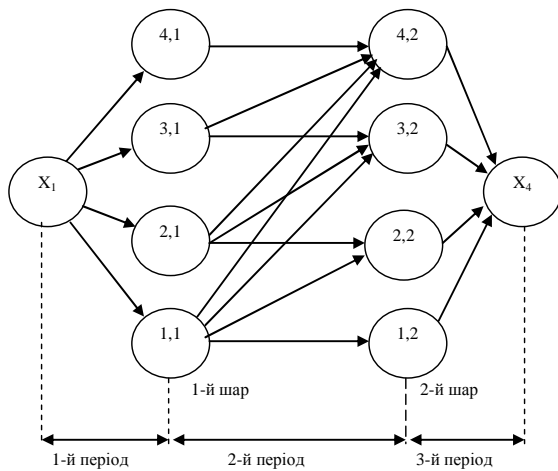


Рис. 1. Приклад мережевої моделі процесу підвищення рівня безпеки ВОПН

Загальна кількість можливих стратегій підвищення рівня безпеки ВОПН для цього випадку складає  $N_s = 10$  :

шлях  $[X_1, (1, 1), (1, 2), X_4] \rightarrow$  стратегія  $\{1, 1, 1, 4\}$ ;

шлях  $[X_1, (1, 1), (2, 2), X_4] \rightarrow$  стратегія  $\{1, 1, 2, 4\}$ ;

шлях  $[X_1, (1, 1), (3, 2), X_4] \rightarrow$  стратегія  $\{1, 1, 3, 4\}$ ;

шлях  $[X_1, (1, 1), (4, 2), X_4] \rightarrow$  стратегія  $\{1, 1, 4, 4\}$ ;

шлях  $[X_1, (2, 1), (2, 2), X_4] \rightarrow$  стратегія

$\{1, 2, 2, 4\}$ ;

шлях  $[X_1, (2, 1), (3, 2), X_4] \rightarrow$  стратегія  $\{1, 2, 3, 4\}$ ;

шлях  $[X_1, (2, 1), (4, 2), X_4] \rightarrow$  стратегія  $\{1, 2, 4, 4\}$ ;

шлях  $[X_1, (3, 1), (3, 2), X_4] \rightarrow$  стратегія  $\{1, 3, 3, 4\}$ ;

шлях  $[X_1, (3, 1), (4, 2), X_4] \rightarrow$  стратегія  $\{1, 3, 4, 4\}$ ;

шлях  $[X_1, (4, 1), (4, 2), X_4] \rightarrow$  стратегія  $\{1, 4, 4, 4\}$ .

**На третьому етапі** розробляється алгоритмічне забезпечення використання мережевої моделі для вибору раціональної стратегії підвищення рівня безпеки ВОПН, тобто послідовність обчислень, за допомогою яких обробляється ця модель та визначається раціональне рішення щодо підвищення рівня безпеки ВОПН.

Вибір найбільш раціональної стратегії підвищення рівня безпеки ВОПН може здійснюватись за різними критеріями [14]. Очевидно, що в першу чергу нас цікавить максимальний рівень безпеки. Однак завжди визначальним фактором будуть також потрібні матеріальні і фінансові витрати. Тому в методичному підході, що пропонується, використовується економічний критерій – мінімізація витрат для певного підвищення рівня безпеки ВОПН. Отже, завдання полягає у виборі найбільш раціональної стратегії дій з точки зору досягнення задовільного результату з мінімальними витратами матеріальних і фінансових ресурсів.

Зіставимо довжині дуги  $S_{ij}^t$  витрати на досягнення й підтримання у періоді  $t$  рівня безпеки  $j$ , якщо у періоді  $(t-1)$  був рівень безпеки  $i$ . Тоді пошук найбільш раціональної стратегії зводиться до визначення шляху, який має мінімальну довжину. Саме найменша сукупність довжин дуг, що поєднує початкову вершину з кінцевою, визначає стратегію, якій відповідає величина витрат для підвищення рівня безпеки ВОПН з  $R_1$  до  $R_4$ .

Для формальної постановки вибору стратегії підвищення рівня безпеки введемо логічну функцію  $X_{kj}^t$ , яка визначає, чи забезпечується у  $k$ -му структурному елементі (підрозділі) ВОПН у періоді  $t$  рівень безпеки, що дорівнює або більше  $j$ , чи ні:

$$X_{kj}^t = \begin{cases} 1, & \text{у } k\text{-му підрозділі у періоді } t \text{ досягається рівень безпеки } j \\ 0, & \text{у } k\text{-му підрозділі у періоді } t \text{ не досягається рівень безпеки } j \end{cases}$$

Визначимо, що у кожному періоді  $t$  для кожного  $k$ -го підрозділу встановлюється лише один рівень безпеки  $j$ , тобто

$$\sum_{j=0}^j X_{kj}^t = 1, \quad k = 1, n, \quad t = 1, T. \quad (3)$$

Умови незменшення рівнів безпеки підрозділів від періоду до періоду задаються виразом

$$\sum_j X_{kj}^t - j \geq \sum_j X_{kj}^{t-1} j, \quad k = 1, n, \quad t = 1, T. \quad (4)$$

Сукупність значень  $X_{ij}^t$ , які задовольняють (3) і (4), є прийнятною стратегією підвищення рівня безпеки  $k$ -го підрозділу ВОПН. У свою чергу, сукупність значень  $X_K \{X_{Kj}^t j, j = \overline{1, J}, t = \overline{1, T}\}$ , яка задовольняє (2) і (3), будемо вважати прийнятною стратегією підвищення рівня безпеки ВОПН у цілому.

Умову підвищення рівня безпеки ВОПН від початкового рівня  $R_1$  до потрібного рівня  $R_T$  можна записати у вигляді

$$\sum_K \sum_j X_{Kj}^t j = R_t, \quad (5)$$

а вимога мінімізації втрат для цього зводиться до мінімізації функції

$$S(x) = \sum_K \sum_i \sum_j X_{Ki}^{t-1} X_{Kj}^t S_{Kij}^t, \quad (6)$$

де  $S_{Kij}^t$  – величина зменшення витрат на безпеку  $k$ -го структурного елемента ВОПН внаслідок досягнення для нього у періоді  $t$  рівня безпеки  $j$  за умови, що у періоді  $(t-1)$  рівень безпеки дорівнював  $i$ . Задача визначення раціональної стратегії підвищення рівня безпеки ВОПН у цілому полягає у мінімізації функції  $S(x)$  при обмеженнях (3) і (4).

Задача вибору стратегії підвищення рівня безпеки окремого структурного елемента ВОПН вирішується аналогічно. Відмінність полягає лише в тому, що в ролі ВОПН виступає його структурний елемент.

## 5. Висновки

Викладений методичний підхід до побудови моделі процесу підвищення рівня безпеки об'єкта підвищеної небезпеки спрямований на підтримку прийняття управлінських рішень щодо запобігання

виникнення техногенних надзвичайних ситуацій, насамперед, на військових об'єктах. Процедура об'єктивного вибору раціональної стратегії підвищення рівня безпеки ВОПН, що запропонована, поєднує використання знань експертів-аналітиків предметної області з побудовою та обчисленням мережевої моделі процесу підвищення рівня безпеки. Її перевагами є, по-перше, відносна простота і наочність, по-друге, високий ступінь формалізації і придатності до використання в сучасних високоінтелектуальних системах підтримки рішень на основі відповідних інформаційних технологій, по-третє, можливість використання для вибору раціональних стратегій підвищення рівня безпеки не тільки військових, а й будь-яких інших об'єктів підвищеної небезпеки.

Важливо, що зазначений підхід зорієнтований на досягнення максимального корисного ефекту в умовах заданих мінімальних ресурсних витрат.

## СПИСОК ЛІТЕРАТУРИ

1. Кузьменко Г.Є., Хомініч В.С. До питань управління безпекою ВОПН // Математичні машини і системи. – 2008. – № 3. – С. 131 – 140.
2. Морозов А.О., Косолапов В.Л. Інформаційно-аналітичні технології підтримки прийняття рішень. – Київ: Наукова думка, 2002. – 232 с.
3. Закон України від 18.01.2001 № 2245-III “Про об'єкти підвищеної небезпеки”. – 4 с.
4. Постанова Кабінету Міністрів від 11.07.2002 № 956 “Про ідентифікацію та декларування безпеки об'єктів підвищеної небезпеки”. – 28 с.
5. Наказ МО України № 172 від 24.05.2004 “Про затвердження Переліку об'єктів Збройних сил України, які підлягають обладнанню автоматичними установками пожежогасіння та пожежної сигналізації”. – 2 с.
6. Наказ МО України № 531 від 04.11.2008 “Про затвердження правил техногенної безпеки у сфері цивільного захисту на об'єктах МО України”. – 6 с.
7. Наказ МНС України № 98 від 23.02.2006 “Про затвердження Методики ідентифікації потенційно небезпечних об'єктів”. – 1 с.
8. Основы обеспечения безопасности артиллерийских arsenалов, баз и складов боеприпасов / Б.Г. Романенко, А.В. Мельников, В.В. Чернов и др. – Пенза: ПААИ, 2001. – С. 245.
9. Антитеррористическая безопасность. [www.kosdormii.ru/page2/article22/](http://www.kosdormii.ru/page2/article22/).
10. О концептуальном проектировании систем безопасности. [www.Ktso.ru/statyi/konsep/konsep\\_3/php](http://www.Ktso.ru/statyi/konsep/konsep_3/php).
11. Системы безопасности. [www.iching.ru/6/Bezopasnost-5.html](http://www.iching.ru/6/Bezopasnost-5.html).
12. Аудит пожарной безопасности. Определение категорий по взрывоопасной и пожарной безопасности. [Nadzor01.ucoz.ru/index/0-8](http://Nadzor01.ucoz.ru/index/0-8).
13. Аверкин Н.Н., Гаазе-Рапопорт М.Г., Поспелов Д.А. Толковый словарь по искусственному интеллекту. – М.: Радио и связь, 1992. – 252 с.
14. Теслер Г.С. Новая кибернетика. – Киев: Логос, 2004. – 404 с.

*Стаття надійшла до редакції 18.03.2009*