DOI: https://doi.org/10.36910/6775-2524-0560-2021-45-02
УДК 517.9, 519.85, 004.9
Димова Ганна Олегівна, к.т.н., доцент,
https://orcid.org/0000-0002-5294-1756
Херсонський державний аграрно-економічний університет, м. Херсон, Україна

АНАЛІЗ МЕТОДІВ ОЦІНКИ ЕФЕКТИВНОСТІ СИСТЕМ ФІЗИЧНОГО ЗАХИСТУ

Димова Г.О. Аналіз методів оцінки ефективності систем фізичного захисту. Статтю присвячено дослідженню існуючих методів оцінки ефективності систем фізичного захисту об'єктів інформатизації. Питання забезпечення безпеки різних об'єктів, в першу чергу, таких як критична інфраструктура, інформатизація, якими в даний час є переважна більшість об'єктів є дуже важливими. Один з найважливіших елементів практично будь-якої системи безпеки – це система фізичного захисту (СФЗ). Крім того, захист інформації включає в себе, серед інших, і фізичний захист, яка полягає в застосуванні організаційних заходів і сукупності засобів, що створюють перешкоди для проникнення або доступу неуповноважених фізичних осіб до об'єкта захисту. Створення такої СФЗ об'єктів інформатизації (ОІ) передбачає аналіз ефективності і уразливості СФЗ як важливий етап розробки будь-якої системи. У свою чергу, складність сучасних СФЗ, а також різноманіття моделей порушників і способів проникнення спричиняє необхідність застосування засобів автоматизації процесів моделювання таких систем. Різні методи аналізу ефективності СФЗ базуються на даних експертних оцінок основних параметрів і, отже, мають високий ступінь суб'єктивності. Вони вимагають трудомістких експериментальних досліджень. Крім того, їх складно використовувати в задачах математичного моделювання. Таким чином, актуальними є питання підвищення точності аналізу ефективності СФЗ ОІ. У статті проведено порівняльний аналіз методів оцінки ефективності систем фізичного захисту, до яких увійшли такі підходи: детерміністичний, логіко-ймовірнісний, ймовірнісно-часовий, метод аналізу ієрархій та нечітких множин. Також були розглянуті відомі комп'ютерні моделі та програмні продукти призначені для виявлення загроз об'єкта інформатизації. Приведені основні характеристики і параметри оцінки ефективності СФЗ та необхідні завдання щодо впровадження системи фізичного захисту.
Ключові слова: системи фізичного захисту, оцінка ефективності, детерміністичний метод, аналіз ієрархій, ймовірнісно-часовий аналіз, нечітка логіка.

Дымова А.О. Анализ методов оценки эффективности систем физической защиты. Статья посвящена исследованию существующих методов оценки эффективности систем физической защиты объектов информатизации. Вопросы обеспечения безопасности различных объектов, в первую очередь, таких как критическая инфраструктура, информатизация, которыми в настоящее время являются подавляющее большинство объектов есть очень важными. Один из важнейших элементов практически любой системы безопасности – это система физической защиты (СФЗ). Кроме того, защита информации включает в себя, среди прочих, и физическую защиту, заключающуюся в применении организационных мер и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.Создание такой СФЗ объектов информатизации (ОИ) предполагает анализ эффективности и уязвимости СФЗ как важный этап разработки любой системы. В свою очередь, сложность современных СФЗ, а также разнообразие моделей нарушителей и способов проникновения влечет за собой необходимость применения средств автоматизации процессов моделирования таких систем. Различные методы анализа эффективности СФЗ базируются на данных экспертных оценок основных параметров и, следовательно, обладают высокой степенью субъективности. Они требуют трудоемких экспериментальных исследований. Кроме того, их сложно использовать в задачах математического моделирования. Таким образом, актуальны вопросы повышения точности анализа эффективности СФЗ ОИ.В статье проведен сравнительный анализ методов оценки эффективности систем физической защиты, в которые вошли следующие подходы: детерминистический, логико-вероятностный, вероятностно-временной, метод анализа иерархий и нечетких множеств. Также были рассмотрены известные компьютерные модели и программные продукты, предназначенные для выявления угроз объекта информатизации. Приведены основные характеристики и параметры оценки эффективности СФЗ и необходимые задачи внедрения системы физической защиты.
Ключевые слова: системы физической защиты, оценка эффективности, детерминистический метод, анализ иерархий, вероятностно-временной анализ, нечеткая логика.

Dymova H. Analysis of methods for assessing the effectiveness of physical protection systems. The article is devoted to the study of existing methods for assessing the effectiveness of physical protection systems of objects of informatization. The issues of ensuring the security of various objects, primarily, such as critical infrastructure, informatization, which are currently the overwhelming majority of objects, are very important. One of the most important elements of almost any security system is the physical protection system (PPS). In addition, information protection includes, among others, physical protection, which consists in the use of organizational measures and a set of means that create obstacles to the penetration or access of unauthorized individuals to the protected object.The creation of such a PPS of objects of informatization (OI) involves the analysis of the effectiveness and vulnerability of PPS as an important stage in the development of any system. In turn, the complexity of modern PPS, as well as the variety of models of intruders and methods of penetration entails the need to use automation tools for modeling such systems. Various methods for analyzing the effectiveness of PPS are based on the data of expert assessments of the main parameters and, therefore, have a high degree of subjectivity. They require laborious experimental research. In addition, they are difficult to use in mathematical modeling problems. Thus, the issues of increasing the accuracy of the analysis of the effectiveness of the PPS OI are topical.The article provides a comparative analysis of methods for assessing the effectiveness of physical protection systems, which include the following approaches: deterministic, logical-probabilistic, probabilistic-temporal, the method of analyzing hierarchies and fuzzy sets. The well-known computer models and software products designed to identify threats to the object of informatization were also considered. The main characteristics and parameters for assessing the effectiveness of the PPS and the necessary tasks of introducing a physical protection system are given.
Keywords: physical protection systems, performance assessment, deterministic method, hierarchy analysis, probabilistic-time analysis, fuzzy logic.

Постановка проблеми. Під ефективністю технічної системи зазвичай розуміють її пристосованість до виконання своєї цільової функції. Зокрема, ефективність системи фізичного захисту (СФЗ) можна трактувати як здатність системи протистояти несанкціонованим діям порушника в рамках проектної загрози.

При цьому розрізняють дві різних сторони поняття «ефективність»:

- effectiveness (результативність) – степінь досягнення результатів, які заплановані;
- efficiency (ефективність) – співвідношення між досягнутими результатами і ресурсами, які були витрачені.

Відповідно до цього запропоновано два різні трактування цього поняття:

- результативна ефективність (РЕ) – ефективність в сенсі результативності;
- економічна ефективність (ЕЕ) – ефективність в сенсі економічності.

Більш правильно розуміти під ефективністю СФЗ саме результативну ефективність, а ефективність в сенсі економічності виділяти в групу комплексних показників виду «ефективність – вартість».

Оцінка ефективності – це процедура (дослідження), що проводиться в рамках аналізу уразливості і спрямована на визначення якісних і/або кількісних показників ефективності, виявлення критичних елементів СФЗ, а також визначення інтегрального показника ефективності системи в цілому. При системному підході до створення СФЗ результати оцінки ефективності служать вихідними даними для етапу робочого проектування системи.

Метою дослідження є аналіз відомих методів оцінки ефективності і визначення можливих шляхів їх оптимізації для можливості використання для різних об'єктів інформатизації.

Аналіз досліджень. Задача розробки моделей та методів аналізу ефективності засобів виявлення систем фізичного захисту об'єкта інформатизації (СФЗ ОІ), а також оцінки ймовірності виявлення порушника є актуальним. Незважаючи на велику кількість публікацій відомих спеціалістів у галузі систем фізичного захисту, таких як Гарсіа М.Л., Петраков А.В., Бузов Г.А. та інші, ряд питань створення та оцінки ефективності СФЗ ОІ залишаються недостатньо дослідженими.

Виклад основного матеріалу й обґрунтування отриманих результатів. Існує декілька методів оцінки ефективності:

- детерміністичний метод;
- логіко-ймовірнісний метод;
- метод аналізу ієрархій;
- метод ймовірнісно-часового аналізу;
- метод нечітких множин.

Детерміністичний підхід [1] є експертним методом оцінки ефективності. Він застосовується при перевірках органами відомчого контролю стану фізичного захисту ядерно і радіаційно-небезпечних об'єктів. В рамках даного методу експерти перевіряють на відповідність реальний стан СФЗ вимогам керівних документів. За числовим значенням показника стану СФЗ визначають степінь її відповідності вимогам стандартів, що і є показником ефективності системи.

Детерміністичний підхід пов'язаний із завданням і подальшою перевіркою обов'язкових вимог, що містяться у відомчих керівних документах (КД), технічному завданні (ТЗ) на проектування, робочому проекті. Цей підхід передбачає проведення комплексних перевірок органами державного нагляду чи відомчого контролю. Ці перевірки можуть проводитися із заданою регулярністю або при зміні вимог до об'єкту внаслідок зміни переліку загроз, модернізації СФЗ та іншого. При цьому контролю піддаються організаційні заходи, комплекс інженерно-технічних засобів, організаційні заходи щодо дії персоналу служби безпеки тощо.

Процедура експертної оцінки може бути побудована по-різному [1]. В одному випадку, результати можуть інтерпретуватися на якісному рівні, а в інших випадках, на підставі отриманих даних можуть конструюватися інтегральні критерії, що відображають стан СФЗ в цілому.

В якості реалізації даного підходу можна звернутися до експертного методу оцінки стану фізичного захисту [2]. Цілями оцінки стану є:

- перевірка відповідності фізичного захисту висунутим до неї вимогам;
- виявлення елементів, які не відповідають вимогам до СФЗ («критичних елементів»).

Для цього розроблена система факторів стану (ФС), які визначають організацію та забезпечення фізичного захисту відповідно до вимог нормативних документів. В цьому випадку розрізняють:

- ФС організаційних заходів (група *a*);
- ФС інженерно-технічних засобів охорони (група *b*);
- ФС дій підрозділів охорони (група *c*).

Процедура оцінки полягає в наступному:

1. Експерт вибирає кілька ФС по групам *a, b, c* відповідно. Кожному ФС кожен експерт призначає визначену «вагу».

2. Кожному ФС експерти дають оцінку степені реального стану ФС (d_n = 0,1,2,3).
3. Визначається середнє значення показника реального стану кожного ФС d_i.

$$d_i = \frac{\sum_{j=1}^{n} d_{ij}}{n} \quad (1)$$

де d_i – показник реального стану i-го ФС, призначеного j-им експертом;
n – число експертів.

Методи логіко-імовірнісного моделювання або логіко-імовірнісного аналізу [3, 4] застосовуються для дослідження надійності та живучості структурно-складних систем, в тому числі СФЗ. В ході застосування методу розробляється модель розвитку загрози об'єкту, що охороняється, у вигляді графа. Розрахунок степені ризику ведеться із застосуванням алгебри логіки і теорії ймовірності. Степінь ризику і визначає ефективність системи.

Ці методи давно застосовуються на практиці [1] для аналізу живучості складних систем. При розрахунку надійності досліджуються умови знаходження системи в працездатному стані, а при аналізі безпеки – умови потрапляння системи в небезпечний стан.

У цьому випадку метою дослідження є визначення степені ризику, що присутній в системі.

Процедура оцінки виглядає наступним чином:

1. Складається сценарій розвитку небезпеки, що представляє собою логіко-ймовірнісну модель функціонування СФЗ. Сценарій представляється у вигляді графа («дерева») і містить події трьох видів: ініційовані, проміжні і кінцевий стан. Ініційовані події описують дії порушника на систему (порушення периметра об'єкту охорони, імітація процедури ідентифікації та ін.). Проміжні події виходять шляхом логічної комбінації двох або більше подій (логічне І, АБО та інше). Кінцева подія описує визначений небезпечний стан системи.
2. Складається функція небезпеки системи $y(z_1, \dots z_n)$. Аргументами цієї функції є ініційовані події, а значенням – кінцева (небезпечна) подія.
3. Функція небезпеки системи замінюється ймовірнісною функцією $P\{ y(z_1, \dots z_n)\}$ наступним чином:
   - z_i замінюється на $P\{z_i = 1\} = R_i$ (ймовірність того, що i-а ініційована подія станеться);
   - z_i' замінюється на $P\{z' = 1\} = Q_i = 1 - R_i$ (ймовірність того, що i-а ініційована подія не станеться).
4. Відшукується значення ймовірнісної функції в припущенні реалізації небезпечної події

$$Y(y) = P\{ y(z_1, \dots z_n) = 1\}. \quad (2)$$

Ця функція і визначає степінь ризику, присутнього в системі.

Недоліком цього методу є значний обсяг трудомістких логічних перетворень при аналізі складних сценаріїв.

Задача *методу аналізу ієрархій*, розроблена Т. Сааті [5], полягає в знаходженні вектора вагових коефіцієнтів

$$\alpha = (\alpha_1, \alpha_2, \dots, \alpha_m) \quad (3)$$

за відомою матрицею попарних порівнянь S.

Згідно методу аналізу ієрархій по трикутній матриці **S** будується наступна повнозаповнена матриця $\bar{S}$:

$$\bar{S} = \begin{bmatrix} 1 & \alpha_{12} & \alpha_{13} & \cdots & \alpha_{1m} \\ \alpha_{21} & 1 & \alpha_{23} & \cdots & \alpha_{2m} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \alpha_{m1} & \alpha_{m2} & \alpha_{m3} & \cdots & 1 \end{bmatrix}, \quad (4)$$

де елементи нижньої трикутної частини α_{ij} ($i > j$) матриці задовольняють співвідношенням

$$\alpha_{ij} = 1/\alpha_{ji} \quad (5)$$

Легко довести, що шуканий вектор

$$\alpha = (\alpha_1, \alpha_2, \dots, \alpha_m)$$

є власним вектором матриці $\bar{S}$, відповідним максимальному власному числу матриці $\lambda = m$ і може бути знайдений як розв'язок системи рівнянь:

$$\bar{S}\alpha = \lambda_{\max}\alpha \tag{6}$$

Існує єдине розв'язання даної системи лінійних алгебраїчних рівнянь, що задовольняє умові

$$\sum_{i=1}^{m} \alpha = 1. \tag{7}$$

Якщо матриця системи (6) задана неточно, то пропонується чисельно визначити її максимальне власне число і відповідний власний вектор.

У методі аналізу ієрархій передбачається, що приватні критерії f_i не обов'язково є числовими функціями і можуть мати якісний неформальний характер. В цьому випадку для кожного критерію f_i ставиться задача ранжирування об'єктів $\{x_1, x_2, ..., x_n\}$ з побудовою на основі діалогу з користувачем відповідної матриці попарних порівнянь і визначенням вектора ваг

$$\alpha' = (\alpha'_1, \ldots, \alpha'_n). \tag{8}$$

Отримані числа α'_j інтерпретуються як значення f_i (x_i), $j = \overline{1,n}$. Таким чином, кожна альтернатива отримує вже числову оцінку по кожному з приватних критеріїв.

Далі здійснюється аналогічна операція по ранжируванню самих приватних критеріїв за важливістю з побудовою вектора ваг

$$\beta = (\beta_1, \ldots, \beta_m).$$

В якості оптимальної альтернативи (їх може бути декілька) вибираємо

$$x^* = \arg\max_i J(x_i), \tag{9}$$

де

$$J(x_i) = \sum_{k=1}^{m} \beta_k f_k(x_i), \quad i = \overline{1,n}, \qquad f_k(x_i) = \alpha_i^k. \tag{10}$$

У *методі ймовірнісно-часового аналізу* [1, 2] для розрахунку ефективності використовують ймовірнісні і часові характеристики процесу проникнення. В основу закладено принцип своєчасного виявлення, згідно з яким ефективність СФЗ визначає сумарна ймовірність виявлення порушника в той момент, коли у сил охорони ще достатньо часу для перехоплення порушника на шляху останнього до мети. Цю ймовірність називають ймовірністю перехоплення.

Ймовірнісно-часовий аналіз є в даний час найбільш використовуваним для оцінки СФЗ [5]. Принципи такого підходу були закладені в кінці 70-х років минулого століття в США для захисту об'єктів департаменту енергетики, а також інших державних об'єктів.

Ефективність фізичного захисту тут розглядається як імовірнісна величина, ймовірність того, що сили охорони, що діють за сигналами технічних засобів, встигають припинити акцію порушника.

Використовуючи математичну модель проникнення порушника можна побудувати модель на основі *нечіткої логіки*.

Для побудови даної моделі нечіткої множини може бути застосований алгоритм Сугено [6]. В даному алгоритмі спосіб обчислення вихідних змінних наступний:

$$\begin{array}{c} L^1\text{: якщо } x_1 = A_1^{(1)} I \ldots I\, x_n = A_n^{(1)}\text{, то} \\ \left\{\begin{array}{c} u_1^{(1)} = c_{01}^{(1)} + c_{11}^{(1)} \cdot x_1 + \ldots + c_{n1}^{(1)} \cdot x_n \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ u_m^{(1)} = c_{0m}^{(1)} + c_{1m}^{(1)} \cdot x_1 + \ldots + c_{nm}^{(1)} \cdot x_n \end{array}\right. \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ L^N\text{: якщо } x_1 = A_1^{(N)} I \ldots I\, x_n = A_n^{(N)}\text{, то} \\ \left\{\begin{array}{c} u_1^{(N)} = c_{01}^{(N)} + c_{11}^{(N)} \cdot x_1 + \ldots + c_{n1}^{(N)} \cdot x_n \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ u_m^{(N)} = c_{0m}^{(N)} + c_{1m}^{(N)} \cdot x_1 + \ldots + c_{nm}^{(N)} \cdot x_n \end{array}\right. \end{array} \tag{11}$$

де $A_j^{(p)}, (j = 1,2,\dots, n; p = 0,1,2,\dots, N)$ – значення лінгвістичних змінних $x_1, x_2, \dots, x_n$;

N – число цих значень (нечітких множин);

$c_{kj}^{(p)}$ – фіксовані числові коефіцієнти $(k = 0,1,2,\dots, n)$;

$u_i^{(p)}$ – складова i-го вихідного сигналу u_i, що відповідає правилу L^p.

Результуюче значення i-го виходу сигналу u_i^* знаходиться як зважене середнє від зазначених чисел $u_i^{(p)}$:

$$u_i^* = \frac{\sum_{p=1}^{N} W^{(p)} \cdot u_i^{(p)}}{\sum_{p=1}^{N} W^{(p)}}, (i = 1,2,\dots, m), \tag{12}$$

де $W^{(p)}$ – вага значення лінгвістичних змінних $x_1, x_2, \dots, x_n$.

$$W^{(p)} = \prod_{i=1}^{n} \mu_{A_i(p)}(x_i) \tag{13}$$

Вага є Т-нормою для перетину нечітких множин $A_j^{(p)}, (j = 1,2,\dots, n)$, обчисленої для конкретних значень $x_1, x_2, \dots, x_n$.

Нечіткий регулятор Такагі-Сугено є компактною системою управління, яка описує механізм логічного висновку з меншими обчислювальними витратами (близько 50-100 разів швидше, ніж існуючі алгоритми) на реалізацію самого алгоритму логічного висновку [6].

Оцінка уразливості є задачею ймовірнісного аналізу і може бути розв'язана відомими способами [6]. Розглянемо це за допомогою відомих *комп'ютерних моделей.*

EASI (Estimate of Adversary Sequence Interruption) є найстарішим програмним продуктом, який застосовується для цих цілей. Це простий і зручний у використанні метод оцінки ефективності СФЗ на заданому маршруті при певних загроз і станах системи фізичного захисту. Дана модель розраховує ймовірність переривання на підставі аналізу взаємодії виявлення, затримки, передачі інформації і реагування.

У моделі використовуються значення параметрів виявлення, затримки, розгортання сил відповідного реагування і встановлення зв'язку, за допомогою яких розраховується результат – ймовірність перехоплення (переривання послідовності дій) на даному маршруті.

Вихідні дані моделі EASI:

- значення P_i для кожного датчика на маршруті;
- ймовірності встановлення аварійного зв'язку з охороною;
- значення часу затримки для кожного T_i і середньоквадратичне відхилення для кожного з цих значень;
- значення часу розгортання сил реагування T_g і середньоквадратичне відхилення для цього значення.

Значення ймовірності перехоплення або ймовірності переривання послідовності дій порушників до вчинення ними несанкціонованих дій є результатами розрахунку по заданим вихідним даним.

Інший інструмент – розрахунок часу затримки, а потім виставлення ймовірностей.

Модель EASI може використовуватися для аналізу уразливості об'єкта, але вона не дозволяє аналізувати ймовірність нейтралізації порушників.

При прийнятті технічних рішень, що впливають на функціонування СФЗ, необхідно враховувати невизначеність, найважливішу характеристику зовнішнього середовища, тобто неповноту, відсутність, недостатність інформації про порушника, явище, процес, або ж невпевненість у достовірності інформації. У сфері забезпечення безпеки є множина джерел виникнення невизначеності для систем самого різного рівня складності і масштабів.

Невизначеність зумовлює появу ситуацій, які не мають однозначного результату (рішення). Серед них особливе місце займають ситуації ризику, яким супроводжують необхідність вибору альтернативи і можливість оцінити ймовірність здійснення обираних альтернатив.

Існують різні види невизначеності:

- кількісна, обумовлена значним числом об'єктів або елементів в ситуації;

- інформаційна, викликана браком інформації або її неточністю з технічних, соціальних та інших причин;
- вартісна – через занадто дорогої або недоступної плати за визначеність;
- професійна – як наслідок недостатнього професіоналізму персоналу (не враховується, наприклад, необхідна кількість факторів, що впливають);
- обмежувальна, яка викликана обмеженнями в ситуації ухвалення рішень, наприклад обмеження по часу та інше.

Для аналізу всіх можливих маршрутів порушників і визначення найбільш вразливих маршрутів потрібні складніші моделі і програми.

Комп'ютерна модель SAVI (System Analysis of Vulnerability to Intrusion), що дозволяє визначити найбільш уразливий маршрут на діаграмі послідовності дій (ДПД) порушників. Аналіз за допомогою цієї моделі починається з ідентифікації цілі порушників і побудови відповідної логічної ДПД з урахуванням індивідуальних характеристик об'єкта. Необхідно визначити значення часу розгортання сил охорони, значення ймовірності виявлення і час затримки для кожного елемента захисту зазначеної на схемі послідовності дії порушників. Вся ця інформація використовується в якості вихідних даних для роботи програми [6].

Програма розраховує 10 найбільш вразливих маршрутів в порядку, відповідному степені їх вразливості. Результати можуть бути також представлені у вигляді графіків і карти маршрутів.

Алгоритм обчислення ймовірності перехоплення, застосовуваний в моделі SAVI, реалізується при двох досить консервативних припущеннях:

- порушникам відомі характеристики системи захисту;
- порушники використовують оптимальні стратегії проникнення.

Усвідомлений вибір рішення по затримці і нейтралізації порушників повинен проводитися на основі порівняння результатів оцінки альтернатив. Тому ставиться задача отримати для кожної альтернативи значення результатів, що характеризують інтенсивність істотних властивостей результатів операції, запланованої до проведення в заданих умовах.

Етапами оцінки вразливості в програмі SAVI є:

- ідентифікація цілей порушників;
- побудова ДПД з урахуванням характеристик об'єкта;
- визначення значень часу затримки і ймовірності виявлення;
- визначення характеру загрози і рівня оснащення порушників;
- опис методів проникнення, які використовуються порушниками;
- визначення стратегії сил реагування;
- визначення часу, необхідного силам реагування для припинення дій порушників;
- аналіз (запуск програми SAVI);
- багаторазове виконання процедури аналізу чутливості системи захисту до зміни параметрів або удосконаленням системи фізичного захисту.

Результати можуть бути представлені у вигляді схем чутливості – найгірше значення сумарної ймовірності виявлення P_i в залежності від часу, необхідного силам реагування T_g, а також схем уразливості – P_i і час, що залишився після переривання для найбільш вразливих маршрутів при заданому значенні T_g.

SAVI також дає можливість отримати текстовий файл в pdf-форматі для подальшої оцінки та аналізу СФЗ. Він включає схеми уразливості і чутливості, діагностичні дані щодо вразливості обраного маршруту, опис обраного маршруту від границь об'єкта до мети і назад (якщо вказана стратегія затримки порушника). Для кожної точки маршруту вказуються методи виявлення і способи їх подолання (вказуються потенційно ефективні, але невикористані кошти виявлення).

ASSESS (Analytic System and Software for Evaluating Safeguards and Security) є найбільш потужною комп'ютерною програмою, яка дозволяє проводити глобальний аналіз системи фізичного захисту об'єкта. ASSESS – це аналітична система і програмне забезпечення для оцінки ефективності систем захисту і забезпечення безпеки, що дозволяє розглядати зовнішніх і внутрішніх порушників і моделювати загрозу від їх змови. Модуль, який аналізує загрозу з боку зовнішніх порушників, розроблений в рамках методики SAVI. Модуль ET дозволяє знаходити найбільш уразливий сценарій для внутрішнього порушника. Модуль BATLE розроблений для оцінки результату перехоплення і сутички сил реагування та порушників.

Висновки та перспективи подальшого дослідження. Як основний недолік, властивого в більшій чи меншій мірі усіх розглянутих вище методів, можна відзначити недостатню степінь обліку імовірнісних характеристик порушника і системи безпеки. У тому числі це стосується недостатньою

мірою обліку: випадкового вибору маршруту порушником, ймовірнісного характеру виявлення несанкціонованих дій, параметрів об'єкта і засобів виявлення, характеристик порушника тощо.

Задача оцінки ефективності СФЗ характеризується, перш за все, високим ступенем апріорної невизначеності характеристик і параметрів:

- моделі порушника (рівень кваліфікації, степінь підготовленості, кількість порушників, наявність апріорної інформації про об'єкт і СФЗ і степінь її повноти та інше);
- тактики дій порушника (обраний маршрут пересування, параметри руху, способи і тривалості подолання перешкод, способи та ймовірність подолання засобів виявлення без тривоги, можливість просування до різних цілей тощо).

Все це призводить до ймовірнісного характеру ряду властивостей і параметрів самої СФЗ. В першу чергу, тих, які визначають її результативну ефективність.

У зв'язку з високим ступенем невизначеності даних про модель порушника, застосування детерміністичних методів представляється малоефективним. На процес проникнення порушника впливає велика кількість параметрів, тому вибір маршруту, час подолання перешкод, вибір методів і засобів подолання і виявлення є випадковими величинами. Таким чином, їх потрібно врахувати ймовірнісними характеристиками. Тому краще за все використання ймовірнісного методу. При цьому для впровадження СФЗ необхідно виконати наступне.

1. Вибрати математичний апарат обліку випадкового вибору маршруту порушником.
2. Врахувати загальні ймовірнісні характеристики, зокрема ймовірності реалізації тієї чи іншої загрози, того чи іншого способу реалізації кожної загрози, нанесення істотного або неприйнятного збитку тощо.
3. Врахувати ймовірнісні характеристики моделі порушника і тактики його дій.
4. Врахувати ймовірнісний характер часу реагування служби безпеки на виявлене порушення.
5. Прийняти до уваги залежність згаданих ймовірнісних параметрів і характеристик від параметрів і характеристик об'єкта і СФЗ.

При цьому необхідно брати до уваги не тільки найпростіші ймовірнісні характеристики, але і більш «тонкі», наприклад, такі як функції розподілу і щільності розподілу ймовірностей тих чи інших параметрів та їх моменти. А також взаємні залежності перерахованих вище характеристик друг від друга.

Найбільшою мірою сформульованим вимогам задовольняє ймовірнісно-часовий метод, який і може бути взятий за основу для опрацювання та реалізації сформульованих вимог і переліку ймовірнісних характеристик і параметрів.

Список бібліографічного опису

1. Панин О. Проблемы оценки эффективности функционирования систем физической защиты объектов. БДИ. 2007. № 72. С. 22-27.
2. Довідник рятувальника: Аварійно-рятувальні та інші невідкладні роботи з ліквідації наслідків радіаційних аварій. К.: УкрНДІЦЗ, 2013. 186 с.
3. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. Чинний від 01.01.1998 р. К., 1997. 11 с.
4. Волхонский В.В., Крупнов А.Г. Особенности разработки структуры средств обнаружения угроз охраняемому объекту. Научно-технический вестник Санкт-Петербургского государственного университета информационных технологий, механики и оптики. 2011. № 4(74). С. 131-136.
5. Саати Т. Метод принятия решений. Метод анализа иерархий. М.: Радио и связь, 1993. 278 с.
6. Чернорyцкий И.Г. Методы принятия решений. СПб.: БХВ-Петербург, 2005. 416 с.

References

1. Panin O. Problems of evaluation of efficiency of functioning of systems of physical protection of objects. BDI. 2007. № 72. Pp. 22–27.
2. Rescuer Handbook: Rescue and other urgent work to eliminate the consequences of radiation accidents. K .: UkrNDICZ, 2013. 186 p.
3. DSTU 3396.2-97. Information protection. Technical protection of information. Terms and definitions. Effective from 01.01.1998, K., 1997. 11 p.
4. Volkhonsky V.V., Krupnov A.G. Features of the development of the structure of tools for detecting threats to a protected object. Scientific and technical bulletin of the St. Petersburg State University of Information Technologies, Mechanics and Optics. 2011. No. 4 (74). Pp. 131-136.
5. Saati T. Method of decision making. Method for analyzing hierarchies. M.: Radio and communication, 1993. 278 p.
6. Chernorutskiy I.G. Decision making methods. SPb.: BHV-Petersburg, 2005. 416 p.