http://arxiv.org/ftp/arxiv/papers/0907/0907.2221.pdf .- Дата доступу: грудень 2012. – Назва з екрану.
4. *Pelqim Spahiu, Ian R. Evans*. Protection Systems that verify and supervise themselves– IEEE ISGT Innovative Smart Grid Technologies Europe.- 2011.- Режим доступу: http://www.ieee-isgt-2011.eu/wordpress/wp-content/uploads/2012/01/ID9_Self-Healing-Grids_Protection_Systems1.pdf.- Дата доступу: грудень 2012. – Назва з екрану.
5. *G.Filatrella, A. H. Nielsen, N. F*. Pedersen Analysis of a power grid using a Kuramoto-like model. Режим доступу: http://arxiv.org/ftp/arxiv/papers/0705/0705.1305.pdf.- Дата доступу: грудень 2012. – Назва з екрану.
6. Уравнение Курамото-Сивашинского. Режим доступу: http://www.d-dm.ru/kse/common/ .- Дата доступу: грудень 2012. – Назва з екрану.
7. *David Lusseau*. "The emergent properties of a dolphin social network". Proceedings of the Royal Society of London B 270: S186–S188. - 2003 - Режим доступу: http://arxiv.org/ftp/cond-mat/papers/0307/0307439.pdf.- Дата доступу: грудень 2012. – Назва з екрану.
8. *Дульнев Г. Н*. Введение в синергетику.— С.-Пб.: Проспект, 1998.
9. *Емельянов В.В., Курейчик В.В., Курейчик В.М.* Теория и практика эволюционного моделирования. – М.: ФИЗМАТЛИТ, 2003. -432 с.
10. *Ю.Ю.Тарасевич*. Перколяция: теория, приложения, алгоритмы. – М.: Едиториал УРСС, 2002. -112 с.: ил
11. *Хайкин С.* Нейронные сети: полный курс, 2-е изд., исп.: Пер. с англ. – М.: ООО «И.Д.Вильямс», 2006. – 1104 с.
12. *Werbos.* "Using Adaptive Dynamic Programming to Understand and Replicate Brain Intelligence: the Next Level Design" - 2006. - Режим доступу: http://arxiv.org/ftp/q-bio/papers/0612/0612045.pdf.- Дата доступу: грудень 2012. – Назва з екрану.
13. *M. He, S.Murugesan, J.Zhang*. "Multiple Timescale Dispatch and Scheduling for Stochastic Reliability in Smart Grids with Wind Generation Integration". – 2010. - Режим доступу: http://arxiv.org/pdf/1008.3932v2.pdf.- Дата доступу: грудень 2012. – Назва з екрану.
14. *Е.С.Вентцель*. Исследование операций. – М. «Советское радио», 1972, 552 с.
15. *Barreiro, J. Gjorgjieva, F.Rieke; E. Shea-Brown*. "When are feedforward microcircuits well-modeled by maximum entropy methods?". – 2010. - Режим доступу: http://arxiv.org/pdf/1011.2797v3.pdf.- Дата доступу: грудень 2012. – Назва з екрану.

Поступила 25.02.2013р.

УДК 539.1.08

В.М. Буртняк, Ю.Л. Забулонов, Ю.О. Мєдвєдєв, м.Київ.

МЕТОД УПРАВЛІННЯ СИСТЕМАМИ ФІЗИЧНОГО ЗАХИСТУ ЕКОЛОГІЧНО НЕБЕЗПЕЧНИХ ОБ'ЄКТІВ

Abstract. The article presents a general description of the method for management of the physical protection systems of environmentally hazardous

facilities. A brief review of existing methods for evaluating the effectiveness of physical protection systems is given, and their disadvantages are pointed out. Then the main principles of the physical protection systems management with use of concepts of information variable, interval of a controllability stock, and feedback loop are described.

Вступ

Разом із глобальним поширенням та доступністю ядерних технологій зростає загроза їх застосування в злочинних цілях. Навіть мала ймовірність того, що терористи можуть викрасти ядерні матеріали, здійснити диверсію на об'єкті ядерної енергетики, або підірвати власноруч виготовлену "брудну бомбу" може призвести до катастрофічних наслідків. Даний факт робить надзвичайно актуальною розробку та застосування ефективних превентивних заходів, з метою протидії терористам. Як зазначалося в [2], через велику кількість невизначеностей при побудові ймовірнісної моделі, спроби аналізу ризиків тероризму з ракурсу терористів не дали надійного результату, (тобто спробі обчислити ймовірності того, що певні терористичні угрупування спробують зробити ті чи інші дії, тим чи іншим способом, без прив'язки до конкретного об'єкту). Крім того, для виготовлення ядерного вибухового пристрою необхідна невелика кількість ядерних матеріалів, які важко виявити при перевезенні чи контрабанді. Зважаючи на ці факти, доцільним є зосередження уваги на удосконаленні систем фізичного захисту (СФЗ) потенційних цілей ядерних терористів, до яких відносяться підприємства ядерного паливного циклу, науково-дослідні установи, на яких розміщені ядерні установки, воєнні об'єкти та ін.

Короткий огляд існуючих методів оцінки ефективності систем фізичного захисту

До найпоширеніших методів аналізу ефективності функціонування СФЗ відносяться детерміністські, логіко-ймовірнісні, ймовірнісно-часові[9].

Суть детерміністичного підходу полягає у встановленні вимог, що містяться у відомчих документах, технічному завданні на проектування, робочому проекті, та їх подальшій перевірці. Перевіряються інженерно-технічні засоби, організаційні заходи, та дії персоналу. Підхід передбачає проведення органами відомчого контролю комплексних перевірок, які проводяться як планово, так і при зміні чи модернізації СФЗ та в ряді інших випадків. Тобто цілями оцінки є: по-перше, перевірка відповідності СФЗ встановленим вимогам, по-друге, виявлення елементів, що не відповідають цим вимогам. Даний метод за своєю суттю є експертним. Процедура його проведення може бути побудована по різному. Результати можуть оцінюватися як на якісному рівні, так і за допомогою інтегральних критеріїв, що відображають стан СФЗ в цілому. Обмеженнями цього методу є можливість невірної оцінки правильного налаштування та розташування інженерно-технічних засобів СФЗ, правильності дій охорони та ін. через

погрішності при встановленні вимог. Через експертний характер методу, негативну роль може також зіграти і людський фактор. Тобто навіть така СФЗ, що відповідає всім встановленим вимогам, може бути нездатною до вирішення встановлених перед нею задач[9].

Логіко-ймовірнісні методи базуються на операціях над функціями булевої алгебри. Ці методи давно застосовуються для аналізу живучості, надійності та безпеки складних систем В логіко-ймовірнісних методах під ефективністю СФЗ розуміється ймовірність перебування системи в безпечному стані в рамках побудованого сценарію розвитку небезпеки.

Ціллю застосування методів є кількісна оцінка безпеки чи небезпеки функціонування системи в цілому. Процес оцінки проходить наступним чином:

1. Розробляється сценарій розвитку небезпеки, який зображується у вигляді графа (логічного дерева). Граф включає події трьох типів: ініціюючі, проміжні та кінцеві. До ініціюючих подій відносяться можливі дії терориста на систему. Проміжні події включають логічні комбінації (кон'юнкція, диз'юнкція та ін.) декількох подій. Кінцеві події зображують певні небезпечні стани системи(наприклад застосування вибухового пристрою в критичній зоні об'єкта). Розробка таких сценаріїв є відповідальним завданням, від повноти виконання якого залежить якість результатів оцінки.
2. За результатами розробки сценарію небезпеки розробляється функція небезпеки системи $y(x_1,x_2,...x_n)$, в якій ініціюючі події є аргументами, а значенням – небезпечний стан системи.
3. Функція небезпеки замінюється на ймовірнісну функцію наступним чином:

- кожен з аргументів $x_1, x_2,...x_n$, замінюється на відповідну ймовірність ініціюючої події $P(x_n=1)=R_n$ (тобто ймовірність того, що n подія відбудеться).
- Шукається значення ймовірнісної функції в допущенні реалізації небезпечної події: $R= P\{y(x_1,x_2,...x_n)=1\}$.

Власне ця функція і визначає величину ризику, присутнього в системі. Зворотня величина характеризує ефективність СФЗ: $E= 1-P\{y(x_1,x_2,...x_n)$.

Застосування даного методу дозволяє зобразити структуру СФЗ, виявити її слабкі місця, та розділити їх по ступеням безпеки. Головним недоліком цього методу є проблема достовірності ймовірностей ініціюючих подій [8].

Ймовірнісно-часовий аналіз є основним методом, що використовується в даний час для аналізу ефективності СФЗ. Ефективність СФЗ розглядається як ймовірність того, що сили охорони, що діють по сигналам технічних засобів, встигнуть нейтралізувати дії терористів. Для конкретної оперативної ситуації перевіряється виконання умови $\Delta T=T_o-T_m<0$, де T_o час переміщення сил охорони, T_m- час переміщення терористів. Оцінюється час переміщення t_o та t_m, для різних етапів дій терористів та охорони. Наприклад для

терористів це можуть бути: час подолання певних бар'єрів, час для здійснення теракту та ін., для охорони- час збору, час необхідний, щоб дістатися до певної точки та ін. Оскільки всі ці часові інтервали t_i є незалежними випадковими величинами, з невідомими законами розподілу, то, при відносно великій кількості етапів l, згідно з центральною граничною теоремою їх сума:

$$T = \sum_{i=1}^{l} t_i$$

є розподіленою за нормальним законом. Тоді математичне очікування часів переміщень охорони і терористів буде дорівнювати:

$$M[T] = \sum_{i=1}^{l} M[t_i];$$

І дисперсія часів переміщень охорони і терористів:

$$D[T] = \sum_{i=1}^{l} D[t_i];$$

Даний метод дозволяє зважене підсумовування диференційних показників, виходячи з однорідності їх фізичної природи. До недоліків слід віднести можливість застосування цього методу лише на об'єктах з дуже великою територією, на яких існує декілька рубежів охорони. Якщо розміри об'єкта зменшуються, достовірність результатів різко знижується, оскільки по перше стає недоцільним застосування центральної граничної теореми, і, по друге, часові інтервали для подолання малих відстаней важко зпрогнозувати[4].

Окрім вищезазначених недоліків розглянутих методів слід відмітити те, що всі вони слугують для разового оцінювання ймовірності ефективного протистояння системи фізичного захисту несанкціонованим діям на певному об'єкті. В цих методах протистояння СФЗ і терористів розглядається відокремлено від технологічних процесів, що відбуваються на цільовому об'єкті(ці процеси розглядаються тільки на стадії проектування, для недопущення втручання чи порушення СФЗ цих процесів), хоча дії терористів, вочевидь, будуть спрямовані саме проти об'єкта, а СФЗ є лише перешкодою на їх шляху. Ці методи не включають поняття контуру зворотнього зв'язку, і не враховують взаємозв'язки між структурними елементами об'єкта та елементами СФЗ, що знижує ефективність управління безпекою цього об'єкта.

Описання методу управління СФЗ

Концепцією методу є недопущення за допомогою контура управління збою технологічного процесу на об'єкті, або порушення цілісності об'єкта внаслідок несанкціонованих дій порушників(терористів). В даному методі використані положення оптимального управління безпекою екологічно-небезпечних об'єктів, описані в [7].

Згідно цього методу, досліджуваний об'єкт зображується у вигляді сукупності структурних елементів (координатних ребер), поєднаних між собою певним чином, характеризуючих його підсистеми, що мають вхідні i_n і вихідні j_n полюси. Оскільки елементи є різнорідними за своїми функціями, то їх зв'язок розглядається як зв'язок потоків інформації. Інформаційною змінною є прямо або опосередковано пов'язана з управлінням об'єкта (елемента) величина, що контролюється, вимірюється, діагностується, обчислюється, транслюється, чи перетворюється згідно заданого закону. Інформаційна змінна може бути як дискретною так і неперервною. Потоком інформації називається інформаційна змінна зі вказаним напрямом передачі інформації. На рис.1. показаний структурний елемент з вхідним *i* та вихідним *j* полюсами, вхідною θ_1 та вихідною θ_2 інформаційними змінними. Передача інформації з вхідного на вихідний полюс характеризується випадковою подією передачі інформації(працездатності елемента) ε_{ji}. Управління безпекою елемента виконується за допомогою контура управління (зворотнього зв'язку), який характеризується подією працездатності контура ε_{ij}. Одна і та сама система може мати різні інформаційні змінні, в залежності від цілей дослідження.

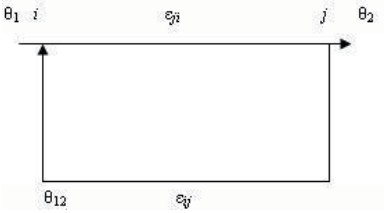

Рис.1.

Наприклад, якщо в якості системи розглядати АЕС, то інформаційними змінними можуть бути: при дослідженні екологічної безпеки- кількість продуктів поділу в реакторі до та після аварії; при дослідженні економічної ефективності забезпечення безпеки та надійності АЕС- витрати на безпеку, і т.д. Поняття інформаційної змінної дозволяє проводити лінійний аналіз для нелінійних систем, виявляти закономірності зв'язків потоків інформації, та на основі цього проводити ефективне управління безпекою об'єкта.

Принцип застосування цієї теорії до СФЗ в найбільш загальному вигляді продемонстрований на рис.2. Екологічно небезпечний об'єкт-потенційна ціль терористів(перший контур), та СФЗ (контур зворотнього зв'язку) являють собою єдину систему. В даному випадку в якості вихідного потоку інформації будемо використовувати величину, що характеризує ймовірність збою технологічного процессу на об'єкті, або порушення цілісності об'єкта внаслідок теракту – R(залежить від типу цільового об'єкта). Під ймовірністю збою технологічного процесу розуміється подія, результатом якої може бути радіоактивне забруднення навколишнього середовища. За відсутності несанкціонованих дій на об'єкті ця величина є близькою до нуля, а з

перетину терористами периметру об'єкта та подоланням кожного бар'єра на шляху до своєї мети це значення буде збільшуватися. Задачею СФЗ як контура управління в даному випадку є утримання значень вхідних потоків інформації, тобто параметрів об'єкта які впливають на значення вищезазначеної ймовірності, на прийнятному рівні. Цей рівень визначається виходячи з концепції інтервала запаса керованості, одного з ключових положень методології[7].

$$n=[z1,z2]$$

Суть цього положення полягає в визначенні верхньої та нижньої межі- z_1,z_2, для контрольованого параметра. Де z_2 – верхня межа контрольованого параметра, при перевищенні якої наступає втрата керованості безпекою об'єкта. Нижня межа z_1 визначається згідно закономірностей попередження настання аварії. Тобто стійке управління антитерористичною безпекою об'єкта виконується за рахунок забезпечення ефективності СФЗ на рівні, достатньому для утримання критичних параметрів об'єкта в рамках інтервала $[0,z_1]$, за наявності несанкціонованих дій на об'єкті. Для цього проводиться управління параметрами, які впливають на ефективність СФЗ, до яких відносяться: ймовірність виявлення, напрацювання на хибне зпрацьовування, час необхідний для подолання кожної перешкоди на шляху терористів, час необхідний групі затримки для прибуття до місця розгортання та ін. Оцінка ефективності проводиться за допомогою моделювання. Разом з оцінкою ефективності проводиться оцінка достатності визначеного рівня ефективності СФЗ для забезпечення безпечного функціонування об'єкта за умови несанкціонованих дій на його території.

Метод оцінки ефективності СФЗ що пропонується враховує зв'язок між діями терористів, СФЗ та цільовим об'єктом.

Рис.2.

Розглянемо цю відмінність на конкретному прикладі, використовуючи вищезгаданий логіко-ймовірнісний метод. Нехай ми маємо об'єкт, що представляє цінність для потенційних порушників. Експертним шляхом визначені критичні елементи об'єкта, які можуть бути цілями терористів. Проаналізуємо шлях терористів до одного з таких елементів. Для досягнення своєї мети терористам необхідно виконати наступні дії: подолати периметр,

перебігти до вхідних дверей, зламати вхідні двері, подолати відстань до цільового приміщення, проникнути всередину. Подолати периметр об'єкта можна двома способами – яким-небудь способом подолати огородження об'єкта (пролом, перелаз та ін.), або проникнути через КПП. Нехай ймовірність подолання периметру об'єкта складає: проникнення через огородження x_1=0.3, проникнення через КПП будь-яким з можливих способів(обман, силове проникнення, таємне проникнення) x_2= 0.4. Ймовірність подолання першого бар'єру – вхідних дверей, x_3=0.5, та другого – дверей до цільового приміщення, x_4= 0.4. Зіставимо граф розвитку сценарія небезпеки рис.3.

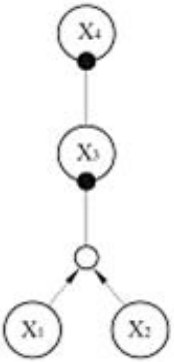

Рис.3.

На основі цього зіставляємо функцію небезпеки системи. Вона виглядає наступним чином:

$$y(x_1,x_2,x_3,x_4)=(x_1 \vee x_2)x_3 \times x_4,$$

Приведемо цю функцію до диз'юнктивної нормальної форми:

$$y(x_1,x_2,x_3,x_4)=x_1x_3x_4 \vee x_2x_3x_4,$$

Далі перетворюємо функцію небезпеки у ймовірнісну для чого замінюємо події значеннями відповідних ймовірностей, і обчислюємо значення ризику:

$$R= (0.3*0.5*0.4)+(0.4*0.5*0.4)=0.14 .$$

Відповідно значення ефективності СФЗ:

$$E = 1-R = 0.86 .$$

В результаті обчислень ми отримали ймовірність того, що терористи протягом виконання свого задуму будуть прагнути до здійснення конкретної цілі, яка розглядається як кінцева точка на шляху терористів. І, відповідно, отримуємо ймовірність того що СФЗ буде ефективно протистояти їх діям по досягненню саме цієї цілі. З позицій поняття контуру зворотнього зв'язку такий підхід є неприпустимим. Оскільки весь об'єкт розглядається як перший контур, то сама присутність порушників на його території змінює значення ймовірності, в нашому випадку, збою технологічного процесу, або цілісності об'єкта. З цього ракурсу ймовірність того - дістанутся терористи до точки

свого призначення чи ні, не відіграє першочергової ролі. А розрахунок будь-яких можливих шляхів терористів по території об'єкта є беззмістовним, оскільки дії терористів в різних ситуаціях є непередбачуваними. Наприклад, повертаючись до вищезазначеного прикладу, якщо досліджуваним об'єктом є АЕС, а очікуваною ціллю проникнення терористів до певного приміщення є вибух, то навіть у випадку затримки охороною об'єкта порушників до досягнення останнього приміщення на схемі, або неможливості подолання останнього бар'єру на їхньому шляху, терористи, зважаючи на обставини, можуть здійснити вибух за місцем свого перебування, що також може призвести до тяжких наслідків. Або зможуть спробувати завдати найбільшої можливої шкоди. В такому випадку, викидаючи елемент R_4 з виразу, отримуємо значення функції небезпеки:

$$R = (0.3*0.5)+(0.4*0.5)=0.35 .$$

що є набагато більшим за початкове.

З такого ракурсу на перший план виходить підвищення вимог до показників ефективності захисту периметру об'єкта. Замість разрахунку можливих траекторій руху терористів визначаються зони небезпеки, в яких перебування порушників значно підвищує ймовірність R. Відповідно ефективність відображає здатність СФЗ утримувати порушників за межами цих зон. Показниками ефективності будуть ймовірність виявлення перетину периметра об'єкта, та ефективність засобів охорони периметру, ймовірність затримки порушників до досягнення ними будь-якої з зон небезпеки, тобто на мінімальній відстані від периметру об'єкта, а також показники ефективності засобів затримки, що перешкоджають потраплянню терористів у вищезазначені зони. В праці [3] пропонується поняття критичної точки виявлення, тобто моменту виявлення, в який сили охорони мають ще достатньо часу для затримки порушників. За аналогією з цим вводиться поняття критичної точки затримки (КТЗ), тобто такого місцеположення на об'єкті, до перетину якого порушниками ймовірність R є прийнятно низькою. КТЗ визначається для кожної зони небезпеки об'єкта, і, згідно цього, визначається оптимальне розміщення засобів виявлення, затримки та сил охорони.

Висновки

На основі положень теорії оптимального управління безпекою екологічно небезпечних об'єктів розроблено новий метод, що дозволяє ефективно управляти системами фізичного захисту. Проведене моделювання методу показало що ефективність СФЗ є керованою величиною. Стійкість до збоїв технологічного процесу на об'єкті, або порушення цілісності об'єкта внаслідок несанкціонованих дій порушників збільшується за рахунок відповідної реакції контуру зворотного зв'язку.

1. *Бондарев П.В., Измайлов А.В., Толстой А.И.*.Физическая защита ядерных объектов. Учебное пособие для вузов.– Москва: МИФИ.– 2008.– 584 с.

2. *Буртняк В.М.,Забулонов Ю.Л., Лисиченко Г.В., Мєдвєдєв Ю.О.* Сучасні підходи до

оцінювання терористичних ризиків // Збірник наукових праць Інституту проблем моделювання в енергетиці.– 2012.– №65.- с. 94-101.
3. *Гарсиа М.* Проектирование и оценка систем физической защиты/Пер. с англ. В.И. Воропаева, Е.Е. Зудина и др. – М.: Мир, АСТ.– 2002. – 386 с.
4. *Звежинский С.С.,Голубков Г.В., Иванов В.А.,Сизов С.М.,* Оценка функциональной эффективности охранной сигнализации малых объектов // Спецтехника и связь. – 2008.– № 3.– с.13-20.
5. *Лисиченко Г.В., Забулонов Ю.Л., Хміль Г.А.*. Природний, техногенний та екологічний ризики: аналіз, оцінка, управління. – К.: Наукова думка. – 2008. – 543 с.
6. *Ліпкан В.А., Нікіфорчук Д.Й., Руденко М.М.*. Боротьба з тероризмом. – Знання України. – 2002. – 254 с.
7. *Пампуро В.И.*. Оптимальное управление безопасностью экологически опасных объектов. Монография.– Киев: Наукова думка.– 2012.– 599 с.
8. *Панин О.А.* Как измерить эффективность? Логико-вероятностное моделирование в задачах оценки систем физической защиты // БДИ.–2008.–№2(77).– с. 20-24.
9. *Панин О.А.* Проблемы оценки эффективности функционирования систем физической защиты объектов // БДИ.– 2007.– № 3(72).– с. 23 − 27.

Поступила 18.02.2013р.

УДК 681.6

А.А.Владимирский, И.А.Владимирский, И.П.Криворучко,
ИПМЭ им. Г.Е.Пухова НАН Украины,
А.П.Иващенко , ГП “Укрметртестстандарт”, г. Киев

РАЗРАБОТКА СРЕДСТВ МЕТРОЛОГИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ ИЗМЕРИТЕЛЕЙ ПАРАМЕТРОВ ДВИЖЕНИЯ ПОДЪЕМНО-ТРАНСПОРТНОГО ОБОРУДОВАНИЯ

Metrology equipment for contact and inertial movement meters are developed and presented.

Группой “Технической диагностики” ИПМЭ им. Г.Е.Пухова НАН Украины совместно с ГП “Укрметртестстандарт” проведены работы по созданию аппаратных и программных средств метрологического обеспечения для аттестации и поверки измерителей параметров движения (ПД) подъемно-транспортного оборудования (ПТО).

Актуальность и своевременность этих работ определяется настоятельной необходимостью разработки и внедрения в производство измерителей ПД всего спектра ПТО – лифтов, эскалаторов, подвесных канатных дорог и пр., являющимися объектами повышенной опасности.

В работе представлены разработка испытательного стенда “Радиан-1” и адаптация автоматизированной виброкалибровочной установки “АВКУ-2”.

