УДК 351.813.12

С.В. Лєнков[1], Я.Я. Винярський[1], О.В. Дергильова[2]

[1]Військовий інститут Київського національного університету імені Тараса Шевченка
[2]Національний університет оборони України

ФОРМАЛІЗАЦІЯ СЛАБКОСТРУКТУРОВАНИХ ЗАДАЧ ПРИ ВИРІШЕННІ ПРАКТИЧНИХ ЗАДАЧ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ДЕРЖАВИ

В статті розглянуто приклад практичного застосування принципу системного дослідження для отримання формальних моделей процесів у системі забезпечення національної безпеки держави. Наводяться зміст моделювання процесів, характерних для даної сфери, зміст дослідження та його структура.
Ключові слова: гомеостатична модель, національна безпека держави, ультрастійкий стан.

Система забезпечення національної безпеки України грунтується на національних інтересах, формується з урахуванням реальних загроз, небезпек і викликів безпеці особистості, суспільства та держави і функціонує в правовому полі, визначеному Конституцією України, законами України, указами і розпорядженнями Президента України, рішеннями Ради національної безпеки і оборони України, постановами і розпорядженнями Кабінету Міністрів України, державними програмами у цій галузі [1]. На систему покладається проведення комплексу погоджених заходів щодо захисту національних інтересів у політичній, економічній, воєнній, інформаційній та інших сферах.

Аналіз факторів впливу на систему забезпечення національної безпеки, зокрема тих факторів, що належать до переліку загроз, небезпек і викликів безпеці, вказує на наявність елементів як якісного, так і кількісного характеру, суттєві залежності між якими до того ж позначені неявно.

Розгляд атрибутів задачі забезпечення національної безпеки держави дозволяє визначити наступне: вхідні дані задачі апріорі окреслені нечітко, є скоріше лінгвістичними, ніж таким, що вкладається в чисельну оцінку, крім того, характеристики об'єктів системи забезпечення національної безпеки не завжди можуть бути визначені точно, часто залежать від неконтрольованих параметрів. Не можна вважати явною залежність між елементами системи.

Даний перелік основних характеристик задачі дозволяє дійти висновку щодо віднесення останньої до класу слабкоструктурованих задач.

Структуровані задачі характеризуються тим, що в них суттєві залежності виявлені настільки явно, що можуть бути описані кількісними залежностями (наприклад, залежностями, що використовуються в дослідженні операцій). Але це не означає відсутність труднощів в опису проблем та їх вирішенні. Однією з значних труднощів на даному рівні може бути, наприклад, масштабність та рівень деталізації проблем (процесів).

Слабкоструктуровані задачі містять в собі елементи якісного та кількісного характеру, причому перші мають тенденцію домінування. У зв'язку з цим їх формалізова-

ний опис може бути здійснений, як правило, тільки за допомогою м'яких формалізмів (наприклад за допомогою нечітких моделей).

До даного класу проблем (ситуацій) відносяться проблеми змішаного характеру. М'які моделі використовуються при здійсненні вибору способів ліквідації наслідків лих. Але на сьогоднішній день немає підстав говорити про існування відпрацьованого механізму встановлення формалізованого змісту даної задачі (тобто – моделі досліджуваного явища). В таких умовах роль теорії можуть прийняти на себе алгоритми та моделі, побудовані на принципах системного дослідження та приведені до єдиної гомеостатичної цілісності.

Метою даної статті є формулювання системотехнічних прийомів формалізації слабко структурованих процесів, притаманних сфері забезпечення національної безпеки держави та порядку застосування зазначених формалізмі для рішення практичних задач.

Дослідження загроз у сфері забезпечення національної безпеки держави вимагає подолання гносеологічної трудності: інформація про об'єкт дослідження не завжди може бути отримана експериментальним шляхом. Типовими можна вважати ситуації, коли експеримент з реальною системою принципово не може бути проведений, або ж є небезпечним. Тому у більшості випадків звертаються до теоретичних методів.

У реальних ситуаціях, що виникають у процесі забезпечення національної безпеки держави поведінка суб'єктів зазначеної сфери далеко не найкраща і не універсальна, в екстремальних ситуаціях може бути навіть програшна. Зважаючи, в першу чергу, на унікальність ситуацій сфери забезпечення національної безпеки, виникає потреба у використанні апарату, який охоплював би багатомірність, неоднозначність та слабкопередбачуваність процесів, різну інформованість сторін, рефлексію та здатність сторін оперативно змінювати цілі (критерії ефективності).

У [2] розвитку ситуацій, формалізація яких ускладнена, надане нове тлумачення: подібний процес розглядається як спосіб взаємодії складних систем з поведінкою, яка є слабкопередбачуваною. Ніяке скільки завгодно докладне знання морфології (устрою) системи не дає можливості визначити її функції (поведінку), і навпаки – ніяке скільки завгодно точне спостереження за поведінкою системи на будь-якому, але кінцевому інтервалі часу, не дає підстав для однозначного визначення поведінки системи у подальшому. При визначенні залежностей між змінними доводиться орієнтуватися на доступні спостереженню та виміру фактори (значення змінних та швидкостей їх зміни). Особливу увагу для дослідника повинні складати фактори, що становлять множину загроз та викликів національній безпеці держави. Апріорі зазначена множина є нечіткою. У разі, якщо дослідника цікавить розвиток ситуації, опис взаємодії систем за допомогою диференціальних рівнянь дає можливість виявити основні особливості динаміки розвитку на достатньо строгому рівні. У свою чергу, використання диференціальних рівнянь веде до швидкого збільшення числа змінних і, як наслідок, для складних оперативних задач скласти всеоб'ємну систему диференціальних рівнянь не вдається. Тому доводиться орієнтуватися на типові і нетипові варіанти ситуацій, які суттєво відрізняються одна від одної і описуються порівняно простими рівняннями. Небезпека випустити з поля зору кращий варіант знижується, адже системне дослідження направляє роботу і породжує раціональні варіанти в процесі розвитку подій. Можна сподіватися, що в числі досліджених варіантів виявиться найкращий або близький до нього варіант, навіть якщо він і не був апріорно визначеним.

Нові резерви визначення рішень, що приймаються в цілях забезпечення національної безпеки держави, відкриває змалювання досліджуваного процесу як інтелектуальної взаємодії. Використання логічних засобів фіксації інтелектуальних процесів, які протікають при взаємодії складних систем, є головною задачею при побудові теоретичних моделей різних фізичних взаємодій. Логічним є припущення, що мислення у даному разі підпорядковане деяким особливим законам. При цьому ні дослідник, ні надсистема, ні системи не володіють повною інформацією про себе, один про одного та про ситуацію:

кожен користується рефлексивним відображенням і має своє власне уявлення про відображення інших. Слід мати на увазі, що невідповідність відображень впливає на хід процесу забезпечення національної безпеки держави та суттєво ускладнює математичну формалізацію.

Навіть використання точних формул при досить неточних даних не дає змоги приписувати результатам розрахунків яку-небудь особливу точність. Практично лише системний підхід (як методологія) та системотехніка (як прикладна дисципліна) дозволяють розв'язувати такі задачі. Концепція системотехніки полягає в представленні реальних або уявних складних систем за допомогою моделей та дослідженні таких моделей.

Компоненти моделей, як правило, виявляються описаними мовами різних теорій без єдиного способу кількісних представлень, внутрішньосистемні закони будуть не універсальними, а обмеженими. В основному із-за цього початкова модель, як правило, неадекватна і в цілому мертва. "Оживлення" моделі системи можливе єдиним способом – встановленням гомеостазу (в кібернетиці гомеостазом називається узгоджений стійкий стан багатозв'язної системи) [3]. Встановлення гомеостазу є основним прийомом, за допомогою якого модель, яка позбавлена достатньої для функціонування інформації, може бути приведена в дію як єдине ціле. Така модель може відтворювати лише найбільш прості риси реальності, але це буде вже динамічна, синергетична модель, яку можна довести до бажаного рівня відповідно до мети рішення конкретної задачі. Схема гомеостатичної моделі механізму забезпечення національної безпеки держави наведена на рис. 1.

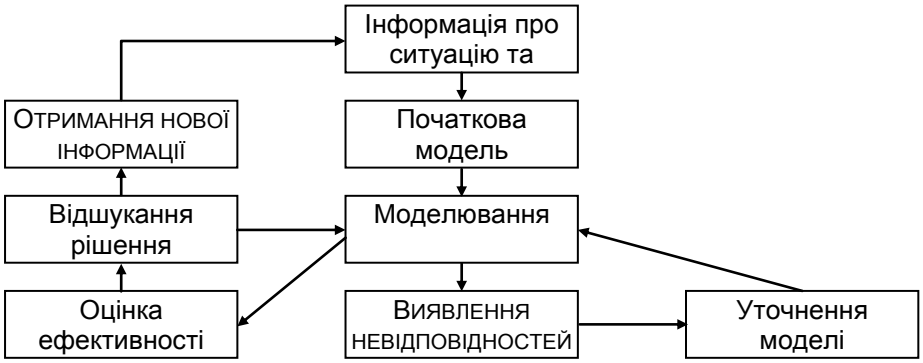

Рис.1 Схема гомеостатичної моделі механізму забезпечення національної безпеки держави

Модель замкнена, що дозволяє реалізувати гомеостатичний процес. Процес продовжується до отримання найкращого ультрастійкого рішення. Ультрастійкість необхідна, оскільки уточнення ситуації може призвести до суттєвої зміни оцінок ефективностей систем та порушення процесу. При встановленні гомеостазу виявляється визначеною робоча область системи та можливе зниження впливу консерватизму досвіду (оскільки стан гомеостазу може суттєво відрізнятися від початкового).

Механізм отримання моделі, яка змальовує вплив ризиків на процес забезпечення національної безпеки держави, повинен будуватися на принципах системного дослідження. Застосування зазначених принципів можна реалізувати в межах схеми, морфологічний опис якої наведено на рис.2.

Висновки

Наведені положення дають змогу розглядати гомеостатичну модель як інструмент дослідження впливу ризиків на процес забезпечення національної безпеки держави. Спеціальні процедури встановлення гомеостазу можуть бути визначені без попереднього накопичення статистичного матеріалу, що дає змогу говорити про гомеостатичні мо-

делі як ситуаційні. У разі досягнення ультрастійкого стану (характерного для прогностичного управління) вони здатні дати прогностичні оцінки розвитку процесів.

Література

1. Концепція (основи державної політики) національної безпеки України: Постанова Верховної Ради України №3/–ВР / Відомості Верховної Ради України. – 1997. – №10. – С.149–156.
2. Дружинин В. В. Введение в теорию конфликта / В. В. Дружинин, Д. С. Конторов, М. Д. Конторов. – М. : Радио и связь, 1989. – 288 с.
3. Рома О. М. Спосіб формалізації конфлікту та його системне моделювання / О. М. Рома, В. Б. Толубко, С. В. Лєнков // Науково-технічний збірник "Захист інформації". – К., 2009. - № 3. – С. 31-34.

Надійшла до редколегії 25.06.2013 р.

Рецензент: д.т.н., проф. Петров А.С.

С.В. Ленков, А.В. Дергильова, Я.Я. Винярський

СИСТЕМОТЕХНИЧЕСКИЕ ПРИЕМЫ ФОРМАЛИЗАЦИИ СЛАБОСТРУКТУРИРОВАННЫХ ЗАДАЧ ДЛЯ РЕШЕНИЯ ПРАКТИЧЕСКИХ ЗАДАЧ СФЕРЫ ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА

В статье рассматривается способ практического применения принципов системного исследования для получения формальных моделей процессов в системе обеспечения национальной безопасности государства. Приводятся содержание моделирования процессов, характерных для данной сферы, содержание исследования и его структура.

Ключевые слова: гомеостатическая модель, национальная безопасность государства, ультрастойкое состояние.

S.V. Lenkov, A.V. Dergilova, Y.Y. Vinyarsky

SYSTEM INTEGRATORS METHODS FORMALIZATION SEMISTRUCTURED PROBLEMS FOR SOLVING PRACTICAL PROBLEMS SERVICES NATIONAL SECURITY STATE

This article contains a way of practical application of principles of system research for reception of formal models of processes in system of support of national safety of the state. The content of research and its structure are resulted the maintenance of modeling of processes, characteristic for the given sphere.

Keywords: homeostatic model, national security of the state, ultraresistant condition.

УДК 004.056.57:656.2

О.А. Нємкова[1]

[1]Університет банківської справи (м. Київ) Національного банку України Львівський інститут банківської справи, доцент кафедри економічної кібернетики

ЗАСТОСУВАННЯ RS–АНАЛІЗУ ДЛЯ ПЕРЕВІРКИ ЯКОСТІ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ

У роботі застосовано RS-аналіз до деяких генераторів псевдовипадкових послідовностей та розраховані значення коефіцієнту Хьорста. Встановлена відповідність результатів аналізу до статистичних властивостей генераторів. Запропоновано використовувати RS-аналіз для тестування генераторів псевдовипадкових послідовностей на наявність персистентності, іншими словами, перевіряти генератори на придатність для застосування у криптографії.

Ключові слова: генератор псевдовипадкової послідовності, коефіцієнт Хьорста, потокове шифрування, лінійний конгруентний генератор, персистентність.

Вступ

Відкритість сучасних соціально-економічних інформаційних систем, за допомогою яких відбувається обробка, збереження та передавання конфіденційної або таємної інформації, потребує застосування криптографічних перетворень масивів даних. Обсяг таких даних може бути різним – невеликим для інформаційного обміну між платіжною системою та індивідуальним користувачем і дуже великим при передачі звукових, тим більш, відео файлів. Якість криптографічного перетворення повинна бути дуже високою, тому що переважно це стосується передачі та збереження банківської інформації, конфіденційних баз даних мобільних операторів, медичних та фармацевтичних компаній, військових розробок та інших даних, що пов'язані з державною таємницею. Все це вимагає в ідеалі необмежених по довжині псевдовипадкових послідовностей. Зростаюча кількість кібератак за останні роки підтверджує висновок про необхідність надійного захисту, чого можна досягти лише за допомогою шифрування даних.

Останнім часом можна почути пропозиції шифрувати значну кількість інформації, яка не тільки передається назовні з локальної корпоративної мережі, але і зберігається на жорстких дисках в системі. Особливо це стосується баз даних конфіденційної інформації. На сьогодні таке шифрування не застосовується, тому інформація, що міститься в багатьох базах даних, може бути прочитана спеціально написаними для цього програмами – павуками. У продажі є такі програмні комплекси (один з них пропонує російська фірма Аналитические бизнес решения), які мають відповідно написані павуки для різноманітних баз даних. Такі програмні комплекси позиціонуються на ринку як такі, що збирають економічну інформацію про конкретну людину. Але зрозуміло, що з їх допомогою можна збирати будь-яку конфіденційну інформацію.

В деяких випадках потрібне швидке криптографічне закриття інформації. Зазвичай для цього використовують потокове шифрування, яке базується на генерації високоякісних псевдовипадкових послідовностей. Перевагами потокового шифрування є його відносна простота, швидкість та відсутність розмноження помилок. Процес шифрування полягає у генерації гами та подальшого накладання її на потік даних. Стійкість шифрів,