9. Высоцкая, Е.В. Методика определения систолической дисфункции миокарда у подростков [Текст]/ Е.В. Высоцкая, А.П. Порван, Л.И. Рак [та ін.] // Восточно-Европейский журнал передовых технологий.- 2012.- №1/3(55).- С. 27-31.
10. Порван, А.П. Оцінка функціонального стану бета-адренорецепторів еритроцитів людини при артеріальній гіпертензії методом КВЧ – діелектрометрії [Текст] / А.П. Порван, Е.А. Архипова, П.С. Красов, Высоцкая Е.В. // Восточно-Европейский журнал передовых технологий. Серия «Прикладные информационные технологии и системы управления». № 6/7 (42). – 2009. – С. 17-21.
11. Факторный, дискриминантный и кластерный анализ [Текст] / Дж. Щ. Ким, Ч.У. Мюллер, У.Р. Клекка [и др.]; под ред. И.С. Енюкова. – М.: Финансы и статистика, 1989. – 215 с.
12. Порван, А.П. Использование дискриминантного анализа для диагностики хронической сердечной недостаточности у подростков [Текст] / А.П. Порван, А.И. Бых, Л.И. Рак, Е.В. Высоцкая // Вестник национального технического университета «ХПИ»- Харьков: НТУ «ХПИ». – 2010. - №31.– С. 16-22.
13. Щукин, Н.А. Использование дискриминантного анализа для диагностики доброкачественных и злокачественных опухолей [Текст] / Н.А. Щукин, Е.В. Высоцкая, А.П Порван, С.Н. Пушкарь //Системи обробки інформації. –2011.- № 2(92). - С. 234 -238.

Пропонується метод оцінки та підвищення адаптивності й достовірності імовірнісної моделі оцінки живучості системи захисту шифрування при рішенні спеціальних завдань моніторингу інформаційного простору

Ключові слова: живучість, імовірнісна модель, моніторинг, функціональність

Предлагается метод оценки и повышения адаптивности и достоверности вероятностной модели оценки живучести системы защиты шифрования при решении специальных задач мониторинга информационного пространства

Ключевые слова: живучесть, вероятностная модель, мониторинг, функциональность

The method of estimation and increase of adaptiveness and authenticity of probabilistic model of estimation vitality of the system defence of encipherement at the decision of the special tasks of monitoring the informative space is offered

Keywords: vitality, probabilistic model, monitoring, functionality

УДК 004.738.5:681.14, 621.396:681.14-2:004.621

ОЦІНКА ЖИВУЧОСТІ СИСТЕМ МОНІТОРІНГУ ІНФОРМАЦІЙНОГО ПРОСТОРУ

Н.Ф. Казакова
Кандидат технічних наук, доцент
Кафедра інформаційних систем в економіці
Одеський національний економічний університет
вул. Преображенська, 8, м. Одеса, Україна, 65082
Контактний тел.: (048) 703-64-18, 050-512-98-99, 094-955-94-18
E-mail: kaz2003@ukr.net

Постановка проблеми в загальному вигляді і її зв'язок з науковими і практичними завданнями

З початку своєї історії *комп'ютерні технології*, тобто технології, що відповідають за зберігання, передачу, обробку, захист та відтворення інформації з використанням комп'ютерів [1], застосовувалися суто для військових цілей і, перш за все, були направлені на зниження впливу людського чинника на процеси ухвалення рішень. На поточний час збереглася актуальність розвитку комп'ютерних технологій стосовно їх використання у системах моніторингу спеціального призначення [2], які функціонують в автоматичному або напівавтоматичному режимах. З самого початку військове застосування комп'ютерів у системах моніторингу інформаційного простору мало на увазі, перш за все, реєстрацію зовнішніх подій, їх обробку та подальшу передачу даних для ухвалення рішень. Зараз *системи моніторингу* – це достатньо широкий клас систем з розширеною функціональністю. В подальшому будемо розуміти, що системами *моніторингу спеціального призначення* (СМСП), які базуються на комп'ютерних технологіях, є такі системи, які функціонують у складі інформаційних мереж загального та/або спеціального використання, та призначені для систематичного отримання, зберігання, передачі, обробки, захисту та достовірного відтворення інформації з заданими властивостями або параметрами про встановлений об'єкт на інтервалах часу, які нерозривно примикають один до одного, протягом яких стан об'єкту істотно не змінюється, з метою прийняття

заданих управлінських рішень. Саме зауваження щодо неістотної зміни інформації та наслідків, які можуть звідси витікати, є однією з основних наукових задач про які йде мова в статті. Суть цього зауваження полягає в тому, що зазначені функції, які виконують СМСП, можуть бути реалізовані лише при достатньому рівні живучості як всієї системи, так і її окремих складових, що забезпечують дієздатність на встановлених часових інтервалах. Особлива роль відводиться живучості системам захисту шифрування циркулюючої інформації: тільки в цьому разі можуть бути забезпечені встановлені показники щодо ступеня конфіденційності, цілісності, доступності та спостережуваності процесів, які відбуваються при обробці інформації в СМСП.

Як показав **аналіз доступних літературних джерел**, перелік яких є у [1-8], робота сучасних СМСП, як і всіх складних технічних систем, характеризується тим, що не всі їх підсистеми та окремі складові об'єкти в однаковому ступені функціонально навантажені. Також зрозуміло, що не всі вони в процесі функціонування використовуються однаково часто. У достатньо змінних умова в яких працюють СМСП трансформується взаємовідношення відмови об'єкта та відмови системи. Так, якщо об'єкт використовується в процесі функціонування рідко, то у разі його відмови навіть при його послідовному підключенні в загальній структурі системи, відмова СМСП може виникнути лише у тому випадку, коли цей об'єкт використовуватиметься. Частота використання об'єкту в процесі функціонування істотно впливає на його надійність та живучість. З урахуванням цього чинника не можна описати живучість системи тільки надійністю її об'єктів. Не зважаючи на достатньо великий обсяг наукових публікацій, дослідженню цього питання уваги було приділено недостатньо. Відповідно, щодо методів оцінки та підвищення адаптивності й достовірності імовірнісної моделі оцінки живучості системи захисту шифрування при рішенні спеціальних завдань моніторингу інформаційного простору, наукові публікації відсутні (за винятком тих, де пропонується спосіб обліку вище зазначеного чинника, заснований на дискретних моделях теорії графів та на методі систематичних випробувань).

Розширений аналіз наукової та технічної літератури показав, що характеристики живучості функціонування багатьох сучасних систем захисту інформаційних ресурсів визначається не тільки їх внутрішньою структурою, характеристиками надійності її об'єктів, але й видом завдань та встановлених вимог, які системи зобов'язані виконувати. Залежно від видів вимог до системи, при її обслуговуванні ставляться відповідні вимоги до показників надійності функціонування. Це пояснюється тим, що кожна з вимог в процесі виконання системою поставлених завдань, може впливати на інтенсивність використання задіяних в системі об'єктів. Звичайно, при цьому слід враховувати відмінність вимоги та інтенсивність її запровадження від інтенсивності інших вимог та їх видів. При виконанні завдання, тобто задачі обслуговування встановленої вимоги, в системі можуть бути задіяні тільки певні об'єкти. Це означає, що система при виконанні завдання матиме рівень надійності та живучості, який відповідає такому типу завдань або типу вимог, який визначається ступенем використання окремих об'єктів системи. У СМСП достатньо часто виникає ситуація, коли один і той же об'єкт входить в систему в сенсі надійності та живучості, але не входить в неї по фізичній суті, тобто в структурній схемі живучості системи наявність його є випадковою залежно від типу вимоги, яка обслуговується системою в даний момент часу. У цій ситуації традиційні методи розрахунку живучості системи захисту по надійності її об'єктів не можуть бути достатньо ефективними, оскільки з їх допомогою не можна врахувати вказану вище випадковість. Це завдання є раніше **невирішеною частиною загальної проблеми** підвищення адаптивності та достовірності імовірнісної моделі оцінки живучості системи захисту шифрування у СМСП.

Виходячи зі сказаного, **метою роботи** є розробка способу розрахунку частоти використання складових елементів системи шифрування інформації у СМСП на основі систематичної моделі математичного очікування та на цій основі – визначення загальної залежності живучості системи моніторингу від надійності її об'єктів з врахуванням забезпечення гарантованого функціонування на встановлених проміжках часу.

Виклад основного матеріалу. В подальшому, для порівняння системи захисту шифрування інформації у СМСП з іншими складними технічними системами, у якості критерію ефективності застосуємо узагальнений показник:

$$E = \frac{K_ж П_о}{C},$$

де $П_о$ – продуктивність системи щодо обслуговування вимог при ідеальній надійності;

C – економічні витрати на обслуговування системи;

$K_ж$ – коефіцієнт живучості системи, який є відношенням числа працездатних станів φ системи по всій множині станів φ_n^j;

j – імовірність узагальненої відмови; n – кількість об'єктів);

$$K_ж = \frac{\varphi}{\varphi_n^j}.$$

Покажемо метод розрахунку надійності СМСП, коли враховується ситуація, при якій об'єкт як є її складовим елементом, так і не входить в структуру залежно від потоку виконуваних системою завдань, тобто обслуговуваних вимог.

Нехай СМСП, що складається з n об'єктів, призначена для обслуговування потоку різних типів вимог. Нехай x_i $(i = 1, 2, 3, ..., n)$ – імовірність безвідмовної роботи i-го об'єкта системи. Позначимо через α_i $(i = 1, 2, 3, ..., n)$ імовірність залучення i-го об'єкта при обслуговуванні даної вимоги з потоку. У статичному режимі функціонування системи ймовірність α_i можна оцінити як відносну частоту появи тієї множини типів вимог, які при обслуговуванні задіють i-й об'єкт системи. Через ρ_i позначи-

мо імовірність використання і -го об'єкта системи в довільний момент часу при нормальному її функціонуванні. Нехай $\tau_i^{(2)}$ – середній час обслуговування вимог, які не задіюють і -й об'єкт. Неважко помітити, що якщо час обслуговування системою всіх вимог у середньому є одинаковим та незмінним, тобто якщо $\tau_i^{(1)} = \tau_i^{(2)}$, то імовірність використання об'єкта збігається з імовірністю його залучення в процес функціонування. Як наслідок – $\rho_i = \alpha_i$.

Якщо частоти появи вимог, які задіюють і -й об'єкт, та частоти появи вимог, що не його задіюють, однакові, то імовірність його використання ρ_i може бути розрахована по формулі:

$$\rho_i = \frac{\tau_i^{(1)}}{\tau_i^{(1)} + \tau_i^{(2)}} + \Theta_i ,$$

де Θ – параметр, що управляє процесом включення об'єкта в роботу СМСП.

У загальному випадку імовірність використання і -го об'єкта в довільний момент часу визначається як відносний час використання цього об'єкта за час функціонування системи, тобто за час обслуговування потоку вимог [3]. Тоді, згідно до цього визначення,

$$\rho_i = \lim_{T\to\infty} \frac{1}{T} \int_0^T \gamma_i(t)dt , \qquad (1)$$

де T – час роботи системи, а $\gamma_i(t)$ у момент часу t може використовувати одне з двох значень: «1», якщо у цей момент і -й об'єкт використовується, і «0» – інакше.

Використовуючи середні характеристики, співвідношення (1) представимо у вигляді:

$$\rho_i = \frac{\alpha_i \tau_i^{(1)}}{\alpha_i \tau_i^{(1)} + (1-\alpha_i)\tau_i^{(2)}} + \Theta_i .$$

Розглянемо ступінь впливу надійності об'єкта на надійність всієї СМСП. Очевидно, що залежно від величин імовірностей ρ_i надійність і -го об'єкта системи буде впливати на надійність системи *істотно* або *не істотно* [4]. Якщо величина ρ_i достатньо мала, тобто виникає ситуація, коли і -й об'єкт використовується рідко, то навіть така відмова знижує надійність системи, але лише тільки в тому випадку, коли і -й об'єкт буде використовуватися для її обслуговування. Виходячи з таких міркувань можна стверджувати, що надійність і -го об'єкта СМСП, що, фактично є імовірністю безвідмовної роботи, являє собою випадкову величину, обумовлену у заданому моменті часу випадковістю вимог, яка приймає значення одиниці, якщо об'єкт не використовується, і значення x_i, якщо і -й об'єкт у цей момент часу використовується для обслуговування вимог. Таким чином для любої випадкової величини, яка впливає на надійність і -го об'єкта СМСП, є сенс розглянути математичне очікування такого випадку. Оскільки природа випадковості значення надійності об'єкта визначається його інтенсивністю використання, то це можна інтерпретувати як стохастичний зв'язок цього об'єкта з іншими об'єктами системи. Відповідно, можна говорити про наявність зв'язку (тобто використання об'єкта та його входження у стосунки з іншими об'єктами), або про його відсутність (об'єкт не використовується та не входить у зв'язок з іншими об'єктами, тобто з погляду надійності системи – в цей момент часу він не є її об'єктом) [3, 4].

Позначивши через β_i математичне очікування надійної роботи і -го об'єкта з урахуванням описаної вище природи випадковості, запишемо:

$$\beta_i = \rho_i x_i + (1-\rho_i)\cdot 1 = 1 - \rho_i(1-x_i) , \qquad (2)$$

де практична імовірність безвідмовної роботи і-го об'єкта СМСП з урахуванням її навантаження і загальної множини та природи вимог (завдань), які система повинна виконувати або обслуговувати.

Користуючись (2), аналогічно виразимо надійність СМСП:

$$B(\vec{x},\vec{\rho}) = \prod_{i=1}^{n} \left[1 - \rho_i(1-x_i)\right], \qquad (3)$$

де $\vec{\rho}$ та $\vec{x}$ – n -мірні вектори, компоненти яких ρ_i та x_i, $(i = 1,2,3,...,n)$. Якщо і -й об'єкт системи зарезервований ідентичними йому $S_i - 1$ об'єктами, то величина (3) прийме вигляд:

$$B(\vec{x},\vec{\rho}) = \prod_{i=1}^{n} \left[1 - \rho_i(1-x_i)^{S_i}\right]. \qquad (4)$$

Отримані співвідношення (3) та (4) дають можливість вирішувати задачі підвищення достовірності математичних моделей для оцінки надійності систем захисту інформації.

Другим чинником підвищення адекватності та достовірності математичних моделей оцінювання надійності, є здатність опису, формалізації та обліку в цих моделях можливості управління надійністю [5]. Дискретне збільшення надійності Θ за рахунок раціонального управління нею досягається вдосконаленням варіацій способів технічної експлуатації, варіацій режиму технічної експлуатації, варіюванням заходів щодо технічного та профілактичного обслуговування. Питання про те як часто та які заходи щодо обслуговування великих систем необхідно проводити з метою забезпечення їх надійної роботу, є одним з основних науково-практичних питань. Це пояснюється тим, що зменшення інтенсивності відмов об'єктів після раціональної процедури регламентних робіт залежить від рівня оптимізації цієї процедури. Зменшення інтенсивності потоку відмов, зміна його імовірнісної структури та обмеженої післядії, може досягатися також спеціальними режимами зовнішніх дій на систему. Однак, слід зазначити, що обсяги робіт експоненціально збільшуються при лінійному збільшені об'єктів у технічній системі. Зважаючи на це, будь-яким чином оптимізувати або надати достатньо раціональні пропозиції щодо надійної роботи СМСП глобальної структури, надзвичайно важко. Єдиною пропозицією, яка може заслуговувати на

увагу, це оцінка надійності окремих складових з врахуванням їх специфічних особливостей. Так, наприклад, окремі інтегральні мікросхеми при радіоактивному опромінюванні різко зменшують час їх життя. Проте, проведення такої процедури може бути виправдане, коли системою виконується важливе завдання, значення якого дозволяє нехтувати зменшенням часу життя об'єкту за рахунок строгішого збереження параметрів в меншому тимчасовому проміжку. Виникає завдання про оптимальне управління надійністю з метою оптимізації певного критерію. Зацікавленість представляє більш загальний випадок цього завдання, а саме – приріст надійності Θ функціонального об'єкта за рахунок управління надійністю без відключення його від загальної системи. В даному випадку мова йде про систему шифрування – надзвичайно важливий та дорогий з економічної точки зору об'єкт СМСП. Зважаючи на це, у разі дослідження технічної надійності системи захисту величина $x+\Theta$ – це надійність системи з урахуванням управління. У моделях, де враховується математичне очікування надійності, застосування надійності Θ є детермінованим, тому як доданок воно виходить за оператора математичного очікування. Отже, $\beta+\Theta$ представлятиме математичне очікування надійності системи за умови управління надійністю та випадкової природи (у часі) завдань, що вирішуються системою (в даному випадку – СМСП).

Позначивши цю величину через $\tilde{B}$, математична модель оцінки надійності (2) породжує більш загальний вираз наступного вигляду:

$$\tilde{B} = 1 - \rho(1 - x) + \Theta \qquad (5)$$

або

$$\tilde{B} = \rho\left(x + \frac{1 - \Theta - \rho}{\rho}\right). \qquad (6)$$

Висновки

Розроблена модель (5) та її модифікація володіють тими ж властивостями, що й раніше показана модель (2). При сумісному використанні моделі (2) та (5) представляють собою метод оцінки та підвищення адаптивності й достовірності імовірнісної моделі оцінки живучості системи захисту шифрування при рішенні спеціальних завдань моніторингу інформаційного простору.

Література

1. Компьютерные технологии [Електронний ресурс] / Портал: Компьютерные технологии. – Режим доступу \www/ URL: http://ru.wikipedia.org/wiki/Портал:Компьютерные_технологии – Заголовок з екрану, доступ вільний.
2. Системы мониторинга специального назначения [Електронний ресурс] / Портал спеціальних ресурсів. – Режим доступу \www/ URL: http://daily.sec.ru/ publication.cfm?pid=34148&cid=12&ppos=3: – Заголовок з екрану, доступ вільний.
3. Гурина, С.А. Живучесть систем защиты информации в условиях внешних воздействий [Текст] / Гурина С.А., Егоров Ф.И., Хорошко В.А. // Захист інформації – 2008. – №2. – С.69-73.
4. Гурина, С.А. Создание информационных моделей систем управления защитой объектов [Текст] / Гурина С.А., Егоров Ф.И., Хорошко В.А. // Вісник ДУІКТ – 2008. – Т.6, №2. – С. 147-153.
5. Петров, А.А. Способ формирования спецфакторов в моделях оценивания живучести систем охраны объектов [Текст] / Петров А.А., Хорошко В.А. // Вісник Східноукраїнського національного університету ім. В. Даля – 2008. – №8 (126), част.1. – С. 22-24.
6. Казакова, Н.Ф. Повышение адаптивности и достоверности вероятностной модели оценки живучести системы защиты шифрования [Текст] / Казакова Н.Ф., Тискина Е.О., Хорошко В.А. // Інформаційна безпека – 2009. – №2(2). – С.69-73.
7. Відновлення та оптимізація інформації в системах прийняття рішень [Текст] : підручник / Баранов В.Л., Браіловський М.М., Казакова Н.Ф. та ін.; під загальн. ред. В.О. Хорошко. – К.: Видн. ДУІКТ, 2009. – 134 с.
8. Казакова, Н.Ф. Скорочення обсягів контрольних випробувань в інформаційних системах за рахунок їх функціональної надмірності [Текст] / Казакова Н.Ф., Согіна Н.М. // Моделювання та інформаційні технології. Зб. наук. праць ІПМЕ НАН України – 2008. – Вип. 49. – С.34-40.