https://doi.org/10.31649/1997-9266-2019-142-1-41-57

УДК 681.327.12

В. В. Ковтун[1]

МОДЕЛЮВАННЯ ДОСТУПНОСТІ ІНФОРМАЦІЙНОЇ СИСТЕМИ КРИТИЧНОГО ЗАСТОСУВАННЯ

[1]Вінницький національний технічний університет

Опис безпеки інформаційної системи критичного застосування (ІСКЗ) у рамках тріади CIA не може вважатися завершеним без прикладної моделі доступності такої системи з урахуванням її архітектурних особливостей, адже передбачається, що ІСКЗ розгортається на мультисерверній платформі, яка включає сервер-реєстраційний центр і множину зв'язаних з ним серверів даних. В загальному вигляді доступність ІСКЗ передбачає виділення авторизованому суб'єкту у відповідь на його вхідний запит ресурсів інформаційного середовища ІСКЗ, скінченний обсяг яких обмежено поняттям віртуальної машини. Архітектурна організація ІСКЗ передбачає, що віртуальні машини можуть створюватися або у інформаційному середовищі сервера-реєстраційного центру або у інформаційному середовищі серверів даних або в обох цих інформаційних середовищах одночасно відповідно до розташування інформаційних ресурсів, до яких звертається авторизований суб'єкт, правил підтримки його дій, сформульованих у системній політиці безпеки, і ступеня завантаженості відповідних інформаційних середовищ. Обмеження доступності пов'язуватимемо з відсутністю вільних ресурсів у ІСКЗ для створення нових віртуальних машин за запитом авторизованих суб'єктів, що призводитиме до тимчасового відхиленні нових вхідних запитів для здійснення сервісних операцій з вивільнення системних ресурсів. У статті представлено нові математичні моделі управління доступністю ІСКЗ, які, на відміну від існуючих, враховують топологічні особливості ІСКЗ, перебіг її сервісних операцій при управлінні доступом авторизованих суб'єктів до інформаційного середовища системи і формалізують зв'язок множини сервісних операцій з множиною відповідей системи на запити авторизованих суб'єктів у вигляді керованого напівмарковського процесу з резервуванням ресурсів на заходи самоубезпечення, що дозволяє за допомогою апарату математичного програмування отримати оптимальну стратегію управління доступністю ІСКЗ із мінімізацією витрат на її функціонування та дозволяє стохастично оцінити доступність системи на будь-якому етапі її життєвого циклу. На основі створених моделей проведено імітаційне моделювання доступності ІСКЗ, реалізованої у програмному середовищі Matlab. Результати досліджень показали, що отримані на основі запропонованих моделей правила реагування на вхідні запити авторизованих суб'єктів в залежності від завантаженості і виконуваних у системному інформаційному середовищі сервісних операцій, дозволяють підтримувати імовірність відхилення вхідних запитів авторизованих суб'єктів в заданих межах, мінімізуючи витрати на функціонування ІСКЗ. Втім, аналіз емпіричних результатів роботи ІСКЗ, правила системної політики безпеки якої синтезовані на основі моделі доступності із резервуванням ресурсів на убезпечення системного інформаційного середовища від дій авторизованих суб'єктів, показав, що за стрімкого зростання інтенсивності запитів від авторизованих суб'єктів з високим показником небезпечності кількість відмов у наданні доступу починає квадратично зростати. Дослідження показали, що для уникнення вищеописаного падіння доступності ІСКЗ варто на етапі проектування закладати 20 % резерв системних ресурсів. Загалом, отримані експериментальні результати підтвердили адекватність запропонованих моделей доступності ІСКЗ.

Ключові слова: інформаційна система критичного застосування, доступність, керований напівмарковський процес, оптимізація, математичне програмування.

Вступ

Безпека інформаційної системи значною мірою визначається її архітектурою або топологією. Сучасні інформаційні системи будуються як на основі централізованої, клієнт-серверної архітектури [1], так і на основі однорангової розподіленої децентралізованої хмарної архітектури [2], [3], у якій, окрім ефективної організації доступу до інформаційних ресурсів, закладено підтримку GRID-технологій, хмарних обчислень і пірінгових мереж. Кожний архітектурний підхід має свої переваги і недоліки [4], [5], які, втім, варто розглядати перш за все з позиції галузевого призначення інформаційної системи. Критичне застосування інформаційної системи визначає специфічні

вимоги до реалізації заходів інформаційної безпеки, зокрема, у забезпеченні доступності інформаційних ресурсів системи для авторизованих суб'єктів, вважаючи фактор вартості функціонування інформаційної системи критичного застосування (ІСКЗ) другорядним. Враховуючи сказане, актуальною задачею є синтез моделі доступності розподіленої ІСКЗ з урахуванням її топології і вбудованих сервісів. При чому, в залежності від обраної базової архітектури системи доведеться досліджувати питання невизначеності елементів або сегментів її топології, не повної достовірності інформації про системні апаратні і програмні ресурси, мінливості поведінки системи в залежності від ступеня її завантаженості, обчислення ступеня небезпеки дій авторизованих суб'єктів тощо.

Аналіз інформаційних джерел дозволив виявити підходи, які використовуються для моделювання доступності актуальних мережевих інформаційних систем. Найчастіше оцінювання готовності та доступності мережевої інформаційної системи здійснюється формально, обмежуючись розрахунком коефіцієнта готовності [2], [3] у вигляді відношення середньої тривалості роботи системи без відмов у доступі до суми цього ж показника з середньою тривалістю робіт, виконуваних для відновлення доступності системи. Простота такого підходу нівелюється його загальністю, що дозволяє рекомендувати його використання лише на першому етапі дослідження доступності системи. Втім, застосовують і стохастичний підхід для оцінювання доступності, готовності та надійності мережевих інформаційних систем [2]—[6], в якому використовують структурні схеми надійності, дерева відмов, марковські мережі і мережі Петрі. У роботах [7], [8] запропоновано марковські моделі для оцінювання готовності мережевих інформаційних систем з урахуванням ієрархічної структури їх топології. У дослідженнях [9], [10] проводиться аналіз і моделювання надійності мережевих інформаційних і GRID-систем та їх сервісів із застосуванням для їх опису марковських процесів і систем масового обслуговування. Втім, всі згадані дослідження стосуються мережевих інформаційних систем без урахування можливості їх критичного застосування, що зумовлює неадекватність цих моделей для опису ІСКЗ через неврахування специфічних сервісів останньої та необхідності підтримування високого рівня конфіденційності і доступності навіть за рахунок значних витрат на функціонування системи. Виявлені обставини зумовлюють доцільність проведення досліджень з метою отримання адекватної спеціалізованої моделі доступності ІСКЗ.

Постановка задачі дослідження

Нехай ІСКЗ реалізовано на основі запропонованої автором архітектури [1]. Під доступністю такої ІСКЗ розумітимемо властивість системи надавати авторизованим суб'єктам доступ до системних інформаційних ресурсів за правилами, сформульованими у системній політиці безпеки, за умови, що тривалість очікування доступу не перевищить заданого значення t_d. Оцінювати доступність ІСКЗ в такому разі будемо за значенням параметра p_i, $0 \le p_i \le 1$, який описуватиме імовірність того, що i-й авторизований суб'єкт отримав доступ до ІСКЗ, очікуючи менше τ_d. Значення параметра p_i залежатиме від: комплексного параметра a_{ir}, який узагальнює інформацію про архітектурні особливостей інформаційної системи, що визначають розташування системних інформаційних ресурсів; комплексного параметра a_{is}, який узагальнює інформацію про доступні для реалізації дії авторизованих суб'єктів ресурси інформаційного середовища ІСКЗ; комплексного параметра a_{pb}, який узагальнює інформацію про правила використання інформаційного середовища ІСКЗ відповідно до повноважень авторизованих суб'єктів, які звертаються до ІСКЗ; комплексного параметра a_{so}, який узагальнює інформацію про порядок активації і регламент проведення необхідних для функціонування ІСКЗ сервісних операцій; часу t_z, коли надійшов запит від авторизованого суб'єкта. Вищезгадані параметри можна узагальнити у вигляді моделі $p_i = f\left(a_{ir}, a_{is}, a_{pb}, a_{so}, t_z\right)$, застосовуючи яку можна поставити, наприклад, задачу оптимізації доступності ІСКЗ вигляду $p_i = f\left(a_{ir}, a_{is}, a_{pb}, a_{so}, t_z\right) \to \max$ за обмежень $\tau_{oz} \le \tau_d$, $o_{ISCU} \le o_d$, де τ_{oz} — тривалість очікування авторизованого суб'єкта на отримання доступу, o_{ISCU}, o_d — фактичні і граничні витрати на функціонування ІСКЗ, відповідно. Постановку задачі оптимізації, звичайно, можна змінювати, але її основна математична модель доступності ІСКЗ вигляду $f\left(a_{ir}, a_{is}, a_{pb}, a_{so}, t_z\right)$ залишатиметься незмінною.

Отже, об'єктом дослідження є процес отримання авторизованим суб'єктом доступу до ІСКЗ.

Предмет дослідження — керований напівмарковський процес, який описує залежність $f\left(a_{ir}, a_{is}, a_{pb}, a_{so}, t_z\right)$ та методи теорії планування експерименту. Задачі дослідження: синтезувати адекватну модель залежності $f\left(a_{ir}, a_{is}, a_{pb}, a_{so}, t_z\right)$, поставити на основі синтезованої моделі задачу оптимізації доступності ІСКЗ, розв'язати її та здійснити аналіз отриманих результатів, застосовуючи положення теорії планування експерименту.

Базова модель доступності ІСКЗ

В загальному випадку комунікація ІСКЗ з суб'єктами, які бажають скористатися її інформаційними ресурсами (ІР), описується двома концепціями: концепцією авторизації суб'єкта для отримання доступу до ІСКЗ і концепцією підтримки інформаційним середовищем (ІС) ІСКЗ дій авторизованих суб'єктів (АС) в рамках їх ролей, описаних у системній політиці безпеки (СПБ). Теорія випадкових процесів дозволяє описати першу концепцію пуассонівським процесом з інтенсивністю λ, а другу — експоненційним розподілом з масштабним коефіцієнтом μ_i^j, де $i \in \{1, 2, \ldots, W\}$ — індекси суб'єктів, а $j \in \{1, 2, \ldots, T\}$ — індекси віртуальних машин (ВМ), які створюються для підтримки дій *i*-го суб'єкта у ІС ІСКЗ. Далі використовуватимемо узагальнювальне поняття ВМ для опису визначеної адміністратором кількості обчислювальних ресурсів, обсягу пам'яті і ширини каналу зв'язку, що одноразово виділяються у ІС ІСКЗ для підтримки дій суб'єкта. Значення W і T задаються на етапі проектування ІСКЗ і описують, відповідно, максимальну кількість АС, роботу яких може підтримувати ІСКЗ у певний момент часу, і максимальну кількість ВМ, які може створювати ІСКЗ для підтримки дій одного суб'єкта, відповідно. Зауважимо, що згідно з [1] ІСКЗ розгортається на мультисерверній платформі, яка включає сервер-реєстраційний центр (СРЦ) і множину зв'язаних з ним серверів даних (СД). Обслуговування запиту АС починається з виділення інформаційних ресурсів СРЦ з подальшим підключенням ресурсів СД за потребою. Делеговані СД інформаційні процеси також характеризуватимемо експоненційними розподілами з масштабними коефіцієнтами ν_i. Введемо змінні x_i^j і y_i, які описуватимуть кількість активних інформаційних потоків між *i*-м АС і j ВМ, які обслуговують його запити на стороні СРЦ, та ВМ, які обслуговують запити *i*-го АС на стороні СД, відповідно. Ці змінні дозволяють оцінити підсумкову кількість інформаційних потоків у суб'єкт-системній взаємодії у вигляді відношень $\sum_{j=1}^{T}\sum_{i=1}^{W} i x_i^j + \sum_{i=1}^{W} i y_i \le B$ і $\sum_{j=1}^{T}\sum_{i=1}^{W} i x_i^j \le M$, де змінна B задає проектну межу кількості інформаційних потоків у ІС ІСКЗ, а змінна M описує проектну межу кількості ВМ у ІС СРЦ.

Функціонування ІСКЗ у контексті оцінювання її доступності для АС описуватимемо простором станів $s = \left[x_1^1, \ldots, x_W^T, y_1, \ldots, y_W, e(s)\right] \in S$, де характеристична змінна $e(s) = \left\{A_n, D_i^j, F_i\right\}$ описує визначену множину системних операцій, що можуть виконуватися у ІС ІСКЗ у довільний момент часу її життєвого циклу. Зокрема, виділимо операцію готовності до прийняття вхідного запиту A_n, в якій у системі достатньо інформаційних ресурсів та активовано відповідні функції її ІС для підтримки дій АС; операцію очищення СРЦ D_i^j, в якій прийняття вхідних запитів неможливе і здійснюється вивільнення зарезервованих для дій *i*-го АС j ВМ у ІС СРЦ; операцію очищення СД F_i, в якій прийняття вхідних запитів неможливе і здійснюється вивільнення зарезервованих за *i*-м АС інформаційних ресурсів ІС СД.

На вхідний запит від АС ІСКЗ, що перебуває у стані s, у ІС якої у цей момент часу виконується операція $e(s)$, може відповісти одним з можливих варіантів надання сервісу, описаних множиною $A = \bigcup_{s \in S} A_s : \left\{-1; 0; \alpha_i^j, \alpha_i\right\}$, де -1 відповідає ситуації відхилення вхідного запиту з причини виконання однієї з операцій очищення, 0 — відхиленню запиту з іншої причини, α_i^j — задоволення вхідного запиту від *i*-го АС з виділенням для його потреб j ВМ у ІС СРЦ, α_i — задоволення вхідного запиту від *i*-го АС з виділенням для його потреб інформаційних ресурсів СД. Охарактеризу-

ємо аналітично зміною $\gamma(s,\alpha)$ швидкість зміни стану системи, яка, перебуваючи у стані s з активною операцією $e(s)$, реагує дією α у відповідь на вхідний запит АС:

$$\gamma(s,\alpha)=\begin{cases}\lambda+\sum\limits_{j=1}^{T}\sum\limits_{i=1}^{W}x_i^j\mu_i^j+\sum\limits_{i=1}^{W}y_i\nu_i, e(s)=A_n\wedge\alpha=0,\\ \lambda+\sum\limits_{j=1}^{T}\sum\limits_{i=1}^{W}x_i^j\mu_i^j+\sum\limits_{i=1}^{W}y_i\nu_i+\mu_\omega^t, e(s)=A_n\wedge\alpha=\alpha_\omega^t,\\ \lambda+\sum\limits_{j=1}^{T}\sum\limits_{i=1}^{W}x_i^j\mu_i^j+\sum\limits_{i=1}^{W}y_i\nu_i+\nu_\omega, e(s)=A_n\wedge\alpha=\alpha_\omega,\\ \lambda+\sum\limits_{j=1}^{T}\sum\limits_{i=1}^{W}x_i^j\mu_i^j+\sum\limits_{i=1}^{W}y_i\nu_i-\mu_\omega^t, e(s)=D_\omega^t\wedge\alpha=-1,\\ \lambda+\sum\limits_{j=1}^{T}\sum\limits_{i=1}^{W}x_i^j\mu_i^j+\sum\limits_{i=1}^{W}y_i\nu_i-\nu_\omega, e(s)=F_\omega\wedge\alpha=-1,\end{cases}\quad(1)$$

де параметр λ описує інтенсивність надходження вхідних запитів, многочлен $\sum\limits_{j=1}^{T}\sum\limits_{i=1}^{W}x_i^j\mu_i^j+\sum\limits_{i=1}^{W}y_i\nu_i$ — ступінь завантаженості ІС ІСКЗ в цілому, а його одночлен $\sum\limits_{i=1}^{W}y_i\nu_i$ — ступінь завантаженості СД ІСКЗ зокрема.

З надходженням вхідного запиту ІСКЗ, що перебуває у стані його очікування $(e(s)=A_n)$, може: відхилити вхідний запит $(\alpha=0)$, не змінюючи при цьому завантаженість ІС; прийняти вхідний запит завантаживши при цьому СРЦ на величину α_ω^t; прийняти вхідний запит завантаживши при цьому СД на величину α_ω. Дії α_ω^t або α_ω виконуються зі швидкістю μ_ω^t або ν_ω, відповідно. Під час виконання системою операцій очищення $e(s)=D_\omega^t$ або $e(s)=F_\omega$, в результаті яких вивільниться D_ω^t ресурсів СРЦ або F_ω ресурсів СД, відповідно, вхідні запити від АС не приймаються $(\alpha=-1)$ з технічних причин, що знижує результуючу швидкість прийняття вхідного запиту на величину μ_ω^t або ν_ω, відповідно. Зауважимо, що обернений до $\gamma(s,\alpha)$ параметр $\tau(s,\alpha)=\gamma(s,\alpha)^{-1}$ описує очікувану тривалість перебування суб'єкт-серверної взаємодії у стані s.

Простір станів доступності ІСКЗ представимо зваженою графоподібною структурою, у якій стани $s\in S$ утворюють вершини графу, зв'язки між ними показують допустимі переходи між станами відповідно до логіки функціонування ІСКЗ у вигляді (1), а ваги зв'язків містять імовірності переходу з вихідного стану s у стан k, $s, k\in S$, в наслідок відповіді α на вхідний запит АС. Деталізуємо опис динаміки системи, формалізувавши імовірності переходу системи зі стану s, у якому виконується операція $e(s)$, у стан k в результаті відповіді α на вхідний запит АС.

Імовірність переходу системи $p(k|s,\alpha)$ зі стану $s=\left[x_1^1,\ldots,x_1^T,\ldots,x_W^1,\ldots x_W^T,y_1,\ldots,y_W,A_n\right]$ у стан k внаслідок відповіді α на вхідний запит від АС опишемо як

$$p(k|s,\alpha)=\begin{cases}\lambda\gamma(s,\alpha)^{-1},\ e(k)=A_n,\\ \mu_i^j\left(x_i^j+1\right)\gamma(s,\alpha)^{-1},\ e(k)=D_i^j\wedge\alpha=\alpha_i^j,\\ \mu_i^j x_i^j\gamma(s,\alpha)^{-1},\ e(k)=D_i^j\wedge\alpha\neq\alpha_i^j,\\ \nu_i\left(y_i+1\right)\gamma(s,\alpha)^{-1},\ e(k)=F_i\wedge\alpha=\alpha_i,\\ \nu_i y_i\gamma(s,\alpha)^{-1},\ e(k)=F_i\wedge\alpha\neq\alpha_i.\end{cases}\quad(2)$$

Імовірність переходу системи $p\left(k\middle|s,\alpha\right)$ зі стану $s=\left[x_1^1,\ldots,x_1^T,\ldots,x_S^1,\ldots x_S^T,y_1,\ldots,y_W,D_\omega^t\right]$ у стан k внаслідок відповіді α на вхідний запит від АС опишемо як

$$p\left(k\middle|s,\alpha\right)=\begin{cases}\lambda\gamma\left(s,\alpha\right)^{-1},\ e\left(k\right)=A_n,\\ \mu_i^j\left(x_i^j-1\right)\gamma\left(s,\alpha\right)^{-1},\ e\left(k\right)=D_i^j\wedge D_i^j=D_\omega^e,\\ \mu_i^j x_i^j\gamma\left(s,\alpha\right)^{-1},\ e\left(k\right)=D_i^j\wedge D_i^j\neq D_\omega^e,\\ \nu_i y_i\gamma\left(s,\alpha\right)^{-1},\ e\left(k\right)=F_i.\end{cases}\tag{3}$$

Імовірність переходу системи $p\left(k\middle|s,\alpha\right)$ зі стану $s=\left[x_1^1,\ldots,x_1^T,\ldots,x_W^1,\ldots x_W^T,y_1,\ldots,y_W,F_\omega\right]$ у стан k внаслідок відповіді α на вхідний запит від АС опишемо як

$$p\left(k\middle|s,\alpha\right)=\begin{cases}\lambda\gamma\left(s,\alpha\right)^{-1},\ e\left(k\right)=A_n,\\ \mu_i^j x_i^j\gamma\left(s,\alpha\right)^{-1},\ e\left(k\right)=D_i^j,\\ \nu_i\left(y_i-1\right)\gamma\left(s,\alpha\right)^{-1},\ e\left(k\right)=F_i\wedge F_i=F_\omega,\\ \nu_i y_i\gamma\left(s,\alpha\right)^{-1},\ e\left(k\right)=F_i\wedge F_i\neq F_\omega.\end{cases}\tag{4}$$

Вирази (1)—(4) є основою для синтезу керованого напівмарковського процесу (КНМП) [11]—[13], який описуватиме доступність ІСКЗ для АС з урахуванням архітектурних особливостей першої. Для наочності отримаємо графічне представлення КНМП доступності ІСКЗ у вигляді UML-діаграм станів [14]. Нехай $W=1$, $T=2$, $s=\left[x_1^1,x_1^2,y_1,e\left(s\right)\right]$, $e\left(s\right)=\left\{A_n,D_i^j,F_i\right\}$. На рис. 1—3 показано діаграми переходу ІСКЗ з вихідних станів $\left[0,1,0,A_n\right]$, $\left[1,1,1,D_1^1\right]$ і $\left[1,2,1,F_1\right]$ у допустимі згідно з (1)—(4) подальші стани в залежності від відповіді α на вхідні запити АС.

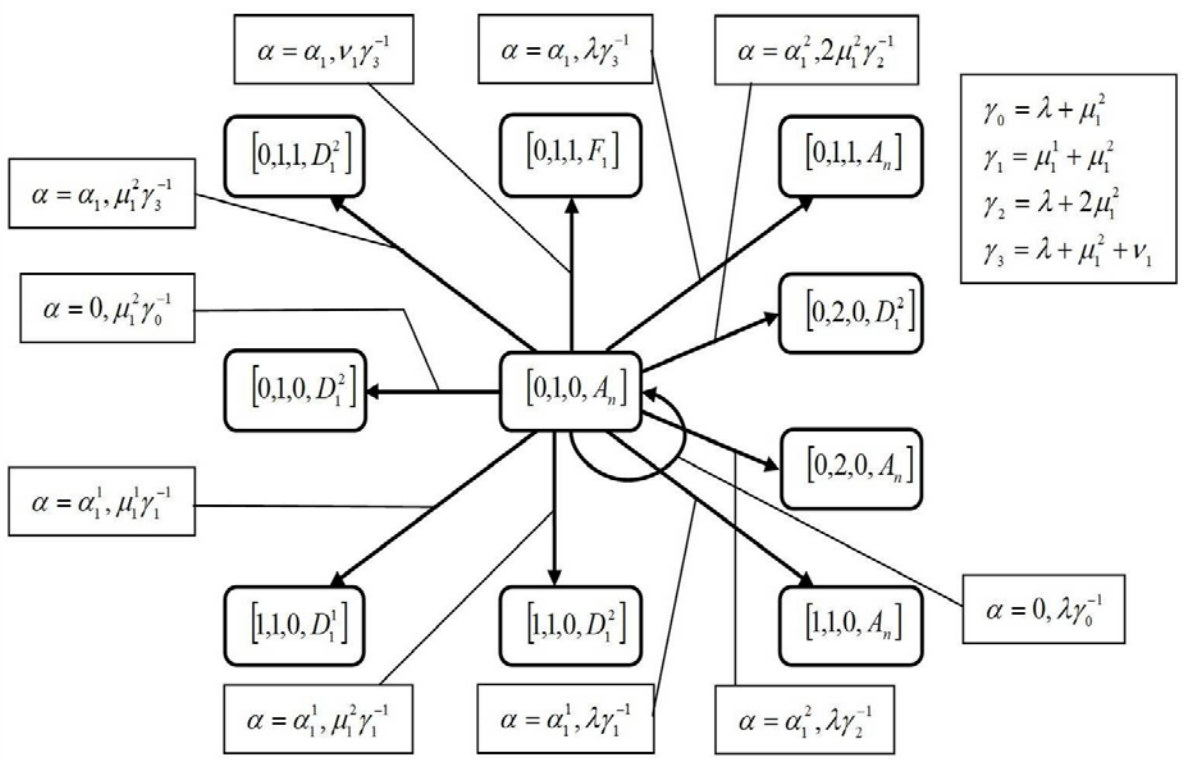


Рис. 1. UML-діаграма переходу ІСКЗ зі стану $\left[0,1,0,A_n\right]$ у допустимі подальші стани в залежності від відповіді α на вхідні запити АС

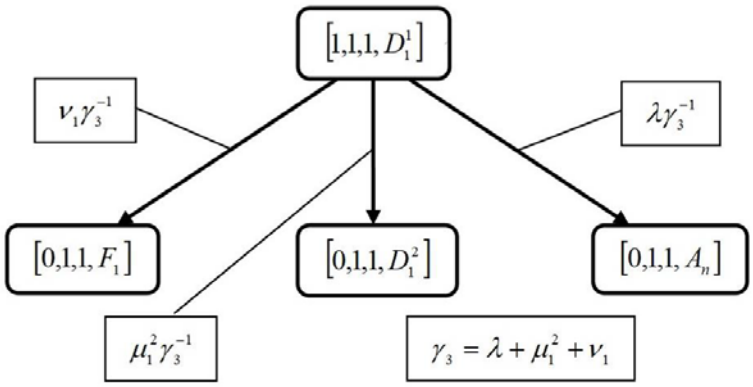


Рис. 2. UML-діаграма переходу ІСКЗ зі стану $[1,1,1,D_1^1]$ у допустимі подальші стани в залежності від відповіді α на вхідні запити АС

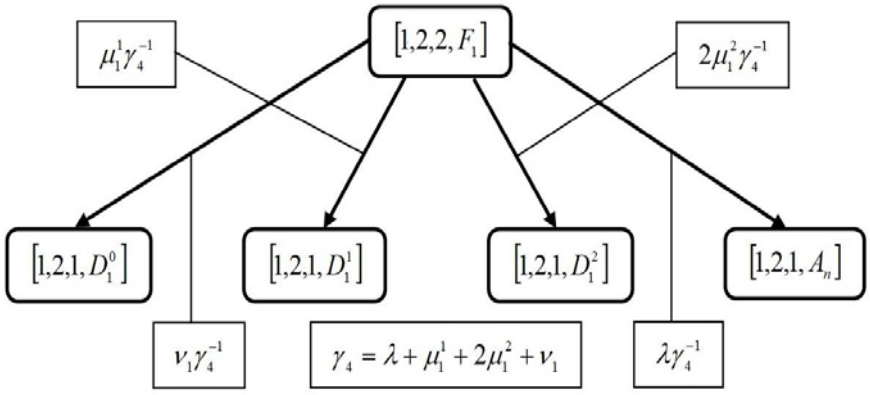


Рис. 3. UML-діаграма переходу ІСКЗ зі стану $[1,2,1,F_1]$ у допустимі подальші стани в залежності від відповіді α на вхідні запити АС

З метою управління доступністю ІСКЗ доповнимо опис стану ІСКЗ у вищенаведеній моделі (1)—(4) дійсною управляючою функцією $r(s,\alpha)$, значення якої описує перевагу від вибору системою, яка перебуває у стані s, дії α у відповідь на вхідний запит від АС. Значення дійсної функції $r(s,\alpha)$ розраховуватимемо як різницю показника $k(s,\alpha)$, як міри доцільності ініціації системної операції $e(s)$, і добутку вартості її реалізації $o(s,\alpha)$ і її тривалості $\tau(s,\alpha)$

$$r(s,\alpha)=k(s,\alpha)-\tau(s,\alpha)\cdot o(s,\alpha). \tag{5}$$

Значення показника доцільності системних операції $k(s,\alpha)$ в контексті ІСКЗ можна розкрити як

$$k(s,\alpha)=\begin{cases} E_\alpha - C_t\left(\mu_i^j\right)^{-1},\ \alpha=\alpha_i^j, \\ E_\alpha - C_t\left(\nu_i\right)^{-1},\ \alpha=\alpha_i, \\ -E_r,\ \alpha=0, \\ 0,\ \alpha=-1, \end{cases} \tag{6}$$

де E_α — накопичувальний показник доступності ІСКЗ, який зростає із задоволенням вхідних запитів, E_r — накопичувальний показник недоступності ІСКЗ, який зростає з відхиленням вхідних запитів, C_t — вартість одиниці машинного часу, витраченого на операції очищення D_i^j або F_i. Показник $o(s,\alpha)$ вводиться в управляючу функцію $r(s,\alpha)$ для нормування вартості обчислювальних та комунікаційних ресурсів, використовуваних у суб'єкт-системній взаємодії у вигляді $o(s,\alpha)=c_b\left(\sum_{j=1}^{T}\sum_{i=1}^{W} ix_i^j+\sum_{i=1}^{W} iy_i\right)+c_e\sum_{j=1}^{T}\sum_{i=1}^{W} ix_i^j$, де c_b — норма вартості комунікаційних ресурсів, а

c_e — норма вартості обчислювальних ресурсів, відповідно.

Користуючись можливостями КНМП, сформулюємо на основі (5) задачу оптимізації доступності ІСКЗ з цільовою функцією

$$\Phi(s,\alpha)=\sum_{s\in S}\sum_{\alpha\in A_s}\left(r(s,\alpha)z(s,\alpha)\right)\to\max \tag{7}$$

і системою обмежень

$$\begin{cases}\sum\limits_{s\in S}\sum\limits_{\alpha\in A_s}\left(\tau(s,\alpha)z(s,\alpha)\right)=1,\\ \sum\limits_{\alpha\in A_k}z(k,\alpha)-\sum\limits_{s\in S}\sum\limits_{\alpha\in A_s}\left(p(k|s,\alpha)z(s,\alpha)\right)=0,\\ \sum\limits_{s\in S}\sum\limits_{\alpha=0}\tau(s,\alpha)z(s,\alpha)\le P_b,\end{cases} \tag{8}$$

де $s,k\in S$, $\alpha\in A_s$, $z(s,\alpha)$ — оптимальна стратегія реагування ІСКЗ на вхідні запити для кожного стану s. Перше обмеження у системі (8) описує аналізований фрагмент життєвого циклу ІСКЗ у вигляді суми оцінок тривалостей станів s, у яких перебуватиме система, реагуючи діями α на вхідні запити АС. Друге обмеження вводиться для балансу вхідних і вихідних зв'язків відповідних станів моделі. Третє обмеження визначає імовірність гарантованої доступності ІСКЗ, для чого суми добутків характеристичних $\tau(s,\alpha)$ і оптимізовуваних $z(s,\alpha)$ параметрів ІСКЗ обмежено пороговим значенням імовірності відхилення запиту АС P_b.

Аналіз сформульованої у вигляді (7), (8) задачі оптимізації дозволяє її класифікувати як задачу лінійного програмування, для розв'язання якої існує універсальний симплекс-метод [15]. Результатом розв'язання такої задачі для конкретної ІСКЗ буде оптимальна стратегія параметризації складових її елементів у вигляді множини оптимальних параметрів $z(s,\alpha)\in Z$, на основі яких можна розрахувати стохастичні оцінки оптимального вибору реакції α у відповідь на вхідний запит для системи, що перебуває у стані s

$$p(s,\alpha)=z(s,\alpha)\left(\sum_{\alpha'\in A_s}z(s,\alpha')\right). \tag{9}$$

Отже, отримано нову математичну модель управління доступністю ІСКЗ, яка, на відміну від існуючих, враховує топологічні особливості ІСКЗ, перебіг її сервісних операцій в управлінні доступом АС до ІС і формалізує зв'язок множини сервісних операцій та множини відповідей системи на запити АС у вигляді КНМП, що, на відміну від існуючих, дозволяє за допомогою апарату математичного програмування отримати оптимальну стратегію управління доступністю ІСКЗ та стохастично оцінити її доступність на будь-якому етапі життєвого циклу.

Модель доступності ІСКЗ з резервуванням ресурсів на убезпечення системного інформаційного середовища від дій авторизованого суб'єкта

Орієнтація на критичне застосування описуваної інформаційної системи робить доцільним доповнення отриманої у вигляді (1)—(4) моделі її доступності урахуванням необхідності резервування ресурсів на заходи для убезпечення системного ІС від дій АС. В такому разі інтенсивність вхідних запитів на виділення ν ВМ $(1\le\nu\le T)$ від i-го АС, рівень загрози безпеці ІСКЗ, від дій якого описується дискретним параметром r $(1\le r\le R)$, опишемо величиною $\lambda_{i,r,\nu}$. ІСКЗ, відповідно, виділить для задоволення вхідного запиту i-го АС $j+f$ ВМ, де $j\le\nu$ ВМ використовуватимуться АС, а f ВМ резервуватимуться на заходи для убезпечення системного ІС від дій АС. Заходи ІС ІСКЗ з підтримки дій i-го АС у рамках прийнятого запиту описуватимуться експоненційним розподілом з масштабним коефіцієнтом μ_i (для j ВМ — $j\mu_i$, відповідно). Змінними x_i^j і x_i^f опишемо кількість ВМ, виділених на підтримку дій i-го АС у рамках прийнятого запиту, і кількість ВМ, зарезервованих на заходи для убезпечення системного ІС від дій i-го АС, відповідно. Зауважимо, що сумарна кількість задіяних у суб'єкт-системної взаємодії ВМ у будь-який момент часу не повинна перевищувати проектно встановленого значення M: $\sum\limits_{i=1}^{W}\sum\limits_{j=1}^{T}jx_i^j+\sum\limits_{i=1}^{W}\sum\limits_{j=1}^{T}(j+f)x_i^f\le M$.

Функціонування ІСКЗ в контексті оцінювання її доступності для АС з резервуванням ресурсів на убезпечення системного ІС від дій останнього описуватимемо простором станів $s=\left[x_1,\ldots,x_T,x_1^f,\ldots,x_T^f,e(s)\right]\in S$, де характеристична змінна $e(s)\in\left\{A_{r,\nu},D_j,D_j^f\right\}$ описує визначену множину системних операцій, що можуть виконуватися у ІС ІСКЗ у довільний момент часу її життєвого циклу. Зокрема, виділимо операцію готовності до прийняття вхідного запиту $A_{r,\nu}$ на виділення ν ВМ для потреб АС, рівень небезпечності якого не перевищує r, операцію очищення ІС D_j, при якій очищаються виділені для потреб АС інформаційні ресурси, задіяні під j ВМ, і операцію очищення зарезервованих ресурсів ІС D_j^f, в якій очищаються інформаційні ресурси, виділені під f ВМ, які здійснювали заходи по убезпеченню системного ІС від дій АС, здійснюваних у виділених останньому j ВМ. На вхідний запит від АС ІСКЗ, що перебуває у стані s, у ІС якої у цей момент часу виконується операція $e(s)$, може відповісти одним з можливих варіантів надання сервісу, описаних множиною $A=\bigcup\limits_{s\in S}A_s:\left\{-1,0,\alpha_i^j,\alpha_i^f\right\}$, де -1 відповідає ситуації відхилення вхідного запиту з причини виконання однієї з операцій очищення, 0 — відхиленню запиту з іншої причини, α_i^j — задоволення вхідного запиту від i-го АС з виділенням для його потреб j ВМ у ІС, α_i^f — задоволення вхідного запиту від i-го АС з виділенням f ВМ для реалізації заходів з убезпечення системного ІС від здійснюваних ним дій. Аналогічно (1), охарактеризуємо зміною $\gamma(s,\alpha)$ швидкість зміни стану системи s з активною операцією $e(s)$, що супроводжується відповіддю α на вхідний запит АС:

$$\gamma(s,\alpha)=\begin{cases}\sum\limits_{i=1}^{R}\sum\limits_{j=1}^{M}\lambda_{i,j}+\sum\limits_{i=1}^{W}\sum\limits_{j=1}^{T}j\left(x_i^j+x_i^f\right)\mu_i, e(s)=A_{r,\nu},\ \alpha=0,\\ \sum\limits_{i=1}^{R}\sum\limits_{j=1}^{M}\lambda_{i,j}+\sum\limits_{i=1}^{W}\sum\limits_{j=1}^{T}j\left(x_i^j+x_i^f\right)\mu_i+\omega\mu_i,\ e(s)=A_{r,\nu},\ \alpha=\alpha_i^{\omega}\vee a_i^f,\\ \sum\limits_{i=1}^{R}\sum\limits_{j=1}^{M}\lambda_{i,j}+\sum\limits_{i=1}^{W}\sum\limits_{j=1}^{T}j\left(x_i^j+x_i^f\right)\mu_i-\omega\mu_i,\ e(s)=D_{\omega}\vee D_{\omega}^f,\end{cases}\tag{10}$$

де параметр ω описує фактичну кількість ВМ, виділених ІСКЗ для підтримки дій АС, виконуваних у межах задоволеного запиту.

Деталізуємо опис динаміки системи, поведінка якої описується (10), формалізувавши імовірності її переходу зі стану s, у якому виконується операція $e(s)$, у стан k в результаті відповіді α на вхідний запит АС.

За аналогією з (2), імовірність переходу системи $p(k|s,\alpha)$ зі стану $s=\left[x_1,\ldots,x_T,x_1^f,\ldots,x_T^f,A_{r,\nu}\right]$ у стан k внаслідок відповіді α на вхідний запит від АС опишемо як

$$p(k|s,\alpha)=\begin{cases}\lambda_{r,\nu}\gamma(s,\alpha)^{-1},\ e(k)=A_{r,\nu},\\ \mu_i j\left(x_i^j+1\right)\gamma(s,\alpha)^{-1},\ e(k)=D_j\wedge\alpha=\alpha_i^j,\\ \mu_i jx_i^j\gamma(s,\alpha)^{-1},\ e(k)=D_j\wedge\alpha\neq\alpha_i^j,\\ \mu_i j\left(x_i^f+1\right)\gamma(s,\alpha)^{-1},\ e(k)=D_j^f\wedge\alpha=\alpha_i^f,\\ \mu_i jx_i^f\gamma(s,\alpha)^{-1},\ e(k)=D_j^f\wedge\alpha\neq\alpha_i^f.\end{cases}\tag{11}$$

Імовірність переходу системи $p(k|s,\alpha)$ зі стану $s=\left[x_1,\ldots,x_T,x_1^f,\ldots,x_T^f,D_{\omega}\right]$ у стан k внаслідок відповіді α на вхідний запит від АС опишемо як

$$p\left(k\left|s,\alpha\right.\right)=\begin{cases}\lambda_{r,v}\gamma\left(s,\alpha\right)^{-1},\ e\left(k\right)=A_{r,v},\\ \mu_i\, j\left(x_i^j-1\right)\gamma\left(s,\alpha\right)^{-1},\ e\left(k\right)=D_j\wedge j=\omega,\\ \mu_i\, jx_i^j\gamma\left(s,\alpha\right)^{-1},\ e\left(k\right)=D_j\wedge j\neq\omega,\\ \mu_i\, jx_i^f\gamma\left(s,\alpha\right)^{-1},\ e\left(k\right)=D_j^f.\end{cases}\tag{12}$$

Імовірність переходу системи $p\left(k\left|s,\alpha\right.\right)$ зі стану $s=\left[x_1,\ldots,x_T,x_1^f,\ldots,x_T^f,D_\omega^f\right]$ у стан k внаслідок відповіді α на вхідний запит від АС опишемо як

$$p\left(k\left|s,\alpha\right.\right)=\begin{cases}\lambda_{r,v}\gamma\left(s,\alpha\right)^{-1},\ e\left(k\right)=A_{r,v},\\ \mu_i\, j\left(x_i^f-1\right)\gamma\left(s,\alpha\right)^{-1},\ e\left(k\right)=D_j^f\wedge j=\omega,\\ \mu_i\, jx_i^f\gamma\left(s,\alpha\right)^{-1},\ e\left(k\right)=D_j^f\wedge j\neq\omega,\\ \mu_i\, jx_i^f\gamma\left(s,\alpha\right)^{-1},\ e\left(k\right)=D_j.\end{cases}\tag{13}$$

Вирази (12), (13) сформульовано з урахуванням того, що всі вхідні запити від АС, що надходять до ІСКЗ, яка виконує одну з операцій очищення ІС D_ω або D_ω^f, автоматично відхилятимуться доки ці сервісні операції не завершаться.

Скориставшись виразами (10)—(13), синтезуємо КНМП, який описуватиме доступність ІСКЗ для АС з резервуванням ресурсів на убезпечення системного ІС від дій останніх. Нехай $W=2$, $T=3$, $f=1$, вихідний стан системи $s=\left[x_1,x_2,x_3,x_1^1,x_2^1,x_3^1,e\left(s\right)\right]=\left[0,1,0,0,1,0,A_{r,2}\right]$, тоді UML-діаграму станів, яка ілюструє процес переходу зі стану s у стани $k=\left\{\left[0,2,0,0,2,0,e\left(s\right)\right],\left[0,1,0,0,1,0,e\left(s\right)\right],\left[0,1,0,0,1,1,e\left(s\right)\right]\right\}$ на основі моделі (10)—(13), покажемо на рис. 4.

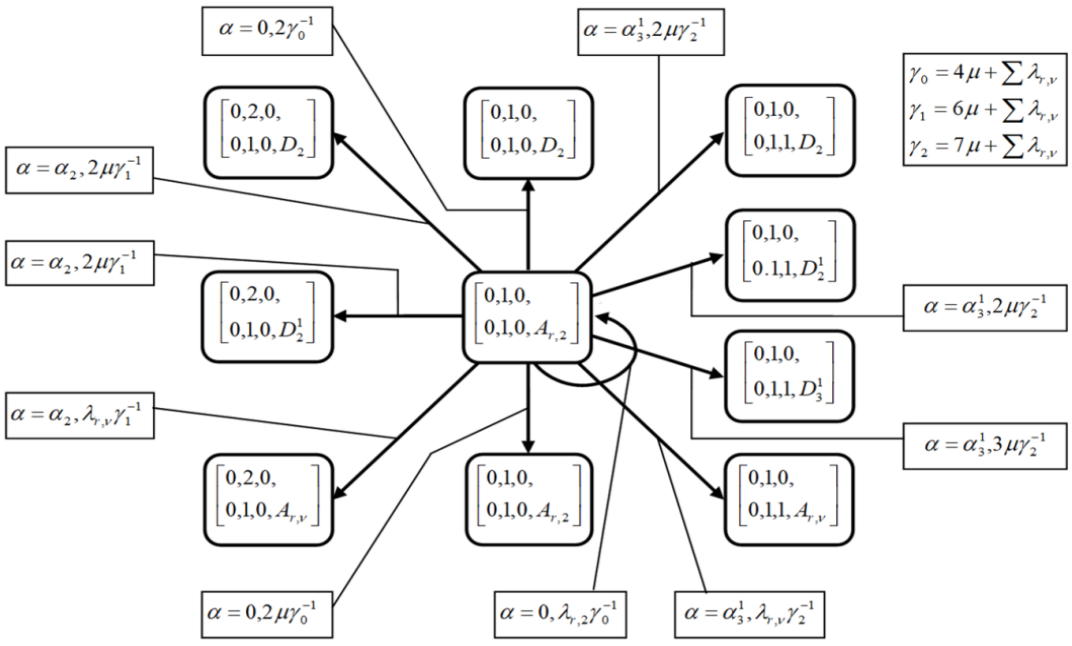


Рис. 4. UML-діаграму станів переходу ІСКЗ зі стану s у стани $k=\left\{\left[0,2,0,0,2,0,e\left(s\right)\right],\left[0,1,0,0,1,0,e\left(s\right)\right],\left[0,1,0,0,1,1,e\left(s\right)\right]\right\}$ згідно з моделлю (10)—(13)

Задачу управління доступністю ІСКЗ з резервування ресурсів на заходи для убезпечення системного ІС від дій АС сформулюємо аналогічно (5), конкретизувавши спосіб визначення показника доцільності системних операції $k\left(s,\alpha\right)$

$$k(s,\alpha)=\begin{cases} E_\alpha - rE_t R^{-1} - C_t\left(j\mu_i\right)^{-1},\ e(s)=A_{r,v}\vee\alpha=\alpha_i^j, \\ E_\alpha + rE_s R^{-1} - C_t\left(j\mu_i\right)^{-1},\ e(s)=A_{r,v}\vee\alpha=\alpha_i^f, \\ E_r r^{-1},\ e(s)=A_{r,v}\vee\alpha=0, \\ 0,\ \alpha=-1, \end{cases} \tag{14}$$

де E_s — накопичувальний показник, що враховує додаткове резервування ВМ для убезпечення ІС ІСКЗ від дій АС, тоді як E_t — накопичувальний показник, що враховує кількість виділення АС ВМ, дії у яких не контролюються ІС. Зростання показника E_s відбивається на зниженні доступності ІСКЗ, адже її ресурси додатково витрачатимуться на задачі самоубезпечення, що, втім, веде до зростання безпеки ІСКЗ. Показник E_t виступає антагоністом показникові E_s. Загалом, ситуації, коли дії АС супроводжуються зростанням показника E_s або E_t, є нетиповими, непередбаченими у СПБ, і є результатом втручання адміністратора у перебіг процесу доступу АС до ІС ІСКЗ. Показник для нормування вартості обчислювальних та комунікаційних ресурсів $\mathrm{o}(s,\alpha)$ представимо у вигляді $\mathrm{o}(s,\alpha)=c_{vm}\left(\sum\limits_{i=1}^{W}\sum\limits_{j=1}^{T} jx_i^j + \sum\limits_{i=1}^{W}\sum\limits_{j=1}^{T}(j+f)x_i^f\right)$, де c_{vm} — норма вартості використання ресурсів однієї ВМ.

Вищеописані адаптації, спрямовані на урахування при оцінюванні доступності ІСКЗ необхідності резервування ресурсів на її самоубезпечення, можна без додаткових модифікацій узагальнити у вигляді задачі оптимізації з цільовою функцією $\Phi(s,\alpha)$, аналогічною (7), і системою обмежень, аналогічною (8). Результатом розв'язання такої задачі для конкретної ІСКЗ буде стратегія управління доступом до її ІС з оптимізацією внутрішньосистемних сервісних операцій, отримувана у вигляді множини оптимальних параметрів $z(s,\alpha)\in Z$, на основі яких формуватимуться оптимальні з позиції СПБ відповіді α від ІСКЗ, що перебуває у стані s на вхідні запити АС. Стохастичну оцінку отриманої оптимальної стратегії управління доступом Z можна отримати на основі (9).

Постановка експерименту і аналіз результатів

Обчислимо оптимальну стратегію управління доступом ІСКЗ, розв'язавши задачу оптимізації (7), (8) у програмному середовищі Matlab [16] за допомогою функції *linprog*, яка входить до Optimization Toolbox, з такими значеннями вихідних параметрів: ІСКЗ дозволяє створювати не більше 2-х ВМ у ІС СРЦ і 2-х ВМ у ІС СД для одного прийнятого від АС вхідного запиту (сесії), шаблон формату стану має вигляд $s=\left[x_1^1,x_1^2,x_2^1,x_2^2,y_1,y_2,e(s)\right]$, стохастичні параметри інтенсивностей запитів $\left[\lambda,\mu_1^1,\mu_1^2,\mu_2^1,\mu_2^2,\nu_1,\nu_2\right]$ встановимо рівними $[12,3,4,5,6,3,5,5,5]$, обмеження на кількість інформаційних потоків $[M,B]$ встановимо рівними $[10,10]$, коефіцієнти для задачі оптимізації доступності ІСКЗ $\left[E_\alpha,E_r,C_t,P_b\right]$ встановимо рівними $\left[6,3,1,5\cdot10^{-3}\right]$. Підставивши вищевказані значення у (7), (8), отримали оптимальні значення налаштувань СПБ у вигляді множини Z, які для наочності узагальнено у вигляді діаграм на рис. 5 для різних варіантів вихідного стану ІСКЗ s, враховуючи, що $\sum\alpha=1$, $x_1^1=\overline{0,10}$, $x_1^2,x_2^1,x_2^2=\overline{0,5}$.

Інтерпретуємо результати, наведені на рис. 5а. Нехай, наприклад, $x_1^1=3$ і $y_1=3$, тобто у певний момент часу ІСКЗ підтримує три активних сесії 1-го АС, кожна з яких використовує 1 ВМ у ІС СРЦ і 1 ВМ у ІС СД. Враховуючи, що за умови експерименту максимальна кількість ВМ, яку можна створити у ІС СРЦ, $M=10$ і максимальна кількість ВМ, яку можна створити у ІС СД $B=10$, то обчислювані ресурси СРЦ і СД завантажені на 30 % і 30 %, відповідно. Для поточного стану s здійснювана ІСКЗ внутрішня операція $e(s)=A_n$, тобто система очікує на вхідний запит. Відповідно до розрахованої оптимальної СПБ відповідь системи на вхідний запит буде α_1^1 (виділення 1 ВМ у ІС СРЦ і 1 ВМ у ІС СД) з імовірністю 65 %, α_2^1 (виділення 2 ВМ у ІС СРЦ і 1 ВМ у ІС СД) з імовірніс-

тю 20 %, α_2 (виділення 2 ВМ у ІС СРЦ) з імовірністю 15 %, тобто СПБ ІСКЗ віддає перевагу збалансованому помірному завантаженню ресурсів СРЦ і СД. Аналогічно, за $x_1^1 = 9$ і $y_1 = 9$ відповідь СПБ на вхідний запит буде: $\alpha_0 = 30\,\%$ (відхилення запиту), $\alpha_1^1 = 30\,\%$ (виділення 1 ВМ у ІС СРЦ і 1 ВМ у ІС СД, причому ресурси ІСКЗ будуть повністю завантажені), $\alpha_1 = 40\,\%$ (виділення 1 ВМ у ІС СРЦ). За $x_1^1 = 10$ відповідь СПБ на вхідний запит буде $\alpha_0 = 100\,\%$.

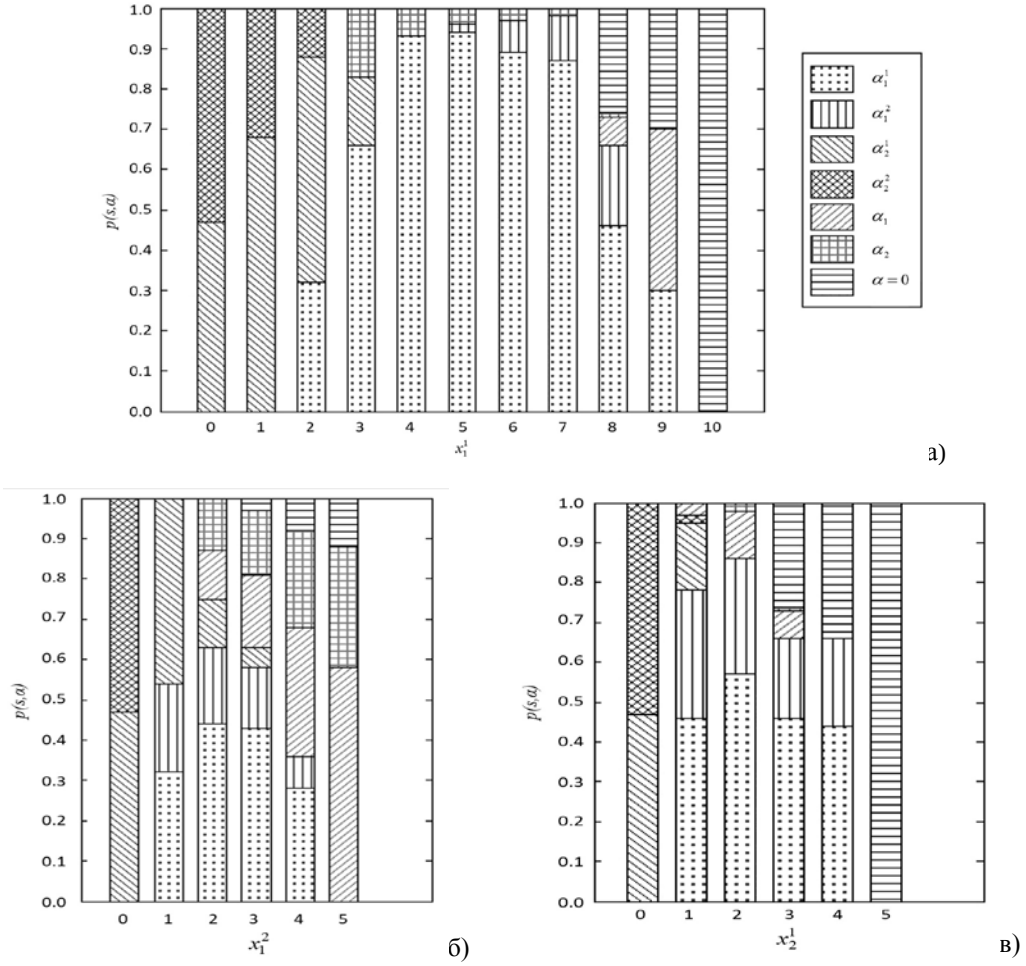


Рис. 5. Оптимальна стратегія відповіді ІСКЗ на вхідний запит АС, якщо:
а — стан $s = \left[x_1^1, 0, 0, 0, y_1 = x_1^1, 0, A_n\right]$, б — стан $s = \left[0, x_1^2, 0, 0, y_1 = 2x_1^2, 0, A_n\right]$, в — стан $s = \left[0, x_1^2, 0, 0, y_1 = 0.5x_1^2, 0, A_n\right]$

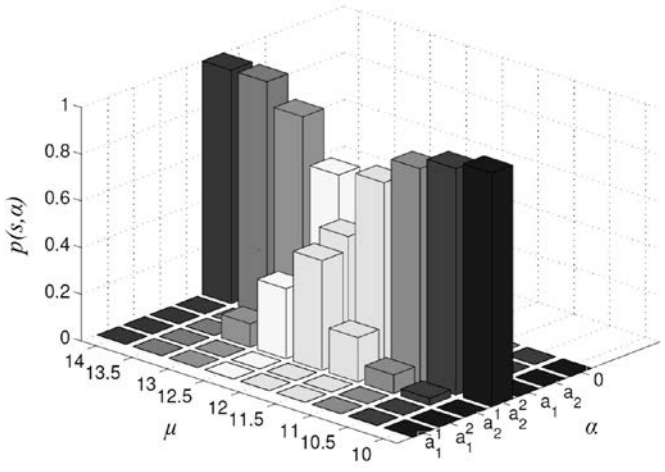


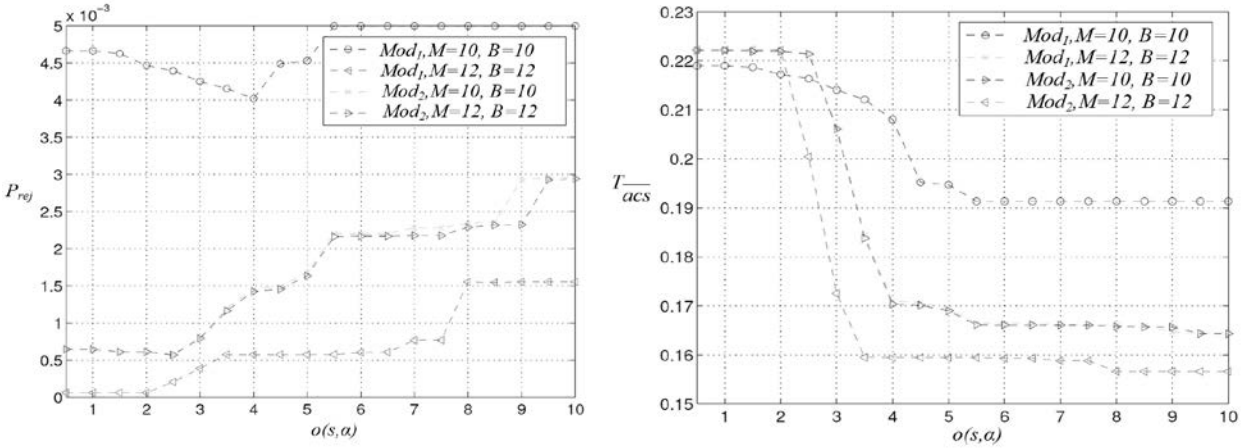
Рис. 6. Візуалізація оптимальної стратегії відповіді ІСКЗ, яка перебуває у стані $s = \left[0, 0, 0, 0, 0, 0, A_n\right]$, на вхідний запит АС

Для візуалізації отриманої внаслідок розв'язання задачі (7), (8) оптимальної СПБ для управління доступністю ІСКЗ приведемо систему у стан $s = \left[0, 0, 0, 0, 0, 0, A_n\right]$ (без урахування інформації про попередні стани), тоді узагальнену оптимальну стратегію управління доступом у вигляді значень імовірностей $p(s, \alpha)$, похідних від керованих змінних задачі оптимізації (7), (8) $z(s, \alpha) \in Z$, які описують варіант відповіді системи α на вхідні запити, що надходять з різною інтенсивністю μ, показано на рис. 6.

З результатів (рис. 6) видно, що у оптимальній стратегії управління доступом ІСКЗ за низької і високої інтенсивності

надходження вхідних запитів спостерігається тенденція до рівномірного завантаження ІС СРЦ і ІС СД. За середньої інтенсивності надходження вхідних запитів ІС СРЦ завантажується більше, що приводить до зростання вартості функціонування системи за одиницю часу але дозволяє підтримувати стохастичну оцінку доступності системи у заданих (8) межах, позаяк обчислювальна потужність, а отже, і швидкість реагування апаратної платформи СРЦ вища за аналогічний показник СД.

Оцінимо залежність доступності ІСКЗ від витрат на функціонування системи $o(s,\alpha)$. Враховуючи, що показник $o(s,\alpha)$ для базової моделі доступності ІСКЗ (далі — Mod_1) і для моделі доступності ІСКЗ з резервуванням ресурсів на убезпечення системного ІС від дій АС (далі — Mod_2) розраховується по-різному, введемо узагальнені показники для оцінювання доступності. Використовуватимемо узагальнений показник імовірності відхилення вхідного запиту $P_{rej} = N_{rej} / N_{all}$, де N_{rej} — кількість відхилених ІСКЗ вхідних запитів, а N_{all} — загальна кількість вхідних запитів за період спостережень T_s, і показник середньої тривалості сервісних операцій $T_{\overline{acs}} = T_s / \left(N_{all} - N_{rej}\right)$, який є узагальненням показника $\tau(s,\alpha)$ для періоду спостережень T_s. Емпіричні значення залежності цих показників від узагальненої вартості використання ІСКЗ за одиницю часу $o(s,\alpha)$ для різних стратегій завантаження ІС СРЦ і ІС СД, кожна з яких задовольняє сформульованій у (8) умові $\sum_{s\in S}\sum_{\alpha=0}\tau(s,\alpha)z(s,\alpha) \le P_b$, показані на рис. 7.



а) б)

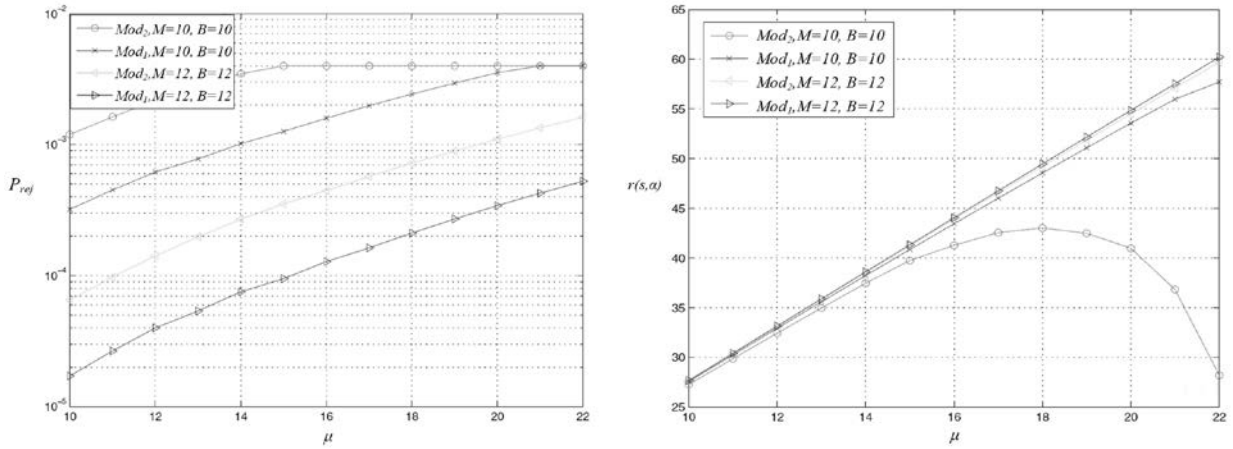
Рис. 7. Визначена з урахуванням відповідної стратегії доступності ІСКЗ залежність узагальненої вартості використання системи за одиницю часу $o(s,\alpha)$ від: а — узагальненого показника імовірності відхилення вхідного запиту P_{rej}; б — середньої тривалості сервісних операцій $T_{\overline{acs}}$

Показані на рис. 7 результати отримано за $P_b = 5\cdot 10^{-3}$. Як видно з рис. 7а, узагальнена імовірність відхилення вхідного запиту P_{rej} зростає зі зростанням узагальненої вартості використання системи за одиницю часу $o(s,\alpha)$ для всіх стратегій управління доступністю ІСКЗ. Втім, найкраща динаміка залежності спостерігається для стратегій, параметри яких наближені до оптимальної. В цілому ж характер залежності P_{rej} від $o(s,\alpha)$ можна пояснити тим, що зростання $o(s,\alpha)$ пов'язано зі зростанням кількості активних ВМ, що природно, приводить до зростання кількості відхилень вхідних запитів. Наведені на рис. 7б результати показують, що для всіх стратегій управління доступністю ІСКЗ значення середньої тривалості сервісних операцій становить скінченну величину, значення якої лише частково залежить від витрат на функціонування системи, а визначається обраною стратегією управління доступністю, що підтверджує актуальність отриманих моделей.

Окремої уваги варте порівняння моделі доступності ІСКЗ з резервуванням ресурсів на убезпечення системного ІС від дій АС Mod_2 з базовою моделлю доступності ІСКЗ Mod_1 за такими критеріями як узагальнена імовірність відхилення вхідного запиту P_{rej} і значення функції якості реакції ІСКЗ на вхідний запит $r(s,\alpha)$, яке розраховується за рівнянням (5) із сегрегацією прави-

ла обчислення показника $k(s,\alpha)$ за видом моделі доступності. Дослідження моделі Mod_2 проводилося в умовах надходження вхідних запитів від АС, кожному з яких присвоєно відповідний рівень загрози безпеці ІСКЗ у вигляді параметра r, значення якого вибиралися з множини значень $\{low, medium, high\} = \{0,2, 0,5, 0,8\}$, відповідно. Правила виділення ВМ на убезпечення системного ІС в залежності від значення параметра *r* для *i*-го АС формулювалися так:

$r_i = medium \to x_i^j = 1,2,3 \to x_i^f = 0,1,2$; $r_i = high \to x_i^j = 1,2,3 \to x_i^f = 1,2,2$. Обмеження $x_i^j \le 3$, $f_i{}^j \le 2$, $M = \{10,12\}$, $B = \{10,12\}$ стосувалися обох досліджуваних моделей. Для проведеного дослідження імовірність того, що вхідний запит надійшов від АС з рівнем $r = \{low, medium, high\}$ становила $\{0,2, 0,3, 0,5\}$, відповідно.



а) б)

Рис. 8. Порівняння моделі доступності ІСКЗ з резервуванням ресурсів на убезпечення системного ІС від дій АС з базовою моделлю доступності ІСКЗ за критерієм: а — узагальненої імовірності відхилення вхідного запиту P_{rej};

б — значенням функції якості реакції ІСКЗ $r(s,\alpha)$ на вхідний запит

Наведені на рис. 8а результати показують, що імовірність відхилення вхідного запиту значною мірою залежить від кількості доступних для створення ВМ апаратних ресурсів у системі, встановлюваних параметрами $[M,B]$, та інтенсивності надходження вхідних запитів. Виділення системних ресурсів на заходи убезпечення не приводять до перевищення глобального обмеження на імовірність відхилення вхідних запитів $P_b = 5 \cdot 10^{-3}$ зі зростанням інтенсивності їх надходження, що говорить про ефективність оптимальних налаштувань СПБ для обох розглянутих моделей доступності ІСКЗ. Втім, для СПБ, сформульованої на основі моделі Mod_2, узагальнена імовірність відхилення вхідних запитів виявляється вищою за значення цього ж показника для СПБ, сформульованої на основі моделі Mod_1. Особливо цікаві результати показані на рис. 8б. Виявилося, що якість реакції ІСКЗ, яка визначається моделлю Mod_2, коли значення параметрів $[M,B] = [10,10]$ починає стрімко знижуватися зі зростанням інтенсивності вхідних запитів, але зі збільшенням значень параметрів $[M,B]$ до $[12,12]$ ситуація покращується до зіставних з моделлю Mod_1 результатів. Таку реакцію можна пояснити вибраними правилами виділення ВМ на убезпечення системного ІС, за яких для АС з $r = 0,8$ співвідношення кількості ВМ на підтримку дій АС до кількості ВМ на заходи убезпечення становить близько $3:2$. В результаті, якщо інтенсивність запитів від «ненадійних» АС домінує у множині вхідних запитів, системі не вистачає до 20 % апаратних ресурсів для ефективного функціонування. Цю обставину необхідно враховувати при проектуванні ІСКЗ.

Узагальнимо емпіричну частину статті оцінюванням адекватності запропонованих моделей в рамках класичної теорії планування експерименту. Сформуємо тестову матрицю вхідних параметрів для АС: $X = \{ID_{ij}, PW_{ij}, VT_{ij}\}$, де $i = \overline{1,N}$ — номер АС, який бажає отримати доступ до ІСКЗ, $j = \overline{1,M}$ — кількість спроб отримання доступу для кожного *i*-го АС, ID_{ij}, PW_{ij}, VT_{ij} — введені

i-м АС в *j*-й спробі отримання доступу дані ідентифікаційної карти, секретний пароль і індивідуальні параметри голосу, відповідно. Для репрезентативності результатів експерименту взято $N = 20$, $M = 70$. Далі проведемо експерименти з отримання доступу АС, індивідуальну інформацію яких систематизовано у *X*, до ресурсів ІСКЗ, управління доступом до ресурсів якої реалізовано без урахування вищеописаних моделей за правилами, описаними у [17]. Результати експериментів представимо у вигляді матриці $Y_e = \left(y_{ij}\right)$, де $y_{ij} = \left\{res_{ij}, t_{ij}\right\}$ — множина, у якій res_{ij} — результат *j*-ї спроби отримання *i*-м АС доступу до ІСКЗ, t_{ij} — час, витрачений АС на реалізацію права на отримання доступу. Оптимізуємо процес управління доступом до ресурсів ІСКЗ, налаштувавши СПБ на основі запропонованої у статті моделі. Проведемо дослідження процесу отримання доступу АС, індивідуальну інформацію яких узагальнено у *X*, до ресурсів ІСКЗ з оптимізованою СПБ, оформивши результати експериментів у вигляді $Y'_e = \left(y'_{ij}\right)$, де $y'_{ij} = \left\{res'_{ij}, t'_{ij}\right\}$ — множина, у якій res'_{ij} — результат *j*-ї спроби отримання *i*-м АС доступу до ІСКЗ з оптимізованою СПБ, а t'_{ij} — час, витрачений АС для отримання доступу. Розрахуємо для *i*-го АС дисперсію відхилень відгуків ІСКЗ з оптимізованою СПБ від результатів ІСКЗ з базовою СПБ: $s_i^2 = M^{-1}\sum_{j=1}^{M}\left(y_{ij} - y'_{ij}\right)^2$. Розрахуємо середнє значення дисперсії для всіх АС, які приймали участь у дослідженнях: $s^2 = N^{-1}\sum_{i=1}^{N} s_i^2$. Оцінювання фактичних відхилень s_i^2 від s^2 за критерієм Фішера показало, що всі відхилення не перевищують табличних значень, що підтверджує адекватність запропонованої у статті моделі оптимізації процесу доступу до ІСКЗ.

Висновки

У проведеному автором моделюванні безпеки ІСКЗ у рамках тріади CIA [17] основну увагу акцентовано на питаннях конфіденційності і цілісності. Втім, опис інформаційної безпеки ІСКЗ не може вважатися завершеним без прикладної моделі доступності такої системи з урахуванням її архітектурних особливостей, адже, згідно з [1], ІСКЗ розгортається на мультисерверній платформі, яка включає сервер-реєстраційний центр і множину зв'язаних з ним серверів даних. Отже, в статті розглянуто актуальне питання моделювання процесу підтримки інформаційним середовищем ІСКЗ дій авторизованих суб'єктів в рамках їх ролей, описаних у системній політиці безпеки.

В загальному вигляді доступність ІСКЗ передбачає виділення авторизованому суб'єкту у відповідь на його вхідний запит ресурсів інформаційного середовища ІСКЗ, скінченний обсяг яких обмежено поняттям віртуальної машини. Архітектурна організація ІСКЗ передбачає, що віртуальні машини можуть створюватися: у інформаційному середовищі сервера-реєстраційного центру; у інформаційному середовищі серверів даних; в обох цих інформаційних середовищах одночасно відповідно до розташування інформаційних ресурсів, до яких звертається авторизований суб'єкт, правил підтримки його дій, сформульованих у системній політиці безпеки, і ступеня завантаженості відповідних інформаційних середовищ. Обмеження доступності пов'язуватимемо з відсутністю вільних ресурсів у ІСКЗ для створення нових віртуальних машин за запитом авторизованого суб'єкта, що приводитиме до тимчасового відхилення нових вхідних запитів для здійснення сервісних операцій з вивільнення системних ресурсів. Отже, потрібно сформулювати правила, які регламентуватимуть відповідь ІСКЗ на вхідний запит авторизованого суб'єкта, проведення сервісних операцій, розміщення віртуальних машин та узгодити ці правила між собою з передбаченням ресурсів на самоубезпечення системи від наслідків дій авторизованих суб'єктів. Ці правила повинні забезпечувати доступність ІСКЗ із заданою імовірністю за мінімізації витрат на функціонування системи.

У статті запропоновано нові математичні моделі управління доступністю ІСКЗ, які, на відміну від існуючих, враховують топологічні особливості ІСКЗ, перебіг її сервісних операцій в управлінні доступом авторизованих суб'єктів до інформаційного середовища системи і формалізують зв'язок множини сервісних операцій з множиною відповідей системи на запити авторизованих суб'єктів у вигляді керованого напівмарковського процесу з резервуванням ресурсів на заходи самоубезпечення, що дозволяє за допомогою апарату математичного програмування отримати оптимальну стратегію управління доступністю ІСКЗ з мінімізацією витрат на її функціонування та отримати

стохастичну оцінку доступності системи на будь-якому етапі її життєвого циклу.

На основі створених моделей проведено імітаційне моделювання доступності ІСКЗ із застосуванням програмного середовища Matlab. Результати досліджень показали, що отримані на основі запропонованих моделей правила реагування на вхідні запити авторизованих суб'єктів в залежності від завантаженості системи і виконуваних у системному інформаційному середовищі сервісних операцій, дозволяють підтримувати імовірність відхилення вхідних запитів авторизованих суб'єктів в заданих межах, мінімізуючи витрати на функціонування ІСКЗ. Втім, аналіз емпіричних результатів показав, що при побудові правил системної політики безпеки на основі моделі доступності ІСКЗ з резервуванням ресурсів на убезпечення системного інформаційного середовища від дій авторизованих суб'єктів за стрімкого зростання інтенсивності запитів від авторизованих суб'єктів з високим показником небезпечності кількість відмов у наданні доступу починає квадратично зростати. Дослідження показали, що для уникнення вищеописаного падіння доступності ІСКЗ варто на етапі проектування закладати 20 % резерв системних ресурсів. Загалом, отримані експериментальні результати підтвердили адекватність запропонованих моделей доступності ІСКЗ.

В подальших дослідженнях планується розглянути формалізацію виду взаємозв'язків між отриманими моделями конфіденційності, цілісність і доступність ІСКЗ з метою структурної оптимізації системи для зменшення витрат на її функціонування.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] В. В. Ковтун «Концепція впровадження автоматизованої системи розпізнавання мовця у процес автентифікації для доступу до критичної системи,» *Вісник Вінницького політехнічного інституту*, № 5, с. 41-52, 2018. https://doi.org/10.31649/1997-9266-2018-140-5-41-52 .

[2] S. K. Dong, F. Machida, and K. S. Trivedi, "Availability Modeling and Analysis of a Virtualized System," in *15th IEEE Pacific Rim International Symposium on Dependable Computing PRDC '09*, pp. 365-371, 2009.

[3] R. Ghosh, F. Longo, V. K. Naik, K. S. Trivedi, "Modeling and performance analysis of large scale IaaS Clouds [Text]" *Future Generation Computer Systems*, vol. 29 (2), pp. 1216-1234, 2013.

[4] Marcello Trovati, Win Thomas, Quanbin Sun, and Georgios Kontonatsios, "Assessment of Security Threats via Network Topology Analysis: An Initial Investigation," in *12th International Conference, GPC, Italy*, vol. 10232, pp. 416-425, 2017. https://doi.org/10.1007/978-3-319-57186-7_31 .

[5] Shibo Luo, Mianxiong Dong, Kaoru Ota, Jun Wu, and Jianhua Li, "A Security Assessment Mechanism for Software-Defined Networking-Based Mobile Networks," *Sensors (Basel, Switzerland*), vol. 15 (8), pp. 31843–31858, 2015. https://doi.org/10.3390/s151229887 .

[6] B. Wei, C. Lin, and X. Kong, "Dependability Modeling and Analysis for the Virtual Data Center of Cloud Computing," *IEEE International Conference on High Performance Computing and Communications*, pp. 784-789, 2011.

[7] T. Thein, and J. S. Park, "Availability Analysis of Application Servers Using Software Rejuvenation and Virtualization," *Journal of Computer Science and Technology*, Institute of Computing Technology Beijing, vol. 24 (2), pp. 339-346, 2009.

[8] R. R. Scadden, R. J. Bogdany, J. W. Clifford, and H. D. Pearthree, "Resilient hosting in a continuous available virtualized environment," *IBM Systems Journal*, Atlanta, vol. 47 (1), pp. 535-548, 2008.

[9] Y. S. Dai, M. Xie, and K. L. Poh, "Reliability of grid service systems," *Computers & Industrial Engineering*, vol. 50 (1–2), pp. 130-147, 2006.

[10] Y. S. Dai, B. Yang, J. Dongarra, and G. Zhang, "Cloud Service Reliability: Modeling and Analysis" [Electronic resource]. Access mode: http://www.netlib.org/utk/ people/JackDongarra/PAPERS/ .

[11] Quanjun Yin, Shiguang Yue, Yabing Zha, and Peng Jiao, "A Semi-Markov Decision Model for Recognizing the Destination of a Maneuvering Agent in Real Time Strategy Games," *Mathematical Problems in Engineering*, vol. 2016, Article ID 1907971, 15 p, 2016. https://doi.org/10.1155/2016/1907971 .

[12] Dongyan Chen, and Kishor S.Trivedi, "Optimization for condition-based maintenance with semi-Markov decision process," *Reliability Engineering & System Safety*, vol. 90, iss. 1, pp. 25-29, 2005. https://doi.org/10.1016/j.ress.2004.11.001 .

[13] Arash Khodadadi, Pegah Fakhari, Jerome R. "Busemeyer Learning to maximize reward rate: a model based on semi-Markov decision processes," *Frontiers in neuroscience*, USA, vol. 8, Article ID 101, 15 p, 2014. https://doi.org/10.3389/fnins.2014.00101.

[14] M. U. Khan, "Representing Security Specifications in UML State Machine Diagrams," *Procedia Computer Science*, vol. 56, pp. 453-458, 2015. https://doi.org/10.1016/j.procs.2015.07.235 .

[15] N. V. Vaidya, and N. W. Khobragade, "Solution of Game Problems Using New Approach," *Journal of Computer Science and Technology. International Journal of Engineering and Innovative Technology (IJEIT)*. vol. 3, iss. 5, pp. 181-186, 2009.

[16] I. Dogan, "Engineering simulation with MATLAB: improving teaching and learning effectiveness," *Procedia Computer Science*, vol. 3, pp. 853-858, 2011. https://doi.org/10.1016/j.procs.2010.12.140 .

[17] O. V. Bisikalo, V. V. Kovtun, M. S. Yukhimchuk, and I. F. Voytyuk, "Analysis of the automated speaker recognition system of critical use operation results," Radio Electronics, Computer Science, Control, № 4, pp. 71-84, 2018. https://doi.org/10.15588/1607-3274-2018-4-7.

Рекомендована кафедрою комп'ютерних систем управління ВНТУ

Стаття надійшла до редакції 28.01.2019

Ковтун В'ячеслав Васильович — канд. техн. наук, доцент, доцент кафедри комп'ютерних систем управління, e-mail: kovtun_v_v@vntu.edu.ua .

Вінницький національний технічний університет, Вінниця

V. V. Kovtun[1]

Modeling of the Information System for Critical Use Accessibility

[1]Vinnytsia National Technical University

Specification of the security of the information system for critical use (ISCU) within the CIA triad can't be considered complete without an application model of such a system's accessibility taking into account its topology, since it is expected that the ISCU will be deployed on a multi-server platform that includes a server-registration center and a set of connected with it data servers. In general, the ISCU's accessibility involves the allocation of an authorized user in response to its input information resource environment, the finite amount of which is limited to the concept of a virtual machine. The topology of the ISCU assumes that virtual machines can be created either in the information environment of the server-registration center or in the information environment of the data servers or in both of these information environments at the same time in accordance with the location of the information resources to which the authorized user addresses, the rules of support for its actions, formulated in the system security policy, and the degree of the functioning capacity of the relevant information environments. Accessibility restriction will be linked to the lack of free resources in the ISCU to create new virtual machines at the request of authorized user, which will temporarily discard new incoming requests for service operations to release system resources. The article presents new mathematical models for managing the ISCU's accessibility, which, unlike the existing ones, take into account the topological features of the ISCU, passing of its service operations in the management of the access of authorized users to the system's information environment and formalize the connection of the set of service operations with a set of system responses on incoming requests of authorized users in the form of a managed semi-markov process with reserve of resources for self-security measures, which allows using the mathematical programming apparatus for optimal management of ISCU's accessibility strategy for minimizing the cost of its operation and allows stochastically assess the system's accessibility at any stage of its life cycle. On the basis of the created models, a simulation of the ISCU's accessibility in the Matlab was conducted. The results of the research showed that the rules of response to incoming requests of authorized users received on the basis of the proposed models, depending on the system's functioning capacity and the service operations with are performed in the system's information environment, allow to maintain the probability of incoming requests rejection of authorized users within the specified threshold, minimizing the costs for the ISCU's functioning. However, the analysis of the empirical results of the ISCU's operation, the rules of the system security policy which were synthesized on the basis of the accessibility model with the resources reservation to the system's self security, showed that with the rapid increase in the intensity of incoming requests from authorized users with high rates of insecure the number of access rejection begins to increase quadratically. Studies have shown that in order to avoid the above described drop in the ISCU's accessibility it is necessary to foresee a system resource reserve of 20 % at the design stage. In general, the experimental results obtained confirmed the adequacy of the proposed ISCU's accessibility models.

Keywords: information system of critical use, accessibility, managed semi-markov process, optimization, mathematical programming.

Kovtun Viacheslav V. — Cand. Sc. (Eng.), Associate Professor, Associate Professor of the Chair of Computer Control Systems, e-mail: kovtun_v_v@vntu.edu.ua

В. В. Ковтун[1]

Моделирование доступности информационной системы критического применения

[1]Винницкий национальный технический университет

Описание безопасности информационной системы критического применения (ИСКП) в рамках триады CIA не может считаться завершенным без прикладной модели доступности такой системы с учетом ее архитектурных особенностей, ведь предполагается, что ИСКП разворачивается на мультисерверний платформе, которая включает сервер-регистрационный центр и множество связанных с ним серверов данных. В общем виде доступность ИСКП предусматривает выделение авторизованному субъекту в ответ на его входной запрос ресурсы информационной среды ИСКП, конечный объем которых ограничен понятием виртуальной машины. Архитектурная организация ИСКЗ предусматривает, что виртуальные машины могут создаваться или в информационной среде серверо-регистрационного центра или в информационной среде серверов данных или в обоих

этих информационных средах одновременно в соответствии с расположением информационных ресурсов, к которым обращается авторизованный субъект, правилами поддержки его действий, сформулированных в системной политике безопасности, и степенями загруженности соответствующих информационных сред. Ограничение доступности связано с отсутствием свободных ресурсов в ИСКП для создания новых виртуальных машин по запросу авторизованного субъекта, что приводит к временному отклонении новых входящих запросов для осуществления сервисных операций по освобождению системных ресурсов. В статье представлены новые математические модели управления доступностью ИСКП, которые, в отличие от существующих, учитывают топологические особенности ИСКП, ход ее сервисных операций при управлении доступом авторизованных субъектов к информационной среды системы и формализуют связь множества сервисных операций с множеством ответов системы на запросы авторизованных субъектов в виде управляемого полумарковского процесса с резервированием ресурсов на мероприятия по обеспечению безопасности информационной среды ИСКП, что позволяет с помощью аппарата математического программирования получить оптимальную стратегию управления доступностью ИСКП с минимизацией затрат на ее функционирование и позволяет стохастической оценить доступность системы на любом этапе ее жизненного цикла. На основе созданных моделей проведено имитационное моделирование доступности ИСКЗ, реализованной в программной среде Matlab. Результаты исследований показали, что полученные на основе предложенных моделей правила реагирования на входящие запросы авторизованных субъектов в зависимости от загруженности и выполняемых в системной информационной среде сервисных операций, позволяют поддерживать вероятность отклонения входящих запросов авторизованных субъектов в заданных пределах, минимизируя затраты на функционирование ИСКП. Впрочем, анализ эмпирических результатов работы ИСКП, правила системной политики безопасности которой были синтезированы на основе модели доступности с резервированием ресурсов на обеспечение безопасности системного информационной среды от действий авторизованных субъектов, показал, что при стремительном росте интенсивности запросов от авторизованных субъектов с высоким показателем неблагонадежности количество отказов в предоставлении доступа начинает квадратично расти. Исследования показали, что во избежание вышеописанного падения доступности ИСКП на этапе проектирования стоит закладывать 20 % резерв системных ресурсов. В общем, полученные экспериментальные результаты подтвердили адекватность предложенных моделей доступности ИСКП.

Ключевые слова: информационная система критического применения, доступность, управляемый полумарковский процесс, оптимизация, математическое программирование.

Ковтун Вячеслав Васильевич — канд. техн. наук, доцент, доцент кафедры компьютерных систем управления, e-mail: kovtun_v_v@vntu.edu.ua