DOI 10.15276/imms.v12.no1-2.114
УДК 004.681.3
Informatics and Mathematical Methods in Simulation
Vol. 12 (2022), No. 1-2, pp. 114-123

ОЦІНКА СТАНІВ ФУНКЦІОНУВАННЯ СИСТЕМИ КІБЕРНЕТИЧНОГО ЗАХИСТУ ДЕРЖАВИ

В.О.Хорошко, Ю.Є. Хохлачова

Національний авіаційний університет,
1, просп. Любомира Гузера, Київ, 03058, Україна, e-mail: professor_va@ukr.net

Розглядаються математичні методи дослідження процесу функціонування системи кібербезпеки держави, накопичення та обробки інформації. З урахуванням того, що в умовах війни Росії проти України задачі кіберзахисту інформаційних систем держави набули не аби якої значення, а полем інформаційної війни стали комп'ютерні мережі. Також показано, що для практичного використання одержаних теоретичних аналітичних результатів немає принципових труднощів. Незважаючи на те, що вони не дуже оглядові та мало відчутні на простий чисельний дотик, бо містять неелементарні функції, при наявності сучасних електронних обчислювальних машин та найрізноманітнішого програмного забезпечення, чисельно-графічні трактування одержаних формул і розв'язки, які в них входять, не є непереборною перепоною для одержання наглядного розв'язку та практичного використання в розрахунку та обґрунтуванні ефективності функціонування системи кібербезпеки держави.
Ключові слова: кібербезпека, кібербезпека держави, системи кібербезпеки держави, оцінка станів функціонування системи, математичні методи функціонування системи, ефективність функціонування системи.

Вступ

Події кінця XX – початку XXI сторіччя проходить на фоні трансформації суспільства від постіндустріального до інформаційного. В світі відбувається стрімкий розвиток інформаційних технологій та їх проникнення у всі сфери діяльності людини: соціальну, економічну, політичну, військову тощо. До основних рис процесу інформаційного суспільства на сучасному етапі відносяться глобалізація та інтенсифікація інформаційних процесів, зміна сучасної картини світу.

Завдяки революції в області інформатизації і комунікації відбуваються значні зміни у сфері кібербезпеки та захисту інформаційних ресурсів держави. Поширився континуум вимірів, в яких може вестися інформаційна війна – сьогодні можна констатувати, що вона ведеться не тільки в традиційних вимірах «простір-час», але і в «інформаційному вимірі» [1].

У сучасних умовах інформаційна інфраструктура держави набуває статусу критичної (життєво важливої для існування) з усіма від цього похідними: вона стає об'єктом першого удару і потребує для свого захисту збалансованої державної політики в інформаційному просторі. Це наглядно показує Росія своїми діями у війні проти України. Тому, до критичної інформаційної інфраструктури належать, в першу чергу, економіка, транспорт, енергетика, фінансова система, системи управління у державі, що забезпечують безпеку та оборону держави тощо. Інформаційна система, система управління, канали зв'язку, системи навігації, розвідка, банківські системи та інші елементи інформаційного середовища потребують захисту від відповідних впливів та атак.

Аналіз подій, що розгортаються в інформаційному просторі, дозволяє відзначати необхідні тенденції [1,2]:

- по-перше, глобальна інформатизація та створення високоінтелектуальних систем управління призводить до глобалізації об'єктів інформаційного впливу, розвитку відповідно до цього форм і способів ведення інформаційного протиборства.
- по-друге, використання світової мережі Internet та електронних засобів масової інформації для маніпулювання свідомістю як світової громадськості, так і населення окремої країни, зміщення та перенос, для цього, центру тяжіння у масовому інформуванні в бік електронних засобів;
- по-третє, перенос тероризму у площину інформатизації;
- по-четверте, наявність конфліктів у інформаційному просторі, при цьому вже зараз це підтверджує Росія.

Таким чином, в умовах сьогодення, коли суспільство практично повністю залежить від застосування інформаційних технологій, полем інформаційної війни стали комп'ютерні мережі, а метою й завданнями – стають задачі кіберзахисту інформаційних систем держави. Слід враховувати, що в умовах війни Росії проти України ці питання набувають не аби якої значення.

Мета роботи

Розглядаються математичні методи дослідження процесу функціонування системи кібербезпеки держави (СКБД), накопичення та обробки інформації.

Основна частина

Дослідження процесу функціонування СКБД щодо накопичення та обробки інформації вимагає застосування різноманітного математичного апарату для вдосконалення структури та форми управління процесом функціонування цієї системи. При цьому слід враховувати, що СКБД має у своєму складі підсистеми, які виконують задачі відповідно до регіону та ситуації. Таке управління передбачає використання досить адекватних математичних методів та моделей для аналізу та оптимізації різноманітних ситуаційних та технологічних процесів. Для побудови високо ймовірного прогнозу оптимального управління подальшим процесом функціонування системи в літературі відомі частково розроблені математичні моделі подібного призначення та проведені на їх основі дослідження для найпоширеніших задач прогнозу процесу функціонування системи. [3]. Проте інколи виникають такі специфічні умови в технологічних процесах, що відомі математичні моделі стають недостатньо адекватними. Розглянемо реальну задачу в термінах теорії масового обслуговування (ТМО) специфіка якої полягає в тому, що система накопичення та обробки інформації починає функціонування та діє лише при наявності накопиченої в ній визначеної кількості необхідної інформації, необхідного забезпечення, або в термінах ТМО – необхідної кількості вимог. Наприклад, створення кінцевої інформації системою або підсистемою може починатися лише в тому випадку, коли накопичена певна первинна кількість даних у вигляді певної бази, певного математичного та програмного забезпечення, що може бути обумовлено використанням певної технології. Надалі обсяг кінцевої інформації, необхідної для прийняття рішень, накопиченої та обробленої утворює достатній запас для подальшого зв'язку зі споживачами до того моменту, коли буде повністю задоволена потреба в цій інформації. Такий спосіб функціонування є найбільш раціональним, оскільки вимагає можливість неповного завантаження СКБД та зниження ефективності використання її ресурсів.

Таким чином маємо наступну інтерпретацію: вимога - квант - набір інформації та можливих програмних комплектуючих, обслужена вимога – готовий накопичений інформаційно оброблений та готовий до вживання продукт. Нагадаємо, що мова йде про обробку та накопичення інформації, її формалізацію та формалізацію лише в сенсі кількості інформації з позицій теорії інформації, без розгляду прикладного сенсу та захисту, що вкладається в цю кількість. Отже, в систему ТМО надходить деяка кількість первинної інформації. Моделюючи течію надходження вважаємо, що найадекватнішна модель його буде коли ймовірність того, що на малий проміжок часу $\Delta(\Delta\rightarrow 0)$ надійде певна кількість m вихідної інформації, дорівнює $\lambda_m\Delta+g(\Delta)$. З даного вихідного припущення випливає, що є стаціонарна неординарна пуасонівська течія. Природно для неї ввести узагальнене позначення параметра $\lambda = \sum_{i=1}^{\infty} \lambda_i$ та припустити виконання умови

$$\sum_{i=1}^{\infty} h_i < \infty, \qquad (1)$$

що є логічним продовженням вихідних даних.

Технологічний цикл (перший канал обслуговування) починається лише тоді, коли накопичена достатня кількість первинної інформації (кількість вимог в черзі), величину якої позначимо r_0.

Наступний технологічний цикл (другий цикл обслуговування) викликається, коли для цього також забезпечено кількість первинної інформації (кількість вимог) r_0, а в системі масового обслуговування їх є не менше $2r_0$. Таким чином n-ий канал включається і може обслуговувати лише після того, коли в системі буде не менше $r_0 n$ вимог; при цьому для простоти дослідження та математичної формалізації обмежень на кількість каналів в системі накладати не будемо, що не є суттєвими обмеженням застосовності результатів, адже реальне співвідношення вхідних параметрів завжди забезпечує досить обмежене граничне значення n. Вважаємо, що час обслуговування однієї вимоги кожним каналом не залежить від обслуговування на інших каналах, від течії вимог і розподілений за показниковим законом. Значення параметра обслуговування знову ж для простоти аналітичних виразів та обчислень покладемо рівним одиниці, що це звужує загальності вихідної задачі, адже параметри усталеного процесу ТМО залежить не від конкретних значень окремих параметрів елементів ТМО, а від їх співвідношення. Тому будь-який параметр можна взяти за одиницю виміру, поклавши його значення рівним одиниці і нормуючи при цьому значення інших параметрів. Таким чином припущення параметра експоненціального обслуговування, рівного одиниці, не має принципового значення.

В цих умовах та припущеннях нас цікавить розподіл кількості зайнятих каналів в режимі роботи системи, що встановлюється. Іншими словами, нас цікавить ймовірність зайнятості каналів технологічного циклу в установленому режимі функціонування, тобто коли накопичено достатню кількість первинної інформації та після цього пройшло відносно багато часу.

Введемо наступні позначення. Нехай p_r, r = 0,1,2,3,… - ймовірність того, що в довільно обраний момент часу в установленому режимі роботи системи обслуговуванням зайнято r каналів; p_k, k=0,1,2,3,… - ймовірність того, що в установленому режимі в довільний момент часу в системі знаходяться k вимог. Як бачимо з введеної формалізації вихідної задачі прогноз, а також управління процесу функціонування СКБД накопичення та обробки інформації визначається саме ймовірностями p_r. Очевидно, що за ймовірностями p_k легко визначити ймовірність p_r. Тому знаходимо ймовірність p_k [4]. Ще раз відмітимо, що сформульована задача не втрачає загальності за припущення, що параметр обслуговування рівний одиниці, адже стаціонарний розподіл p_k визначається не конкретними значеннями параметрами потоку та обслуговування, а їх співвідношенням. Якщо в реальній системі параметр обслуговування m то пронормувавши відповідно параметр потоку, можна користуватися результатами, що отримані нижче.

Подовжимо формалізацію та позначимо [x] – ціла частина величини x; $\beta(t)$ – число вимог, що знаходяться в системі в момент часу t. Неважко побачити, що введений до розгляду процес $\beta(t)$ являє собою однорідний ланцюг Маркова, і визначається ймовірностями переходу за малий час $\Delta(\Delta\to 0)$ у вигляді

$$p\{[\beta(t)^* = k] \to^{\Delta} \{\beta(t+\Delta) = k\}\} = 1 - \left(\lambda + \left[\frac{\lambda}{r_0}\right]\right)\Delta + g(\Delta),$$
$$p\{[\beta(t) = k] \to^{\Delta} \{\beta(t+\Delta) = k+m\}\} = \lambda_m \Delta + g(\Delta), m \ge 1, \quad (2)$$
$$p\{[\beta(t) = k] \to^{\Delta} \{\beta(t+\Delta) = k-1\}\} = \left[\frac{k}{r_0}\right]\Delta + g(\Delta).$$

З початкових умов про роботу системи випливає, що стани ланцюга $\beta(t)$ діляться на два класи. Стани $\{0,1,2,\dots,r_0\text{-}2\}$ утворюють клас незворотніх станів (інформаційно-програмне накопичення), тому що процес $\beta(t)$ попадаючи у множину станів $\{r_0\text{-}1, r_0, r_0+1,\dots\}$, вже ніколи не повернеться до множини станів $\{0,1,2,\dots,r_0\text{-}2\}$, оскільки обсяг інформаційних запасів щодо нормального функціонування системи не може зменшитися більш ніж до r_0-1 рівня в силу технологічного … функціонування системи. Математично це видно із співвідношення (2). Інші стани $\{r_0\text{-}1, r_0, r_0+1,\dots\}$ утворюють замкнений клас сполучених станів, тому що як вихід з (2), від'ємні стрибки процесу $\beta(t)$ можуть бути лише одиничними, що відповідає реальній ситуації, коли закінчення обслуговування відбувається по одному, тобто одинарно. Зі сказаного можна зробити висновок, що коли

$$p\{\beta(t)=k\}=p_k(t)$$

То, незалежно від розподілу β(t) ,границі

$$\lim_{t\to\infty} p_k(t) = p_k, \qquad k = 0,1,2,\dots, \qquad (3)$$

За введених умов шукані ймовірності завжди існують, тобто ланцюг $\beta(t)$ є ергодичним. Факт ергодичності ланцюга $\beta(t)$ встановлюється теоремою.

Теорема. Якщо $\beta(0)$ є $\{r_0\text{-}1, r_0, r_0+1\}$, то ланцюг Маркова $\beta(t)$ має стаціонарний розподіл і значить, всі його стани $\{r_0\text{-}1, r_0, r_0+1,\dots\}$ утворюють ергодичний клас.

Доведення. Розглянемо рівняння для визначення стаціонарних імовірностей $\{P_k\}$. Як слідує з співвідношення (2) вони мають такий вигляд

$$\lambda p_{r0-1} = p_{r0};$$
$$\left(\lambda + \left[\frac{k}{r_0}\right]\right)p_k = \left[\frac{k+1}{r_0}\right]p_{k+1} + \sum_{j=r-1}^{k-1} p_j\lambda_{k-j}, k \ge r_0. \qquad (4)$$

Припустимо $p_k=q_{k+1-r0}$, $k\ge r_0$-1. Тоді (4) набуває вигляду

$$hq_0 = q_1;$$
$$\left(\lambda + \left[\frac{m+r_0-1}{r_0}\right]\right)q_m = \left[\frac{m+r_0}{r_0}\right]q_{m+1} + \sum_{t=0}^{m-1} q_1\lambda_{m-t}, m \ge 1. \qquad (5)$$

Для зручності обчислень аналітичних перетворень та подальших викладок введемо твірні функції послідовностей λ_m і q_m , тобто

$$L(z) = \sum_{m=1}^{\infty} \lambda_m z^m, \theta(z) = \sum_{m=0}^{\infty} q_m z^m \; (|z| \le 1). \qquad (6)$$

Згідно одержаних визначень (5) маємо

$$\frac{\lambda - L(z)}{1-z}\theta(z) = \sum_{m=0}^{\infty}\left[\frac{m+r_0}{r_0}\right]q_{m+1}z^m,$$

або в позначення правої частини

$$\theta'_{1/r_0}(z) = \frac{h - L(z)}{1-z}\theta(z), \qquad (7)$$

де для компактності виразу приймемо позначення

$$\theta'_{1/r_0}(z) = \sum_{m=0}^{\infty}\left[\frac{m+r_0}{r_0}\right]q_{m+1}z^m.$$

Перетворимо вираз, позначений $\theta'_{1/r0}(z)$ наступним чином: зважаючи на те, що ціла частина $\left[\frac{m+r_0}{r_0}\right]$ для будь-якого $m=nr_0+k$ є незмінною для всіх $k \varnothing [0,r_0-1]$, перейдемо від сумування за індексом до індексу, а саме

$$\theta'_1(z) = \sum_{m=0}^{\infty}\left[\frac{m+r_0}{r_0}\right]q_{m+1}z^m = \sum_{k=0}^{r_0-1}\sum_{n=0}^{\infty}\left[\frac{nr_0+k+r_0}{r_0}\right]q_{nr_0+k+1}\,z^{nr_0+k}$$
$$= \sum_{k=0}^{r_0-1}\sum_{n=0}^{\infty}(n+1)q_{nr_0+k+1}z^{nr_0+k}$$
$$= \frac{1}{r_0}\left\{\theta^1(z) + \sum_{k=0}^{r_0-1}(r_0-k+1)\sum_{n=0}^{\infty}q_{nr_0+k+1}z^{nr_0+k}\right\}$$
$$= \frac{1}{r_0}\theta'(z) + \frac{1}{r_0 z}\sum_{k=1}^{r_0}(r_0-k)\sum_{n=0}^{\infty}q_{nr_0+k}z^{nr_0+k}.$$

Тепер позначимо через $\sqrt[r_0]{1} = \varepsilon_0, \varepsilon_1, \varepsilon_2, \dots, \varepsilon_{r_0-1}$ корені r$_0$-го ступеня з одиниці, тобто

$$\varepsilon_k = \cos\frac{2\pi k}{r_0} + i\sin\frac{2\pi k}{r_0} \qquad (8)$$

($k=0,1,2,\dots,r_0-1$).

Оскільки сума k–их ступенів їх

$$\varepsilon_0^k + \varepsilon_1^k + \varepsilon_2^k + \cdots + \varepsilon_{r_0-1}^k = \begin{cases} r_0, \text{якщо } k \text{ без залишку ділиться на } r_0\,, \\ 0, \text{якщо } k \text{ не ділиться на } r_0\,, \end{cases}$$

то можна записати

$$\sum_{j=0}^{r_0-1}\varepsilon_j^{-k}\,\theta(\varepsilon_j z) = \sum_{j=0}^{r_0-1}\varepsilon_j^{-k}\sum_{m=0}^{\infty}q_m\,\varepsilon_j^m z^m = \sum_{m=0}^{\infty}q_m z^m\sum_{j=0}^{r_0-1}\varepsilon_j^{m-k} = r_0\sum_{n=0}^{\infty}q_{nr_0+k}z^{nr_0+k} \qquad (9)$$

Використовуючи співвідношення (6) – о(9) отримаємо

$$\frac{\lambda - L(z)}{1-z}\theta(z) = \frac{1}{r_0}\theta(z) + \frac{1}{zr_0^2}\sum_{k=1}^{r_0-1}(r_0-k)\sum_{j=0}^{r_0-1}\varepsilon_j^{-k}\,\theta(\varepsilon_j r),$$

або спростивши рівність і розв’язуючи її відносно похідної, маємо

$$\theta'(z) = r_0\frac{\lambda - L(z)}{1-z}\theta(z) - \frac{1}{zr_0}\sum_{t=1}^{r_0-1}t\sum_{j=0}^{r_0-1}\varepsilon_j^t\theta(\delta_j z) \qquad (10)$$

Оскільки для j ϵ {1,2,…,r_0-1} має місце рівність

$$\sum_{j=1}^{r_0-1} r\varepsilon_j^t = \frac{\varepsilon_j}{(\varepsilon_j-1)^2}\left[(r_0-1)\varepsilon_j^{r_0} - r_0\delta_j^{r_0-1}+1\right],$$

що виходить з тотожності

$$\sum nx^n = \frac{x}{(1-x)^2}[(N-1)x^N - Nx^{N-1}+1](x\neq 1)$$

і рівності $\varepsilon_j^{r_0}=1$,то маємо

$$\sum_{t=1}^{r_0-1} t\varepsilon_j^t = \frac{r_0}{\varepsilon_j-1}(j=1,2,\dots,r_0-1), \tag{11}$$

що разом з (10) дозволяє записати

$$\theta'(z) = \left(r_0\frac{\lambda-L(z)}{1-z} - \frac{r_0-1}{2z}\right)\theta(z) + \frac{1}{z}\sum_{j=1}^{r_0-1}\frac{\theta(\varepsilon_j z)}{1-\varepsilon_j}. \tag{12}$$

Відмітимо, що в частинному випадку при $r_0=1$ (коли не існує обсягу інформації для нормальної роботи системи, точніше технологічний процес не вимагає необхідних запасів інформаційних та програмних ресурсів) співвідношення (12) набуває вигляду

$$\theta'(z) = \frac{\lambda-L(z)}{1-z}\theta(z), \tag{13}$$

що разом з умовою $\theta(1)=1$ дає знайомий результат

$$\theta(z) = exp\left\{-\int_z^1 \frac{\lambda-L(u)}{1-u}du\right\}, \tag{14}$$

який досить добре відомий в літературі для системи масового обслуговування з необхідною кількістю каналів. [5] Якщо L(z)=λz (тобто потік ординарний), то

$$\theta(z) = e^{h(z-1)}$$

І шуканий розподіл в цьому окремому випадку добре відомий тобто

$$p_k = q_k = e^{-\lambda}\frac{\lambda^k}{k!}(k\geq 0).$$

Маємо частковий побічний результат з ТМО, який одержаний раніше іншими авторами. [6] Нас цікавить загальний розв’язок поставленої задачі. А тому продовжимо займатися розв’язуванням отриманого диференційно-функціонального рівняння (10). Введемо позначення

$$\theta_j(z) = \theta\left(E_j z\right)\ (j=0,1,2,\dots,r_0-1).$$

Підставляючи в (10) замість z значення ε_jz, отримаємо

$$\theta'_e(z) = \left(\varepsilon_e r_0\frac{\lambda-L(\varepsilon_e z)}{1-\varepsilon_e z} - \frac{r_0-1}{2z}\right)\theta_e(z) + \frac{1}{2}\sum_{j=0}^{r_0-1}\left(1-\varepsilon_j\right)^{-1}\theta_{j+k}(mod\ r_0)(z), \tag{15}$$

(l=0,1,2,…,r_0-1).

Вводячи вектор-стовпчик (для зручності записаний рядком)

$$\bar{\theta}(z) = \{\theta_0(z),\theta_1(z),\dots,\theta_{r_0-1}(z)\}.$$

І матрицю

$$P(z) = \begin{Vmatrix} P_{0,0}(z) & \dots & P_{0,r_0-1}(z) \\ \dots & \dots & \dots \\ P_{r_0-1,0}(z) & \dots & P_{r_0-1,r_0-1}(z) \end{Vmatrix},$$

де сегменти

$$P_{ee}(z) = \varepsilon_e z_0 \frac{\varepsilon - L(\varepsilon_e z)}{1-\varepsilon_e z} - \frac{r_0-1}{2z},$$

$$P_{ee}(z) = z^{-1}(1-\varepsilon_{k-1})^{-1},\ (k \neq l).$$

І корені з від'ємним індексом визначені $\varepsilon_{-k} = \varepsilon_k^{-1}$, можемо переписати систему лінійних диференціальних рівнянь (15) у матричному вигляді

$$\frac{d}{dz}\bar{\theta}(z) = p(z)\bar{\theta}(z).\ (16)$$

Оскільки як при всіх *l* має місце $\theta_e(0) = q_0$, то систему (16) потрібно розв'язувати разом з початковою умовою

$$\bar{\theta}(0) = q_0\bar{e},\ \ (17)$$

де

$$\bar{e} = \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}.$$

Розв'язок системи (16), (17) (див. [7]) можливо подати у вигляді

$$\theta(z) = q_0 \Omega_0^z(P)\bar{e}, \qquad (18)$$

де матриця $\Omega_0^z(P)$- матрицант, що відповідає матриці P(z) на проміжку (0,z). Згідно [7], $\Omega_0^z(P)$можна обчислювати за будь-яким із наступних правил:

$$\Omega_0^z(P) = \sum_{k=0}^{\infty}\left[\int_0^2 p(u)du\right],$$

$$\Omega_0^z(P) = \lim_{n\to\infty}\left[e^{\frac{z}{n}P(z)} e^{\frac{z}{n}P(\frac{(n-1)z}{n})} \dots e^{\frac{z}{n}P(\frac{z}{n})}\right],$$

$$\Omega_0^z(P) = \int_0^z [E + P(u)]du = \lim_{n\to\infty}\left[E + P(z)\frac{z}{n}\right]\left[E + P\left(\frac{(n-1)z}{n}\right)\frac{z}{n}\right]\dots\left[E + P\left(\frac{z}{n}\right)\frac{z}{n}\right],$$

де E – одинична матриця.

З приводу представлення (18) відмітимо наступне: цей вираз має невизначеність в нулі, тому вираз треба розуміти в сенсі правої границі. В дійсності $\Omega_0^z(P)$ не існує, так як елементи матриці P(z) в околі нуля не тільки не обмежені, а і до того ж не інтегровані через наявність в них доданку виду $\frac{c}{z}$. Однак границя $\lim_{\varepsilon\to+0}\Omega_E^z(p)\bar{e}$ існує оскільки:

а) при множинні матриці на e отримуємо вектор-стовпчик, елементи якого є сумою рядків матриці:

б) в матриці P(z) суми рядків вже не містять «недобрих» додатків типу e/z, тому що

$$\sum_{\substack{k=0 \\ \overline{k\neq 1}}}^{r_0-1}\frac{1}{1-\varepsilon_k - 1} - \frac{r_0-1}{2} = 0.\ \ (19)$$

Дійсно, згідно з рішенням (11)

$$r_0 \sum_{\substack{k=0 \\ k\neq 1}}^{r_0-1} \frac{1}{1-\varepsilon_k - 1} = r_0 \sum_{k=0}^{r_0-1} \frac{1}{1-\varepsilon_k} = -\sum_{t=1}^{r_0-1} t \sum_{k=1}^{r_0-1} \varepsilon'_k = -\sum_{t=1}^{r_0-1} t \sum_{k=1}^{r_0-1} \varepsilon_t^{tk}$$
$$= -\sum_{t=1}^{r_0-1} t \sum_{k=1}^{r_0-1} (\varepsilon_t)^k = -\sum_{t=1}^{r_0-1} t \frac{\varepsilon_t^{r_0} - \varepsilon_t}{\varepsilon_t - 1} = \sum_{t=1}^{r_0-1} t \frac{r_0(r_0-1)}{2},$$

що рівносильно рівності (19).

Зі сказаного маємо, що (18) потрібно розуміти як

$$\theta(z) = q_0 \lim_{\varepsilon \to +0} \Omega_\varepsilon^z(p)\bar{e}.$$

Нехай матриця

$$\Omega_\varepsilon^z(p) = \left\| \overline{\omega}_{lk}^{(\varepsilon)}(z) \right\|, (l, k = 0,1,2, \dots, r_0 - 1),$$

має елементи, що задовольняють співвідношення.

$$\lim_{\varepsilon \to +0} \sum \overline{\omega}_{lk}^{(\varepsilon)}(z) = \overline{\omega_l}(z),$$

Тоді будемо мати:

$$\emptyset(z) = \theta_0(z) = q_0 \overline{\omega}_0(z),$$

або, використовуючи умову нормування $\emptyset(1) = 1$, остаточно отримаємо

$$\emptyset(z) = \frac{\overline{\omega}_0(z)}{\overline{\omega}_0(1)}. \quad (20)$$

Тобто, стаціонарний розподіл ланцюга Маркова β_k існує. Його твірна функція, що повністю визначає шуканий розподіл співпадає з правою частиною отриманої рівності (20).

Цим доведено, що всі стани $\{r_0\text{-}1, r_0, r_0+1, \dots\}$ утворюють один ергодичний клас, тобто теорема повністю доведена.

Якщо розглядати окремий випадок – потік вимог ординарний ($L(z)=\lambda z$), то стаціонарний розподіл може бути знайдений в явному вигляді, тому що β_k в такому припущені є частковим випадком процесу розмноження і загибелі. Дійсно, в окремому частинному випадку, що розглядається

$$p_k\left(\lambda + \left[\frac{k}{r_0}\right]\right) = \lambda p_{k-1} + \left[\frac{k+1}{r_0}\right] p_{k+1}, (k \geq r_o - 1),$$

або

$$\lambda p_k - \left[\frac{k+1}{r_0}\right] p_{k+1} = \lambda p_{k-1} - \left[\frac{k}{r_0}\right] p_k, (k \geq r_o - 1). \quad (21)$$

Оскільки $\lambda p_{r0} - 1 = p_{r0}$, то з виразу (21) маємо

$$p_k = \frac{\lambda}{\left[\frac{k}{r_0}\right]} p_{k-1}, (k \geq r_0),$$

або, отримуючи вираз через значення p_{r_0-1}, маємо

$$p_k = \frac{\lambda^{k+1-r_0}}{\left[\frac{k}{r_0}\right]\left[\frac{k-1}{r_0}\right] \dots \left[\frac{r_0}{r_0}\right]} p_{r_0-1}, (k \geq r_0). \quad (22)$$

Використовуючи умову нормування $\sum_{k=r_0-1}^{\infty} p_k = 1$, останню рівність остаточно можна переписати у вигляді

$$p_k = \left(\sum_{l=r_0}^{\infty} \frac{\lambda^l}{\prod_{j=r_0}^{l-1} \left[\frac{j}{r_0}\right]} \right)^{-1} \frac{\lambda^{k+1}}{\prod_{j=r_0}^{k} \left[\frac{j}{r_0}\right]}, (k \geq r_0 - 1). \quad (23)$$

Зупинимось детальніше на ще одному окремому під випадку даного випадку, тобто розглянемо $r_0 = 2$. Неважко показати, що при цьому підвипадку величини p_k є коефіцієнтами розкладу в степеневі ряди бесселевих функцій чисто уявного аргументу. Дійсно з (22) при $r_0 = 2$ отримаємо

$$p_{2k} = c \frac{\lambda^{2k+1}}{\left[\frac{2}{2}\right]\left[\frac{3}{2}\right]\dots\left[\frac{2k-1}{2}\right]\left[\frac{2k}{2}\right]} = c \frac{\lambda^{2k+1}}{k!\,(k-1)!},$$

$$p_{2k} = c \frac{\lambda^{2k}}{\left[\frac{2}{2}\right]\left[\frac{3}{2}\right]\dots\left[\frac{2k-1}{2}\right]\left[\frac{2k}{2}\right]} = c \frac{\lambda^{2k}}{(k-1)!\,(k-1)!}.$$

Тоді в силу цих співвідношень можна записати рівності:

$$\sum_{k=1}^{\infty} p_{2k}\, z^{2k} = \lambda c \sum_{k=1}^{\infty} \frac{(\lambda z)^{2k}}{k!\,(k-1)!} = \lambda^2 cz \frac{(\frac{1}{2} 2\lambda z)^{1+2r}}{r!\,(r+1)!} = \lambda^2 cz I_1(2\lambda z);$$

$$\sum_{k=1}^{\infty} p_{2k-1} z^{2k-1} = \lambda c \sum_{k=1}^{\infty} \frac{(\lambda z)^{2k-1}}{(k-1)!\,(k-1)!} = \lambda^2 cz \sum_{r=0}^{\infty} \frac{(\frac{1}{2} 2\lambda z)^{2r}}{r!\,r!} = \lambda^2 cz I_0(2\lambda z),$$

а з цих рівностей виходить:

$$p(z) = \sum_{k=1}^{\infty} p_k z^k = z \frac{I_0(2\lambda z) + I_1(2\lambda z)}{I_0(2\lambda) + I_1(2\lambda)}, \qquad (24)$$

з цього рівняння маємо

$$p_1 = \frac{1}{I_0(2\lambda) + I_1(2\lambda)} \ . \qquad (25)$$

Одержані аналітичні результати дозволяють визначити стаціонарні імовірності станів процесів функціонування системи, які розглядаються.

Потрібно відмітити, що розрахункову формулу (23) в явному вигляді можна поширити (також узагальнити) для під випадку неординарного потоку з геометричним розподілом вимог у групі. Отримані аналітичні формули (20), (23)-(25) дозволяють знаходити стаціонарні ймовірності станів процесу функціонування СКБД, яка розглядалась та підсистеми, які є в її складі, при специфічних припущеннях, характерною серед яких є деякий початковий обсяг первинної інформації, що дорівнює r_0-1.

Висновки

Слід зауважити, що для практичного використання одержаних теоретичних аналітичних результатів немає принципових труднощів. Незважаючи на те, що вони не дуже оглядові та мало відчутні на простий чисельний дотик, бо містять неелементарні функції, при наявності сучасних ЕОМ та найрізноманітнішого програмного забезпечення, чисельно-графічні трактування одержаних формул і розв’язки, які в них входять, не є непереборною перепоною для одержання наглядного розв’язку та практичного використання в розрахунку та обґрунтуванні ефективності функціонування СКБД.

Список літератури

1. Козюра В.Д., Хорошко В.О., Шелест М.Є., Ткач Ю.М., Балюнов О.О. Захист інформації в комп’ютерних системах. Ніжин: Орхідея, 2020. 236с.

2. Браіловський М.М.,Зибін С.В, Пискун І.В., Хорошко В.О., Хохлачова Ю.Є. Технології захисту інформації. К: Компринт, 2021. 296с.

3. Опірський І.Р. Загальні проблеми прогнозування НСД в інформаційних системах держави. *Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні*. 2015. Вип. 2(30). С. 31-34.

4. Вентцель Е.С. Теория вероятностей. М., Наука 1969. 464с.

5. Анисимов В.В., Закусило О.К., Донченко В.С. Элементы теории массового обслуживания и ассиметричного анализа систем. К: Вища школа, 1998. 249с.

6. Хинчин А.Я. Работы по математической теории массового обслуживания. М: ФМЛ, 1993. 242с.

7. Гантмахер Ф.Ф. Теория матриц. М: Наука, 1997. 659с.

ASSESSMENT OF THE STATES OF FUNCTIONING OF THE STATE CYBERNETIC PROTECTION SYSTEM

V.O. Khoroshko, Yu.Ye. Khokhlachova

National Aviation University,
1, pr. Lubomir Guzar, Kyiv, 03058, Ukraine, e-mail: professor_va@ukr.net

In this work, mathematical methods of researching the process of functioning of the state cyber security system, accumulation and processing of information are considered. Taking into account the fact that in the conditions of Russia's war against Ukraine, the tasks of cyber protection of the state's information systems have gained considerable importance, and computer networks have become the field of information warfare. It is also shown that there are no fundamental difficulties for the practical use of the obtained theoretical analytical results. Despite the fact that they are not very comprehensive and not very perceptible to a simple numerical touch, because they contain non-elementary functions, in the presence of modern electronic computers and a wide variety of software, numerical and graphic interpretations of the obtained formulas and the solutions included in them are not is an insurmountable obstacle for obtaining a visual solution and practical use in calculating and justifying the effectiveness of the state's cyber security system.

Keywords: cyber security, state cyber security, state cyber security systems, assessment of system functioning states, mathematical methods of system functioning, efficiency of system functioning.