УДК 004.621

ХОРОШКО Володимир Олексійович
ХОХЛАЧОВА Юлія Євгеніївна
ВИШНЕВСЬКА Наталія Сергіївна

ЧАС ПРИЙНЯТТЯ РІШЕНЬ У СИСТЕМІ КІБЕРЗАХИСТУ ДЕРЖАВИ

Постановка проблеми. В умовах сьогодення питання кіберзахисту як складової інформаційного захисту держави є надзвичайно актуальним для України та світової спільноти.

Кібербезпека є пріоритетним напрямом державної політики у сфері розвитку електронного простору та становлення інформаційного суспільства в Україні. Під кібербезпекою (кіберзахистом) слід розуміти захищення кіберпростору держави, за якого забезпечується сталий розвиток інформаційного суспільства та комунікаційного середовища, своєчасне виявлення, запобігання та нейтралізація кібератак.

Об'єктами кіберзахисту зокрема є:

– комунікаційні системи всіх форм власності, у яких обробляються національні інформаційні ресурси;

– об'єкти критичної інформаційної інфраструктури.

Забезпечення кібербезпеки в Україні ґрунтується на таких принципах:

– відкритості, доступності, стабільності та захищеності кіберпростору, розвитку мережі Інтернет та відповідальних дій у кіберпросторі;

– державно-приватної взаємодії, широкої співпраці з громадським суспільством у сфері кібербезпеки та кіберзахисту;

– міжнародного співробітництва з метою недопущення використання кіберпростору у протиправних цілях.

Слід ураховувати, що використання кіберпростору [1; 2] розширює можливості людей у спілкуванні, сприяє розвитку інформаційних технологій, досліджень та інновацій, промисловості й економіки. Водночас переваги сучасного кіберпростору неминуче ведуть до виникнення нових загроз людям, суспільству, національній і міжнародній безпеці. Разом з ініціативами природного (ненавмисного) походження зростають кількість і потужність кібератак, умотивованих інтересами окремих осіб, груп, держав та об'єднань країн.

Тому необхідно застосовувати різні методи протидії їм, зокрема й математичні методи моделювання, побудови та аналізу моделей як кібератак, так і кіберзахисту.

Підвищення ефективності математичного моделювання систем кіберзахисту інформації держави можна забезпечити за рахунок моделювання як комплексної системи, так і підсистем, які входять до її складу. Ця необхідність стимулює розробку моделей та алгоритмів, які дають змогу вирішувати складні задачі керування системою й обробки інформаційних потоків. Важливим є питання побудови вихідного розподілення сумарного навантаження підсистем та каналів зв'язку систем кіберзахисту інформації (СКЗІ) не тільки держави, а ще й суспільства та окремих підприємств, організацій [3]. Крім того, потрібно щодо кожної задачі комплексної системи кіберзахисту інформації визначити допусковий інтервал рішення з урахуванням:

– завдання директивних строків (термінів) вирішення задач;

– інформаційних взаємозв'язаних задач обробки та передачі інформації.

Визначення допускових інтервалів рішення здійснюється в декілька етапів.

На першому етапі проводиться прив'язка директивних термінів вирішення задач до моментів реального часу, визначених для задач СКЗІ технологічним цілям контролю й управління, тривалість яких визначається періодом часу, протягом якого отримані дані щодо вирішення задач управління системою кіберзахисту об'єкта відображають об'єктивну реальність із завданою точністю, що дає змогу приймати правильне рішення з управління СКЗІ об'єкта.

На другому етапі здійснюється вирішення взаємозв'язку директивних термінів вирішення задач кіберзахисту інформації. Директивні терміни регламентують час можливого початку та необхідного закінчення виконання завдання на мережі та визначаються зовнішніми факторами. Взаємозв'язок директивних термінів вирішення реалізується з урахуванням інформаційних зв'язків між задачами, які визначаються в процесі кіберзахисту інформації та аналізу інформаційно-логічної структури заданого комплексу задач управління кіберзахистом об'єкта.

На третьому етапі з урахуванням взаємозв'язків директивних термінів вирішення задач і завдання інформаційних залежностей між ними визначаються допустимі інтервали обробки та передачі інформації по мережі при забезпеченні функціонування СКЗІ.

Аналіз останніх досліджень і публікацій. Проблематиці прийняття рішень у системі кіберзахисту держави приділяла увагу низка науковців, зокрема Р. Грищук, Ю. Даник, О. Жданов, О. Жолдаков, В. Томашевський [1; 8].

Аналіз літератури показує, що в теперішній час немає єдиного підходу до комплексного вирішення проблеми синтезу математичних моделей та алгоритмів визначення часу прийняття рішень у системі як захисту, так і кіберзахисту інформації [4; 5]. Це питання на сьогодні через свою багатоаспектність усе ще є малодослідженим, і тому потребує проведення подальшого наукового пошуку.

Метою є дослідження третього етапу щодо визначення допустимих термінів вирішення інформаційно залежних задач систем кіберзахисту інформації.

Виклад основного матеріалу. Проблема синтезу математичних моделей та алгоритмів визначення часу прийняття рішень у системі як захисту, так і кіберзахисту інформації є частиною невирішеної загальної проблеми забезпечення інформаційної безпеки в комплексних системах технічного захисту та кіберзахисту інформації.

Розглянемо постановку та вирішення цієї задачі. Задано: взаємопов'язана підмножина Z_1, яка складається з n задач обробки та передачі інформації, що передбачають виконання СКЗІ, вимагаючи N підсистем та L каналів зв'язку $Z_1 = \{Z_j\}$.

Відомі характеристики кожної задачі, що вирішується: Z_j – трудоємкість рішення W_j щодо задач обробки інформації та обсяг інформації V_j, що передається, для задач обміну інформацією по каналах зв'язку, директивні погодження термінів можливого початку d_j^H та закінчення завдання d_j^K. Взаємозв'язок задач Z_1 описується множиною X_j та Y_j – відповідно множина інформаційних входів у задачу $Z_j^{вх}$ і множина інформаційних виходів з $Z_j^{вих}$. Вимагається визначити для кожної $Z_j \in Z_1$, $j = \overline{1,n}$ такі кордони допустимого інтервалу її вирішення на межі t_j^H та t_j^K, що

$$\left[t_j^H, t_j^K\right] \subseteq \left[d_j^H, d_j^K\right].$$

Однак вирішення всіх Z_j у межах допустимого інтервалу $\left[t_j^H, t_j^K\right]$ потребує мінімуму затрат на створення й експлуатацію захищеного компоненту технічних засобів мережі.

Математична постановка задачі полягає в такому: визначити такі t_j^H, t_j^K, які досягають мінімуму поступово поштового функціоналу

$$C = \min_{t_j^H, t_j^K} \left\{ \sum_{e=1}^{E} \Theta_{1e} \sum_{i=1}^{N} \sum_{j=1}^{n} \left(\frac{W_j \Pi_{ji}}{t_j^K - t_j^H} \right)^{\beta_{1e}} + \sum_{q=1}^{Q} \Theta_{2g} \sum_{i=1}^{L} \sum_{j=1}^{l} \left(\frac{N_j \eta_j}{t_j^K - t_j^H} \right)^{\beta_{2q}} \right. . \quad (1)$$

При таких обмеженнях:

$$d_j^H - t_j^H \le 0, \ j = \overline{1,n}, \quad (2)$$

$$t_j^K - d_j^K \le 0, \ j = \overline{1,n}, \quad (3)$$

$$t_j^H - t_j^K \le 0, \ j = \overline{1,n}, \quad (4)$$

$$t_j^K - \min_a \left\{ t_a^H \mid a \in Y \right\} \ge 0, \ j = \overline{1,n}. \quad (5)$$

Обмеження (2) і (3) враховують завдані директивні терміни вирішення задач Z_j. Обмеження (4) задає умови не нульової довжини допускового інтервалу рішення Z_j. Обмеження (5) містить вимогу, відповідно до якої допускові інтервали задач, пов'язаних інформаційно, не повинні перетинатися.

$$\Pi_{ji} = \begin{cases} 1 & \text{, якщо j-та задача розподілена для обробки на і-ту підсистему} \\ 0 & \text{, в основному випадку} \end{cases}$$

та

$$\Pi_{ji} = \begin{cases} 1 & \text{, якщо і-та задача обміну інформацією l-му каналу зв'язку} \\ 0 & \text{, в основному випадку} \end{cases}$$

Критерій С у (1) описує сумарні приведені затрати на створення та експлуатацію технічних засобів мережі, спроєктованої для обслуговування задач Z_1. Е та $\Theta_{1e} > 0$; $\Theta_{1e} > 0$; $\beta_{1e} \geq 0$; $\beta_{2eq} \geq 0$ – константи.

Задачі (1)–(5) належать до класу задач нелінійного математичного програмування. При їх вирішенні можуть бути використані відомі методи теорії нелінійного програмування. Характерною особливістю задач (1) – (5) є їхня велика розмірність, зумовлена кількістю задач, що розв'язуються на мережі та знаходяться в інформаційному взаємозв'язку. Одним з ефективних підходів до вирішення нелінійних оптимальних задач великої розмірності є використання апроксимаційних методів теорії нелінійного програмування [6], суть яких полягає в тому, що рішення кінцевої нелінійної задачі здійснюється в результаті вирішення послідовності задач простішого виду, що потребують значно менших обчислювальних затрат, ніж вихідна задача.

Лінійна апроксимація не завжди ефективна, так як дає можливість отримати лише достатньо наближене значення.

Останнім часом з'явилися наукові праці, у яких запропоновано підхід до усунення цього недоліку: вирішуємих допоміжних квадратичних задач. Метод мінімізації, використаний у дослідженнях, посідає серед усіх таких методів особливе місце. Це пояснюється тим, що, на відміну від інших методів цього класу, він сходиться з будь-якого початкового наближення та не потребує припущень щодо випуклості функцій і суворої позитивної визначеності матриці других похідних функцій Лагранжа, а також має досить просту структуру допоміжної квадратичної задачі.

У загальному випадку метод лініалізації передбачає лінійну швидкість сходження. Однак існує модифікація методу [7; 8], за якої при значному віддаленні від точки екстремума швидкість сходження лінійна, а при достатній близькості до нього – квадратична.

Особливістю вирішення квадратичних задач є те, що в них ураховуються тільки ті обмеження, у яких порушення допустимості найбільші. Вказана особливість зменшує розмірність допоміжних задач і тим самим зменшує обчислювальну складність вихідної нелінійної задачі.

Розглянуті переваги методу лініалізації зумовлюють визначення допустимих інтервалів у постановці задачі (1)–(5).

Для роботи алгоритму методу лініалізації необхідно вибрати початкове наближення до рішення $t_j^H(0)$, $t_j^K(0)$, $j=\overline{1,n}$, яке задовільняє системі нерівностей $(2)-(5)$. Нехай множина взаємозв'язаних задач Z_1 розбита на R – інформаційних рангів по n_r задач у r-м ранзі, $r=\overline{1,R}$. Алгоритм початкового наближення такий:

Крок 1 $r:=1$.

Крок 2 $j:=1$.

Крок 3 $t_j^H(0):=d_j^H+\Delta t$.

Крок 4 $t_j^K(0):=t_j^H(0)+\Delta t$.

Крок 5 $j:=j+1$.

Крок 6 Якщо $j\le n_r$, перехід на крок 3, інакше на крок 7.

Крок 7 $r:=r+1$.

Крок 8 Якщо $r\le R$, перехід на крок 9, інакше на крок 17.

Крок 9 $j:=j+n_{r-1}$.

Крок 10 $t_{\min}^H:=\min_a\left\{t_a^H(0)\mid a\in X_j\right\}$.

Крок 11 $t_j^H:=t_{\min}^H+2\Delta t$.

Крок 12 Якщо $d_i^H>t_j^H(0)$, перехід на Крок 13, інакше 14.

Крок 13 $t_j^H(0):=d_i^H+\Delta t$.

Крок 14 $t_j^K(0):=t_j^H+\Delta t$.

Крок 15 $j:=j+1$.

Крок 16 Якщо $j\le n_r$, перехід на Крок 10, інакше на Крок 7.

Крок 17 Кінець.

Вибір значення Δt здійснюється залежно від завдання директивних термінів вирішення d_j^H, d_j^K, $j=\overline{1,n}$.

Нехай $t_j(0)=\left\{t_j^H(0),t_j^K(0)\right\}$ та $\bar{t}(0)=\left\{t_j(0)\right\}$, $j=\overline{1,n}$ – початкове приближення до рішення, отримане в результаті роботи алгоритму, приведеного раніше, і нехай задана точність E, 0<E<1. Розглянемо роботу алгоритму методу лініалізації [6] на к-тому кроці, коли вже отримаємо *к*-те наближення $\delta>0$ до рішення (*к*). Побудова *(к+1)*-го наближення $\bar{t}(k+1)$ проводиться таким чином:

1. Задача квадратичного програмування:

$$\min_{P} \left\{ \left[\overline{C}^{T}(\bar{t}(k)), \overline{P} \right] + \frac{1}{2} \| \overline{P} \|^2 \right\},$$

$\left[\overline{\varphi_S}(\bar{t}(k)), \overline{P} \right] + \varphi_S \left[\bar{t}(k) \right] \le 0$, $s \in S_\delta[\bar{t}(k)]$, вирішується стосовно $\overline{p}$.

Тут $S_\delta(\bar{t}) = \left\{ s \in S : \overline{\varphi_S}(\bar{t}) \ge \max_{s \in S} \varphi_s(t) - \delta \right\}$, $\delta > 0$;

$\Phi = \left\{ \overline{\varphi_s}(\bar{t}) \right\}$ – множина функцій таких, як

$$\overline{\varphi_S} = (t) \begin{cases} d_S^H - t_{S_1}^H, S = \overline{1,n}, \\ t_{S-n}^K - d_{S-n}^K, S = \overline{(n+1),2n}, \\ t_{S-2n}^K - t_{S-2n}^K, S = \overline{(2n+1),3n}, \\ t_{S-3n}^K - \min_{a} \left\{ t_a^H \mid a \in \frac{1}{5} - 3n \right\}, S = \overline{(3n+1),4n}; \bar{t} = \left\{ t_j \right\}, t_j = \left\{ t_j^H, t_j^K \right\}, j = \overline{1,n}; \end{cases}$$

$\| \overline{P} \|$ – евклідова норма вектора $\overline{p}$.

Вирішення задачі (6) – вектор $\overline{p}(k) = \overline{p}[\bar{t}(k)]$. (6)

2. Знаходимо перше значення $S = 0,1,...,$ при якому буде виконана така нерівність:

$$\overline{\varphi}\left[\bar{t}(k) + \frac{1}{2^S} \overline{p}(k) \right] + N \max_{s \in S} \overline{\varphi}_S \left[t(k) + \frac{1}{2^S} \overline{p}(k) \right] \le \overline{\varphi}\left[\bar{t}(k) \right] + N \max_{s \in S} \overline{\varphi}_S \left[\bar{t}(k) \right] - \frac{1}{2^S} \varepsilon \| \overline{p}(k) \|^2 . \quad (7)$$

Якщо ця нерівність уперше використовувалася при $S = S_0$, то зазначимо, що

$$a(k) = 2^{-S_0}, \bar{t}(k+1) = \frac{1}{t}(k) + (k)\overline{p}(k). \quad (8)$$

Отже, на кожному кроці алгоритму виконується така нерівність:

$$\overline{\varphi}\left[\bar{t}(k+1) \right] + N \max_{s \in S} \overline{\varphi}_s \left[\bar{t}(k) + 1 \right] \le \overline{\varphi}\left[\bar{t}(k) \right] + N \max_{s \in S} \overline{\varphi}_s \left[\bar{t}(k+1) \right] - a(k) \varepsilon \| \overline{p}(k) \|^2 .$$

У (8) показано, що вибір $a(k)$ на кожній ітерації проходить за кінцеве число дроблень одиниці навпіл, та обґрунтована східність алгоритму. У частковості доведено, що, якщо функція цілі та обмеження опуклі, то алгоритм сходиться за кінцеве число кроків при будь-якому $a < 0$.

Усі обмеження (2)–(5) лінійні, отже, вони опуклі. Наведений аналіз функції цілі (1), показав, що вона є опуклою функцією. Отже, для задачі (1)–(5) алгоритм лініалізації сходить за кінцеве число кроків при будь-якому $a < 0$.

При використанні методу лініалізації основної операції, що потребує значних обчислювальних затрат, є рішення квадратичної задачі (6). При виборі методу її вирішення слід ураховувати, що для контролю правильності вибору константи N у (7) при вирішенні (6) необхідно отримати відповідні множники Лагранжа $\overline{U}(\overline{P})$. Тому при вирішенні задачі (6) доцільно перейти до подвійної задачі, яка має такий вигляд:

$$U = \left\{ \overline{U}^T \cdot G\overline{U} + h^T \overline{U} \,|\, \overline{U} \geq 0 \right\}, \tag{9}$$

де $G = A \cdot \overline{A}^T$, $\overline{h}^T = A\overline{b} + \overline{C}^T \left[\overline{t}(k) \right]$;

A – матриця;

S – той рядок, що містить у собі компоненти вектора $\overline{\varphi}_S \left[\overline{t}(k) \right]$;

$\overline{b}$ – вектор;

$\overline{S}$ – компонента, що дорівнює значенню функції $\overline{\varphi}_S \left[\overline{t}(k) \right]$.

Для вирішення задачі (9) доцільно використовувати ітераційний алгоритм, який подає деяке видозмінення методу Гауса – Зайделя. Вибір цього алгоритму зумовлений тим, що, по-перше, він достатньо простий щодо реалізації на ПЕОМ, по-друге, його структура, похибки обчислювань на окремих ітераціях не впливають на східність ітераційного процесу в цілому.

Указаний алгоритм при вирішенні задачі (9) має такий вигляд:

$$U_i^{(n+1)} = \max(0, \omega_i^{(n+1)}), \tag{10}$$

$$\omega_i^{(n+1)} = \frac{1}{g_0} \left(\sum_{j=1}^{i-1} g_{ij} U_j^{(n+1)} + h_i + \sum_{j=i+1}^{m} g_{ij} U_j^n \right), \tag{11}$$

де U_i – i-та компонента вектора $\overline{U}$;

n – номер ітерації;

g_{ij} – елемент матриці G;

m – розмірність вектора $\overline{U}$.

Описаний алгоритм реалізується у вигляді комплексу прикладних програм щодо аналізу ефективності алгоритмів визначення часу прийняття рішень системами кіберзахисту інформації.

Висновки. Запропонований варіант вирішення задач та наведені результати можуть бути використані для розроблення ефективних алгоритмів визначення часу прийняття рішень на основі математичних моделей для систем підтримки прийняття рішень системою кіберзахисту інформації, а також моделювання складних технічних систем та оцінювання ефективності використання

різних інформаційно-обчислювальних систем. Такий підхід разом з іншими дасть можливість вирішувати загальну проблему забезпечення інформаційної безпеки в комплексних системах технічного захисту та кіберзахисту інформації держави, що сприятиме сталому розвиткові інформаційного суспільства й комунікаційного середовища.

Список використаних джерел

1. Грищук Р. В., Даник Ю. Г. Основи кібернетичної безпеки. Житомир : ЖНАНЕУ, 2016. 636 с.

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

3. Хорошко В. О., Казакова Н. Ф. Наукові задачі синтезу організаційно-технологічної схеми створення програмного забезпечення для комп'ютерних мереж з обмеженим доступом. *Захист інформації.* 2009. № 4. С. 11–18.

4. Козюра В. Д., Пикун И. В., Хорошко В. А. Выбор момента времени для проведения операции воздействия на информацию. *Інформаційна безпека людини, суспільства, держави*. 2011. № 2. С. 76–83.

5. Дахно Н. В., Тискина Е. О., Хорошко В. А. Расчет времени эффективности процесса принятия решения в системах защиты информации. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2011. № 2 (5). С. 36–43.

6. Фельдман Л. П., Петренко А. І., Дмитрієва О. А. Чисельні методи в інформації. Київ : Вид. група BHV, 2006. 480 с.

7. Томашевський В. М. Моделювання систем. Київ : Вид. група BHV, 2007. 352 с.

8. Томашевський В. М., Жданов О. Г., Жолдаков О. О. Вирішення практичних завдань методами комп'ютерного моделювання. Київ : Корнійчук, 2001. 267 с.

Анотація. У статті проведено аналіз літератури, який показує відсутність у теперішній час єдиного підходу до комплексного вирішення проблеми синтезу математичних моделей та алгоритмів визначення часу прийняття рішень у системі як захисту, так і кіберзахисту інформації. Також проаналізовано дослідження етапу щодо визначення допустимих термінів вирішення інформаційно залежних задач систем кіберзахисту інформації з урахуванням взаємозв'язків директивних термінів вирішення задач і завдання інформаційних залежностей між ними, визначено допустимі інтервали обробки та

Abstract. The rationale of the article is based on the research that performs the current failure of a holistic approach to the comprehensive solution to the problem of synthesizing mathematical models and algorithms for determining the time of decision-making in cyber security and information protection as a whole. The researched stage to determine the acceptable terms of solving information-dependent tasks of cyber security information systems taking into account the correlations between the directive terms of solving problems and the tasks of information dependency between them was also carried out. The intervals of processing

передачі інформації по мережі при забезпеченні функціонування систем кіберзахисту інформації. Наведено результати, які можуть бути використані при розробці ефективних алгоритмів визначення часу прийняття рішень на основі математичних моделей для систем підтримки прийняття рішень системою кіберзахисту інформації, а також для моделювання складних технічних систем та оцінки ефективності використання різних інформаційно-обчислювальних систем.

Ключові слова: кібербезпека, кіберзахист, кібератаки, система кіберзахисту, інформаційний захист, захист держави, кіберпростір, канали зв'язку.

and transmitting information over the network ensuring the functioning of cyber security information systems were specified. The results that can be used in the drafting of operating system algorithms for determining the time of decision-making based on mathematical models for decision-making support systems with the help of cyber security information systems, as well as for modeling complex technical systems and evaluating the effectiveness of using several information computing systems are given.

Key words: cyber security, cyber defense, cyber attacks, cyber defense system, information protection, state protection, cyber space, communication channels.