НОВІ ЗАСОБИ КІБЕРНЕТИКИ, ІНФОРМАТИКИ, ОБЧИСЛЮВАЛЬНОЇ ТЕХНІКИ ТА СИСТЕМНОГО АНАЛІЗУ

О.І. СТАСЮК, Р.В. ГРИЩУК, Л.Л. ГОНЧАРОВА

УДК 004.9

МАТЕМАТИЧНІ ДИФЕРЕНЦІЙНІ МОДЕЛІ І МЕТОДИ ОЦІНКИ КІБЕРБЕЗПЕКИ ІНТЕЛЕКТУАЛЬНИХ КОМП'ЮТЕРНИХ МЕРЕЖ КЕРУВАННЯ ТЕХНОЛОГІЧНИМИ ПРОЦЕСАМИ ЕЛЕКТРОПОСТАЧАННЯ ЗАЛІЗНИЦЬ

Анотація. Проведено аналіз проблеми кібербезпеки комп'ютерних мереж керування електропостачанням на рівні залізниці і запропоновано граф топології комп'ютерної мережі керування електроспоживанням. На основі теорії диференційних перетворень Пухова запропоновано ряд диференційних математичних моделей оцінки рівня кібербезпеки комп'ютерної мережі керування електропостачанням. Для диференційних зображень запропоновано критерій кібербезпеки і розроблено принцип мінімаксу для найгіршого варіанту поєднання інтенсивності кібератак і потоку захисних дій. Розроблено метод інтелектуального пошуку оптимальної стратегії кібербезпеки шляхом дослідження функціоналу на екстремум для стохастичної інтенсивності потоків кібернетичних атак.

Ключові слова: кібербезпека, кіберпростір, кіберзагрози, диференційні математичні моделі, диференційні перетворення, інтелектуальні методи, захист інформації.

ВСТУП

Інтенсивний розвиток сучасних інтегральних технологій виготовлення надвеликих інтегральних схем і мікропроцесорних пристроїв відкрив широкі можливості для об'єднання великої кількості комп'ютерних засобів у вигляді розподілених локальних, корпоративних і транснаціональних обчислювальних мереж і став основою безпрецедентного розвитку комп'ютерних, телекомунікаційних та інтелектуальних технологій як бази глобальної інформатизації суспільства [1, 2]. Захист інформаційного простору в процесі глобальної інформатизації країни, згідно з сучасними уявленнями, розглядається як домінуючий компонент національної безпеки [3]. Тому перехід до інформаційного суспільства зумовив гостру потребу в гарантуванні кібербезпеки інформаційного простору та побудові інформаційно-безпечних розподілених комп'ютерних мереж і систем підвищеної інформаційної стійкості до кібератак. У межах розв'язання комплексу задач захисту інформаційного простору сучасні інтелектуальні системи кіберзахисту мають бути орієнтовані, насамперед, на формування і накопичення нових знань у сфері виявлення і реагування на кібератаки, у тому числі на несанкціонований доступ, розроблення засобів і методів протидії кібернетичним атакам та методів підвищення рівня кіберстійкості розподілених обчислювальних мереж з метою забезпечення потрібного рівня надійності процесів переробки та передачі інформації [4]. Ефективне функціонування інтелектуальних систем кіберзахисту буде можливим, якщо їхня архітектура адекватно відображатиме топо-

логію відповідних комп'ютерних мереж, а компоненти системи захисту, функціонально орієнтовані за типами задач, тісно взаємодіятимуть один з одним, щоб забезпечити можливість реконфігурації апаратних та програмних засобів для адаптації в реальному режимі часу до зміни трафіку, прийняття спільних рішень та обміну інформаційними даними [5, 6]. Для такої організації інтелектуальна система кіберзахисту являє собою взаємопов'язану, ешелоновану та безперервно контрольовану систему захисту, спроможну оперативно реагувати на комплекс віддалених і локальних кібератак.

ПОСТАНОВКА ЗАДАЧІ

Дослідження, проведені у зв'язку з потребою в захисті інформації від кіберзагроз, показали, що постійне наростання рівня інтенсивності кібератак зумовлено, з одного боку, величезними масштабами інформаційного кіберпростору, а з іншого боку, наявністю широкого спектру різнохарактерних зв'язків між його окремими вузлами і сегментами [4]. Внаслідок інтенсивного розвитку безпровідних комунікацій, пов'язаних з системами навігації, відеонагляду, нових технологій передачі інформації та сучасних комп'ютеризованих систем оперативного диспетчерського керування, з'явилася сукупність нових класів кібератак. Особливості організації кіберпростору і можливість передачі інформації та сигналів у різних напрямках сприяли появі максимально небезпечних і складних загроз, що мають комплексну структуру, агресивний характер дій та можуть постійно адаптуватися до системи кіберзахисту та її компонентів. Атакуючою стороною можуть виступати не лише хакери чи їхні групи, а й кібервійська потенційних агресорів, що може призвести до виникнення небезпеки та суттєвих втрат. Інтенсивне зростання кількості витончених кібернетичних атак змусило розробників включити комплекс захисних функцій у проекти нових розподілених обчислювальних мереж. Це — спектр рішень, що об'єднують дані про можливі загрози, сукупність правил кібербезпеки і комп'ютерно-орієнтовані методи примусового управління захистом у всіх контактних вузлах та сегментах мережі [5, 6]. Досвід експлуатації розподілених комп'ютерних мереж і систем управління електроспоживанням залізничним транспортом показав, що у зв'язку з постійним збільшенням кількості факторів дестабілізації, які впливають на цілісність, доступність і конфіденційність інформаційних ресурсів, захист критично важливих компонентів кіберпростору можна забезпечити шляхом створення нових методів інтелектуального розпізнавання кіберзагроз і оцінки рівня інформаційної стійкості. При цьому, обґрунтування критеріїв кібербезпеки краще будувати на основі умов організації максимально сприятливого середовища на базі організації інтелектуального сервісу захисту для роботи споживачів та інших систем кібернетичного простору, а не формувати захист інформаційного простору залежно від максимальної кількості кіберпогроз [4, 7]. У зв'язку з цим виникає потреба у проведенні додаткових досліджень основних властивостей і топологічних характеристик кіберпростору, докладному і ретельному аналізі динаміки його розвитку в різних аспектах часу, від миттєвих до багаторічних, а також методів керування динамікою. Очевидно, що для успішної протидії кібератакам і кібертероризму та гарантування відповідного рівня кібербезпеки інформаційних ресурсів, потрібно створити нові моделі і методи підвищеної інтелектуальної складності і розмірності, які дадуть змогу оцінити рівень захисту контактних вузлів, сегментів і всього кібернетичного простору та розробити способи обґрунтування критеріїв кіберстійкості [4, 5].

Метою роботи є розроблення математичних диференційних моделей і методів оцінки кібербезпеки, компонентів корпоративних інтелектуальних комп'ютерних мереж керування електропостачанням залізниць, які дадуть змогу здійснювати аналіз і управління стійкістю кіберпростору до наявних і нових кіберзагроз.

МАТЕМАТИЧНІ ДИФЕРЕНЦІЙНІ МОДЕЛІ

Організація інфраструктури розподіленого комп'ютерного середовища керування швидкоплинними технологічними процесами постачання електроенергії залізницям ґрунтується на комп'ютерному змінному моніторингу всієї сукупності аналогових та дискретних параметрів, які характеризують штатні та аномальні режими функціонування систем електропостачання та силового електричного обладнання тягових підстанцій. Будь-які фактори дестабілізації, які чинять вплив на цілісність, конфіденційність і доступність інформаційних ресурсів кібернетичного простору керування електроспоживанням на тягу, можуть зумовити значні порушення функціонування транспортної системи країни і, як наслідок, призвести до великих втрат. Захист критично важливих вузлів, компонентів і сегментів інфраструктури кіберпростору в умовах постійного зростання кількості витончених дестабілізаційних динамічних впливів можна забезпечити шляхом проведення досліджень спільних властивостей математичних моделей функціонування складних енергетичних систем, архітектури розподілених комп'ютерних мереж керування електропостачанням і особливостей процесів, що протікають внаслідок численних зв'язків між учасниками кіберпростору. Результати досліджень є дуже важливим фактором суттєвого підвищення ефективності систем, що забезпечують захист від спектра подібних загроз і є основою організації системи інтелектуального сервісного захисту. Завдяки створенню математичних моделей підвищеної інформаційної складності і розмірності відкривається можливість для формування і накопичення нових знань про кібератаки і особливості кібертероризму. На базі отриманих знань можна створити нові методи інтелектуальної оцінки кіберстійкості інформаційної інфраструктури, засоби інтелектуального розпізнавання кіберзагроз в умовах наростаючої динаміки числа дестабілізаційних впливів, а також розробити нові технології керування явищами безпеки для успішної протидії кібератакам, кібертероризму та забезпечення потрібного рівня кібербезпеки. Формування кіберпростору залізниці передбачає забезпечення захисних функцій у проекті створення або розширення комп'ютерних систем захисту. Побудова більш ефективної системи безпеки інформації означає не організацію достатньо складної архітектури, а реалізацію інфраструктури таким чином, щоб вузли і компоненти її були гармонійно взаємопов'язані і, завдяки спільному функціонуванню, давали змогу більш якісно виявляти кіберзагрози, реалізовувати їх нейтралізацію і, відповідно, суттєво зменшити втрати. Переважною особливістю сучасних інтелектуальних систем захисту є адекватність топології кіберпростору і архітектури системи захисту [4]. Організований таким чином кіберпростір залізниці дає змогу здійснювати в режимі реального часу адаптацію до зміни трафіку шляхом реконфігурації апаратно-програмних засобів, що відкриває широкий спектр можливостей інтелектуального сервісу в процесі захисту інформаційних ресурсів. Логічна структура комп'ютерного середовища керування технологічними процесами електропостачання залізниць гармонійно пов'язана з топологією системи кіберзахисту від впливу кібератак для підвищення рівня стійкості кіберпростору. Її можна представити у вигляді автономних або взаємопов'язаних архітектур типу «зірка» і «кільце». Головною її характеристикою є те, що архітектура комп'ютерного середовища керування електроспоживанням адекватно відображає систему кіберзахисту інфор-

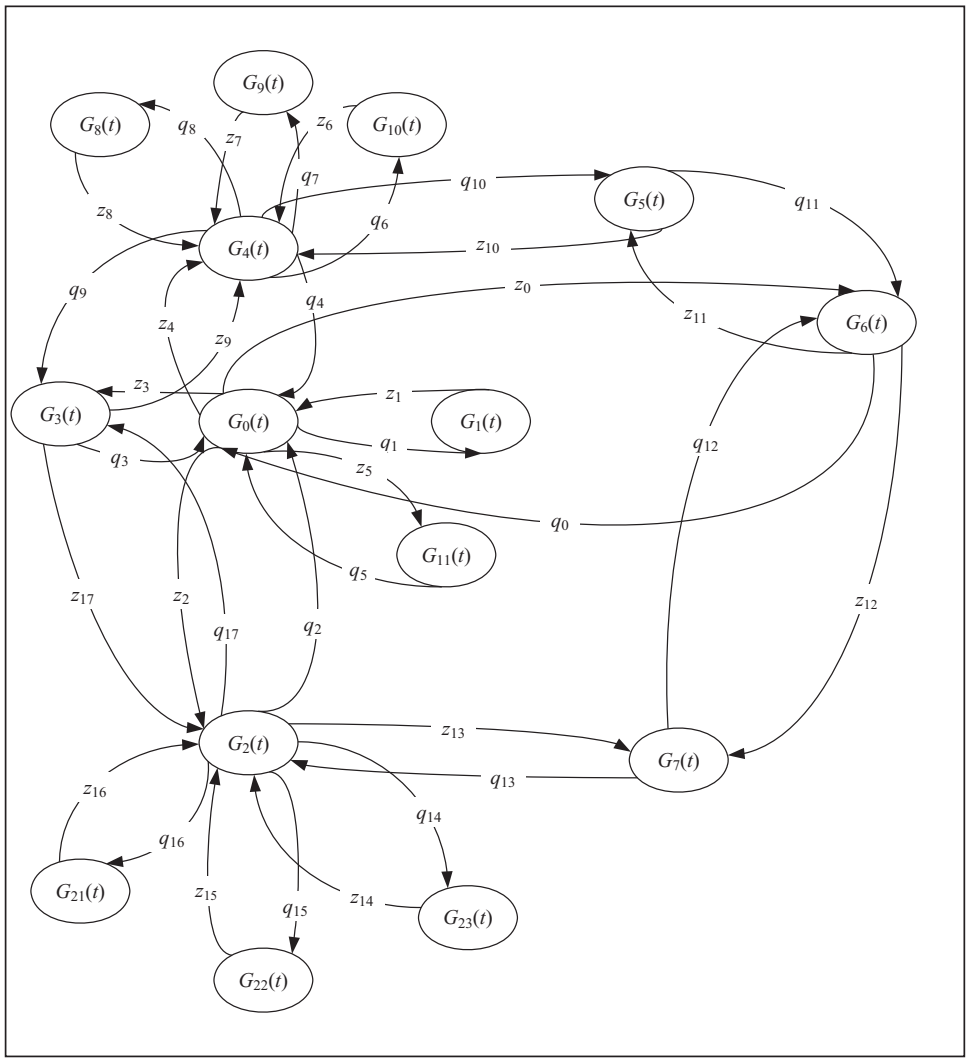

Рис. 1. Граф станів системи кібербезпеки розподіленої компютерної мережі дистанції електропостачання залізниць

маційних ресурсів і може бути представлена у вигляді графа, наведеного на рис. 1. Вузли графа являють собою комп'ютерні або мікропроцесорні засоби, які реалізують задану сукупність функцій. Наведений сегмент топології комп'ютерної мережі містить центральний сервер керування електропостачанням залізниці $G_0(t)$; сервер бази даних і формування єдиного інформаційного простору $G_1(t)$; вузол зв'язку з головними мережами тягових підстанцій $G_2(t)$; вузол зв'язку з мережею Internet $G_3(t)$; вузол зв'язку з корпоративними обчислювальними мережами $G_4(t)$; сервер оперативно-диспетчерського керування електропостачанням $G_5(t)$; вузол інтелектуального оброблення і захисту інформації $G_6(t)$; вузол формування звітних документів $G_7(t)$; вузол, що є корпоративною обчислювальною мережею залізниці $G_8(t)$; вузол, що є корпоративною обчислювальною мережею обленерго $G_9(t)$; вузол, що є корпоративною обчислювальною мережею організацій вищого рівня $G_{10}(t)$; вузол, що є корпоративною обчислювальною мережею ринку електроенергії $G_{11}(t)$; вузли, що є відповідними локальними обчислювальними мережами проведення моніторингу і керування електропостачанням на рівні тягових підстанцій $G_{21}(t)$,

$G_{22}(t)$, $G_{23}(t)$. Позначимо $q_i(t)$ інтенсивність потоків атак, а $z_j(t)$ — інтенсивність потоків захисних функцій, які реалізуються у системі і переводять її з одного стану в інший. Для проведення досліджень комп'ютерної архітектури, представленої у вигляді графа на рис. 1, синтезуємо математичну модель для визначення ймовірностей стану вузлів графа. Скориставшись потрібним набором правил і формул, для спрощення аналізу, запишемо систему рівнянь Колмогорова для центрального сервера $G_0(t)$ у такому вигляді [4, 8]:

$$\begin{cases} \dfrac{dP_{G_0}(t)}{dt} = -(z_0 + z_1 + z_2 + z_3 + z_4 + z_5)P_{G_0}(t) + q_1 P_{G_1}(t) + q_2 P_{G_2}(t) + \\ \qquad + q_3 P_{G_3}(t) + q_4 P_{G_4}(t) + q_5 P_{G_{11}}(t); \\ \dfrac{dP_{G_1}(t)}{dt} = -q_1 P_{G_1}(t) + z_1 P_{G_0}(t); \\ \dfrac{dP_{G_6}(t)}{dt} = -(z_{11} + z_{12} + q_0)P_{G_6}(t) + z_0 P_{G_0}(t) + q_{11} P_{G_5}(t) + q_{12} P_{G_7}(t); \\ \dfrac{dP_{G_{11}}(t)}{dt} = -q_5 P_{G_{11}}(t) + z_5 P_{G_0}(t); \\ \dfrac{dP_{G_2}(t)}{dt} = -(z_{13} + q_2 + q_{14} + q_{15} + q_{16} + q_{17})P_{G_2}(t) + z_2 P_{G_0}(t) + q_{13} P_{G_7}(t) + \\ \qquad + z_{14} P_{G_{23}}(t) + z_{15} P_{G_{22}}(t) + z_{16} P_{G_{21}}(t) + z_{17} P_{G_3}(t); \\ \dfrac{dP_{G_3}(t)}{dt} = -(z_9 + q_3 + z_{17})P_{G_3}(t) + q_9 P_{G_4}(t) + z_3 P_{G_0}(t) + q_{17} P_{G_2}(t); \\ \dfrac{dP_{G_4}(t)}{dt} = -(q_4 + q_6 + q_7 + q_8 + q_9 + q_{10})P_{G_4}(t) + z_4 P_{G_0}(t) + z_9 P_{G_3}(t) + \\ \qquad + z_8 P_{G_8}(t) + z_7 P_{G_9}(t) + z_6 P_{G_{10}}(t) + z_{10} P_{G_5}(t), \end{cases} \tag{1}$$

для таких умов нормування і початкових умов відповідно:

$$\begin{gathered} P_{G_0}(0) + P_{G_1}(0) + P_{G_2}(0) + P_{G_3}(0) + P_{G_4}(0) + P_{G_6}(0) + P_{G_{11}}(0) = 1, \\ P_{G_0}(0) = 1,\ P_{G_1}(0) = P_{G_2}(0) = \ldots = P_{G_6}(0) + P_{G_{11}}(0) = 0. \end{gathered} \tag{2}$$

Для подальшого проведення досліджень скористаємося фундаментальними положеннями теорії диференційних перетворень Пухова, представлених такою парою математичних залежностей для побудови диференційної математичної моделі графа (див. рис. 1):

$$P_i(k) = \frac{H^k}{k!}\left[\frac{d^k P_i(t)}{dt^k}\right]_{t=0} \doteq P_i(t) = \sum_{k=0}^{k=\infty}\left(\frac{t}{H}\right)^k P_i(k), \tag{3}$$

де $P_i(t)$ — первісна функція аргументу t, яку можна n разів диференціювати і яка має ряд відповідних обмежень, включаючи свої похідні; $P_i(k)$ — диференційне Т-зображення первісної функції $P_i(t)$; H — масштабний коефіцієнт, розмірність якого збігається з розмірність аргументу t, його, зазвичай, обирають на умовах $0 \le t \le H$ на всьому діапазоні функції-оригіналу $P_i(t)$; $\doteq$ — символ відповідності між функцією-оригіналом $P_i(t)$ і його диференційним Т-зображенням $P_i(k)$. Внаслідок прямого диференційного перетворення, записаного ліворуч від символу $\doteq$, формується диференційне Т-зображення функції-

оригіналу $P_i(t)$ у вигляді дискретної функції $P_i(k)$ цілочислового аргументу $k = 0, 1, 2, \ldots$ На основі сукупності значень Т-дискрет функції цілочислового аргументу $P_i(k)$, $k = 0, 1, 2, \ldots$, використавши обернене диференційне перетворення, що розташоване праворуч від символу $\doteq$, отримуємо функції-оригіналу $P_i(t)$.

Після відповідних перетворень системи рівнянь (1) за допомогою математичних залежностей (3) побудуємо диференційну математичну модель у такому вигляді:

$$\begin{cases}
\dfrac{dP_{G_0}(k+1)}{dt} = \dfrac{H}{k+1}[-(z_0+z_1+z_2+z_3+z_4+z_5)P_{G_0}(k)+q_1P_{G_1}(k)+ \\
\qquad +q_2P_{G_2}(k)+q_3P_{G_3}(k)+q_4P_{G_4}(k)+q_5P_{G_{11}}(k)]; \\
\dfrac{dP_{G_1}(k+1)}{dt} = \dfrac{H}{k+1}[-q_1P_{G_1}(k)+z_1P_{G_0}(k)]; \\
\dfrac{dP_{G_6}(k+1)}{dt} = \dfrac{H}{k+1}[-(z_{11}+z_{12}+q_0)P_{G_6}(k)+z_0P_{G_0}(k)+q_{11}P_{G_5}(k)+q_{12}P_{G_7}(k)]; \\
\dfrac{dP_{G_{11}}(k+1)}{dt} = \dfrac{H}{k+1}[-q_5P_{G_{11}}(k)+z_5P_{G_0}(k)]; \\
\dfrac{dP_{G_2}(k+1)}{dt} = \dfrac{H}{k+1}[-(z_{13}+q_2+q_{14}+q_{15}+q_{16}+q_{17})P_{G_2}(k)+z_2P_{G_0}(k)+ \\
\qquad +q_{13}P_{G_7}(k)+z_{14}P_{G_{23}}(k)+z_{15}P_{G_{22}}(k)+z_{16}P_{G_{21}}(k)+z_{17}P_{G_3}(k)]; \\
\dfrac{dP_{G_3}(k+1)}{dt} = \dfrac{H}{k+1}[-(z_9+q_3+z_{17})P_{G_3}(k)+q_9P_{G_4}(k)+z_3P_{G_0}(k)+q_{17}P_{G_2}(k)]; \\
\dfrac{dP_{G_4}(k+1)}{dt} = \dfrac{H}{k+1}[-(q_4+q_6+q_7+q_8+q_9+q_{10})P_{G_4}(k)+z_4P_{G_0}(k)+ \\
\qquad +z_9P_{G_3}(k)+z_8P_{G_8}(k)+z_7P_{G_9}(k)+z_6P_{G_{10}}(k)+z_{10}P_{G_5}(k)].
\end{cases} \tag{4}$$

Оскільки для $k = 0$, згідно з (3), для $t = 0$ кожного i-го параметру $P_i(t)$ виконується відповідна рівність $P_i(t=0) = P_i(k=0)$, нормовані і початкові умови можна представити таким чином відповідно:

$$P_{G_0}(0)+P_{G_1}(0)+P_{G_2}(0)+P_{G_3}(0)+P_{G_4}(0)+P_{G_6}(0)+P_{G_{11}}(0) = 1,$$

$$P_{G_0}(k=0) = 1,\ P_{G_1}(k=0) = P_{G_2}(k=0) = \ldots = P_{G_6}(k=1)+P_{G_{11}}(k=0) = 0.$$

Для спрощення процедур аналізу введемо певні обмеження на інтенсивність потоків кібератак $q_i(t)$ та захисних дій $z_j(t)$, а також приймемо такі обмеження:

$$\begin{gathered}
0 < q_i(t) \le q_{i\max}, \\
0 < z_j(t) \le z_{j\max}, \\
z_0 = z_1 = \ldots = z_{15} = z_{16} = z, \\
q_0 = q_1 = \ldots = q_{15} = q_{16} = q.
\end{gathered} \tag{5}$$

Виходячи з умов нормування (2) і (5), запишемо перше рівняння системи (1) у такому вигляді:

$$\frac{dP_{G_0}(t)}{dt} = -6zP_{G_0}(t)+q(1-P_{G_0}(t)). \tag{6}$$

У результаті диференційних перетворень [9] рівняння (6) набуде вигляду Т-моделі:

$$P_{G_0}(k+1)=\frac{T}{k+1}[-6zP_{G_0}(k)+q(\text{ъ}(k)-P_{G_0}(k))], \tag{7}$$

де T — тривалість процесів кіберзахисту або кібернападу в системі $T=H$; k — цілочисловий аргумент $k=0,1,2,\ldots$; $\text{ъ}(k)$ — теда, що набуває значень

$$\text{ъ}(k)=\begin{cases}1 & \text{для } k=0,\\ 0 & \text{для } k\geq 1.\end{cases}$$

Для рівняння (7) дискрети диференціальних спектрів дорівнюють

$$\begin{gathered}P_{G_0}(0)=[P_{G_0}(t_0)]=1,\\ k=0\Rightarrow P_{G_0}(1)=-6Tz,\\ k=1\Rightarrow P_{G_0}(2)=3zT^2(6z+q),\\ k=2\Rightarrow P_{G_0}(3)=-zT^3(6z+q)^2.\end{gathered} \tag{8}$$

Для спектра дискрет (8) критерій кібербезпеки в області оригіналів можна записати у загальному вигляді як [4]:

$$\Theta_{G_0}(t)=\frac{1}{T}\int\limits_{t=t_0}^{T}P_{G_0}(t)\,dt. \tag{9}$$

Після прямого перетворення в області зображень математичний вираз (9) набуде вигляду [9]

$$\Theta_{G_0}=\sum_{k=0}^{k=8}\frac{P_{G_0}(k)}{k+1}. \tag{10}$$

Після підстановки (8) у (10) отримаємо функціонал виду

$$\Theta_{G_0}=1-3zT+zT^2(6z+q)-\frac{1}{4}zT^3(6z+q)^2. \tag{11}$$

На основі математичної залежності (11) знайдемо екстремум функціоналу

$$\begin{cases}\dfrac{d\Theta_{G_0}(z,q)}{dz}=0,\\ \dfrac{d\Theta_{G_0}(z,q)}{dq}=0.\end{cases} \tag{12}$$

Як наслідок, маємо

$$z=\frac{1}{6T},\ q=\frac{1}{T}. \tag{13}$$

Тоді рівень кіберзахисту (11) з урахуванням (13) матиме такий вигляд:

$$\Theta_{G_0}\approx 0.67 \tag{14}$$

Після операції оберненого диференційного перетворення [2, 9] модель кібербезпеки для центрального сервера матиме такий вигляд:

$$P_{G_0}\approx 1-6zt+3zt^2(6z+q)-zt^3(6z+q)^2. \tag{15}$$

Аналогічно можна для кожного вузла графа (див. рис. 1) отримати математичні моделі виду (15) для визначення рівня кібербезпеки розподіленої комп'ютерної мережі керування електропостачанням залізниці.

ВИСНОВКИ

1. Проведено аналіз комплексної проблеми гарантування кібербезпеки в розподілених комп'ютерних системах і мережах. Обґрунтовано напрямок досліджень, пов'язаний з інтелектуалізацією швидкоплинних технологічних процесів постачання електроенергії на тягу, як основи організації систем кібербезпеки комп'ютерних мереж керування електроспоживанням, безпеки швидкісних перевезень та створення енергоощадних технологій споживання.

2. Наведено методи представлення функцій часового аргументу у вигляді спектра дискрет, для яких для диференційних зображень запропоновано стратегію кіберзахисту, суть якої полягає в пошуку закону керування інтенсивністю захисних дій під час стохастичної зміни потоків кібератак. Розроблено критерій оцінки рівня кібербезпеки та запропоновано методи пошуку оптимальних рішень.

3. Для аналізу локальних мереж керування електропостачанням на тягу дистанції залізниці, представленої у вигляді графа (див. рис. 1), розроблено математичні диференційні моделі для синтезу в аналітичній формі математичних залежностей оцінки рівня кібербезпеки та ймовірностей стану для кожного вузла графа, як основи створення інтелектуальних комп'ютерних засобів захисту інформаційних ресурсів мереж керування електроспоживанням.

СПИСОК ЛІТЕРАТУРИ

1. Стасюк О.І., Гончарова Л.Л., Максимчук В.Ф. Методи організації інтелектуальних електричних мереж залізниць на основі концепції SMART-Grid. *Інформаційно-керуючі системи на залізничному транспорті.* 2014, № 2. С. 29–37.
2. Stasuk O.I., Goncharova L.L. Differential mathematical models to investigate the computer network architecture of an all-mode system of control over a distance of railways. *Cybernetics and Systems Analysis.* 2017. Vol. 53, N 1. P. 157–164.
3. Stasuk O.I., Goncharova L.L. Mathematical models of computer intellectualization of technologies for synchronous phasor measurements of parameters of electric networks. *Cybernetics and Systems Analysis.* 2016. Vol. 52, N 5. P. 825–830.
4. Стасюк О.І., Гончарова Л.Л. Математична модель кібербезпеки мереж керування електропостачанням тягових підстанцій. *Кибернетика и системный анализ*. 2017. Т. 53, № 3. С. 170–179.
5. Стасюк А.И., Гончарова Л.Л. Математические модели и методы анализа компьютерных сетей управления электроснабжением тяговых подстанций железных дорог. *Международный научно-технический журнал «Проблемы управления и информатики»*. 2017. № 1. С. 34–43.
6. Opanasenko V.N., Kryvyi S.L. Partitioning the full range of boolean functions based on the threshold and threshold relation. *Cybernetics and Systems Analysis*. 2012, Vol. 48, N 3. P. 459–468.
7. Opanasenko V.N., Kryvyi S.L. Synthesis of adaptive logical networks on the basis of Zhegalkin polynomials. *Cybernetics and Systems Analysis.* 2015. Vol. 51, N 6. P. 969–977.
8. Венцель Е.С. Исследование операций. Москва: Сов. радио, 1972. 552 с.
9. Пухов Г.Е. Преобразования Тейлора и их применение в электротехнике и электронике. Київ: Наук. думка, 1978. 259 с.

Надійшла до редакції 26.06.2017

А.И. Стасюк, Р.В. Грищук, Л.Л. Гончарова

МАТЕМАТИЧЕСКИЕ ДИФФЕРЕНЦИАЛЬНЫЕ МОДЕЛИ И МЕТОДЫ ОЦЕНКИ КИБЕРБЕЗОПАСНОСТИ ИНТЕЛЛЕКТУАЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ ЭЛЕКТРОСНАБЖЕНИЯ ЖЕЛЕЗНЫХ ДОРОГ

Аннотация. Проведен анализ проблемы кибербезопасности компьютерных сетей управления электроснабжением на уровне железной дороги и предложен граф топологии компьютерной сети управления электропотреблением. На основе теории дифференциальных преобразований Пухова предложен ряд дифференциальных математических моделей оценки уровня кибербезопасности компьютерной сетей управления электроснабжением. В области дифференциальных изображений предложен критерий кибербезопасности и разработан принцип минимакса для наихудшего сочетания интенсивности кибератак и потока защитных действий. Разработан метод интеллектуального поиска оптимальной стратегии кибербезопасности путем исследования на экстремум функционала при стохастической интенсивности потоков кибернетических атак.

Ключевые слова: кибербезопасность, киберпространство, киберугроза, дифференциальные математические модели, дифференциальные преобразования, интеллектуальные методы, защита информации.

O.I. Stasiuk, R.V. Grishchuk, L.L. Goncharova

DIFFERENTIAL MATHEMATICAL MODELS AND METHODS FOR ASSESSING THE CYBERSECURITY OF INTELLIGENT COMPUTER NETWORKS OF CONTROL OF TECHNOLOGICAL PROCESSES OF RAILWAY POWER SUPPLY

Abstract. The authors analyze the problem of cybersecurity of computer networks of railway power supply and propose the graph of topology of the computer network of energy consumption control. Based on the theory of Pukhov's differential transformations, a number of differential mathematical models are proposed to assess the cybersecurity of computer networks of power control. In the field of differential images, a cybersecurity criterion is proposed and the minimax principle is developed for the worst combination of the intensity of cyber attacks and the flow of protective actions. The method of predictive search for the optimal cyber security strategy by the extremum analysis of the functional under stochastic flow intensity of cyber attacks is developed.

Keywords: cybersecurity, cyberspace, cyber threat, a differential mathematical model, differential conversion, intelligent techniques.

Стасюк Олександр Іонович,
доктор техн. наук, професор, проректор з наукової роботи Державного університету інфраструктури транспорту, Київ, e-mail: X177@rambler.ru.

Грищук Руслан Валентинович,
доктор техн. наук, старший науковий співробітник, начальник відділу наукового центру Житомирського військового інституту імені С.П. Корольова, e-mail: Dr.Hry@i.ua.

Гончарова Лідія Леонідівна,
кандидат техн. наук, доцент Державного університету інфраструктури транспорту, Київ, e-mail:ktarael@yandex.ru.