УДК 004.9

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

МАТЕМАТИЧНА МОДЕЛЬ КІБЕРБЕЗПЕКИ КОМП'ЮТЕРНОЇ МЕРЕЖІ КЕРУВАННЯ ЕЛЕКТРОПОСТАЧАННЯМ ТЯГОВИХ ПІДСТАНЦІЙ

Анотація. На основі аналізу проблеми кібербезпеки показано, що подолати загрози кібератак можна лише за умови розв'язання комплексу взаємозумовлених задач, особливості яких випливають з топології кіберпростору. Запропоновано граф, що адекватно відображає топологію системи електропостачання комп'ютерної мережі керування електропостачанням тягових підстанцій та його математичну модель, як базу для створення сучасних моделей кібербезпеки. В основу розробленої математичної моделі кібербезпеки комп'ютерної мережі покладено теорію диференційних перетворень Пухова. Формалізовано критерій кібербезпеки, запропоновано принцип мінімаксу для мінімізації функціонала у випадках найгіршого поєднання інтенсивності потоків кібератак і захисних дій. Розроблено інтелектуальний метод пошуку оптимальної стратегії гарантування кібербезпеки комп'ютерної мережі шляхом дослідження на екстремум формалізованого функціонала.

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

ВСТУП

Постійне зростання інтенсивності кібератак у кіберпросторі, що призводять до великих матеріальних втрат, є логічним результатом прогресу еволюції створення та впровадження сучасних інформаційно-інтелектуальних та мережевих технологій [1, 2, 9]. У сфері кібернетичної безпеки поява складних кібератак, комплексна архітектура яких базується на великій розмірності кіберпростору і широкому діапазоні можливостей різних напрямків передавання інформації, набула загрозливого характеру для критичної інфраструктури великих корпорацій, важливих промислових об'єктів і державних установ [3]. Головними тенденціями розвитку загроз кібербезпеки є постійне збільшення не тільки інтенсивності кібератак, а й нарощення їхньої складності шляхом багатоетапного впливу на кіберпростір. Сучасні методи соціальної інженерії та новітні досягнення в сфері комп'ютерних технологій відкривають кіберзлочинцям широкі можливості для створення нових технологій кібернападів, що адаптуються до топології кіберпростору і можуть негативно впливати на інтереси корпорацій і держав. Без цілеспрямованих активних дій, які зорієнтовані на гарантування безпеки процесів керування в системах різноманітної природи, в кіберпросторі можуть розвиватися все більш небезпечні і складні загрози системного характеру [3]. Таким чином, проблема гарантування кібербезпеки на об'єктах критичної інфраструктури (таких як комп'ютерна мережа керування електропостачанням тягових підстанцій залізниць) є актуальною, а тому передбачає розв'язання комплексу взаємозумовлених задач з урахуванням особливостей організації топології кіберпростору та низки характеристик, пов'язаних з організацією взаємозв'язків та передаванням інформації між вузлами та сегментами [4, 5, 10].

ПОСТАНОВКА ПРОБЛЕМИ

Пошук перспективних напрямків розв'язання комплексної проблеми організації ефективної системи гарантування безпеки призвело до появи сучасних, створених на загальносистемних позиціях концептуальних підходів і наукових досліджень у сфері організації кібербезпеки підвищеної стійкості [4]. Така

організація передбачає вивчення специфічних властивостей кіберпростору за сукупністю параметрів, що відображають динаміку розвитку й зміни в різних екстремальних та часових умовах і методів керування в реальному часі. Важливим також є теоретичне обґрунтування підходів і критеріїв визначення сукупності показників кібербезпеки і розроблення математичних моделей кіберпростору, включаючи низку базових факторів, для оцінювання і визначення рівня впливу на якість його функціювання. Головним при цьому є створення математичних моделей для визначення комплексу числових безпекових характеристик комп'ютерної мережі. Такими характеристиками є, у першу чергу, ступінь загроз кібербезпеки, оцінка рівня ефективності кіберзахисту, величина кіберризику тощо. Забезпечення високого рівня стійкості кіберпростору, що перебуває під постійним впливом кібернетичних загроз, можливе шляхом створення спеціальних методів аналізу топології інфраструктури інформаційного простору та розроблення рекомендацій для її оптимізації [2, 4]. Застосування переваг багатозв'язної архітектури кіберпростору відкриває широкі можливості для розроблення інтелектуальних методів, орієнтованих на отримання нових знань у сфері кібербезпеки. Сучасні інтелектуальні методи дозволяють проводити в реальному часі ситуаційне дослідження стану кібербезпеки та оцінювати його рівень, прогнозувати можливість появи кібератак та запобігання їм, впроваджувати інтелектуальну ідентифікацію користувачів тощо.

Подібний підхід є пріоритетним при організації комп'ютерних систем і мереж динамічного керування швидкоплинними технологічними процесами постачання електроенергії. Виявилося, що розв'язання проблеми організації надійності функціювання складних енергетичних об'єктів, до яких належать системи електропостачання залізниць, тісно пов'язане з розв'язанням комплексу задач кібербезпеки в розподілених комп'ютерних мережах керування електропостачанням на рівні тягових підстанцій. Подібна організація інтелектуальних систем електропостачання на тягу дозволяє суттєво підвищити рівень безпеки руху потягів та забезпечити високий рівень технології перевізного процесу. Прогрес у сфері сучасних інформаційних технологій організації кібербезпеки комп'ютерного середовища керування системами електропостачання залізниць призводить до широкого спектру наукових досліджень нових концептуальних підходів та синтезу математичних моделей і комп'ютерно-орієнтованих методів захисту інформаційного кіберпростору та гарантування безпеки його функціювання [1, 4].

Мета роботи — розроблення математичної моделі кібербезпеки комп'ютерної мережі керування електропостачанням тягових підстанцій для подальшого проведення на її основі аналізу стійкості сегменту кіберпростору, закріпленого за залізницею, від проявів нових та невідомих кіберзагроз.

ДИФЕРЕНЦІЙНІ МАТЕМАТИЧНІ МОДЕЛІ

Формування локального комп'ютерного середовища для впровадження безперервного моніторингу якості функціювання систем електропостачання і силового електрообладнання тісно пов'язане з розв'язанням спектра задач, орієнтованих на нейтралізацію випадкових і цілеспрямованих кібератак, щоб забезпечити цілісність інформації для оперативного керування швидкоплинними технологічними процесами постачання електроенергії на тягу. Домінантною особливістю сучасних інтелектуальних мереж електропостачання є адекватність топології тягової підстанції та архітектури комп'ютерного середовища, представленого розподіленою локальною комп'ютерною мережею. Його інформаційний ресурс формується з єдиних загальносистемних позицій на основі принципу єдності і синхронності векторних вимірювань в енергетиці [1]. Логічна структура комп'ютерного середовища оперативного керування електроспоживанням може мати довільну архітек-

туру, але головним її показником є те, що вона повинна адекватно відображати топологію організації електричної системи електропостачання на рівні тягових підстанцій [2]. Досвід експлуатації інтелектуальних електричних систем показав, що гармонійно пов'язані між собою типи обчислювальних архітектур «зірка» і «кільце», що складаються з сукупності вузлів і стосуються оптимізації електропостачання, енергозбереження, а також із захистом комп'ютерної інформації від впливу кібератак та підвищенням стійкості кіберпростору [1, 2, 4, 5], використовують, зазвичай, як логічну структуру комп'ютерного середовища.

На рис. 1 у вигляді графа наведено схемну реалізацію архітектури комп'ютерного середовища тягової підстанції постачання електроенергії залізницям. На основі цього графа синтезуємо диференційну математичну модель і на її базі сформулюємо критерій кібербезпеки та побудуємо інтелектуальні комп'ютерно-орієнтовані методи кіберзахисту в реальному часі. Вузли P_0 і P_1 графа, наведеного на рис. 1, — це центральний сервер локальної мережі керування і сервер бази даних відповідно. Організація обміну інформацією між вузлами у розподіленій комп'ютерній мережі та реалізація передавання даних по Інтернет здійснюється за допомогою вузлів P_2 і P_3. Процедури опитування датчиків комерційного обліку електроенергії реалізовані у вузлі P_4, диспетчерського керування електропостачанням — у вузлі P_5, а зчитування інформації з мікропроцесорних систем керування електроспоживанням здійснюється вузлом P_6. При цьому дуги графа являють собою інтенсивність потоку кібератак $\lambda_j(t)$ та інтенсивність потоку захисних дій $\gamma_j(t)$ відповідно. Вузли графа P_i під впливом інтенсивності потоків кібератак $\lambda_j(t)$ та відповідно захисних дій $\gamma_j(t)$ перебувають у стані, який характеризується ймовірністю $P_j(t)$ $(i = 0, 1, \ldots, 6)$.

Із застосуванням графа локальної мережі (див. рис. 1) будемо синтезувати математичну модель у вигляді системи диференціальних рівнянь Колмогорова–Чепмена з відповідними початковими умовами [4, 6]:

$$\begin{cases} \dfrac{dP_0(t)}{dt} = -(\lambda_0+\lambda_1+\lambda_2+\lambda_3+\lambda_4)P_0(t)+\gamma_0P_1(t)+\gamma_1P_5(t)+\gamma_2P_4(t)+ \\ \qquad +\gamma_3P_3(t)+\gamma_4P_2(t); \\ \dfrac{dP_1(t)}{dt} = -\gamma_0P_1(t)+\lambda_0P_0(t); \\ \dfrac{dP_2(t)}{dt} = -(\gamma_4+\lambda_7+\lambda_5+\gamma_6)P_2(t)+\lambda_6P_5(t)+\lambda_4P_0(t)+\gamma_7P_6(t); \\ \dfrac{dP_3(t)}{dt} = -(\gamma_9+\gamma_{13}+\gamma_3+\lambda_8)P_3(t)+\lambda_{13}P_6(t)+\lambda_3P_0(t)+\gamma_8P_4(t); \\ \dfrac{dP_4(t)}{dt} = -(\gamma_8+\gamma_2+\lambda_{11}+\lambda_{10})P_4(t)+\lambda_8P_3(t)+\lambda_2P_0(t)+\gamma_{11}P_5(t); \\ \dfrac{dP_5(t)}{dt} = -(\lambda_{12}+\gamma_{11}+\gamma_1+\lambda_6)P_5(t)+\lambda_{11}P_4(t)+\lambda_1P_0(t)+\gamma_6P_2(t); \\ \dfrac{dP_6(t)}{dt} = -(\gamma_7+\lambda_{13})P_6(t)+\gamma_{13}P_3(t)+\lambda_7P_2(t). \end{cases} \tag{1}$$

Система диференціальних рівнянь (1) справедлива за додержання умов нормування $P_0(t_0)+P_1(t_0)+\ldots+P_6(t_0)=1$ в момент $t_0=0$ та початкових умов

$$P_0(0)=1,\ P_1(0)+P_2(0)+\ldots+P_6(0)=0. \tag{2}$$

Для системи диференціальних рівнянь (1) вважають, що кібератаки на інформаційні ресурси в системах відбуваються на деякому інтервалі $[t_0, T]$, а поточний час t перебування системи в інформаційному конфлікті обирають з умов $t \in [t_0, T]$.

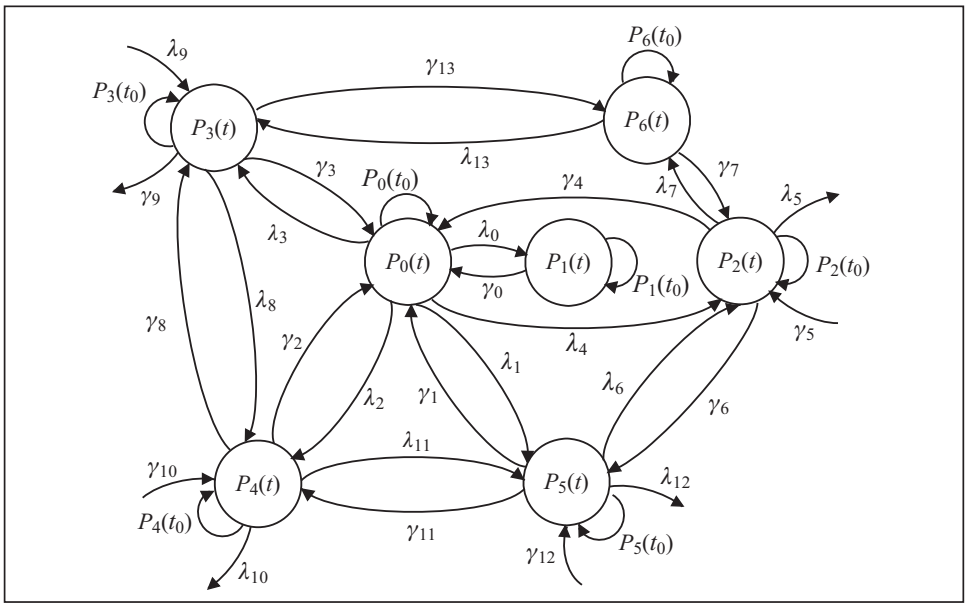

Рис. 1. Графова комп'ютерно-орієнтована модель кібербезпеки обчислювальних мереж тягових підстанцій залізниць

Обмеження на інтенсивності потоків кібератак $\lambda_j(t)$ та на інтенсивність захисних дій $\gamma_j(t)$ запишемо у вигляді

$$0 \le \lambda_j \le \lambda_{j\max},\ 0 \le \gamma_j \le \gamma_{j\max}, \tag{3}$$

де $\lambda_{j\max}$, $\gamma_{j\max}$, $j = 0, 1, \ldots, 6$, — максимальні інтенсивності потоків кібератак і захисних дій відповідно.

З метою узагальнення одержаного результату та спрощення математичних викладок запропоновано такі умови:

$$\lambda_0 = \lambda_1 = \ldots = \lambda_{13} = \lambda,\ \gamma_0 = \gamma_1 = \ldots = \gamma_{13} = \gamma. \tag{4}$$

Виходячи з умов нормування, можна стверджувати, що

$$P_1(t) + P_2(t) + P_3(t) + P_4(t) + P_5(t) = 1 - P_0(t) - P_6(t). \tag{5}$$

Тоді із врахуванням (4) та (5) система (1) набуде вигляду

$$\begin{cases} \dfrac{dP_0(t)}{dt} = -(5\lambda + \gamma)P_0(t) + \gamma(1 - P_6(t)); \\ \dfrac{dP_1(t)}{dt} = -\gamma P_1(t) + \lambda P_0(t); \\ \dfrac{dP_2(t)}{dt} = -2(\gamma + \lambda)P_2(t) + \lambda(P_0(t) + P_5(t)) + \gamma P_6(t); \\ \dfrac{dP_3(t)}{dt} = -(3\gamma + \lambda)P_3(t) + \lambda(P_0(t) + P_6(t)) + \gamma P_4(t); \\ \dfrac{dP_4(t)}{dt} = -2(\gamma + \lambda)P_4(t) + \lambda(P_0(t) + P_3(t)) + \gamma P_5(t); \\ \dfrac{dP_5(t)}{dt} = -2(\gamma + \lambda)P_5(t) + \lambda(P_0(t) + P_4(t)) + \gamma P_2(t); \\ \dfrac{dP_6(t)}{dt} = -(\gamma + \lambda)P_6(t) + \gamma P_3(t) + \lambda P_2(t). \end{cases} \tag{6}$$

Математичні моделі (1), (6) є основою для синтезу диференційних математичних моделей і інтелектуальних методів кіберзахисту з метою забезпечення

оперативного керування електропостачанням залізниць в умовах ризику проявів кіберзагроз.

З метою синтезу диференційних математичних моделей кібербезпеки у подальшому пропонується скористатися фундаментальними поняттями теорії диференційних перетворень Пухова. Відповідні математичні залежності прямого та оберненого диференційного перетворення мають вигляд [7]

$$X(k) = \underline{x}(k) = \frac{H^k}{k!}\left[\frac{d^k x(t)}{dt^k}\right]_{t=0} \quad \overline{\div}\, x(t) = \sum_{k=0}^{k=\infty}\left(\frac{t}{H}\right)^k X(k), \tag{7}$$

де $x(t)$ — функція-оригінал, що являє собою безперервну, нескінченне число разів диференційовану функцію аргументу t, яка обмежена разом із усіма своїми похідними; $X(K)$ — функція цілочислового аргументу k, що являє собою диференціальне зображення оригінала; H — масштабна постійна, що має ту ж розмірність, що і аргумент t, і вибрана, як правило, в діапазоні $0 \le t \le H$, на якому розглянуто функцію-оригінал $x(t)$; знак $\overline{\div}$ являє собою символ відповідності між оригіналом $x(t)$ та диференціальним зображенням $X(K)$, $(K = 0, 1, 2, \dots)$.

За умови, що $H = T$, на основі диференційних перетворень Пухова (7) запишемо систему рівнянь (6) в області диференціальних зображень у вигляді T-моделі [4, 7]:

$$\begin{cases} P_0(k+1) = \dfrac{T}{k+1}[-(5\lambda+\gamma)P_0(k) + \gamma(\text{ъ}(k) - P_6(k))]; \\ P_1(k+1) = \dfrac{T}{k+1}[-\gamma P_1(k) + \lambda P_0(k)]; \\ P_2(k+1) = \dfrac{T}{k+1}[-2(\gamma+\lambda)P_2(k) + \lambda(P_0(k) + P_5(k) + \gamma P_6(k))]; \\ P_3(k+1) = \dfrac{T}{k+1}[-(3\gamma+\lambda)P_3(k) + \lambda(P_0(k) + P_6(k) + \gamma P_4(k))]; \\ P_4(k+1) = \dfrac{T}{k+1}[-2(\gamma+\lambda)P_4(k) + \lambda(P_0(k) + P_3(k) + \gamma P_5(k))]; \\ P_5(k+1) = \dfrac{T}{k+1} - 2(\gamma+\lambda)P_5(k) + \lambda(P_0(k) + P_4(k) + \gamma P_2(k)); \\ P_6(k+1) = \dfrac{T}{k+1}[-(\gamma+\lambda)P_6(k) + \gamma P_3(k) + \lambda P_2(k)], \end{cases} \tag{8}$$

де $\text{ъ}(k)$ — тейлорівська одиниця (теда), яку визначають згідно з умовами

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

Застосувавши диференційні перетворення (7) для початкових умов (2) системи диференціальних рівнянь (6), одержимо при $t_0 = 0$ і відповідно $k = 0$ початкові умови в області T-зображень у вигляді

$$P_0(0) = P_0(t_0) = 1, \;\; P_i(0) = P_i(t_0) = 0, \;\; i = 1, 2, \dots, 6. \tag{9}$$

Система диференціальних T-рівнянь (8), яка подана у вигляді сукупності алгебраїчних залежностей, є базовою для визначення величин ймовірностей $P_0(t) + P_1(t) + \dots + P_6(t)$ вузлів графа моделі кібератак на інформаційні ресурси локальної обчислювальної мережі тягової підстанції. Підставивши в систему T-рівнянь (8) значення цілочислового аргументу $k = 1, 2, \dots$, одержимо спектр дискрет $P_i(1)$, $P_i(2)$, $P_i(3)$, $i = 1, 2, \dots, 6$, які в сукупності формують розв'язок цієї системи в T-області.

Для цілочислових аргументів $k = 0, 1, 2$ одержимо такі спектри:

$$k := 0 \Rightarrow \begin{cases} P_0(1) = -5T\lambda; \\ P_1(1) = T\lambda; \\ P_2(1) = T\lambda; \\ P_3(1) = T\lambda; \\ P_4(1) = T\lambda; \\ P_5(1) = T\lambda; \\ P_6(1) = 0; \end{cases} \quad k := 1 \Rightarrow \begin{cases} P_0(2) = \frac{5}{2} T^2 \lambda (5\lambda + \gamma); \\ P_1(2) = -\frac{1}{2} T^2 \lambda (5\lambda + \gamma); \\ P_2(2) = -T^2 \lambda (3\lambda + \gamma); \\ P_3(2) = -T^2 \lambda (3\lambda + 2\gamma); \\ P_4(2) = -\frac{1}{2} T^2 \lambda (6\lambda + \gamma); \\ P_5(2) = -\frac{1}{2} T^2 \lambda (6\lambda + \gamma); \\ P_6(2) = \frac{1}{2} T^2 \lambda (\lambda + \gamma); \end{cases}$$

$$k := 2 \Rightarrow \begin{cases} P_0(3) = -T^3 \lambda \left(\gamma^2 + \frac{17}{2} \gamma\lambda + \frac{125}{6} \lambda^2 \right); \\ P_1(3) = \frac{1}{3} T^3 \lambda \left(\frac{1}{2} \gamma^2 + 5\gamma\lambda + \frac{25}{2} \lambda^2 \right); \\ P_2(3) = \frac{1}{3} T^3 \lambda \left(\frac{5}{3} \gamma^2 + 7\gamma\lambda + \frac{31}{3} \lambda^2 \right); \\ P_3(3) = \frac{1}{3} T^3 \lambda \left(\frac{11}{2} \gamma^2 + 11\gamma\lambda + 16\lambda^2 \right); \\ P_4(3) = \frac{1}{2} T^3 \lambda \left(\frac{1}{3} \gamma^2 + 3\gamma\lambda + \frac{31}{3} \lambda^2 \right); \\ P_5(3) = T^3 \lambda^2 \left(2\gamma + \frac{31}{6} \lambda \right); \\ P_6(3) = -\frac{1}{3} T^3 \lambda \left(\frac{5}{2} \gamma^2 + 5\gamma\lambda + \frac{7}{2} \lambda^2 \right). \end{cases} \tag{10}$$

Одержавши спектр з дискрет (9), (10), який описує моделі кібербезпеки спеціалізованої локальної мережі тягової підстанції, формалізуємо критерій кібербезпеки обчислювальних мереж тягових підстанцій залізниць у вигляді [7]

$$\Theta_i(t) = \frac{1}{T} \int_{t_0}^{T} P_i(t) dt, \quad i = 1, 2, \ldots, 6. \tag{11}$$

У локальних обчислювальних мережах тягових підстанцій залізниць завдання кібербезпеки розв'язуються в умовах антагонізму суб'єктів інформаційного конфлікту. Враховуючи це, домінантним у таких умовах є дотримання суб'єктами конфлікту принципу мінімаксу. При здійсненні процедур гарантування кібербезпеки для досягнення системою заданих показників захищеності раціонально дотримуватися стратегії формування таких значень γ_j, які мінімізують плату суб'єкта гарантування безпеки $\Theta_i(\lambda_j, \gamma_j)$ за витрати відповідних ресурсів при максимальних інтенсивностях потоків кібератак, тобто [7, 8]

$$\Theta_i^*(\lambda_j, \gamma_j) = \min_{\gamma_j \in E_\gamma} \max_{\lambda_j \in E_\lambda} \Theta_i(\lambda_j, \gamma_j), \quad i = 1, 2, \ldots, 6. \tag{12}$$

При моделюванні стратегії кібератак супротивна сторона ймовірно виходить з умов формування таких стратегій λ_j, що максимізують плату $\Theta_i(\lambda_j, \gamma_j)$, за умови її мінімізації системою безпеки γ_j, тобто

$$\Theta_i^*(\lambda_j, \gamma_j) = \max_{\lambda_j \in E_\lambda} \min_{\gamma_j \in E_\gamma} \Theta_i(\lambda_j, \gamma_j), \; i = 1, 2, \ldots, 6. \tag{13}$$

За умови виконання рівності (13), а також рівності

$$\min_{\gamma_j \in E_\gamma} \max_{\lambda_j \in E_\lambda} \Theta_i(\lambda_j, \gamma_j) = \max_{\lambda_j \in E_\lambda} \min_{\gamma_j \in E_\gamma} \Theta_i(\lambda_j, \gamma_j) = \Theta_i^{*\,\mathrm{opt}}(\lambda_j^{\mathrm{opt}}, \gamma_j^{\mathrm{opt}}) \qquad (14)$$

отримані стратегії λ_j^{opt} та γ_j^{opt} є оптимальними. Стратегія гарантування кібербезпеки полягає в пошуку закону зміни потоку інтенсивності захисних дій γ_j, яка реалізує мінімізацію функціонала (11) при стохастичній інтенсивності потоків кібератак λ_j відповідно у межах (3). У зв'язку з антагонізмом цілей суб'єктів інформаційного конфлікту домінантною стратегією гарантування кібербезпеки буде стратегія на основі принципу мінімаксу [7], тобто

$$\min_{\gamma_j \in E_\gamma} \max_{\lambda_j \in E_\lambda} \Theta_i(t, P_i(t), \lambda_j, \gamma_j). \qquad (15)$$

У рамках прийнятих обмежень (3) застосування мінімаксної стратегії (15) дозволяє мінімізувати функціонал (11) навіть у випадках найгіршого поєднання інтенсивності потоків кібератак λ_j з довільним законом потоку інтенсивності з захисних дій γ_j.

Застосувавши пряме перетворення (4) до функціоналу (11) і використавши обчислені згідно з (8) значення сукупності T-дискрет (9), (10), запишемо процедуру оптимізації через дискрети диференціального спектра $P_i(k)$ у вигляді [7, 8]

$$\Theta_i^* = \sum_{k=0}^{k=\infty} \frac{P_i(k)}{k+1}. \qquad (16)$$

На основі обчислених дискрет (6)–(8) згідно з (16) при $i=0$ для вузла P_0 локальної мережі — центрального сервера локальної мережі керування тягової підстанції, вираз (16) набуватиме вигляду

$$\Theta_0^*(\lambda, \gamma) \approx 1 - \frac{5}{2}T\lambda + \frac{5}{2}T^2\lambda(5\lambda + \gamma) - T^3\lambda\left(\gamma^2 + \frac{17}{2}\gamma\lambda + \frac{125}{6}\lambda^2\right). \qquad (17)$$

Процес пошуку оптимальних стратегій інтенсивності потоків кібератак λ_j^{opt} та потоку інтенсивності захисних дій γ_j^{opt} з обмеженнями (3) функціонала Θ_i^* тісно пов'язаний з дослідженням його на екстремум шляхом підстановки у вираз (16) значень відповідних дискет $P_i(k)$, $i = 1, 2, \ldots, 6$.

Відомо, що необхідним для існування екстремуму функціонала $\Theta_0^*(\lambda, \gamma)$ згідно з теоремою Куна–Такера є умови, що дозволяють визначити оптимальну стратегію гарантування кібербезпеки вигляду [8]

$$\begin{cases} \dfrac{d}{d\gamma_j}(\Theta_0^*(\lambda_j, \gamma_j)) = 0; \\ \dfrac{d}{d\lambda_j}(\Theta_0^*(\lambda_j, \gamma_j)) = 0; \\ \ldots \\ \dfrac{d}{d\gamma_j}(\Theta_4^*(\lambda_j, \gamma_j)) = 0; \\ \dfrac{d}{d\lambda_j}(\Theta_4^*(\lambda_j, \gamma_j)) = 0; \\ \ldots \\ \dfrac{d}{d\gamma_j}(\Theta_6^*(\lambda_j, \gamma_j)) = 0; \\ \dfrac{d}{d\lambda_j}(\Theta_6^*(\lambda_j, \gamma_j)) = 0. \end{cases} \qquad (18)$$

Для вузла P_0 локальної мережі інтенсивність потоку кібератак та захисних дій дорівнюватиме відповідно

$$\begin{cases} \lambda = \dfrac{16}{69T}, \\ \gamma = \dfrac{47}{69T}, \end{cases} \tag{19}$$

а рівень захищеності — відповідно

$$\Theta_0^* \approx 0.61. \tag{20}$$

Знайдені стратегії (19) є оптимальними, оскільки для них виконуються достатні умови [8].

Одержаний результат (20) свідчить про те, що побудова локальної комп'ютерної мережі тягової підстанції за моделлю (див. рис. 1) забезпечуватиме достатньо високий рівень кіберзахисту усієї системи від потенційно небезпечних кібератак.

Провівши операцію оберненого диференційного перетворення (7) для обраного прикладу, одержимо модель гарантування кібербезпеки вузла P_0 у загальному вигляді:

$$P_0(t) \approx 1 - 5T\lambda + \frac{5}{2}T^2\lambda(5\lambda + \gamma) - T^3\lambda\left(\gamma^2 + \frac{17}{2}\gamma\lambda + \frac{125}{6}\lambda^2\right). \tag{21}$$

Точність моделі (21) та їй подібних досягають кількістю дискрет диференціального спектра, які входять до складу моделі. Аналогічно можна визначити інші моделі кібербезпеки для локальної обчислювальної мережі тягової підстанції.

ВИСНОВКИ

1. Аналіз проблеми кібербезпеки в розподілених комп'ютерних середовищах, орієнтованих на керування складними енергетичними об'єктами, показав, що постійне збільшення інтенсивності кібератак набуває загрозливого характеру для інформаційної інфраструктури. Розв'язання цієї проблеми потребує розв'язання комплексу взаємнозумовлених задач з врахуванням властивостей топології кіберпростору та низки характеристик, пов'язаних з організацією взаємозв'язків, і особливостей передавання інформації.

2. Показано, що забезпечення високого рівня стійкості кіберпростору, який знаходиться під постійним впливом кіберзагроз, можливе шляхом розроблення спеціальних методів аналізу топології інфраструктури і використання переваг та оптимізації багатозв'язної архітектури як основи створення сучасних інтелектуальних методів, орієнтованих на отримання нових знань у сфері кібербезпеки для ситуаційного аналізу, оцінки рівня захищеності, прогнозу та запобігання появі можливих кібератак.

3. Запропоновано логічну структуру розподіленого комп'ютерного середовища у вигляді графа, що адекватно відображає топологію організації електричної системи електропостачання на рівні тягових підстанцій, на базі якого синтезовано математичну модель, описану системою диференціальних рівнянь Колмогорова–Чепмена, для побудови диференційних математичних моделей та інтелектуальних методів кіберзахисту.

4. На основі теорії диференційних перетворень Пухова розроблено диференційну математичну модель кібербезпеки комп'ютерного середовища динамічного керування електропостачанням, яка записана у вигляді сукупності алгебричних залежностей системою диференціальних T-рівнянь. Це відкрило можливість визначити в аналітичному вигляді ймовірності вузлів графа моделі

кібератак на інформаційні ресурси локальної обчислювальної мережі тягової підстанції.

5. Формалізовано критерій кібербезпеки комп'ютерного середовища, показано, що стратегія гарантування кібербезпеки полягає в пошуку закону зміни потоку інтенсивності захисних дій, яка реалізує мінімізацію функціонала при стохастичній інтенсивності потоків кібератак. З огляду на антагонізм цілей суб'єктів інформаційного конфлікту запропоновано стратегію гарантування кібербезпеки на основі принципу мінімаксу, яка дозволяє мінімізувати функціонал навіть у випадках найгіршого поєднання інтенсивності потоків кібератак з довільним законом потоку інтенсивності із захисних дій. Розроблено інтелектуальний метод пошуку оптимальної стратегії гарантування кібербезпеки інформаційних ресурсів для досягнення кіберпростором заданих показників захищеності на основі визначення інтенсивності потоків кібератак λ_j^{opt} та потоку інтенсивності захисних дій γ_j^{opt} шляхом дослідження на екстремум функціонала $\Theta_i^*(\lambda_j, \gamma_j)$, що реалізується в області T-зображень з використанням дискрет диференціального спектра ймовірностей вузлів графа.

СПИСОК ЛІТЕРАТУРИ

1. Стасюк О.І., Гончарова Л.Л. Математичні моделі комп'ютерної інтелектуалізації технологій синхронних векторних вимірювань параметрів електричних мереж. *Кибернетика и системный анализ*. 2016. Т. 52, № 5. С 186–192.
2. Стасюк О.І., Гончарова Л.Л. Математичні моделі і методи комп'ютерного керування електропостачанням залізниць на основі диференційних перетворень Пухова. *Электронное моделирование.* 2016. Т. 38, № 4. С 127–139.
3. Грищук Р.В., Даник Ю.Г. Основи кібернетичної безпеки. За заг. ред. Ю.Г. Даника. Житомир: ЖНАЕУ, 2016. 636 с.
4. Стасюк О.І., Гончарова Л.Л. Диференційні математичні моделі дослідження комп'ютерної архітектури всережимної системи керування дистанцією електропостачання залізниць. *Кибернетика и системный анализ*. 2017. Т. 53, № 1. С. 184–192.
5. Буткевич О.Ф., Левконюк А.В., Стасюк О.І. Підвищення надійності моніторингу допустимості завантажень контрольованих перетинів енергосистем. *Технічна електродинаміка*. 2014. № 2. С. 56–67.
6. Венцель Е.С. Исследование операций. Москва: Сов. радио, 1972. 552 с.
7. Пухов Г.Е. Преобразования Тейлора и их применение в электротехнике и электронике. Киев: Наук. думка, 1978. 259 с.
8. Грищук Р. В. Теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальних ігор та диференціальних перетворень. Житомир: РУТА, 2010. 280 с.
9. Калашников А.О. Пример использования теоретико-игрового подхода в задачах обеспечения кибербезопасности информационных систем. *Вопросы кибербезопасности*. 2014. № 1 (2). С. 49–54. URL: http://cyberrus.com/wp-content/uploads/2014/03/49-54.pdf.
10. Шматова Е.С. Выбор стратегии ложной информационной системы на основе модели теории игр. *Вопросы кибербезопасности*. 2015. № 5 (13) С. 36–40. URL: http://cyberrus.com/wp-content/uploads/2015/12/36-40-513-15_7.-Шматова.pdf.

Надійшла до редакції 21.12.2016

А.И. Стасюк, Р.В. Грищук, Л.Л. Гончарова
МАТЕМАТИЧЕСКАЯ МОДЕЛЬ КИБЕРБЕЗОПАСНОСТИ КОМПЬЮТЕРНОЙ СЕТИ УПРАВЛЕНИЯ ЭЛЕКТРОСНАБЖЕНИЕМ ТЯГОВЫХ ПОДСТАНЦИЙ

Аннотация. На основе анализа проблемы кибербезопасности показано, что ее решение связано с решением комплекса взаимообусловленных задач, особенности которых вытекают из топологии киберпространства. Предложен граф, который адекватно отражает топологию системы электроснабжения компьютерной сети управления электроснабжением тяговых подстанций и его математическую модель, как основу для создания современных моделей кибербезопасности. В основу разработанной математической модели кибербезопасности компьютерной сети положена теория дифференциальных преобразований Пухова. Формализован критерий кибербезопасности, предложен принцип минимакса для минимизации функционала в случаях наихудшего сочетания интенсивности потоков кибератак и защитных действий. Разработан интеллектуальный метод поиска оптимальной стратегии обеспечения кибербезопасности компьютерной сети путем исследования на экстремум формализованного в статье функционала.

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

A.I. Stasiuk, R.V. Hryshchuk, L.L. Goncharova
A MATHEMATICAL MODEL OF CYBER SECURITY COMPUTER NETWORK CONTROL IN POWER SUPPLY OF TRACTION SUBSTATIONS

Abstract. Based on the analysis of the problem of cybersecurity we show that its solution is related to the solution of a set of interdependent problems whose features are derived from the topology of cyberspace. We propose a graph, which adequately reflects the topology of the power system computer network for power control of traction substations and its mathematical model as the basis for the creation of contemporary models of cybersecurity. The basis of the developed mathematical model of cybersecurity computer networks is the Pukhov theory of differential transformations. We formalize the criterion of cybersecurity and propose minimax principle for minimization of the functional in the worst combination of flow intensity of cyber attacks and defensive actions. We develop an intelligent method to find the optimal strategy of cyber security computer networks by the extremum analysis of the formalized functional.

Keywords: cybersecurity, cyberspace, cybercyberthreat, mathematical models, differential conversion, intelligent techniques, protection of information.

Стасюк Олександр Іонович,
доктор техн. наук, професор, завідувач кафедри Державного економіко-технологічного університету транспорту, Київ, e-mail: X177@rambler.ru.

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

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