УДК 004.9

МАТЕМАТИЧНІ КОМП'ЮТЕРНО-ОРІЄНТОВАНІ МОДЕЛІ БЕЗПЕКИ ІНФОРМАЦІЇ ОБЧИСЛЮВАЛЬНИХ МЕРЕЖ ТЯГОВИХ ПІДСТАНЦІЙ ЗАЛІЗНИЦЬ

Олександр Стасюк, Руслан Грищук, Лідія Гончарова

На основі проведеного аналізу комплексної проблеми безпеки інформаційних ресурсів локальних обчислювальних мереж тягових підстанцій залізниць показано, що загальновизнаним у світі є напрямок пов'язаний з інтелектуалізацією обчислювальних мереж, як основи для покращення безпеки руху залізничного транспорту й створення перспективних енергозберігаючих технологій електроспоживання. Сформовано логічну структуру локальної обчислювальної мережі оперативного управління електропостачанням у вигляді графа, що відображає топологічні характеристики тягової підстанції, а також розроблено її математичну модель у вигляді системи диференціальних рівнянь. Використано сучасні методи диференціальних перетворень для визначення ймовірностей станів вузлів графа локальної обчислювальної мережі тягової підстанції. Сформульовано критерій безпеки інформації і наведено стратегії її забезпечення на основі принципу мінімаксу. Наведено необхідні і достатні умови існування екстремуму, що дозволяють визначити оптимальну стратегію пошуку.

Ключові слова: *математичні моделі, комп'ютерно - орієнтовані методи, Т-спектр, ідентифікація, аналіз, методи синтезу, тягові мережі, електричні системи.*

ВСТУП. Логічним результатом прогресу еволюції впровадження комп'ютерних і інформаційних технологій для організації, в реальному часі, оперативного керування швидкоплинними технологічними процесами постачання електроенергії залізничному транспорту, є поява інтелектуальних обчислювальних мереж, як основи для покращення безпеки руху залізничного транспорту й створення перспективних енергозберігаючих технологій електроспоживання [1]. У той же час, проблема організації надійності функціонування інтелектуальних комп'ютерних мереж управління електричним господарством залізниць, тісно пов'язана з проблемами їх кібернетичної та інформаційної безпеки, безпеки інформації та захисту інформації. Безпека інформації в інтелектуальних обчислювальних мережах, передбачає рішення комплексу взаємообумовлених задач, пов'язаних із забезпеченням цілісності інформації, її доступності та конфіденційності [2]. Пошук нових шляхів вирішення задачі безпеки інформації для забезпечення ефективного функціонування інтелектуальних обчислювальних мереж в енергетичному секторі залізниць, стимулював появу широкого спектру наукових досліджень, створення нових концептуальних підходів і, як наслідок, відкрив новий етап для синтезу, з загальносистемних позицій, математичних моделей та комп'ютерно-орієнтованих алгоритмів забезпечення безпеки підвищеної стійкості. Аналіз проведених авторами досліджень і публікацій в сфері організації безпеки інформації та її захисту в локальних і корпоративних обчислювальних мережах показав, що для ефективного і надійного функціонування інтелектуальних комп'ютерних мереж залізниць,актуальними залишаються питання щодо запобігання втраті інформації, її спотворенню, несанкціонованому доступу до неї, а також нецільовому й незаконному використанню її на всіх етапах життєвого циклу [1, 2]. Прогрес у сфері інформаційних технологій створив передумови для появи широкого спектру різноманітних методів і засобів захисту інформаційних ресурсів в комп'ютерних системах і мережах. Головними, при цьому, є фізичне збереження програмних і мікропроцесорних засобів від пошкоджень, забезпечення цілісності інформаційних ресурсів та доступу до них за умови відповідності ідентифікаторів визначеним у відповідній стратегії безпеки показникам,організація процедур нейтралізації випадкових або цілеспрямованих атак на інформацію, що обробляється, ідентифікація ступенів підготовки потенційних порушників і формування сукупності відповідних засобів захисту [5–7]. Подальший прогрес в IT-секторі обумовлює необхідність створення нових комп'ютерно-орієнтованих моделей інтелектуальних електричних мереж залізниць, що передбачають використання комплексу перспективних наукових і інженерних рішень в сфері організації спеціальних комп'ютерних мережу правління швидкоплинними технологічними процесами електропостачання, енергозбереження і безпеки руху потягів [8]. На сьогодні локальні, корпоративні і глобальні обчислювальні мережі отримали стрімкий розвиток завдяки значному прогресу інтегральних технологій виготовлення надвеликих інтегральних схем і постійному ускладненню задач обробки та подання інформації. Аналіз процесу еволюції інноваційного перетворення

мереж електропостачання показав, що єдиним методом організації високого рівня ефективності їх функціонування,є розробка інтелектуальних електричних мереж шляхом взаємоінтеграції електромережевої інфраструктури і комп'ютерних обчислювальних мереж на основі єдиної інформаційної моделі, базуючись на принципах єдиного інформаційного простору та синхронної інформаційної взаємодії [1]. Сформовані таким чином мережі електропостачання, спроможні накопичувати «знання» для оптимізації оперативного і стратегічного управління та створювати основу для розробки новітніх енергозберігаючих і безаварійних ІТ- рішень у цій галузі [2]. Невід'ємною частиною ефективного функціонування інтелектуальних мереж електропостачання на тягу, є організація надійного захисту інформаційних ресурсів. Захист комп'ютерних мереж може бути реалізований шляхом використання різних методів таких як організаційні, законодавчі, математичні, апаратні, програмні, морально-етичні, які в сукупності значно розширюють можливості захисту оброблювальної інформації. При цьому, для забезпечення заданого рівня захищеності інформації в процесі її переробки і передачі, в системі інформаційної безпеки комп'ютерних мереж керування необхідно створити спеціальні структури для оцінювання надійності програмно-апаратних засобів захисту та можливості організації періодичного і епізодичного контролю користувачами або контролюючими органами їх ефективності функціонування [8]. Цей факт стимулював широкий діапазон наукових пошуків в сфері розробки математичних моделей і методів моделювання кібератак на інформаційні ресурси з метою аналізу функціонування і оцінювання ефективності засобів захисту.

МЕТА РОБОТИ. Розробка математичних комп'ютерно-орієнтованих моделей безпеки інформації, як основи для створення перспективних методів захисту інформації локальних комп'ютерних мереж оперативного керування електропостачанням тягових підстанцій залізниць, моделювання процесів атак на інформаційні ресурси та аналізу надійності систем інформаційної безпеки для пошуку ефективних шляхів підвищення функціонування інтелектуальних мереж електропостачання, енергозбереження і безпеки руху.

ОСНОВНИЙ МАТЕРІАЛ ДОСЛІДЖЕННЯ. Проблема безпеки інформації локальних обчислювальних мереж для оперативного управління швидкоплинними технологічними процесами постачання електроенергії на тягу, реалізації безперервного моніторингу якості функціонування систем електропостачання включаючи силове електрообладнання тягових підстанцій, тісно пов'язана з рішенням комплексу задач, що забезпечують цілісність інформації, антивірусний захист,збереження програмних і апаратних засобів, а також нейтралізацію випадкових і цілеспрямованих кібератак. Невід'ємною частиною надійного функціонування відповідного сегмента системи захисту локальної мережі тягової підстанції є організація процесу оцінювання ефективності засобів захисту інформаційних ресурсів, яка реалізується за методикою, котра враховує спектр технічних характеристик об'єкта, включаючи технічні рішення архітектурних особливостей комп'ютерного середовища та можливих варіантів реалізації засобів захисту. Враховуючи особливості організації інтелектуальних мереж електропостачання на тягу, головним елементом яких є адекватність топології тягової підстанції і архітектури обчислювальної мережі, в основу ідеології формування первинних інформаційних ресурсів використовується принцип формування єдиного інформаційного середовища з загальносистемних позицій, що відповідає умовам єдності і синхронності вимірювання [7]. Логічна структура локальної обчислювальної мережі оперативного управління електропостачанням, як показано в роботах [1, 2], може бути організована у вигляді довільної фізичної архітектури, що відображає топологічні характеристики тягової підстанції. Як вузли такої мережі використовуються мікропроцесорні засоби, пов'язані з оптимізацією процесів оперативного електропостачання включаючи комерційний облік, моніторинг і визначення ресурсу електричного обладнання і тощо. Для організації динаміки логічної структури обчислювальної мережі, без суттєвої зміни її архітектури, можливе використання комутаторів або магістральних маршрутизаторів. Як показує досвід експлуатації, в якості логічної структури в більшості випадків використовуються гармонійно пов'язані топології типу «зірка» і «кільце». Фрагмент топології «кільце» включає ряд вузлів, кожен із яких виконує сукупність функцій пов'язаних з оперативним електропостачанням і енергозбереженням. Як вузли сегмента,фізична топологія якого подана «зіркою», використовуються сервери для реалізації загального керування, ведення бази даних єдиного інформаційного простору та реалізації обміну інформацією як між вузлами локаль-

ної мережі, так і з верхніми ієрархічними рівнями керування електропостачанням.

На рис. 1 подано схемну реалізація графа, як основи формування математичних моделей безпеки інформації спеціалізованої локальної мережі тягової підстанції. Вузли графа S_0, S_1 – це центральний сервер мережі керування і сервера бази даних. Обмін інформацією в рамках корпоратив-ної обчислювальної мережі залізниці і передача даних по Internetреалізується за допомогою вузлів S_2 і S_3. Функціональні обов'язки з опитування системи комерційного обліку електроенергії виконує вузол S_4, а сервер диспетчерського центру, відповідно вузол S_5.

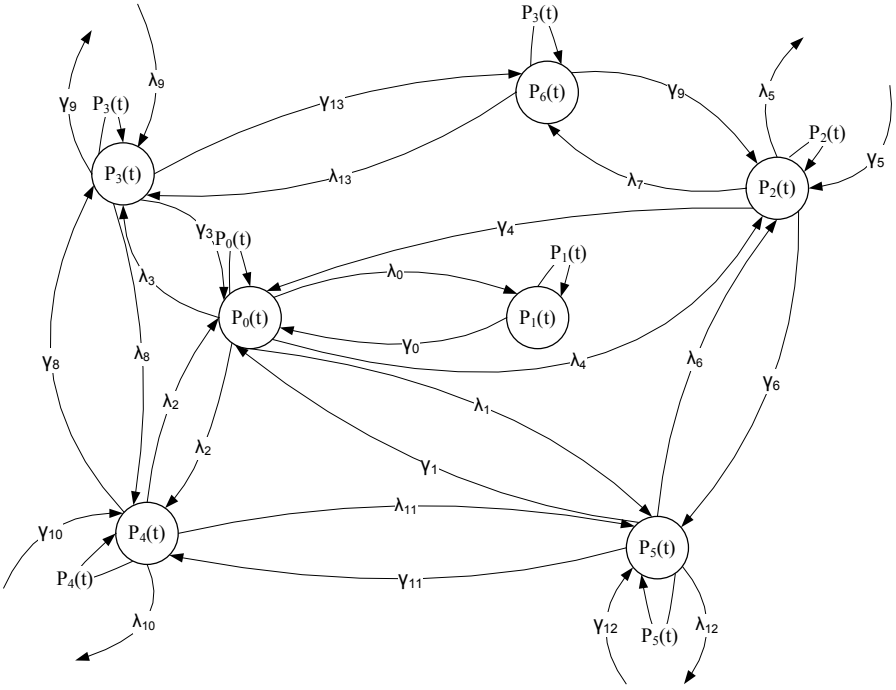

Рис. 1. Графова комп'ютерно-орієнтована модель безпеки інформації обчислювальних мереж тягових підстанцій залізниць

На вузол S_6 покладено функції з опитування всіх мікропроцесорних систем тягової підстанції. Дугами графа подані інтенсивність потоку кібератак $\lambda_j(t)$ та інтенсивність потоку захисних дій $\gamma_j(t)$ відповідно. Під впливом інтенсивності потоків кібератак $\lambda_j(t)$ та захисних дій $\gamma_j(t)$, кожний із вузлів S_i графа може перебувати у стані який характеризується відповідною ймовірністю $P_i(t)$ $(i=0,1,\ldots,6)$. На основі положень теорії масового обслуговування, використовуючи граф локальної мережі (див. рис. 1),синтезуємо математичну модель у вигляді системи диференціальних рівнянь Колмогорова-Чепмена з відповідними початковими умовами[4]. Отримана математична модель є основою для визначення, за допомогою сучасних методів диференційних перетворень, ймовірностей $P_0(t), P_1(t),\ldots,P_6(t)$ стану відповідних вузлів $S_0, S_1,\ldots,S_6$ графа локальної мережі тягової підстанції, а також критерію захищеності інформаційних ресурсів [4, 5]. При такому підході, система диференціальних рівнянь, включаючи початкові умови, матиме вигляд

$$\frac{dP_0(t)}{dt}=\lambda_1P_5(t)+\lambda_2P_4(t)+\lambda_3P_3(t)+\lambda_4P_2(t)+\gamma_0P_1(t)+\beta_1P_0(t),$$

$$\frac{dP_1(t)}{dt}=\lambda_0P_0(t)-\gamma_0P_1(t),\ \frac{dP_2(t)}{dt}=\lambda_7P_6(t)+\gamma_4P_0(t)+\gamma_6P_5(t)+\beta_2P_2(t),$$

$$\frac{dP_3(t)}{dt}=\lambda_8P_4(t)+\gamma_3P_0(t)+\beta_3P_3(t),\ \frac{dP_4(t)}{dt}=\lambda_{11}P_5(t)+\gamma_2P_0(t)+\gamma_8P_3(t)+\beta_4P_4(t), \quad (1)$$

$$\frac{dP_5(t)}{dt}=\lambda_6P_2(t)+\gamma_1P_0(t)+\beta_5P_5(t),\ \frac{dP_6(t)}{dt}=\lambda_{13}P_3(t)+\gamma_7P_2(t)+\beta_6P_6(t).$$

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

$$P_0(0)=1,\ P_1(0)+P_2(0)\ldots+P_6(t_0)=0. \qquad (2)$$

У системі диференціальних рівнянь (1) вважається, що кібератаки на інформаційні ресурси в систем відбуваються на деякому інтервалі $[t_0,\mathrm{T}]$, а поточний час t перебування системи в інформаційному конфлікті в обирається з умов $t\in[t_0,T]$. Обмеження на інтенсивності потоків кібератак $\lambda_j(t)$ та на інтенсивність захисних дій $\gamma_j(t)$ подано виразами вигляду

$$0\le\lambda_j\le\lambda_{j\max},\ 0\le\gamma_j\le\gamma_{j\max}, \qquad (3)$$

де $\lambda_{j\max}$, $\gamma_{j\max}$ – максимальні інтенсивності потоків кібератак і захисних дій відповідно $j=0,1,\ldots6$.

Розв'язання системи диференціальних рівнянь (1) з початковими умовами (2) можна достатньо ефективно реалізувати шляхом застосування диференціальних перетворень Пухова [3], що може бути представлено відповідними математичними прямого і зворотного диференційного перетворення як

$$X(k)=\underline{x}(k)=\frac{H^k}{k!}\left[\frac{d^k x(t)}{dt^k}\right]_{t=0} \quad \dot{-} \quad x(t)=\sum_{k=0}^{k=\infty}\left(\frac{t}{H}\right)^k X(k), \qquad (4)$$

де $x(t)$ – функція-оригінал, що представляє собою безперервну, нескінченне число раз диференційовану функцію аргументу t яка обмежена разом з усіма своїми похідними; $X(K)$ – функція цілочислового аргументу K, що представляє собою диференціальне зображення оригіналу; H – масштабна постійна, що має ту ж розмірність що й аргумент t і вибирається, як правило в діапазоні $0\le t\le H$ на якому розглядається функція оригінал $x(t)$; $\dot{-}$ – символ відповідності між оригіналом $x(t)$ і диференціальним зображенням $X(K)$, $(K=0,1,2,\ldots)$. На основі перетворень Пухова (4) представимо систему рівнянь (1) в сфері диференціальних зображень у вигляді Т-моделі наступним чином

$$P_0(k+1)=\frac{H}{k+H}\left[\lambda_1P_5(k)+\lambda_2P_4(k)+\lambda_3P_3(k)+\lambda_4P_2(k)+\gamma_0P_1(k)+\beta_1P_0(k)\right],$$

$$P_1(k+1)=\frac{H}{k+H}\left[\lambda_0P_0(k)-\gamma_0P_1(k)\right],$$

$$P_2(k+1)=\frac{H}{k+H}\left[\lambda_7P_6(k)+\gamma_4P_0(k)+\gamma_6P_5(k)+\beta_2P_2(k)\right],$$

$$P_3(k+1)=\frac{H}{k+H}\left[\lambda_8P_4(k)+\gamma_3P_0(k)+\beta_3P_3(k)\right],\ P_4(k+1)=\frac{H}{k+H}\left[\lambda_{11}P_5(k)+\gamma_2P_0(k)+\gamma_8P_3(k)+\beta_4P_4(k)\right], \qquad (5)$$

$$P_5(k+1)=\frac{H}{k+H}\left[\lambda_6P_2(k)+\gamma_1P_0(k)+\beta_5P_5(k)\right],$$

$$P_6(k+1)=\frac{H}{k+H}\left[\lambda_{13}P_3(k)+\gamma_7P_2(k)+\beta_6P_6(k)\right],$$

де $-\beta_1=-(\lambda_0+\gamma_1+\gamma_2+\gamma_3+\gamma_4)$; $\beta_2=-(\lambda_4+\lambda_6+\gamma_7)$, $\beta_3=-(\lambda_3+\lambda_{13}+\gamma_8+\gamma_{13})$, $\beta_4=-(\lambda_2+\lambda_8+\gamma_{11})$, $\beta_5=-(\lambda_1+\lambda_{11}+\gamma_6+\gamma_{11})$, $\beta_6=-(\lambda_7+\gamma_{13})$.

Застосувавши диференційні перетворення (4) для початкових умов (2) системи диференціальних рівнянь (1) одержимо при $t_0=0$ і, відповідно, $k=0$ початкові умови в області Т-зображень у вигляді

$$P_0(0)=P_0(t_0)=1,\ P_i(0)=P_i(t_0)=0,\ i=1,2,\ldots,6. \qquad (6)$$

Системи диференціальних Т-рівнянь (5), поданих у вигляді сукупності алгебричних залежностей, є базовими для визначення величин ймовірностей $P_0(t),P_1(t),\ldots,P_6(t)$ вузлів графа моделі кібератак на інформаційні ресурси локальної обчислювальної мережі тягової підстанції. Реалізувавши підстановку в систему Т- рівнянь (5) значення цілочислового аргументу $k=0,1,2$, одержимо спектр дискрет $P_i(1),P_i(2),P_i(3)$, $i=1,2,\ldots,6$ які в сукупності і представляють рішення цієї системи в Т-області. Для визначення рішення $P_0(t),P_1(t),\ldots,P_6(t)$ в області оригіналів, тобто

дійсного аргументу t, необхідно зробити підстановки отриманого спектру дискрет $P_i(1), P_i(2), P_i(3), i=1,2,\ldots,6$ до зворотного перетворення Пухова згідно виразу (3).Завдяки тому, що початкові умови в області Т-зображень відомі і визначаються згідно (6), то, за аналогією до вищеописаного, реалізуємо підстановку в систему рівнянь (5) при $k=0$ значення Т-початкових умов (6) й одержимо

$$P_0(1)=H\beta_1,\ P_1(1)=H\lambda_0,\ P_2(1)=H\gamma_4,$$
$$P_3(1)=H\gamma_3, \qquad (7)$$
$$P_4(1)=H\gamma_2,\ P_5(1)=0,\ P_6(1)=0.$$

Реалізувавши підстановку в систему алгебричних залежностей (5) значення цілочислового аргументу $k=1$ та отриманих дискрет(5), одержимо відповідно спектр Т- дискрет $P_i(2),\ i=1,2,\ldots,6$ у вигляді

$$P_0(2)=\frac{H^2}{2}\left[\lambda_2\gamma_2+\lambda_3\gamma_3+\lambda_4\gamma_4+\lambda_0\gamma_0+\beta_1^2\right],$$
$$P_1(2)=\frac{H^2}{2}\left[\beta_1-\gamma_0\right]\lambda_0,$$
$$P_2(2)=\frac{H^2}{2}\left[\beta_1+\beta_2\right]\gamma_4,$$
$$P_3(2)=\frac{H^2}{2}\left[\lambda_8\gamma_2+\left(\lambda_0+\beta_3\right)\gamma_3\right], \qquad (8)$$
$$P_4(2)=\frac{H^2}{2}\left[\lambda_8\gamma_3+\left(\beta_1+\beta_4\right)\gamma_2\right],$$
$$P_5(2)=\frac{H^2}{2}\gamma_1\beta_1,$$
$$P_4(2)=\frac{H^2}{2}\left[\lambda_{13}+\gamma_4\right]\gamma_3.$$

Реалізував обчислення необхідної сукупності Т- дискрет $P_i(0),\ P_i(1),\ P_i(2)$, згідно з (5) і реалізувавши згідно з виразом (4) зворотне перетворення, визначимо шукані функції – оригінали $P_i(t)$, .. дійсного аргументу t які по суті і є рішення системи диференціальних рівнянь (1) в аналітичному вигляді, що можна записати в розгорнутому вигляді

$$P_i(t)=\sum_{k=0}^{k=\infty}\left(\frac{t}{H}\right)^k P_i(k)=P_i(0)+$$
$$\frac{t}{H}P_i(1)+\left(\frac{t}{H}\right)^2 P_i(2)+\ldots,\ i=1,2,\ldots,6. \qquad (9)$$

При рішенні системи диференційних рівнянь масштабну сталу H визначимо такою, що дорівнює тривалості T здійснення кібератак з інтенсивністю λ_j, тобто $H=T$. Тоді, на основі виразів (6), (8), (9) і застосовуючи зворотне перетворення отримаємо

$$P_i(t)=\sum_{k=0}^{k=\infty}\left(\frac{t}{T}\right)^k P_i(k),\ i=1,2,\ldots,6, \qquad (10)$$

подамо рішення системи диференціальних рівнянь в області оригіналівв аналітичному вигляді

$$P_0(t)=1+\beta_1 t+\left(\lambda_2\gamma_2+\lambda_3\gamma_3+\lambda_4\gamma_4+\lambda_0\gamma_0+\beta_1^2\right)\frac{t^2}{2},$$
$$P_1(t)=\lambda_0 t+\left(\beta_1-\gamma_0\right)\lambda_6\frac{t^2}{2},$$
$$P_2(t)=\gamma_4 t+\left(\beta_1-\beta_2\right)\gamma_4\frac{t^2}{2},$$
$$P_3(t)=\gamma_3 t+\left[\lambda_8\gamma_2+\left(\lambda_0+\beta_3\right)\gamma_3\right]\frac{t^2}{2}, \qquad (11)$$
$$P_4(t)=\gamma_2 t+\left[\lambda_8\gamma_3+\left(\beta_1+\beta_4\right)\gamma_2\right]\frac{t^2}{2},$$
$$P_5(t)=\gamma_1\beta_1\frac{t^2}{2},$$
$$P_6(t)=\left(\lambda_{13}-\gamma_4\right)\gamma_3\frac{t^2}{2}.$$

Отримавши значення ймовірностей $P_i(t)$, $i=1,2,\ldots,6$ для стану кожного з вузлів (див. рис. 1), формалізуємо критерій захищеності інформаційних ресурсів обчислювальних мереж тягових підстанцій залізниць у вигляді

$$\Theta_i(t)=\frac{1}{T}\int_{t=t_0}^{T}P_i(t)dt,\ i=1,2,\ldots,6. \qquad (12)$$

У локальнихобчислювальних мережах тягових підстанцій залізниць завдання безпеки інформаційних ресурсів вирішуються в умовах антагонізму суб'єктів інформаційного конфлікту. Зважаючи на це, домінуючим у таких умовах є дотримання суб'єктами конфлікту принципу мінімаксу. При реалізації процедур забезпечення безпеки інформації для гарантування досягнення системою заданих показників захищеності, раціонально дотримуватися стратегії формування таких значень γ_j, які мінімізують плату суб'єкта забезпечення безпеки $\Theta_i(\lambda_j,\gamma_j)$ за витрати відповідних ресурсів при максимальних інтенсивностях потоків кібератак, тобто

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

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

$$\Theta_i^*\left(\lambda_j,\gamma_j\right)=\max_{\lambda_j\in E_\lambda}\min_{\gamma_j\in E_\gamma}\Theta_i\left(\lambda_j,\gamma_j\right),\ i=1,2,\ldots,6. \quad (14)$$

За умови виконання рівності (13) і (14)

$$\min_{\gamma_j\in E_\gamma}\max_{\lambda_j\in E_\lambda}\Theta_i\left(\lambda_j,\gamma_j\right)= \max_{\lambda_j\in E_\lambda}\min_{\gamma_j\in E_\gamma}\Theta_i\left(\lambda_j,\gamma_j\right)=\Theta_i^{*opt}\left(\lambda_j^{\ opt},\gamma_j^{\ opt}\right), \quad (15)$$

шукані стратегії $\lambda_j^{\ opt}$ та $\gamma_j^{\ opt}$, називаються оптимальними. Стратегія забезпечення безпеки інформації 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 домінуючою стратегією забезпечення безпеки інформації буде стратегія на основі принципу мінімакса [5], тобто

$$\min_{\gamma_j\in E_\gamma}\max_{\lambda_j\in E_\lambda}\Theta_i\left(t,P_i(t),\lambda_j,\gamma_j\right). \quad (16)$$

У рамках прийнятих обмежень (3), застосування мінімаксної стратегії (16) дозволяє мінімізувати функціонал (11) навіть у випадках найгіршого сполучення інтенсивності потоків кібератак λ_j з довільним законом потоку інтенсивності з захисних дій γ_j. Застосувавши пряме перетворення (4) до функціоналу (12) і використавши обчислені згідно (4)–(8) значення сукупності Т-дискрет $P_0(t),P_1(t),\ldots,P_6(t)$, $i=1,2,\ldots,6$, реалізуємо процедуру оптимізації через дискрети диференціального спектра $P_i(k)$ у вигляді [3]

$$\Theta_i^*=\sum_{k=0}^{k=\infty}\frac{P_i(k)}{k+1}. \quad (17)$$

На основі обчислених дискрет(6)–(8), згідно з (17) при $i=0$ для S_0 - го вузла локальної мережі, тобто $P_0(k)$

$$\Theta_{i=0}^{\ *}\left(\lambda_j,\gamma_j\right)\approx 1+\frac{1}{2}\beta_1 T-\frac{1}{6}\left(\lambda_2\gamma_2+\lambda_3\gamma_3+\lambda_4\gamma_4+\lambda_0\gamma_0+\beta_1^{\ 2}\right)T^2. \quad (18)$$

Процес пошуку оптимальних стратегій інтенсивності потоків кібератак $\lambda_j^{\ opt}$ та потоку інтенсивності захисних дій $\gamma_j^{\ opt}$, з обмеженнями (3) функціоналу Θ_i^* невід'ємно пов'язаний з дослідженням його на екстремум шляхом підстановки в вираз (17) значень відповідних дискрет $P_i(t)$, $i=1,2,\ldots,6$. Відомо, що необхідними умовами існування екстремуму функціонала $\Theta_i^*\left(\lambda_j,\gamma_j\right)$ згідно теореми Куна-Такера,є умови, що дозволяють визначити оптимальну стратегію забезпечення безпеки інформації вигляду [4, 5]

$$\begin{cases}\dfrac{d}{d\gamma_0}\left(\Theta_0^*\left(\lambda_j,\gamma_j\right)\right)=0;\\ \ldots\\ \dfrac{d}{d\gamma_4}\left(\Theta_0^*\left(\lambda_j,\gamma_j\right)\right)=0;\\ \dfrac{d}{d\lambda_0}\left(\Theta_0^*\left(\lambda_j,\gamma_j\right)\right)=0;\\ \ldots\\ \dfrac{d}{d\lambda_4}\left(\Theta_0^*\left(\lambda_j,\gamma_j\right)\right)=0.\end{cases} \quad (19)$$

Реалізувавши підстановку $\Theta_{i=0}^{\ *opt}\left(\lambda_j,\gamma_j\right)$ згідно виразу (18) в систему рівнянь (19) і взявши відповідно частинні похідні одержимо систему лінійних алгебричних рівнянь, розв'язавши які і одержимо оптимальні стратегії $\lambda_j^{\ opt}$ та $\gamma_j^{\ opt}$. Знаки екстремумів у стратегіях $\lambda_j^{\ opt}$ та $\gamma_j^{\ opt}$ визначаються на основі перевірки достатніх умов

$$\begin{cases}\dfrac{d^2}{d\gamma_0^{\ 2}}\left(\Theta_0^*\left(\lambda_j,\gamma_j\right)\right)>0;\\ \ldots\\ \dfrac{d^2}{d\gamma_4^{\ 2}}\left(\Theta_0^*\left(\lambda_j,\gamma_j\right)\right)>0;\\ \dfrac{d^2}{d\lambda_0^{\ 2}}\left(\Theta_0^*\left(\lambda_j,\gamma_j\right)\right)<0;\\ \ldots\\ \dfrac{d^2}{d\lambda_4^{\ 2}}\left(\Theta_0^*\left(\lambda_j,\gamma_j\right)\right)<0.\end{cases} \quad (20)$$

Проводячи дослідження за аналогією, тобто, підставивши значення $\Theta_{i=0}^{\ *opt}\left(\lambda_j,\gamma_j\right)$ із (18) в систему рівнянь (20) і взявши другі частинні похідні,отримують систему алгебричних рівнянь рішення яких показує на виконання або невиконання достатніх умов. Обчисливши значення оптимальних стратегій $\lambda_j^{\ opt}$ та $\gamma_j^{\ opt}$ згідно (19), що відповідають умовам (20) і підставивши їх в (18) визначається рівень захищеності інформації S_0 - го вузла графа, що відображає локальну обчислювальну мережу управління електропостачанням тягової підстанції.

ВИСНОВКИ

1. Проведено аналіз комплексної проблеми забезпечення безпеки інформації локальних об-

числювальних мереж тягових підстанцій залізниць орієнтованих для керування в реальному часі швидкоплинниммитехнологічними процесами постачання електроенергії на тягу. Показано, що загальновизнаним у світі є напрямок пов'язаний з інтелектуалізацією обчислювальних мереж, як основи для покращення безпеки руху залізничного транспорту й створення перспективних енергозберігаючих технологій електроспоживання, який досягається у тому числі й за рахунок створення та впровадження математичних моделей, комп'ютерно-орієнтовних методів і апаратно-програмних засобів спеціального призначення.

2. Запропоновано логічну структуру локальної обчислювальної мережі оперативного управління електропостачанням у вигляді графа, що відображає топологічні характеристики тягової підстанції і розробленої математичну модель у вигляді системи диференціальних рівнянь Колмогорова-Чепмена для визначення множини ймовірностей стану відповідно до вузлів графа і характеристик локальної мережі тягової підстанції. Створена модель є основою для організації інформаційнозахищених обчислювальних мереж та реалізації прогресивних ІТ- засобів енергозбереження і безпеки руху.

3. Використано сучасний математичний апарат диференціальних перетворень Пухова для створення математичних диференціальних моделей, що представляють собоюТ-зображення диференційних рівнянь Колмогорова-Чепмена, завдяки чому відкрилась можливість достатньо просто отримати їх рішення в аналітичному вигляді для визначення ймовірностей станів вузлів графа локальної обчислювальної мережі тягової підстанції – як основи створення інтелектуальних засобів захисту інформаційних ресурсівлокальних обчислювальних мереж управління постачанням електроенергії на тягу залізницям.

4. На основі отриманих аналітичних значень ймовірностей стану вузлів графа сформульовано критерій забезпечення безпеки інформації і наведено стратегії її забезпечення на основі принципу мінімаксу, як пошук закону зміни потоку інтенсивності захисних дійпри стохастичній інтенсивності потоків кібератак. Показано процедури оптимізації в області Т-зображень з використанням дискрет диференційного спектра ймовірностей вузлів графа, а також наведено необхідні і достатні умови існування екстремуму, що дозволяють визначити оптимальну стратегію пошуку.

ЛИТЕРАТУРА

[1]. Стасюк О. І. Методи організації інтелектуальних електричних мереж залізниць на основі концепції SMARTGrid/ О. І. Стасюк, Л. Л. Гончарова, В. Ф. Максимчук // Інформаційно-керуючі системи на залізничному транспорті. – 2014, № 2 – С. 29–37.

[2]. Гончарова Л. Л. Информационные технологии мониторинга режимов электрических сетей на основе дифференциальных Т-моделей. / Л. Л. Гончарова // Інформаційно-керуючі системи на залізничному транспорті. – 2009.– № 4 – С. 93-97.

[3]. Пухов Г. Е. Преобразовании Тейлора и их применение в электротехнике и электронике /Г. Е. Пухов. – К. : «Наукова думска», 1978. – 259с.

[4]. Венцель Е.С. Исследованиеопераций – М.: «Сов.радио»ю, 1972. – 551 с.

[5]. Грищук Р. В. Теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальних ігор та диференціальних перетворень : монографія / Р. В. Грищук. – Житомир : РУТА, 2010. – 280 с.

[6]. Корченко О.Г. Системи захисту інформації/ О. Г. Корченко. – К. : НАУ, 2004. – 262 с.

[7]. Грищук Р. В. Атаки на інформацію в інформаційно-комунікаційних системах / Р. В. Грищук //Сучасна спеціальна техніка. – К. : ДНДІ МВС України, 2011. – № 1 (24). – С. 61–66.

[8]. Стасюк О.І. Методи синтезу розподілених комп'ютерно-інтегрованих мереж і технологій інтелектуалізації, моніторингу та оптимізації режимів електропостачання і енергозбереження залізниць/ О. І. Стасюк, Л. Л. Гончарова, В. Ф. Максимчук // Інформаційно-керуючі системи на залізничному транспорті. – 2015, № 1 – С. 23–34.

REFERENCES

[1]. Stasiuk O.I., Goncharova L.L., Maxymchuk V.F. Methods of railway smart grids organizations based on the SMART Grid concept, Information management systems for rail transport, 2014, № 2, P. 29-37.

[2]. Goncharova L.L. Information technology of electrical networks modes monitoring on the basis of differential T-models., Information management systems for rail transport., 2009, № 4, P. 93-97.

[3]. Pukhov G.E. Taylor transformations and their application in electrical engineering and electronics / G. E. Pukhov., K., "Scientific Thought", 1978, 259p.

[4]. Wenzel E.S. Research of operations, M. "Sov.radio" 1972, 551p.

[5]. Grischuk R.V. Theoretical basis of attacks on information processes modeling by methods of differential games and differential transformations theories: monograph, Zhitomir:: RUTA, 2010, 280 p.

[6]. Korchenko O.G. Information protection systems, K: NAU, 2004, 262 p.

[7]. Grischuk R.V. Attacks on the information in the information and communication systems, Modern special machinery., K: State Research Institute of MIA of Ukraine, 2011, № 1 (24), P. 61-66.

[8]. Stasiuk O.I., Goncharova L.L., Maxymchuk V.F. Methods of distributed computer integrated networks and technologies intellectualization

synthesis, monitoring and optimization of power and energy efficiency of railways, Information management systems for rail transport, 2015, № 1, P. 23-34.

МАТЕМАТИЧЕСКИЕ КОМПЬЮТЕРНО-ОРИЕНТИРОВАННЫЕ МОДЕЛИ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ ТЯГОВЫХ ПОДСТАНЦИЙ ЖЕЛЕЗНЫХ ДОРОГ

На основе проведенного анализа комплексной проблемы безопасности информационных ресурсов локальных вычислительных сетей тяговых подстанций железных дорог показано, что общепризнанным в мире является направление связанное с интеллектуализацией вычислительных сетей, как основы улучшения безопасности движения железнодорожного транспорта и создания перспективных энергосберегающих технологий электропотребления. Сформировано логическую структуру локальной вычислительной сети оперативного управления электроснабжением в виде графа, который отображает топологические характеристики тяговой подстанции, а также разработано его математическую модель в виде систем дифференциальных уравнений. Применены современные методы дифференциальных преобразований для определения вероятностей состояний узлов графа представляющего локальную вычислительную сеть тяговой подстанции. Сформулировано критерии безопасности информации и приведены стратегии ее обеспечения на основе принципа минимакса. Приведены необходимые и достаточные условия существования экстремума, что открывает возможность нахождения оптимальной стратегии поиска.

Ключевые слова: математические модели, компьютерно-ориентированные методы, Т-спектр, идентификация, анализ тяговые сети, электрические системы.

MATHEMATICAL COMPUTER-BASED MODELS OF RAILWAY TRACTION SUBSTATIONS COMPUTER NETWORKS INFORMATION SECURITY

Based on the analysis of the complex security issues of local area networks railway traction substations information resources shown that generally accepted in the world is the direction of intellectualization of computer networks, as a basis for improving the safety of railway transport and the development of advanced energy-saving technologies of electricity consumption. Formed logical structure of a local area network operational management of power supply in the form of a graph that displays the topological characteristics of traction substation, and also developed a mathematical model of it in the form of systems of differential equations. Applied modern methods of differential transformations to determine the probabilities of the states of nodes of the graph representing the local area network of traction substation. Formulated criteria for information security and provided strategies for ensuring the principle of minmax. The necessary and sufficient conditions for an extremum, which opens up the possibility of finding the optimal search strategy. Showed the necessary and sufficient conditions for an extremum, which opens up the possibility of finding the optimal search strategy.

Index terms: mathematical models, computer-oriented methods, T spectrum, identification, analysis traction network, electrical system.

Стасюк Олександр Іонович, доктор технічних наук, професор, лауреат Державної премії України в галузі науки і техніки, завідувач кафедри «Автоматизація та комп'ютерно-інтегровані технології транспорту», Державний економіко-технологічний університет транспорту.
E-mail: X177@ rambler.ru.
Стасюк Александр Ионович, доктор технических наук, профессор, лауреат Государственной премии Украины в области науки и техники, заведующий кафедрой «Автоматизация и компьютерно-интегрированые технологии транспорта», Государственный экономико-технологический университет транспорта.
Stasiuk Alexander, doctor of technical sciences, professor, laureate of the State Prize of Ukraine in Science and Technology, Head of Automation and Computer-Integrated Technologies of Transport department, State Economic and Technological University of Transport.

Грищук Руслан Валентинович, доктор технічних наук, старший науковий співробітник, начальник науково-дослідного відділу інформаційної та кібернетичної безпеки наукового центру Житомирського військового інституту імені С. П. Корольова.
E-mail: Dr.Hry@i.ua.
Грищук Руслан Вадентинович, доктор технических наук, старший научный сотрудник, начальник научно-исслежовательского отдела информационной и кибернетической безопасности научного центра Житомирского военного института им. С.П.Корольова.
Grischuk Ruslan, doctor of technical sciences, Senior Researcher, Zhytomyr military institute of S.P. Korolev chief research department of information and cyber security research.

Гончарова Лідія Леонідівна, кандидат технічних наук, доцент, доцент кафедри «Автоматизація та комп'ютерно-інтегровані технології транспорту», Державний економіко-технологічний університет транспорту.
E-mail: ktarael@jandex.ru.
Гончарова Лидия Леонидовна, кандидат технических наук, доцент, доцент кафедры «Автоматизация и компьютерно-интегрированые технологии транспорта», Государственный экономико-технологический университет транспорта.
Goncharova Lidiya, PhD in Eng., Associate Professor of Automation and Computer-Integrated Technologies of Transport department, State Economic and Technological University of Transport.