УДК 004.9

А.И. Стасюк, Л.Л. Гончарова, Г.М. Голуб

МЕТОДЫ ОЦЕНКИ КИБЕРБЕЗОПАСНОСТИ РАСПРЕДЕЛЕННЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ УПРАВЛЕНИЯ ЭЛЕКТРОПОТРЕБЛЕНИЕМ ДИСТАНЦИЙ ЭЛЕКТРОСНАБЖЕНИЯ

Введение

Процесс эволюции инновационно-инвестиционного преобразования систем электроснабжения железнодорожного транспорта как основы создания перспективных энергосберегающих технологий и организации безаварийных перевозок способствовал развитию интеллектуальных электрических сетей [1–3]. Интеллектуальные энергетические системы организуются формированием общесистемной информационной модели, на принципах единого информационного пространства и синхронного информационного взаимодействия, при взаимоинтеграции электросетевой топологии и архитектуры распределенной компьютерной сети управления электроснабжением. Синтезированные таким образом современные интеллектуальные системы электроснабжения открывают возможность не только оптимизировать процессы оперативного и стратегического управления электропотреблением, а также способны накапливать новые знания о железнодорожной энергетике для разработки новейших энергосберегающих и безаварийных технологий скоростных перевозок. В то же время опыт эксплуатации энергосистем показал, что неотъемлемая часть эффективного функционирования интеллектуальных сетей электроснабжения на тягу — организация надежной защиты информационных ресурсов [1–5, 6]. Внедрение и эксплуатация современных информационных технологий в электроэнергетике создали предпосылки появления спектра разнообразных способов, методов и средств защиты информационных ресурсов в компьютерных системах и сетях управления электроснабжением. Доминирующим в процессе защиты компьютерной информации является обеспечение целостности информационных ресурсов, доступа к ним при условии соответствия идентификаторов, определенных в соответствующей стратегии безопасности, а также физическое сохранение программных ресурсов, нейтрализация случайных или целенаправленных кибератак на информацию и идентификацию возможных нарушителей в целях формирования комплекса соответствующих средств защиты [4, 7, 8]. Для обеспечения необходимого уровня защищенности информационных ресурсов в интеллектуальных системах электроснабжения в процессе регистрации информации, передачи ее и переработки необходимы соответствующие специальные подсистемы, которые в режиме управления электроснабжением реализуют периодический и эпизодический контроль, а также оценку надежности системы, программно-аппаратных средств и информации.

Постановка проблемы

Обеспечение высокого уровня надежности и качества функционирования интеллектуальных компьютерных сетей дистанций электроснабжения на тягу тесно связано с решением проблемы кибернетической и информационной безопасности. Поскольку за основу идеологии организации интеллектуальных сетей электроснабжения взят принцип адекватности топологии дистанции электроснабжения и архитектуры распределенной компьютерной сети для реализации совокупности

процедур управления быстропротекающими технологическими процессами, организация безопасности информационных ресурсов предусматривает решение комплекса взаимообусловленных задач, связанных с обеспечением целостности информации, ее доступности и конфиденциальности. Поэтому неотъемлемая часть системы киберзащиты — способность ее в процессе функционирования интеллектуальной сети дистанции электроснабжения оценивать уровень эффективности программно-аппаратных средств защиты информационных ресурсов на основе критериев, позволяющих учитывать общие особенности спектра технических характеристик энергетического объекта, совокупность инженерных решений архитектурных особенностей компьютерной среды, возможных математических моделей и методов защиты. Эта особенность функционирования интеллектуальных сетей электроснабжения стимулировала возникновение широкого спектра научных исследований в области создания новых концептуальных подходов и разработку математических методов моделирования кибератак на информационные ресурсы. Сформулированные современные критерии оценки эффективности средств защиты открыли новый этап в области синтеза математических моделей, компьютерно-ориентированных методов и алгоритмов обеспечения безопасности повышенной устойчивости [3,4,7].

Цель настоящей публикации — разработка компьютерно-ориентированных математических моделей и методов, ориентированных на анализ интеллектуальных сетей дистанций электроснабжения железных дорог и оценку кибербезопасности информационных ресурсов как основы создания перспективных методов защиты информации.

Математическая модель оценки кибербезопасности

Интеллектуальная сеть дистанции электроснабжения реализует совокупность процедур управления быстропротекающими технологическими процессами снабжения электрической энергии на тягу путем проведения непрерывного скользящего мониторинга штатных и аномальных режимов системы электроснабжения, силового электрооборудования тяговых подстанций и систем релейной и микропроцессорной защиты. Логическая структура распределенной компьютерной сети интеллектуальной системы дистанции электроснабжения, что отражает ее топологические характеристики, может быть представлена в виде графа, как показано на рисунке. Узлы графа — это компьютерные средства, функционально-ориентированные на выполнение тех или иных функций, как показано на рисунке. Интенсивность потока атак представлена величиной $q(t)$, а интенсивность потока защитных действий — $Z(t)$. Совокупность потоков $q(t)$, $Z(t)$, протекающих в системе, — основа перехода ее из одного состояния в другое, которую будем относить к классу Пуассоновских [5].

Для исследования компьютерной архитектуры всережимной системы управления дистанции электроснабжения, представленной в виде графа (см. рисунок), синтезируем математическую модель для определения, в первую очередь, вероятностей $P_0(t)$, $P_1(t)$, $P_2(t)$, $P_3(t)$, $P_4(t)$, $P_5(t)$, $P_6(t)$, $P_7(t)$, $P_{21}(t)$, $P_{22}(t)$, $P_{23}(t)$ состояния узлов системы. Запишем систему уравнений Колмогорова, используя для этого необходимый набор правил и формул [6, 9]:

$$\frac{dP_0(t)}{dt} = q_1P_1(t) + q_2P_2(t) + q_3P_3(t) + q_4P_4(t) + q_0P_6(t) - (Z_0 + Z_1 + Z_2 + Z_3 + Z_4)P_0(t),$$

$$\frac{dP_1(t)}{dt} = Z_1P_0(t) + q_1P_1(t),$$

$$\frac{dP_2(t)}{dt} = Z_2P_0(t) + Z_8P_7(t) + Z_{10}P_3(t) + Z_{21}P_{21}(t) + Z_{22}P_{22}(t) +$$

$$+Z_{23}P_{23}(t)-(q_2+q_8+q_2+q_{10}+q_{21}+q_{22}+q_{23})P_2(t),$$

$$\frac{dP_3(t)}{dt}=Z_3P_0(t)+Z_9P_4(t)+q_{10}P_2(t)-(q_3+q_9+Z_{10})P_3(t),$$

$$\frac{dP_4(t)}{dt}=q_5P_5(t)+q_9P_3(t)+Z_4P_0(t)-(q_4+Z_5+Z_9)P_4(t),$$

$$\frac{dP_5(t)}{dt}=q_6P_6(t)+Z_5P_4(t)-(q_5+Z_6)P_5(t), \qquad (1)$$

$$\frac{dP_6(t)}{dt}=q_7P_7(t)+Z_0P_0(t)+Z_6P_5(t)-(q_0+q_6+Z_7)P_6(t),$$

$$\frac{dP_7(t)}{dt}=q_8P_2(t)+Z_7P_6(t)-(q_7+Z_8)P_7(t),$$

$$\frac{dP_{21}(t)}{dt}=q_{21}P_2(t)-Z_{21}P_{21}(t),$$

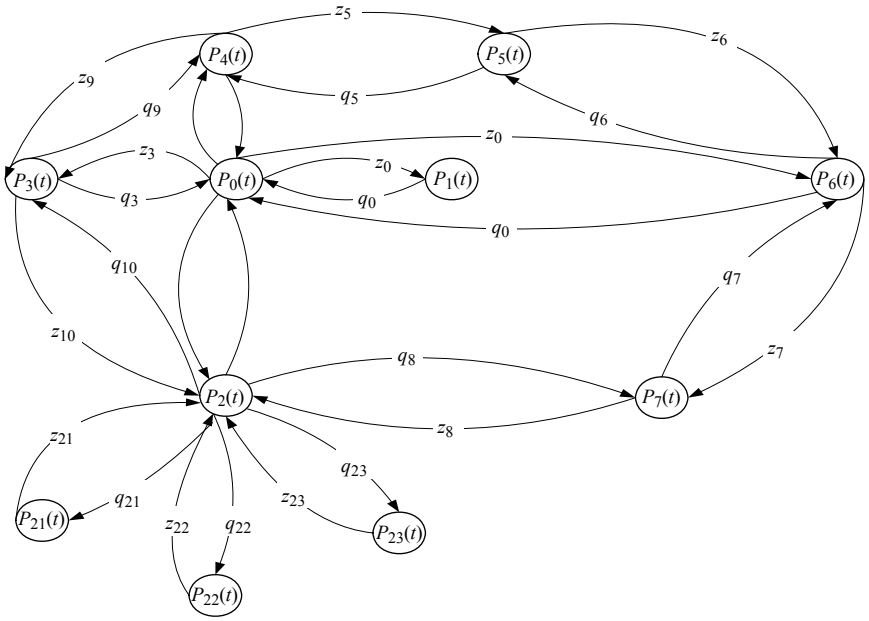
$$\frac{dP_{22}(t)}{dt}=q_{22}P_2(t)-Z_{22}P_{22}(t),$$

$$\frac{dP_{23}(t)}{dt}=q_{23}P_2(t)-Z_{23}P_{23}(t)$$

с соответствующими начальными условиями:

$$P_0(t_0)+P_1(t_0)+...+P_7(t_0)+P_{21}(t_0)+P_{22}(t_0)+P_{23}(t_0)=1,\ \ t_0=0,$$

$$P_0(t_0)=1,\ \ P_1(t_0)+P_2(t_0)+...+P_7(t_0)+P_{21}(t_0)+P_{22}(t_0)+P_{23}(t_0)=0.$$



Примечание: $P_0(t)$ — узел, представляющий собой центральный сервер управления на уровне дистанции электроснабжения; $P_1(t)$ — узел сервера базы данных и формирования единого информационного пространства; $P_2(t)$ — центральный узел связи; $P_3(t)$ — узел связи с Internet; $P_4(t)$ — узел сервера оперативного диспетчерского управления электроснабжением; $P_5(t)$ — узел, представляющий собой сервер проведения мониторинга в железнодорожной энергетике; $P_6(t)$ — узел формирования отчетных документов; $P_7(t)$ — узел интеллектуальной обработки и защиты информации; $P_{21}(t)$, $P_{22}(t)$, $P_{23}(t)$ — узлы связи с соответствующими локальными вычислительными сетями тяговых подстанций.

Используя положения теории дифференциальных преобразований, представим систему уравнений (1) в области изображений в виде дифференциальной математической модели. Для этого применим дифференциальные преобразования Пухова, выраженные следующей парой математических зависимостей [7]:

$$P_i(k) = \frac{H^k}{k!}\left[\frac{d^k P_i(t)}{dt^k}\right]_{t=0} \doteq P_i(t) = \sum_{k=0}^{k=\infty}\left(\frac{t}{H}\right)^k P_i(k). \qquad (2)$$

Здесь $P_i(t)$ — первоначальная функция аргумента t, которую можно n раз дифференцировать и которая имеет ряд соответствующих ограничений, включая свои производные; $P_i(k)$ — дифференциальное T-изображение первоначальной функции $P_i(t)$; H — масштабный коэффициент, размерность которого совпадает с размерностью аргумента t, как правило, выбирается на условиях $0 \le t \le H$ на всем диапазоне функции-оригинала $P_i(t)$; $\doteq$ — символ соответствия между функцией-оригиналом $P_i(t)$ и его дифференциальным T-изображением $P_i(k)$.

Благодаря прямому дифференциальному преобразованию, что находится слева от символа $\doteq$, формируется дифференцированное T-изображение функции-оригинала $P_i(t)$ в виде дискретной функции целочисленного аргумента $k = 0, 1, 2, ...$ На основе совокупности значений T-дискрет функции целочисленного аргумента $P_i(k)$, $k = 0, 1, 2, ...$, используя обратное дифференциальное преобразование, которое находится справа от символа $\doteq$, получим функции оригинала (t). Заметим, что при $k = 0$ согласно (2) для любого мгновенного значения t каждого i-го параметра выполняется соответствующее равенство $P_i(t) = P_i(k)$.

На основе выражения (2) сформируем дифференциальную математическую модель для исследования компьютерной сети всережимной системы управления дистанции электроснабжения железных дорог в следующем виде [4, 8]:

$$P_0(k+1) = \frac{H}{k+1}[q_1P_1(k) + q_2P_2(k) + q_3P_3(k) + q_4P_4(k) + q_0P_6(k) - \beta_1P_0(k)],$$

$$P_1(k+1) = \frac{H}{k+1}[Z_1P_0(k) - q_1P_1(k)],$$

$$P_2(k+1) = \frac{H}{k+1}[Z_2P_0(k) + Z_8P_7(k) + Z_{10}P_3(k) +$$

$$+ Z_{21}P_{21}(k) + Z_{22}P_{22}(k) + Z_{23}P_{23}(k) - \beta_2P_2(k)],$$

$$P_3(k+1) = \frac{H}{k+1}[Z_3P_0(k) + Z_9P_4(k) + q_{10}P_2(k) - \beta_3P_3(k)],$$

$$P_4(k+1) = \frac{H}{k+1}[q_5P_5(k) + q_9P_3(k) + Z_4P_0(k) - \beta_4P_4(k)],$$

$$P_5(k+1) = \frac{H}{k+1}[q_6P_6(k) + Z_5P_4(k) - \beta_5P_5(k)], \qquad (3)$$

$$P_6(k+1) = \frac{H}{k+1}[q_7P_7(k) + Z_0P_0(k) + Z_6P_5(k) - \beta_6P_6(k)],$$

$$P_7(k+1)=\frac{H}{k+1}[q_8P_2(k)+Z_7P_6(k)-\beta_7P_7(k)],$$

$$P_{21}(k+1)=\frac{H}{k+1}[q_{21}P_2(k)-Z_{21}P_{21}(k)],$$

$$P_{22}(k+1)=\frac{H}{k+1}[q_{22}P_2(k)-Z_{22}P_{22}(k)],$$

$$P_{23}(k+1)=\frac{H}{k+1}[q_{23}P_2(k)-Z_{23}P_{23}(k)]$$

с начальными условиями, которые в области дифференциальных изображений представляются следующим образом: $P_0(t)=P_0(0)=1$, $P_i(t)=P_i(0)=0$, $P_{2i}(t)=P_{2i}(0)=0$, $k=0$, $t_0=0$, $i=0,1,2,\ldots$, где $\beta_1=(Z_0+Z_1+Z_2+Z_3+Z_4)$; $\beta_2=(q_2+q_8+q_{10}+$ $+q_{21}+q_{22}+q_{23})$; $\beta_3=(q_3+q_9+q_{10})$; $\beta_4=(q_4+Z_5+Z_9)$; $\beta_5=(q_5+Z_6)$; $\beta_6=$ $=(q_0+q_6+Z_7)$; $\beta_7=(q_7+Z_8)$.

Полученная дифференциальная математическая модель (3) — основа для определения в аналитическом виде значений вероятностей $P_0(t)$, $P_1(t)$, $P_2(t)$, $P_3(t)$, $P_4(t)$, $P_5(t)$, $P_6(t)$, $P_7(t)$, $P_{21}(t)$, $P_{22}(t)$, $P_{23}(t)$ состояния узлов компьютерной архитектуры всережимной системы управления дистанции электроснабжения на тягу, представленной в виде графа на рисунке.

После выполнения подстановки значений начальных условий $P_0(t)=P_0(0)=1$, $P_i(t)=P_i(0)=0$, $P_{2i}(t)=P_{2i}(0)=0$, $k=0$, $t_0=0$, $i=0,1,2,\ldots$, в дифференциальную математическую зависимость, представленную выражением (3), при $k=0$, получим спектр дискрет $P_i(1)$, $P_{2i}(1)$:

$$P_0(1)=-H\beta_1,\ P_1(1)=HZ_1,\ P_2(1)=HZ_2,\ P_3(1)=HZ_3,\ P_4(1)=HZ_4,$$

$$P_5(1)=0,\ P_6(1)=HZ_0,\ P_7(1)=0,\ P_{21}(1)=0,\ P_{22}(1)=0,\ P_{23}(1)=0.$$

Проведя аналогичную операцию при $k=1$, т.е. реализовав подстановку полученных значений $P_i(1)$, $P_{2i}(1)$ в систему уравнения (3), получим спектр значений $P_i(2)$, $P_{2i}(2)$:

$$P_0(2)=\frac{H^2}{2}[q_1Z_1+q_2Z_2+q_3Z_3+\beta_1^2],\ P_1(2)=\frac{H^2}{2}Z_1(\beta_1+Z_1),$$

$$P_2(2)=\frac{H^2}{2}[Z_{10}Z_3-Z_2(\beta_1+\beta_2)],\ P_3(2)=\frac{H^2}{2}[q_{10}Z_2+Z_9Z_4-Z_3(\beta_1+\beta_3)],$$

$$P_4(2)=\frac{H^2}{2}[Z_9Z_3-Z_4(\beta_1+\beta_4)],\ P_5(2)=\frac{H^2}{2}[q_6Z_0+Z_5Z_4],$$

$$P_6(2)=\frac{H^2}{2}Z_0(\beta_1+\beta_6),\ P_7(2)=\frac{H^2}{2}(q_8Z_2+Z_7Z_0),$$

$$P_{21}(2)=\frac{H^2}{2}q_{21}Z_2,\ P_{22}(2)=\frac{H^2}{2}q_{22}Z_2,\ P_{23}(2)=\frac{H^2}{2}q_{23}Z_2.$$

Подставим полученные T-дискретами $P_i(0)$, $P_{2i}(0)$; $P_i(1)$, $P_{2i}(1)$; $P_i(2)$, $P_{2i}(2)$ в обратное дифференциальное преобразование $P_i(t)=\sum_{k=0}^{k=\infty}\left(\frac{t}{H}\right)^k P_i(k)$, бу-

дем иметь значения вероятностей $P_0(t)$, $P_1(t)$, $P_2(t)$, $P_3(t)$, $P_4(t)$, $P_5(t)$, $P_6(t)$, $P_7(t)$, $P_{21}(t)$, $P_{22}(t)$, $P_{23}(t)$ состояния узлов графа компьютерной сети, что в аналитическом виде можем записать так:

$$P_0(t) = 1 - \beta_1 t + \frac{t^2}{2}(q_1 Z_1 + q_2 Z_2 + q_3 Z_3 + \beta_1^2), \quad P_1(t) = Z_1 t - \frac{t^2}{2} Z_1(\beta_1 + t_1),$$

$$P_2(2) = Z_2 t \frac{t^2}{2}[Z_{10} Z_3 - Z_2(\beta_1 + \beta_2)], \quad P_3(t) = Z_3 t \frac{t^2}{2}[q_{10} Z_2 + Z_9 Z_4 - Z_3(\beta_1 + \beta_3)],$$

$$P_4(t) = Z_4 t \frac{t^2}{2}[q_9 Z_3 - Z_4(\beta_1 + \beta_4)], \quad P_5(t) = \frac{t^2}{2}[q_6 Z_0 + Z_5 Z_4], \tag{4}$$

$$P_6(t) = Z_0 t - \frac{t^2}{2} Z_0(\beta_1 + \beta_6) = \left[1 - \frac{t}{2}(\beta_1 + \beta_6)\right] Z_0 t, \quad P_7(t) = \frac{t^2}{2}(q_8 Z_2 + Z_7 Z_0),$$

$$P_{21}(t) = \frac{t^2}{2} q_{21} Z_2, \quad P_{22}(t) = \frac{t^2}{2} q_{22} Z_2, \quad P_{23}(t) = \frac{t^2}{2} q_{23} Z_2.$$

Сформированные значения вероятностей $P_0(t)$, $P_1(t)$, $P_2(t)$, $P_3(t)$, $P_4(t)$, $P_5(t)$, $P_6(t)$, $P_7(t)$, $P_{21}(t)$, $P_{22}(t)$, $P_{23}(t)$ состояния каждого узла графа, локальной сети управления дистанции электроснабжением используем для формирования критерия защищенности информационных ресурсов, что можно записать [2, 7, 9]

$$\Theta_i(t) = \frac{1}{2} \int_{t=t_0}^{T} P_i(t)\, dt, \quad i = 0, 1, 2, \ldots \tag{5}$$

Поскольку задачи безопасности информационных ресурсов в компьютерных сетях решаются в условиях антагонизма субъектов информационного конфликта, то несмотря на это, доминирующим в таких условиях является соблюдение субъектами конфликта принципа минимакса. Достижение системой заданных показателей защищенности возможно путем рационального определения стратегии формирования таких значений z_j, которые минимизируют плату субъекта обеспечения безопасности $\Theta_i(q_j, z_j)$ за истраченные соответствующие ресурсы при максимальной интенсивности потоков кибератак, т.е.

$$\Theta_i{}^*(q_j, z_j) = \min_{q_j \in E_q} \max_{z_j \in E_z} \Theta_i(q_j, z_j), \quad i = 0, 1, 2, \ldots \tag{6}$$

В процессе моделирования стратегии кибератак противоборствующие стороны вероятно исходят из условия формирования таких стратегий q_j, которые максимизируют плату $\Theta_i(q_j, z_j)$, при условии ее минимизации системой кибербезопасности z_j, т.е.

$$\Theta_i{}^*(q_j, z_j) = \min_{q_j \in E_q} \max_{z_j \in E_z} \Theta_i(q_j, z_j), \quad i = 0, 1, 2, \ldots \tag{7}$$

Очевидно, что при условии выполнения выражений (6) и (7)

$$\min_{z_j \in E_z} \max_{q_j \in E_q} \Theta_i(q_j, z_j) = \max_{q_j \in E_q} \min_{z_j \in E_z} \Theta_i(q_j, z_j) = \Theta_i^{*\mathrm{opt}}(q_j^{\mathrm{opt}}, z_j^{\mathrm{opt}}), \tag{8}$$

поисковые стратегии q_j^{opt} и z_j^{opt} называются оптимальными. Стратегия обеспечения безопасности информации заключается в поиске закона изменения потока интенсивности защитных действий z_j, которая реализует минимизацию функ-

ционала (5) при стохастической интенсивности потоков кибератак q_j в соответствующих пределах. Поэтому в связи с антагонизмом целей субъектов информационного конфликта доминирующей стратегией обеспечения безопасности информации будет стратегия на основе принципа минимакса [3, 8], т.е.

$$\min_{z_j \in E_z} \max_{q_j \in E_q} \Theta_i(t, P_i q_j, z_j). \tag{9}$$

Применение минимаксной стратегии (9) позволяет минимизировать функционал (5) даже в случаях наихудшего сочетания интенсивности потоков кибератак q_j с произвольным законом потока интенсивности по защитным действиям z_j. Применив прямое дифференциальное преобразование (2) к функционалу (5) и использовав вычисленные согласно (3), (4) значения совокупности *T*-дискрет $P_i(0)$, $P_{2i}(0)$; $P_i(1)$, $P_{2i}(1)$; $P_i(2)$, $P_{2i}(2)$, реализуем процедуру оптимизации дискретами дифференциального спектра $P_i(k)$ в виде [2, 7]

$$\Theta_i^* = \sum_{k=0}^{k=\infty} \left(\frac{P_i(k)}{k+1} \right). \tag{10}$$

На основе вычисленных, согласно выражению (10), дискрет $P_i(0)$, $P_{2i}(0)$; $P_i(1)$, $P_{2i}(1)$; $P_i(2)$, $P_{2i}(2)$ для каждого S_0-го узла локальной сети можно записать

$$\Theta_{i=0}{}^*(q_j, z_j) \approx 1 - \frac{1}{2}\beta_1 T - \frac{1}{6}(q_1 z_1 + q_2 z_2 + q_3 z_3 + \beta_1^2) T^2. \tag{11}$$

Процедура поиска оптимальных стратегий интенсивности потоков кибератак q_j^{opt} и потока интенсивности защитных действий z_j^{opt} функционала Θ_i^* неразрывно связана с исследованием его на экстремум путем подстановки в выражение (10) значений соответствующих дискрет: $P_i(0)$, $P_{2i}(0)$; $P_i(1)$, $P_{2i}(1)$; $P_i(2)$, $P_{2i}(2)$. Известно, что необходимые условия существования экстремума функционала $\Theta_i{}^*(q_j, z_j)$ по теореме Куна–Такера — условия, позволяющие определить оптимальную стратегию обеспечения безопасности информации вида [9, 10]

$$\begin{cases} \dfrac{d}{dz_0}(\Theta_0^*(q_j, z_j)) = 0, \\ \ldots\ldots \\ \dfrac{d}{dz_{23}}(\Theta_{23}^*(q_j, z_j)) = 0, \end{cases} \quad \begin{cases} \dfrac{d}{dq_0}(\Theta_0^*(q_j, z_j)) = 0, \\ \ldots\ldots \\ \dfrac{d}{dq_{23}}(\Theta_{23}^*(q_j, z_j)) = 0. \end{cases} \tag{12}$$

Реализовав в соответствии с (11) подстановку $\Theta_i^{*\text{opt}}(q_j, z_j)$ в систему уравнений (12) и взяв производные, получим систему линейных алгебраических уравнений, решив которые, получим оптимальные стратегии q_j^{opt} и z_j^{opt}. При этом знаки экстремумов в стратегиях q_j^{opt} и z_j^{opt} определяются на основе проверки достаточных условий путем

$$\begin{cases} \dfrac{d^2}{dz_0^2}(\Theta_0^*(q_j, z_j)) > 0, \\ \ldots\ldots \\ \dfrac{d^2}{dz_{23}^2}(\Theta_0^*(q_j, z_j)) > 0, \end{cases} \quad \begin{cases} \dfrac{d^2}{dq_0^2}(\Theta_0^*(q_j, z_j)) > 0, \\ \ldots\ldots \\ \dfrac{d^2}{dq_{23}^2}(\Theta_0^*(q_j, z_j)) > 0. \end{cases} \tag{13}$$

Проводя исследования по аналогии, т.е., подставив значения $\Theta_{i=0}^{*\text{opt}}(q_j, z_j)$ из (11) в систему уравнений (13) и взяв вторые производные, получим систему алгебраических уравнений, решение которых указывает на выполнение или невыполнение достаточных условий. Вычислив значение оптимальных стратегий q_j^{opt} и z_j^{opt} согласно (12), которые соответствуют условиям (13), и подставив их в (11), определим уровень защищенности информации S_0-го узла графа, отражающего локальную вычислительную сеть управления дистанции электроснабжением на тягу.

Заключение

Анализ комплексной проблемы обеспечения безопасности информации в локальных вычислительных сетях управления дистанциями электроснабжения показал, что это общепризнанное в мире направление, связанное с интеллектуализацией компьютерных сетей, как основы для улучшения безопасности движения железнодорожного транспорта, и создания перспективных энергосберегающих технологий электропотребления.

Разработана математическая модель локальной сети дистанции электроснабжения, представленной в виде графа и записанной системой дифференциальных уравнений Колмогорова–Чепмена для анализа локальных компьютерных сетей управления электропотреблением.

На основе теории дифференциальных преобразований Пухова предложена дифференциальная математическая модель для определения в аналитической форме вероятностей состояний узлов графа локальной вычислительной сети дистанции электроснабжения, как основы создания интеллектуальных средств защиты информационных ресурсов локальных компьютерных сетей.

Сформулирован критерий обеспечения безопасности информации и приведены стратегии киберзащиты на основе принципа минимакса, как поиск закона изменения потока защитных действий при стохастической интенсивности потоков кибератак. Приведены методы оптимизации в области *T*-изображений с использованием дискрет дифференциального спектра вероятностей узлов графа. Разработан метод определения стратегии поиска оптимума на основе приведенных необходимых и достаточных условий существования экстремума.

О.І. Стасюк, Л.Л. Гончарова, Г.М. Голуб

МЕТОДИ ОЦІНКИ КІБЕРБЕЗПЕКИ РОЗПОДІЛЕНИХ КОМП'ЮТЕРНИХ МЕРЕЖ УПРАВЛІННЯ ЕЛЕКТРОСПОЖИВАННЯМ ДИСТАНЦІЙ ЕЛЕКТРОПОСТАЧАННЯ

Аналіз проблеми кібербезпеки показав, що розв'язання її тісно пов'язане з рішенням комплексу взаємообумовлених задач та особливостей впливу топології кіберпростору. Запропоновано граф топології системи електроспоживання комп'ютерної мережі керування дистанцій електропостачання. На основі диференційних перетворень Пухова запропоновано математичні моделі кібербезпеки комп'ютерної мережі керування електропостачанням. Формалізовано критерій кібербезпеки і наведено принцип мінімакса для випадку найгіршого сполучення інтенсивності потоків кібератак і захисних дій. Розглянуто інтелектуальний метод пошуку оптимальної стратегії кібербезпеки шляхом дослідження на екстремум запропонованого функціонала.

A.I. Stasiuk, L.L. Goncharova, G.M. Golub

METHODS FOR ASSESSING THE CYBERSECURITY OF DISTRIBUTED COMPUTER NETWORKS OF CONTROL OF ELECTRICITY CONSUMPTION OF POWER SUPPLY DISTANCES

The analysis of the problem of cybersecurity showed that its solution is deeply connected with the solution of a set of interrelated tasks and the peculiarities of the influence of the topology of cyberspace. A graph showing the topology of the power consumption system of a computer network for controlling the power supply distance is proposed. On the basis of Pukhov differential transformations mathematical models of cybersecurity of a computer network of electric power supply control are offered. The criterion of cybersecurity is formalized and the minimax principle is given for the case of the worst combination of the intensity of cyber-attacks and defensive actions. An intellectual method of searching for an optimal cybersecurity strategy by examining the extremum of the proposed functional is considered.

1. *Стасюк А.И., Гончарова Л.Л., Максимчук В.Ф.* Методы организации интеллектуальных электрических сетей железных дорог на основе концепции SMART- Grid // Информационно-управляющие системы на железнодорожном транспорте. — 2014. — № 2. — С. 29–37.
2. *Стасюк А.И., Гончарова Л.Л.* Математические модели компьютерной интеллектуализации технологий синхронных векторных измерений параметров электрических сетей // Кибернетика и системный анализ. — 2016. — **52**, № 5. — С. 41–49.
3. *Стасюк А.И., Гончарова Л.Л.* Дифференциальные математические модели для исследования компьютерной архитектуры всережимной системы управления дистанцией электроснабжения железных дорог // Там же. — 2017. — **53**, № 1. — С. 184–192.
4. *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. 104–113.
5. *Буткевич А.Ф., Левконюк А.В., Стасюк А.И.* Повышение надежности мониторинга допустимости загрузок контролируемых сечений энергосистем // Техническая электродинамика. — 2014. — № 2. — С. 56–67.
6. *Стасюк А.И., Гончарова Л.Л.* Математические модели и методы компьютерного управления электроснабжением железных дорог на основе дифференциальных преобразований Пухова // Электронное моделирование. — 2016. — **38**, № 4. — С. 127–139.
7. *Пухов Г.Е.* Преобразования Тейлора и их применение в электротехнике и электронике. Київ : Наук. думка, 1978. — 259 с.
8. *Венцель Е.С.* Исследование операций. — М. : Сов. радио, 1972. — 552 с.
9. *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. — **48**, N 3. — P. 459–468.
10. *Opanasenko V.N., Kryvyi S.L.* Synthesis of adaptive logical networks on the basis of zhegalkin polynomials // Cybernetics and Systems Analysis. — 2015. — **51**, N 6. — P. 969–977.

Получено 27.03.2017