Баранов В.Л., д.т.н., профессор (ГУИКТ, Украина)
Молодецкая Е.В., аспирант
Baranov V.L.
Molodetska K.V.

ЧИСЛЕННО-АНАЛИТИЧЕСКИЙ МЕТОД МОДЕЛИРОВАНИЯ ДИНАМИЧЕСКИХ ПРОЦЕССОВ В СИСТЕМАХ ЗАЩИТЫ ИНФОРМАЦИИ
NUMERICAL-ANALYTICAL METHOD FOR MODELING OF DYNAMIC PROCESSES IN INFORMATION PROTECTION SYSTEMS

Предложен численно-аналитический метод моделирования нестационарных процессов в системах защиты информации. Метод основан на построении прямого и обратного дифференциальных спектров в области дифференциальных преобразований. Это позволяет повысить точность моделирования динамических процессов в области оригиналов.

There has been suggested a numerical-analytical method for modeling nonstationary processes in information security. The method is based on building direct and inverse differential spectra of differential change. This helps improve the accuracy of modeling of dynamic processes in the originals.

Интенсивное развитие технических систем защиты объектов информационной деятельности требует разработки нестационарных моделей процессов защиты информации и методов их моделирования. Известно множество математических моделей динамических процессов в системах защиты информации [1,2]. Большинство этих моделей описывается линейными дифференциальными уравнениями с постоянными параметрами, для которых существуют точные аналитические решения. Такие модели имеют узкую область применения, поскольку большинство динамических процессов в системах защиты информации описываются нелинейными дифференциальными уравнениями либо линейными дифференциальными уравнениями с переменными параметрами. Моделирование таких процессов реализуют на ЭВМ на основе применения численных методов решения дифференциальных уравнений. В случае анализа динамических процессов на больших временных интервалах численные методы проявляют численную неустойчивость, которая приводит к качественным изменениям моделируемого процесса.

<u>Анализ последних исследований и публикаций</u> [3,4] показал, что для решения проблемы численной неустойчивости разрабатываются новые численно-аналитические методы решения нелинейных дифференциальных уравнений на основе дифференциальных преобразований, предложенных академиком Г.Е. Пуховым.

<u>Целью работы</u> является разработка численно-аналитического метода моделирования динамических процессов на основе дифференциальных преобразований.

Рассмотрим математическую модель процессов защиты информации в техническом объекте (ТО) в векторном виде:

$$\frac{dP(t)}{dt} = f(t, P(t), \lambda(t), \mu(t)),\ P(0) = P_0,\ 0 \le t \le T, \tag{1}$$

где $P(t)$ - вектор вероятностей нахождения ТО в заданных состояниях,

$\lambda(t)$ - вектор интенсивностей защитных действий,

$\mu(t)$ - вектор интенсивностей атак,

P_0 - вектор начальных условий,

$[0,T]$ - интервал времени t моделирования динамического процесса,

f - заданная аналитическая функция.

Как показано в работе [2] векторы интенсивностей $\lambda(t)$ и $\mu(t)$ могут быть найдены на основе дифференциально-игрового метода моделирования процессов защиты информации. Поэтому систему (1) можно представить в виде:

$$\frac{dP(t)}{dt} = \varphi(t, P(t)),\; P(0) = P_0,\;\; 0 \le t \le t_m, \tag{2}$$

В случае моделирования системы (2) на значительном временном интервале применяют метод припасовывания на основе дифференциальных преобразований [4]. Временной отрезок $[0, t_m]$ разбиваем на n равных частей $H = \frac{t_m}{n}$.

Математическую модель (2) представляют в виде системы локальных векторных уравнений:

$$\frac{dP_i(t)}{dt} = \varphi_i(t, P_i(t)),\; P(0) = P_0, \tag{3}$$

где $i = 0,1,2...,n$.

К математической модели (3) применяют смещенные дифференциальные преобразования [4]:

$$P_i(k) = \frac{H^k}{k!}\left[\frac{d^k P(t)}{dt^k}\right]_{t=t_i}, \tag{4}$$

$$P_i(t) = \sum_{k=0}^{\infty}\left(\frac{t - t_i}{H}\right)^k P_i(k), \tag{5}$$

где k - целочисленный аргумент, принимающий значения $0,1,2,...,\infty$.

Систему локальных уравнений (3) переводят прямыми дифференциальными преобразованиями (4) в область изображений:

$$P_i(k+1) = \frac{H}{k+1}\Phi_i\big(T_i(k), P_i(k)\big),\; P(0) = P_0, \tag{6}$$

где Φ_i - изображение функции φ_i, $H = \frac{t_m}{n}$.

Рекуррентный вид выражения (6) позволяет последовательно вычислить дискреты дифференциального спектра $P_i(k+1)$, присваивая целочисленному аргументу k значения $0,1,2,...,\infty$.

Стыковка локальных уравнений выполняется по выражениям:

$$P_{i+1}(m) = \frac{H^m}{m!}\sum_{k=1}^{\infty} D^m P_i(k),\; m = 0,1,2,...,q. \tag{7}$$

где введено обозначение:

$$D^m P_i(k) = \frac{(k+m)!}{k!\,H^m} P_i(k+m). \tag{8}$$

После вычисления дискрет дифференциальных спектров $P_i(k+1)$ с помощью обратных дифференциальных преобразований (5) осуществляет перевод локальных векторов состояния $P_i(k)$ из области изображений во временную область $P_i(t)$.

Недостаток метода припасовывания (3)-(8) локальных уравнений заключается в накоплении погрешности в процессе обратных преобразований (5), так как количество дискрет дифференциального спектра ограничивается в процессе вычисления конечной величиной q. С целью достижения требуемой точности вычислений необходимо выбирать достаточно малый шаг H. Это приводит согласно выражению $n = \frac{T}{H}$ к резкому увеличению количества локальных уравнений n при $H \to 0$. В результате объем вычислений для моделирования нестационарного процесса на значительном временном интервале $\left[0,t_m\right]$ резко увеличивается и моделирование в реальном времени нестационарных процессов защиты информации становится проблемным.

С целью снижения объема вычислений и повышения точности моделирования предлагается усовершенствовать метод припасовывания следующим образом. Как в методе припасовывания разбиваем временной отрезок $\left[0,t_m\right]$ на n равных частей $H=\frac{t_m}{n}$. Математическую модель (2) представим в виде системы локальных векторных уравнений (3), которую рассмотрим в двух точках t_i и t_{i+1}, где $t_{i+1}=t_i+H$. К математической модели (3) применим смещенные дифференциальные преобразования в точке $t=t_i$:

$$P_i(k)=\frac{h^k}{k!}\left[\frac{d^kP(t)}{dt^k}\right]_{t=t_i}, \tag{9}$$

$$P_i(t)=\sum_{k=0}^{\infty}\left(\frac{t-t_i}{h}\right)^k P_i(k), \tag{10}$$

где $h=\frac{H}{2}$.

Система локальных уравнений (3) после дифференциальных преобразований (9) в области изображений принимает следующий вид:

$$P_i(k+1)=\frac{h}{k+1}\Phi_i(T_i(k),P_i(k)),\ P(0)=P_0, \tag{11}$$

где $i=0,1,2,...,n-1$.

Рекуррентное выражение (11) позволяет найти дифференциальные спектры $\mathrm{P_i(k)}$ в каждой точке $\mathrm{t_i}$. Эти дифференциальные спектры в дальнейшем будем называть прямыми дифференциальными спектрами, так как на их основе обратные дифференциальные преобразования (10) позволяют восстановить функцию $P_i(t)$ на отрезке $\left[t_i,t_i+h\right]$ при изменении временного аргумента t от точки t_i до точки t_i+h в направлении увеличения временного аргумента.

Систему локальных уравнений (3) переведем также в область изображений на основе смещенных дифференциальных преобразований в точке $t=t_{i+1}$:

$$P_{i+1}(k)=\frac{h^k}{k!}\left[\frac{d^kP(t)}{dt^k}\right]_{t=t_i+1}, \tag{12}$$

$$P_{i+1}(t)=\sum_{k=0}^{\infty}\left(\frac{t-t_{i+1}}{h}\right)^k P_{i+1}(k), \tag{13}$$

где $h=\frac{H}{2}$.

Применив дифференциальные преобразования (12) к системе локальных уравнений (3), получим ее изображение в виде:

$$P_{i+1}(k+1)=\frac{h}{k+1}\Phi_{i+1}(T_{i+1}(k),P_{i+1}(k)), \tag{14}$$

где $i=0,1,2,...,n$.

Обозначим нулевую неизвестную дискрету $P_{i+1}(0)$ символом P_{i+1}. По рекуррентному выражению (14) от начальной дискреты $P_{i+1}(0)=P_{i+1}$ рассчитаем дифференциальный спектр $P_{i+1}(k)$ в аналитическом виде, присваивая целочисленному аргументу k значения $0,1,2,...,q$.

Дифференциальный спектр $P_{i+1}(k)$ будем называть обратным дифференциальным спектром, так как он позволяет по выражению (13) восстановить функцию на отрезке $[t_i+h, t_i+2h]$ при уменьшении временного аргумента t от точки t_i+2h до точки t_i+h. Выберем в качестве точки сопряжения функции $P_i(t)$и $P_{i+1}(t)$ точку t_i+h. Тогда имеем:

$$P_i(t_i+h)=P_{i+1}(t_i+h). \tag{15}$$

Подстановка (10) при $t=t_i+h$ и (13) при $t=t_i+h$, $t_{i+1}=t_i+2h$ в выражение (15) дает уравнение для вычисления неизвестной величины $P_{i+1}=P_i(t_i+2h)=P_{i+1}(t_{i+1})$:

$$\sum_{k=0}^{\infty} P_i(k)=\sum_{k=0}^{\infty}(-1)^k P_{i+1}(k). \tag{16}$$

На практике вместо уравнения (16) используют приближенное уравнение, составленное из конечного количества дискрет дифференциальных спектров $P_i(k)$ и $P_{i+1}(k)$:

$$\sum_{k=0}^{q} P_i(k)\approx\sum_{k=0}^{q}(-1)^k P_{i+1}(k), \tag{17}$$

где $k=0,1,2,...,q$; $i=0,1,2,...,n-1$.

Учитывая, что выражение (10) описывает функцию $P_i(t)$ в виде ряда Тейлора, то приближенную оценку погрешности замены бесконечного ряда конечным можно выполнить по Коши и обоснованно выбрать значение q.

На основании выражения (17) численно-аналитическое моделирование динамического процесса (3) выполняют следующим образом. По выражению (11) при $i=0$ и $P(0)=P_0$ численно рассчитывают дифференциальный спектр $P_0(k)$. Затем по выражению (14) при $i=0$ и $P_1(0)=P_1$ аналитически формируют дифференциальный спектр $P_1(k)$.

Подстановка дифференциальных спектров $P_0(k)$ и $P_1(k)$ в выражение (17) при $i=0$ дает уравнение для вычисления неизвестной величины $P_1(t=H)=P_1$. Первый шаг вычислений завершен. Второй и все последующие шаги вычислений функции $P_i(t=iH)$ выполняются аналогичным образом. Например, на втором шаге вычислений при $i=1$, $P_1(0)=P_1(t=H)=P_1$ по рекуррентному выражению (11) численно рассчитывают дифференциальный спектр $P_1(k)$. Затем по выражению (14) при $i=1$, $P_2(0)=P_2$ аналитически определяют дифференциальный спектр $P_2(k)$. Подстановка дифференциальных спектров $P_1(k)$ и $P_2(k)$ в выражение (17) при $i=1$ дает уравнение для вычисления P_2. Дальнейшие вычисления выполняются аналогичным образом.

В работе [5] показано, что на одном шаге вычислений оценка сверху погрешности определения функции $P_i(iH)$ по уравнению (17) в 2^q раз меньше оценки сверху погрешности, которую дает метод припасовывания, где q – количество учитываемых дискрет дифференциальных спектров $P_i(k)$ и $P_{i+1}(k)$.

Выводы. Предложен численно-аналитический метод моделирования динамических процессов в системах защиты информации, который по сравнению с методом припасовывания снижает верхнюю оценку погрешности моделирования в 2^q раз, где q – количество учитываемых при моделировании дискрет дифференциальных спектров.

Литература

1. *Пархуць Л.Т., Хорошко В.А.* Нестационарные модели систем информационного обеспечения процессов защиты объектов // Защита информации: Сб. науч. трудов НАУ. – Спец. вып., 2008. – С. 224-228.

2. *Грищук Р.В.* Метод диференціально-ігрового Р-моделювання процесів нападу на інформацію//Інформаційна безпека: Матеріали наук.-практ. конф. (Україна, Київ, 26-27 березня 2009 р.)/Ред. кол. В.Г. Кривуца, В.О. Хорошко, М.Т. Корнійчук та ін. К.:ДУІКТ, 2009. – С.3-7.
3. *Баранов В.Л., Водоп'ян С.В., Костюченко Р.М.* Метод моделювання фізичних процесів на основі диференціальних перетворень нелінійних крайових задач//Вісник ЖДТУ. – 2007. – №2(41). – С.59-65.
4. *Пухов Г.Е.* Дифференциальные спектры и модели. – Киев: Наук. думка, 1990. – 184 с.
5. *Баранов В.Л., Баранов Г.Л., Фролова О.Г.* Порівняння методів моделювання динамічних процесів основними та зміщеними диференціальними перетвореннями//Проблеми інформатизації та управління: Зб. наук. пр. – Вип. 10. – К.:НАУ, 2004. – С.72-77.