2. *Гери М., Джонсон Д.* Вычислительные Машины и труднорешаемые задачи. – М.: Мир, 1982.
3. *Красный Д.Г.* Анализ эффективности модифицированного алгоритма Алексеева приближенного решения неоднородной распределительной задачи // Системный анализ, управление и обработка информации – Ростов-на-Дону: Изд-во ДГТУ, 2007, №1.
4. *Плотников В.Н., Зверев В.Ю.* Методы быстрого распределения алгоритмов в вычислительных системах // Техническая кибернетика. – 1974, №3.

УДК 681.3

А.В. Крупенин

МОДЕЛИРОВАНИЕ МЕТОДА ОЦЕНКИ ЭФФЕКТИВНОСТИ СИСТЕМЫ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ ИНФОРМАЦИОННОЙ СФЕРЫ АВТОМАТИЗИРОВАННЫХ СИСТЕМ В ЗАЩИЩЁННОМ ИСПОЛНЕНИИ

Эффективность функционирования автоматизированных систем в ЗИ будет полностью зависеть от подсистемы управления уровнем информационной безопасности, основой которой являются средства противодействия несанкционированному доступу (НСД).

НСД к автоматизированным системам критически важных объектов (КВО) может осуществляться террористическими или криминальными структурами в течении их функционирования в любые, произвольные моменты времени. Поэтому при разработке математического инструментария систем противодействия необходимо НСД учитывать как стохастический процесс.

Известно, что наиболее эффективным методом исследования стохастических процессов является математическое моделирование [1]. Среди методов математического моделирования наибольшее распространение получили методы имитационного и аналитического моделирования [1].

Указанные методы широко применяются в исследовании сложных систем, благодаря своей эффективности, оперативности и дешевизне по сравнению с их натурными испытаниями.

Вместе с тем, несмотря на неоспоримые достоинства, методы имитационного и аналитического моделирования процессов функционирования средств противодействия угрозам безопасности информационной сферы, каждая в отдельности обладают рядом недостатков.

К основным недостаткам имитационных моделей необходимо отнести невозможность учета всего многообразия параметров, описывающих поведение физической системы, что приводит, в некоторых случаях, к противоречивым результатам. Аналитические модели обладают невысокой адекватностью реальным процессам, из-за недостаточно полного учёта всех параметров реальной системы, а ограничиваясь лишь основными параметрами их функционирования.

Однако [3] комбинация аналитических и имитационных моделей может существенно упростить описание процесса, т.е. позволяет описать параметры классическими математическими методами и использовать их результаты с требуемой точностью и адекватностью моделируемым процессам при проведении имитационного моделирования, что обеспечивает низкую стоимость расчетов.

Например, основу математического описания могут составить формализованные процедуры мониторинга и защиты информационного пространства системы

управления ОВД. Каждая процедура соответствует конкретной возможности средств системы противодействия угрозам информационной сферы (СПУИС) по обеспечению её защищенности. При этом процедура противодействия угрозам безопасности $\Pi_K^{(no)}$ определяется как кортеж: $\Pi_K^{(no)} = \langle I\kappa,\ F_K\ ,\ \Psi_K \rangle$, в котором I_K – идентификатор *к*-ой процедуры; F_K – структурированное множество функций, реализующих *к*-ую процедуру; Ψ_K – временная характеристика *к*-ой процедуры противодействия угрозам безопасности, представляемая, в свою очередь, в виде кортежа:

$$\Psi_K = \langle \psi_K^{(1)}, \psi_K^{(2)}, \psi_K^{(3)}\ , \psi_K^{(4)} \rangle,$$

где $\psi_K^{(1)}$, $\psi_K^{(2)}$, $\psi_K^{(3)}$ и $\psi_K^{(4)}$ – характеристики случайного времени реализации K-ой процедуры.

На множестве $\{\Pi_K^{(no)}\}, \kappa = 1,2,\ldots,I, I = |\{\Pi_K^{(no)}\}|$ процедур определим отношение зацепленности между ними и опишем его матрицей вероятностей переходов $\|P\|$, определяющей порядок следования процедур. При этом для каждой строки матрицы справедливо условие: $\sum_{l=1}^{I} P_{Kl} = 1$.

Геометрическим изображением отношений зацепленности процедур является ориентированный граф [2]: $G = G(\{\Pi_K^{(no)}\}, \|P\|)$, множества вершин и дуг P_{Kl} которого совпадают с исходными множествами процедур $\{\Pi_K^{(no)}\}$ и отношений $\|P\|$ между ними, соответственно.

Множество F_K функций, реализующих процедуру $\Pi_K^{(no)}$, формально представляется в виде массива $\|\Omega_K\|$ их временных характеристик размерностью $|F_K| \times 4$. Каждая j-я строка матрицы ($j = 1,2,\ldots,|F_K|$) имеет вид:

$$\Omega_{Kj} = \langle \omega_{Kj}^{(1)}, \omega_{Kj}^{(2)}, \omega_{Kj}^{(3)}\ , \omega_{Kj}^{(4)} \rangle, \qquad (1)$$

где $\omega_{Kj}^{(1)}$, $\omega_{Kj}^{(2)}$, $\omega_{Kj}^{(3)}$ и $\omega_{Kj}^{(4)}$ – характеристики случайного времени реализации j-ой функции.

Определим на множестве (1) отношение операционной зацепленности между функциями $f_{Kj} \in F_K$, $j = 1, 2, \ldots, |F_K|$, и опишем его с помощью матрицы вероятностей переходов $\|p_{Kj}\|$, структура которой аналогична структуре матрицы $\|P\|$.

Геометрическим эквивалентом матричного описания отношений является ориентированный граф: $g_K = g_K(F_K, \|p_{Kj}\|)$, множество вершин которого совпадает с множеством (1) функций, а множество связей между вершинами - с множеством отношений между функциями.

Данный методический подход даёт возможность разработать комплексную математическую модель СПУИС и на её базе провести вычислительный эксперимент по оценке её типовых возможностей с различной структурой антивирусных средств.

Исходя из того, что нижний уровень структуры показателей эффективности СПУИС представляется временными показателями, а имитация смены состояний ориентированного графа, в соответствии с порядком выполнения функций, определяемым матрицей вероятностей переходов $\|p_{Kj}\|$, позволяет сформировать множество $C_{(q)}$ состояний, составляющих q-ю реализацию модели, то, в свою очередь, позволяет определить время выполнения процедуры, соответствующее данной реализации:

$$\tau^{(1)}_{K(q)} = \sum_{j=1}^{|F_K|} \delta_{Kj(q)} \cdot \tau_{Kj(q)}, \qquad (2)$$

где $\delta_{uj(q)} = \begin{cases} 1, \ если\, c_{Kj(q)} \in C_{(q)}, \\ 0, если\, c_{Kj(q)} \notin C_{(q)}, \end{cases}$

$\tau_{Kj(q)}$ – время, соответствующее времени выполнения функции F_{Kj} при q-ой реализации модели противодействия угрозам безопасности информационной сферы.

На рис. 1 приводится алгоритм выполнения имитационной программы противодействия. Содержание блок-схемы алгоритма обозначает следующее.

Блок 1. Ввод исходных данных. В качестве исходных данных при реализации алгоритма используются следующие двумерные массивы:

$\|\Omega\|$ – описание времен выполнения функций;

$\|p\|$ – порядок следования функций,

а также количество функций, составляющих процедуру $N = |F|$.

Блок 2. Обнуление элементов одномерного массива $\vec{\delta} = (\delta_1, \delta_2, \ldots, \delta_N)$.

Если в процессе моделирования какой-либо элемент массива равен единице, то это означает, что моделировалось выполнение функции, соответствующей данному элементу.

Блок 3. Установка счетчика номеров функций n и значения первого элемента массива $\vec{\delta}$ единичными.

Блок 4. Определение случайной величины Rand, равномерно распределенной в интервале (0;1).

Блоки 5-8. Определение разности: $d_l = |p_{nl} - Rand|$ между вероятностью перехода от заданной функции на остальные и значением Rand.

Блок 9. Определение минимального из значений $d_l, l = 1,2,\ldots,N$ и его номера (**Блоки 10-13**).

Блок 14. Установка номера следующей выполняемой функции и единицы в соответствующий элемент массива $\vec{\delta}$.

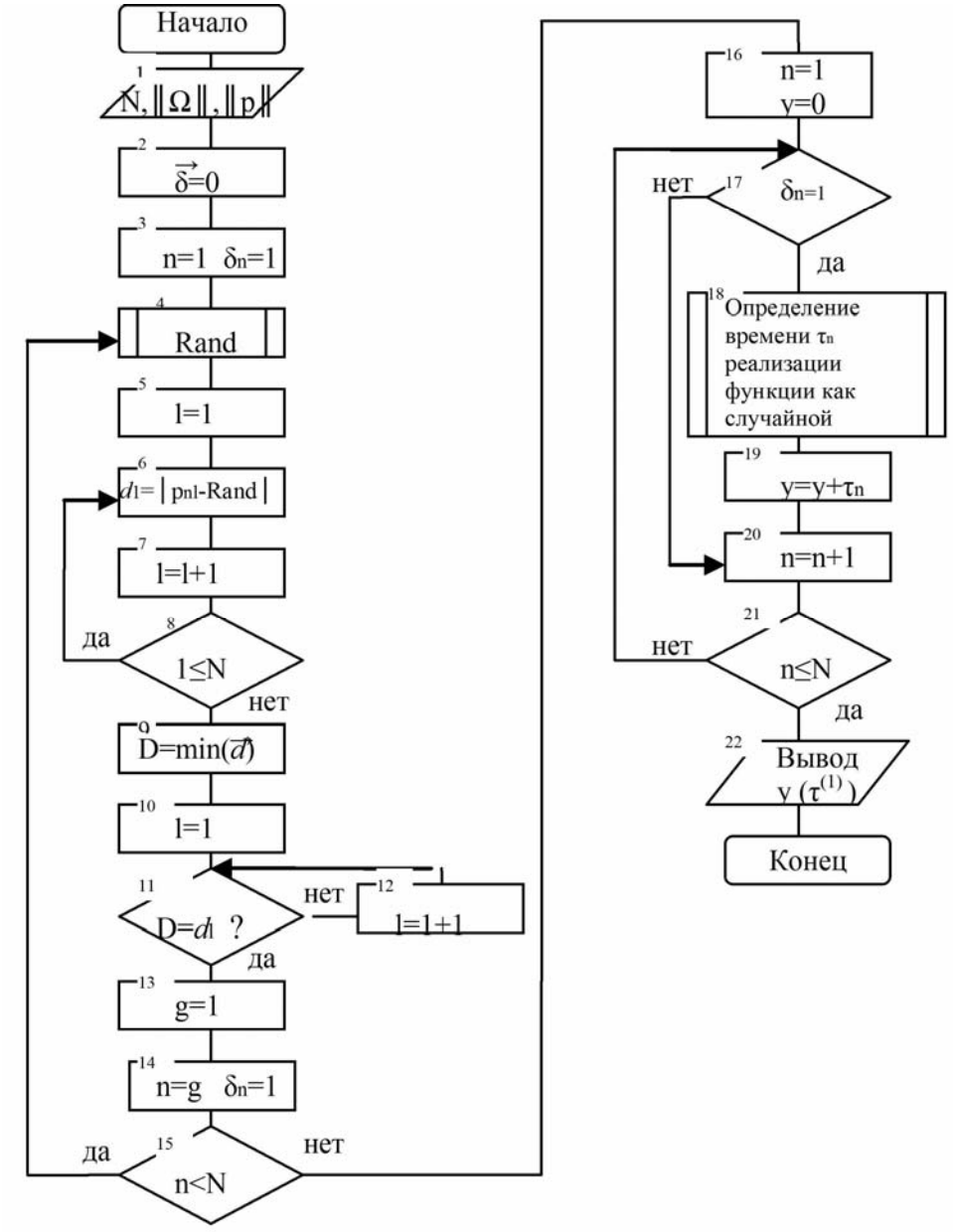

Рис. 1. Алгоритм моделирования процедуры противодействия угрозам информационной сферы

Блок 15. Анализ верхней границы массива $\|p\|$.

Блок 16. Установка в единицу счетчика n элементов в массиве $\vec{\delta}$ и в ноль значения времени $\tau^{(1)}$ выполнения процедуры.

Блок 17. Если элемент δ_n равен единице, то при выполнении процедуры n-я функция выполнялась, иначе переход на блок 20.

Блок 18. Определение времени τ_n реализации n-ой функции:

$$\tau_n = \begin{cases} \omega_n^{(2)} + \left(\omega_n^{(2)} + \omega_n^{(3)}\right) \cdot Rand, \text{ при равномерном законе распределения} \\ -\omega_n^{(2)} \cdot \ln\left(Rand\right), \text{ при экспоненциальном законе распределения} \\ \omega_n^{(2)} + \dfrac{1.73 \cdot \left(2 \cdot \sum_{l=1}^{6} Rand - 6\right)}{2.44} \cdot \omega_n^{(3)}, \text{ при нормальном законе распределения} \end{cases}$$

Блок 19. Накопление суммы значений времен выполненных функций.

Блок 20. Увеличение на единицу значения счетчика элементов массива $\vec{\delta}$.

Блок 21. Если просмотрены все N элементов массива $\vec{\delta}$, то переход на блок 22, иначе - на блок 17.

Блок 22. Вывод значения $\tau^{(1)}$ времени выполнения процедуры.

Множество $\left\{\tau^{(1)}_{\kappa,(q)}\right\}$, $q = 1,2,\ldots,Q$ реализаций процедуры является исходным для получения статистически устойчивых характеристик моделируемого процесса [4,5]. С этой целью производится аппроксимация получаемой выборки одним из типовых законов распределения: равномерным, экспоненциальным, нормальным по критерию Колмогорова-Смирнова [6].

В соответствии с алгоритмами формирования системы показателей эффективности СПУИС второй и последующий уровни её структуры представляются вероятностными показателями.

С целью построения математической модели для получения численных значений показателей второго уровня структуры воспользуемся методическим подходом, основанном на сходстве формы показателя вида $P(k < m)$ и классической функции распределения вероятностей.

Решение подобных задач моделирования известны [5]. Для нашего случая найдём аналитические выражения для показателей, аналогичных показателям вида (3).

В основу этих аналитических выражений положена известная обобщенная формула [5]:

$$P\left(k \le m\right) = 1 - P\left(m < k\right) = 1 - \int_0^{\overline{k}} f_{(m)}(x)\,dx \ , \qquad (3)$$

в которой

$$\overline{k} = \mu \circ \varphi = \int_0^{\infty} y \int_0^{\infty} f_{(\mu)}(y - z)\, f_{(\varphi)}(z)\,dz\,dy \ , \qquad (4)$$

где $f_{(\mu)}$, $f_{(\varphi)}$ и $f_{(m)}$ плотности распределений случайных величин μ, φ и m, соответственно.

Вместе с тем имеется ряд ограничений на применение выражений вида (4):

1) случайные величины μ и φ могут аппроксимироваться равномерным, экспоненциальным или нормальным законом распределения;

2) случайная величина времени m аппроксимируется экспоненциальным законом распределения;

3) величина $\bar{k}$ представляет собой комбинацию не более двух случайных величин:

$$\bar{k} = \mu \circ \varphi . \tag{5}$$

Ограничение 1 и 2 являются несущественными.

Ограничение 3 является существенным, так как, согласно формальному описанию структуры показателей эффективности СПУИС, время $\tau_m^{(2)}$, $m=1,2,\ldots,|\{y_m(w=2)\}|$, $\{y_m(w=2)\}\in\{z_j\}$ противодействия угрозам информационной сферы является комбинацией от двух до четырех случайных величин времени реализации средствами СПУИС своих функций.

С целью преодоления данного ограничения представим:

$$\tau_m^{(2)} = \sum_{h=1}^{H} \circ\, \tau_h^{(1)} = \tau_1^{(1)} \circ \sum_{h=2}^{H} \circ\, \tau_h^{(1)} = \tau_1^{(1)} \circ \mathrm{T}^{(1)} . \tag{6}$$

Представим второе слагаемое выражения (6) $\mathrm{T}^{(1)}$ как результат многократной реализации последовательности $\tau_2^{(1)}, \tau_3^{(1)}, \ldots, \tau_H^{(1)}$ случайных величин имитационной моделью, с последующей его аппроксимацией равномерным, экспоненциальным или нормальным законом распределения. Это позволит случайную величину $\tau_m^{(2)}$ представить через (3) следующим образом: $\tau_m^{(2)} = \tau_1^{(1)} \circ \mathrm{T}^{(1)} = \mu \circ \varphi$ и воспользоваться для ее определения известными соотношениями, приведенными в табл. 1, в которой использованы следующие обозначения:

Р – равномерный закон распределения вероятностей с минимальным значением $\mu_{\min}$ $(\varphi_{\min})$ и максимальным значением $\mu_{\max}$ $(\varphi_{\max})$;

Э – усеченный экспоненциальный закон распределения вероятностей со средним значением $\bar{\mu}(\bar{\varphi})$ и минимальным значением $\mu_{\min}$ $(\varphi_{\min})$;

Н – усеченный нормальный закон распределения вероятностей со средним значением $\bar{\mu}(\bar{\varphi})$, среднеквадратичным отклонением $\sigma_{(\alpha)}$ $(\sigma_{(\beta)})$ и минимальным значением $\mu_{\min}$ $(\varphi_{\min})$;

Ф – функция Лапласа.

Таблица 1

Используемые в аналитических расчетах законы распределения

		μ		
		Р	Э	Н
φ	Р	$\bar{k}=\frac{\mu_{\min}+\mu_{\max}}{2}+\frac{\varphi_{\min}+\varphi_{\max}}{2}$	$\bar{k}=\frac{(\varphi_{\max}-\varphi_{\min})}{2}\times\exp\left(\frac{\mu_{\min}}{\bar{\mu}}\right)$	$\bar{k}=\frac{(\varphi_{\max}+\varphi_{\min})}{4}\times\left[1+\Phi\left(\frac{\bar{\mu}-\mu_{\min}}{\sqrt{2}\cdot\sigma_{(\mu)}}\right)\right]$
	Э	$\bar{k}=\frac{(\mu_{\max}-\mu_{\min})}{2}\times\exp\left(\frac{\varphi_{\min}}{\bar{\varphi}}\right)$	$\bar{k}=\frac{\bar{\varphi}\cdot(\bar{\mu}+\mu_{\min})}{\bar{\mu}+\bar{\varphi}}\times\exp\left(\frac{\varphi_{\min}}{\bar{\varphi}}\right)$	$\bar{k}=\frac{\bar{\varphi}+\varphi_{\min}}{2}\times\exp\left(\frac{\sigma^2_{(\mu)}+2\cdot\bar{\mu}\cdot\bar{\varphi}}{2\cdot\bar{\varphi}^2}\right)\times\left[1+\Phi\left(\frac{\sigma^2_{(\mu)}+\mu\cdot\bar{\varphi}-\bar{\varphi}\,\mu_{\min}}{\sqrt{2}\cdot\bar{\varphi}\,\sigma_{(\mu)}}\right)\right]$
	Н	$\bar{k}=\frac{(\mu_{\max}+\mu_{\min})}{4}\times\left[1+\Phi\left(\frac{\bar{\varphi}-\varphi_{\min}}{\sqrt{2}\cdot\sigma_{(\mu)}}\right)\right]$	$\bar{k}=\frac{\bar{\mu}+\mu_{\min}}{2}\times\exp\left(\frac{\sigma^2_{(\mu)}+2\cdot\bar{\mu}\cdot\bar{\varphi}}{2\cdot\mu^2}\right)\times\left[1+\Phi\left(\frac{\sigma^2_{(\varphi)}+\bar{\mu}\cdot\bar{\varphi}-\bar{\mu}\cdot\varphi_{\min}}{\sqrt{2}\cdot\bar{\mu}\cdot\sigma_{(\varphi)}}\right)\right]$	$\bar{k}=\bar{\mu}+\bar{\varphi}$

Методика планирования вычислительного эксперимента. Исследования возможностей СПУИС с помощью разработанных алгоритмов структуризации частных показателей необходимо проводить методами вычислительных экспериментов в соответствии с предлагаемой методикой планирования:

1. Выбор типовых вариантов структуры СПУИС (рассматриваются все типовые варианты систем).

2. Формальное описание процедур противодействия угрозам безопасности критически важным сегментам информационной сферы (формулируется описание процедур противодействия).

3. Оценка временных характеристик отдельных процедур противодействия угрозам безопасности, как композиция соответствующих функций противодействия с использованием рассмотренных ранее математических моделей (определяем аналитические выражения для временных характеристик отдельных частных процессов).

4. Оценка показателей эффективности СПУИС первого уровня иерархии, согласно алгоритмов моделирования. Временные характеристики определяются в виде статистических выборок путем имитационного моделирования выполнения функций процедур противодействия угрозам безопасности. Полученные статистические выборки аппроксимируются типовыми законами распределения (равномерным, усеченным экспоненциальным и усеченным нормальным).

5. Рассчитываются показатели эффективности СПУИС второго уровня иерархии, согласно аналитическим моделям. Математические выражения при этом определяются на основе законов распределения временных характеристик процедур противодействия угрозам безопасности. При этом соответствующие вероятностные характеристики определяются на основе комбинаций временных показателей первого уровня иерархии.

6. Находятся показатели эффективности СПУИС третьего уровня иерархии.

7. Определяется интегральный (обобщенный) показатель эффективности СПУИС как показатель четвертого уровня иерархии и её частных показателей.

Заключение

1. В данной работе разработана методика аналитического описания информационных систем ОВД с учетом системы противодействия угрозам НСД в виде кортежа выполняемых процедур, которые описаны матрицей вероятностей переходов. В качестве геометрического эквивалента матричного описания отношений представлен ориентированный граф. Имитация смены состояний ориентированного графа позволяет сформировать множество состояний и определить время выполнения процедуры, соответствующее данной реализации.

2. На основе изложенного методического подхода разработана комплексная модель оценки СПУИС на базе совместного использования имитационного и аналитического моделирования, что минимизирует количество используемых формул, за счет того, что на уровне процедур противодействия угрозам реализуется аналитическими выражениями, а на уровне функций противодействия – имитационными моделями.

3. Разработан алгоритм для оценки СПУИС автоматизированных комплексов управления ОВД субъекта РФ и методика планирования вычислительного эксперимента.

Разработанный метод комбинированного моделирования позволяет осуществлять оптимальный выбор СПУИС из множества типовых средств при проектировании автоматизированных систем ОВД. При этом математическая модель обладает определенной универсальностью относительно времени реализации средствами своих функций, позволяя аппроксимировать его равномерным, экспоненциальным или нормальным законом распределения по критерию сходимости Колмогорова-Смирнова.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Моисеев Н.Н.* Математические задачи системного анализа. – М.: Наука, 1981. – 488 с.
2. *Татт У.* Теория графов / Пер. с англ. – М.: Мир, 1988. – 424 с.
3. *Золотарева Е.А.* Особенности синтеза математической модели для оценки показателей эффективности системы противодействия угрозам безопасности критически важным элементам информационной сферы // Современные проблемы борьбы с преступностью: Материалы Всероссийской научно-практ. конф., Часть 2. – Воронеж: Изд-во ВИ МВД России, 2003. – С. 54-55.
4. *Бусленко Н.П.* Моделирование сложных систем. – М.: Наука, 1978. – 400 с.
5. *Гнеденко Б.В.* Курс теории вероятностей: Учебник. – М.: Наука, 1988.
6. *Айзерман М.А., Малишевский А.В.* Некоторые аспекты общей теории выбора лучших вариантов // Автоматика и телемеханика. – 1982, № 2. – С. 65-83.

УДК 004.045

С.Г. Синица

МЕТОДЫ И МОДЕЛИ ГИБКОЙ РАЗРАБОТКИ ОПЕРАЦИЙ НАД РЕСУРСАМИ В КОЛЛЕКТИВНЫХ ИНФОРМАЦИОННЫХ СРЕДАХ*

Введение. Успешности внедрения информационных систем (ИС) способствует гибкая методология разработки и внедрения [1], основными чертами которой являются *обозримость содержания спецификации ИС* в форме, пригодной для удалённого согласования с заказчиком без привлечения ИТ-специалистов с его

* Работа выполнена при поддержке РФФИ (грант 06-07-96618).