УДК 004.056.5:004.052

А.О. Смагина, ассистент
Севастопольский национальный технический университет
ул. Университетская 33, г. Севастополь, Украина, 99053
E-mail: kvt@sevgtu.sebastopol.ua

СТАТИСТИЧЕСКАЯ ОЦЕНКА ВРЕМЕНИ ПРЕБЫВАНИЯ СИСТЕМЫ НЕОДНОРОДНОГО СОСТАВА В ВЫДЕЛЕННЫХ СОСТОЯНИЯХ ДЛЯ НЕСТАЦИОНАРНОГО РЕЖИМА

В статье решается задача организации защиты доступа в системах неоднородного состава. Рассматривается методика оценки времени пребывания в выделенных состояниях для нестационарного режима с целью повышения эффективности криптографической защиты.

Ключевые слова: *системы неоднородного состава, нестационарный режим, криптографическая защита.*

Функционирование современных человеко-машинных систем (ЧМС) требует специальной организации криптографической защиты доступа к их ресурсам. Такие системы часто становятся объектами противодействия со стороны конкурирующих структур, подвергаются действию вирусных атак, несанкционированных попыток проникновения и др. В процессе оценки состояния современных ЧМС требуется многократно принимать самые различные решения по степени ее работоспособности, производительности, помехозащищенности и т.п. Последовательность принимаемых решений в ряде случаев строго определена имеющимися техническими условиями, требованиями и регламентом. В некоторых иных случаях последовательность таких решений должна конструироваться оперативно с учетом складывающей ситуации и предыстории. Качество принимаемых решений зависит не только от квалификации экспертов по принятию решений, но и во многом определяется качеством априорной информации, имеющейся в их распоряжении. В то же время условия функционирования ЧМС все более усложняются, что во многом отражает характер современных рыночно-производственных отношений. В общем случае угрозы компьютерной безопасности можно условно разделить на два типа: пассивные и активные. К пассивным угрозам относят все действия, целью которых является раскрытие передаваемой информации (перехват и анализ потока данных), к активным – любое воздействие, приводящее к искажению и/или уничтожению передаваемой информации [1]. Известны работы, в которых деятельность ЧМС рассматривается и с точки зрения защиты информации, лежащей в основе организации их функционирования [2]. Существующие методики анализа, исследования, моделирования таких систем еще не в достаточной степени учитывают вновь появившиеся угрозы информационной безопасности. В рамках данной работы предлагается развитие методов системного анализа, ориентированных на решение задач противодействия внешним атакам на ЧМС, направленным на нарушение их нормального функционирования. Будем рассматривать ЧМС как структурное единство трех основных компонент: программной (П-компонента), технической (Т-компонента) и человека-оператора. Последний в ЧМС, как известно, может исполнять различные функции: ЛПР, оператор-исполнитель, оператор-ремонтник, эргатический резерв [3].

Для большинства систем санкционированный доступ к ним осуществляется посредством использования одного ключа (например, парольный доступ), что не обеспечивает защиту системы на должном уровне. Нарушителю в таком случае достаточно раскрытия единственного ключа для получения доступа ко всем ресурсам ЧМС. Очевидно, что такие системы обладают недостаточной устойчивостью к атакам и не обеспечивают требуемый уровень безопасности. Таким образом, возникает задача построения системы защиты, которая обеспечивает требуемый уровень криптостойкости.

Прикладные аспекты современной теории массового обслуживания решают не все задачи, в частности, остается открытым и до конца нерешенным вопрос оценки времени пребывания системы в выделенных состояниях для нестационарного режима. Целью данной работы является описание методики оценки времени в нестационарном режиме для ЧМС.

Для систем неоднородного состава предлагается установить криптографическую защиту следующей структуры: для получения доступа к ресурсам ЧМС необходим ввод всех трех ключей – П-компоненты, Т-компоненты и пароль оператора. Предполагаем, что атака нарушителя может быть направлена на взлом этих ключей и завершена успешно, если нарушитель получил несанкционированное право доступа ко всей системе, т.е. к каждой ее компоненте. Если у нарушителя нет хотя бы одного из ключей, атаки могут быть продолжены. После обнаружения факта успешной атаки в системе начинается случайный процесс восстановления, который оканчивается восстановление защиты системы. Общность рассмотрения этой задачи обеспечивается тем, что интенсивность атак и восстановления зависит от структурного элемента.

В зависимости от интенсивности восстановления криптостойкости ЧМС можно выделить три основных класса систем: восстанавливаемые; частично восстанавливаемые; невосстанавливаемые системы. Системы первого класса в свою очередь подразделяются на системы с зависимым и независимым восстановлением.

В предположении, что атака может успешно пройти по двум структурным элементам, зависимое восстановление подразделяют на следующие типы:

— успешная атака на техническую часть – восстановление криптостойкости Т-компоненты средствами П-компоненты под управлением оператора;

— успешная атака на П-компоненту – восстановление системы средствами Т-компоненты под управлением оператора;

— успешная атака на пароль оператора – возможно восстановление защиты как средствами Т-компоненты, так и средствами П-компоненты;

— успешная атака на ключ оператора и П-компоненту – восстановление криптостойкости средствами Т-компоненты;

— успешная атака на ключ оператора и Т-компоненту – восстановление защиты доступа средствами П-компоненты;

— успешная атака на П и Т-компоненты – восстановление системы оператором.

Среди ЧМС второго класса выделяют системы с восстановлением криптостойкости:

а) оператора и программной части (невосстанавливаемая техническая часть);

б) оператора и техники (невосстанавливаемая программная часть);

в) программной и технической части (невосстанавливаемые функции оператора);

г) человека-оператора (невосстанавливаемые техническая и программная части);

д) техники (невосстанавливаемые функции оператора и программная часть);

е) программной части (невосстанавливаемые функции оператора и техническая часть).

Графы, изображенные на рисунке 1, соответствуют системам неоднородного состава, состоящим из человека-оператора, выполняющего функции ЛПР, связанные с управлением политикой безопасности, настройкой программ или обслуживанием технической части, программной части П, и технической части Т.

Состояния системы описываются с точки зрения получения нарушителя доступа к функциям ЧМС. В этом случае рассматриваемые системы могут находиться в следующих состояниях:

1) S_0 — право доступа к функциям оператора, П и Т-компонентам закрыто ($ЧПТ$);

2) S_1 — право доступа к функциям оператора получено, доступ к П и Т-компонентам закрыт ($\overline{Ч}ПТ$);

3) S_2 — право доступа к функциям оператора и Т-компоненты закрыто, доступ к П-компоненте получен ($Ч\overline{П}Т$);

4) S_3 — право доступа к функциям оператора и П-компоненте закрыто, доступ к Т-компоненте получен ($ЧП\overline{Т}$);

5) S_4 — доступ к Т-компоненте закрыт, право доступа к функциям оператора и П-компоненте получено ($\overline{Ч}\,\overline{П}Т$);

6) S_5 — право доступа к функциям оператора закрыто, доступ к П и Т-компонентам получен ($Ч\overline{П}\overline{Т}$);

7) S_6 — доступ к П-компоненте закрыт, право доступа к функциям оператора и Т-компоненте получено ($\overline{Ч}П\overline{Т}$);

8) S_7 — все три ключа вскрыты ($\overline{Ч}\,\overline{П}\,\overline{Т}$).

Стойкость компонент ЧМС характеризуется следующими показателями:

а) для человека-оператора — интенсивность атак ξ и интенсивность восстановления криптостойкости системы ν ($ч^{-1}$);

б) для программной части — интенсивность атак ϵ ($ч^{-1}$) и интенсивность восстановления криптостойкости системы θ ($ч^{-1}$);

в) для технической части — интенсивность атак λ ($ч^{-1}$) и интенсивность восстановления криптостойкости системы μ ($ч^{-1}$).

На рисунках 1, б-д показаны графы, описывающие ЧМС с частичным восстановлением, т.е. если не восстанавливается, например, криптостойкость Т-компоненты (рисунок 1, б), то из графа полностью исключаются переходы по μ. Аналогичным образом для всех трех компонент. Приведенная система графов является целой, функционально полной и непротиворечивой. Класс графов является открытым и может быть расширен.

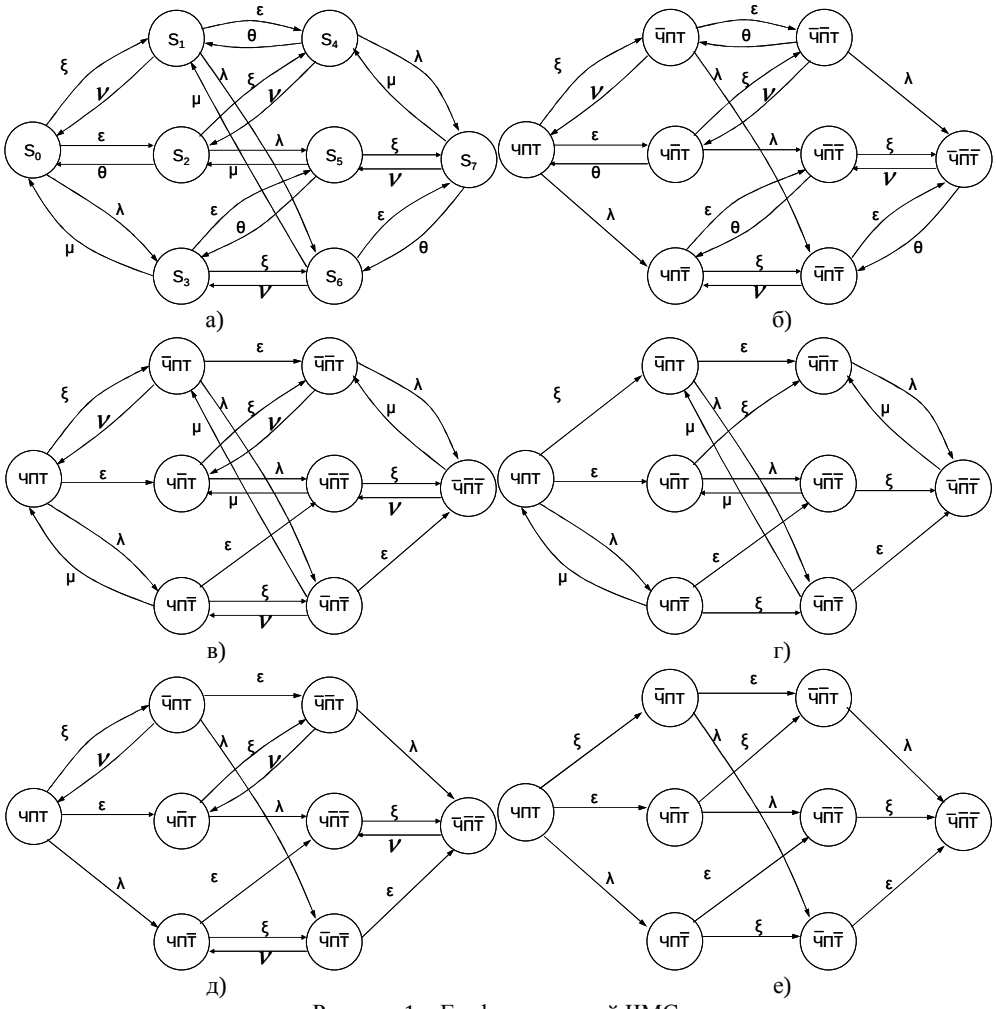

Рисунок 1 – Графы состояний ЧМС:
а) с полным восстановлением; б) с невосстанавливаемой технической частью; в) с невосстанавливаемой программной компонентой; г) с невосстанавливаемыми ЧО и программной частью;
д) с невосстанавливаемыми технической и программной частями; е) полностью невосстанавливаемая

Процесс структурной динамики интенсивностей атак и последующего восстановления для ЧМС, приведенной на рисунке 1,а, можно описать системой дифференциальных уравнений (1):

$$\begin{cases} \frac{\mathrm{d}P_{S_0}(t)}{\mathrm{d}t} = \nu P_{S_1}(t) + \theta P_{S_2}(t) + \mu P_{S_3}(t) - \xi P_{S_0}(t) - \varepsilon P_{S_0}(t) - \lambda P_{S_0}(t) \\ \frac{\mathrm{d}P_{S_1}(t)}{\mathrm{d}t} = \theta P_{S_4}(t) + \xi P_{S_0}(t) + \mu P_{S_6}(t) - \nu P_{S_1}(t) - \varepsilon P_{S_1}(t) - \lambda P_{S_1}(t) \\ \frac{\mathrm{d}P_{S_2}(t)}{\mathrm{d}t} = \varepsilon P_{S_0}(t) + \nu P_{S_4}(t) + \mu P_{S_5}(t) - \theta P_{S_2}(t) - \xi P_{S_2}(t) - \lambda P_{S_2}(t) \\ \frac{\mathrm{d}P_{S_3}(t)}{\mathrm{d}t} = \lambda P_{S_0}(t) + \theta P_{S_5}(t) + \nu P_{S_6}(t) - \mu P_{S_3}(t) - \varepsilon P_{S_3}(t) - \xi P_{S_3}(t) \\ \frac{\mathrm{d}P_{S_4}(t)}{\mathrm{d}t} = \varepsilon P_{S_1}(t) + \xi P_{S_2}(t) + \mu P_{S_7}(t) - \theta P_{S_4}(t) - \nu P_{S_4}(t) - \lambda P_{S_4}(t) \\ \frac{\mathrm{d}P_{S_5}(t)}{\mathrm{d}t} = \varepsilon P_{S_3}(t) + \lambda P_{S_2}(t) + \nu P_{S_7}(t) - \theta P_{S_5}(t) - \mu P_{S_5}(t) - \xi P_{S_5}(t) \\ \frac{\mathrm{d}P_{S_6}(t)}{\mathrm{d}t} = \xi P_{S_3}(t) + \lambda P_{S_1}(t) + \theta P_{S_7}(t) - \nu P_{S_6}(t) - \mu P_{S_6}(t) - \varepsilon P_{S_6}(t) \\ \frac{\mathrm{d}P_{S_7}(t)}{\mathrm{d}t} = \lambda P_{S_4}(t) + \xi P_{S_5}(t) + \varepsilon P_{S_6}(t) - \mu P_{S_7}(t) - \nu P_{S_7}(t) - \theta P_{S_7}(t) \end{cases} \quad (1)$$

при условии $\sum_{i=0}^{7} P_{S_i} = 1$.

В предположении, что интенсивности атак $\xi, \varepsilon, \lambda$ и восстановления ν, θ, μ для выделенного отрезка времени является постоянными, уравнение разрешимо численными методами. В более общем случае, когда интенсивности атак и восстановления защиты доступа являются функциями времени, решение можно получить средствами систем математического моделирования (например, *Maple*, *MathCAD* и др.).

Рассмотрим фрагмент системы неоднородного состава с полным восстановлением КС (рисунок 2). Последовательность смены состояний с указанием их идентификаторов образует траекторию, которую будем обозначать цепочкой следующих символов $S_0 \leftrightarrow S_1 \leftrightarrow S_4 \leftrightarrow S_7$. Этой цепочке соответствует последовательность атак на ЧМС и восстановления КС. Будем считать, что усилия нарушителя направлены на необходимость в первую очередь получить пароль оператора, затем ключ П-компоненты, и только потом – ключ Т-компоненты. Если система восстанавливается с меньшей интенсивностью, чем происходят атаки, то в конечном итоге, система окажется взломана.

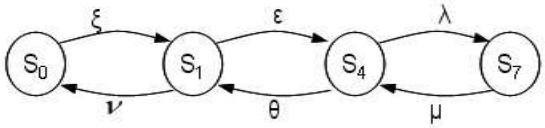

Рисунок 2 – Фрагмент ЧМС с полным восстановлением

Рассмотренный фрагмент в той или иной степени присутствует в каждом графе из указанного класса и является достаточным для исследований на нем процессов структурной динамики, что дает возможность перейти к аналитическому моделированию.

Процесс структурной динамики системы под воздействием интенсивностей атак и последующих восстановлений можно описать системой нестационарных дифференциальных уравнений (2), которая описывает состояния $ЧПТ$, $\overline{Ч}ПТ$, $\overline{Ч\,П}\overline{Т}$, $\overline{Ч\,П\,Т}$:

$$\begin{cases} \dfrac{\mathrm{d}P_{S_0}(t)}{\mathrm{d}t} = \nu(t)P_{S_1}(t) - \xi(t)P_{S_0}(t); \\ \dfrac{\mathrm{d}P_{S_1}(t)}{\mathrm{d}t} = \xi(t)P_{S_0}(t) + \theta(t)P_{S_4}(t) - \nu(t)P_{S_1}(t) - \varepsilon(t)P_{S_1}(t); \\ \dfrac{\mathrm{d}P_{S_4}(t)}{\mathrm{d}t} = \varepsilon(t)P_{S_1}(t) + \mu(t)P_{S_7} - \theta(t)P_{S_4}(t) - \lambda(t)P_{S_4}(t); \\ \dfrac{\mathrm{d}P_{S_7}(t)}{\mathrm{d}t} = \lambda(t)P_{S_4}(t) - \mu(t)P_{S_7}(t). \end{cases} \quad (2)$$

В предположении, что интенсивности атак ξ, ε, λ и восстановления ν, θ, μ для выделенного отрезка времени является постоянными, система (2) разрешима, и на ее основании можно получить функции, описывающие динамику вероятностей пребывания в выделенных состояниях.

$$P_{S_0}(t) = C_o \exp(r_0 t)\cdot a1 + C_1 \exp(r_1 t)\cdot a2 + C_2 \exp(r_2 t)\cdot a3 + C_3 \exp(r_3 t)\cdot a4;$$
$$P_{S_1}(t) = C_o \exp(r_0 t)\cdot b1 + C_1 \exp(r_1 t)\cdot b2 + C_2 \exp(r_2 t)\cdot b3 + C_3 \exp(r_3 t)\cdot b4;$$
$$P_{S_4}(t) = C_o \exp(r_0 t)\cdot f1 + C_1 \exp(r_1 t)\cdot f2 + C_2 \exp(r_2 t)\cdot f3 + C_3 \exp(r_3 t)\cdot f4;$$
$$P_{S_7}(t) = C_o \exp(r_0 t)\cdot d1 + C_1 \exp(r_1 t)\cdot d2 + C_2 \exp(r_2 t)\cdot d3 + C_3 \exp(r_3 t)\cdot d4,$$

где r_i – корни характеристического уравнения с коэффициентами {0, $\xi\mu\theta + \xi\mu\varepsilon + \xi\varepsilon\lambda + \nu\theta\mu$, $\mu\xi + \xi\theta + \xi\lambda + \xi\varepsilon + \theta\mu + \nu\mu + \varepsilon\mu + \nu\theta + \nu\lambda + \varepsilon\lambda$, $\xi + \mu + \theta + \lambda + \varepsilon + \nu$ }; fi – степень свободы; $bi = \dfrac{\theta(\xi + r_i)}{\varepsilon\xi + \xi r_i + \nu r_i + \varepsilon r_i + (r_i)^2} fi$; $ai = \dfrac{\nu}{\xi + r_i} bi$; $di = \dfrac{\lambda}{\mu + r_i} fi$; C_0, C_1, C_2, C_3 – произвольные постоянные, определяемые из начальных условий.

На практике случаи получения полного доступа к ЧМС сравнительно редки. Поэтому вероятностью перехода в состояние S_7 в некоторых случаях можно пренебречь. Далее будем рассматривать три состояния: $S_0 \leftrightarrow S_1 \leftrightarrow S_4$. Динамика переходов в этом случае описывается системой уравнений (3):

$$\begin{cases} \dfrac{\mathrm{d}P_{S_0}(t)}{\mathrm{d}t} = \nu(t)P_{S_1}(t) - \xi(t)P_{S_0}(t); \\ \dfrac{\mathrm{d}P_{S_1}(t)}{\mathrm{d}t} = \xi(t)P_{S_0}(t) + \theta(t)P_{S_4}(t) - \nu(t)P_{S_1}(t) - \varepsilon(t)P_{S_1}(t); \\ \dfrac{\mathrm{d}P_{S_4}(t)}{\mathrm{d}t} = \varepsilon(t)P_{S_1}(t) - \theta(t)P_{S_4}(t). \end{cases} \quad (3)$$

В предположении, что интенсивности атак ξ, ε и восстановления ν, θ для выделенного отрезка времени является постоянными, система (3) разрешима, и на ее основании можно получить функции, описывающие динамику вероятностей пребывания в выделенных состояниях.

$$P_{S_0}(t) = \frac{\nu\theta}{\pi} + C_1\exp(\alpha t) + C_2\exp(\beta t);$$

$$P_{S_1}(t) = \frac{\xi\theta}{\pi} + \frac{\alpha+\xi}{\nu}C_1\exp(\alpha t) + \frac{\beta+\xi}{\nu}C_2\exp(\beta t);$$

$$P_{S_4}(t) = \frac{\varepsilon\xi}{\pi} - \frac{1+\alpha+\xi}{\nu}C_1\exp(\alpha t) + \frac{1+\beta+\xi}{\nu}C_2\exp(\beta t),$$

где $\alpha = -\dfrac{\nu+\varepsilon+\theta+\xi}{2} + \left(\left(\dfrac{\nu+\varepsilon+\theta+\xi}{2}\right)^2 - (\varepsilon\xi+\nu\theta+\theta\xi)\right)^{1/2}$; $\beta = -\dfrac{\nu+\varepsilon+\theta+\xi}{2} - \left(\left(\dfrac{\nu+\varepsilon+\theta+\xi}{2}\right)^2 - (\varepsilon\xi+\nu\theta+\theta\xi)\right)^{1/2}$;

C_1, C_2 – произвольные постоянные, определяемые из начальных условий.

Графики, отображающие динамику пребывания системы в выделенных состояниях, изображены на рисунке 3.

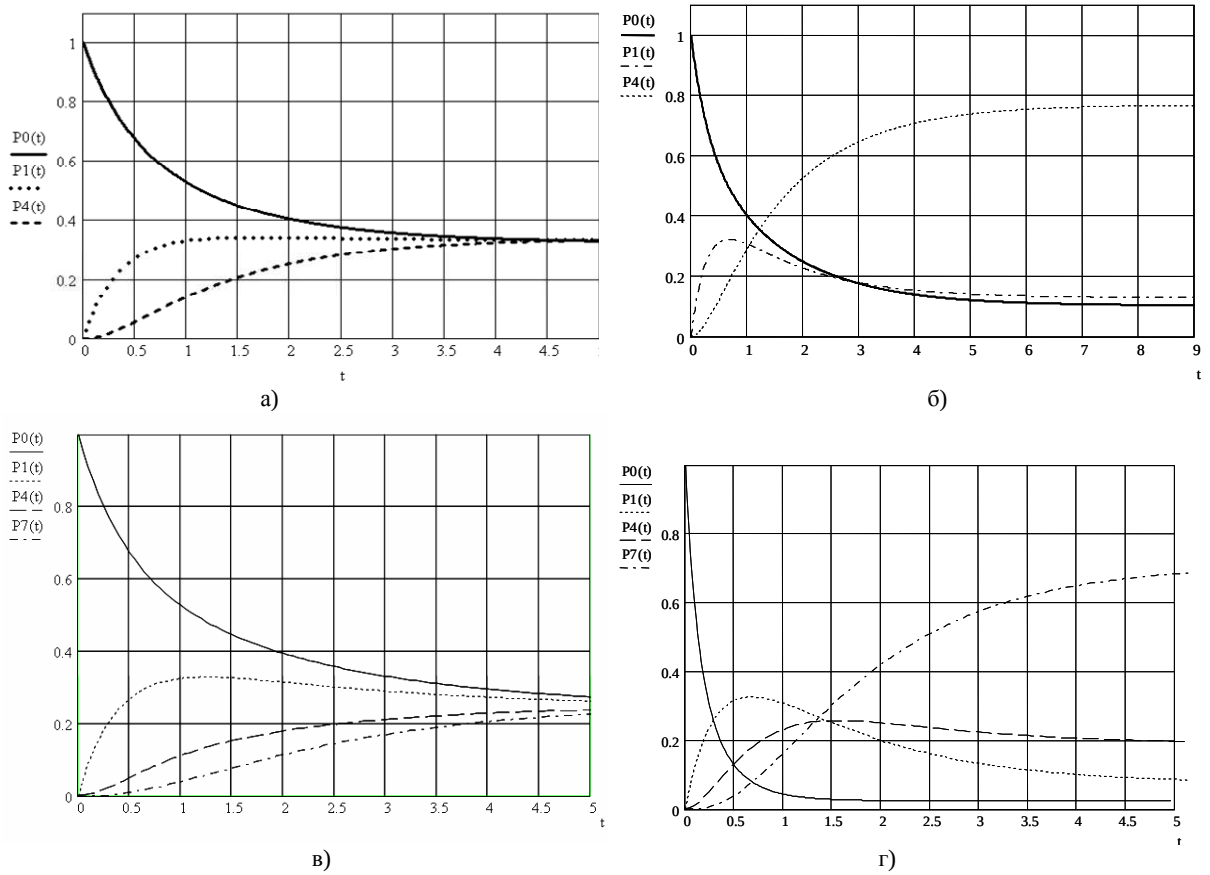

Рисунок 3 – Зависимость вероятности пребывания ЧМС в выделенных состояниях от времени

С помощью методики, изложенной в [4], могут быть найдены следующие параметры:

1) плотность распределения случайной величины T

$$f(t) = \lambda_{i,i-1} P_i(t) + \lambda_{j,j+1} P_j(t),$$

где $\lambda_{i,i-1}$ — интенсивность выхода из i-го состояния; $\lambda_{j,j+1}$ — интенсивность выхода из j-го состояния;

2) математическое ожидание времени пребывания в группе состояний $i,\ldots, j$ по формуле

$$\bar{t}_{i,\ldots,j} = \int_0^\infty t f(t) dt .$$

Разработана имитационная модель и проведены статистические оценки математического ожидания, которые дали удовлетворительные совпадения с вероятностными оценками. Близость оценок в значительной степени определяется следующими двумя факторами:

1) относительной нагрузкой узла ρ, которая определяется отношением интенсивности входящего потока к выходящему и значительно меньше единицы;

2) точность оценки также приближается к статистической в том случае, когда все выходные и входные интенсивности одного порядка.

Были проведены эксперименты с использованием имитационной модели, получены следующие результаты: для менее 100 экспериментов ошибка составила порядка 5 %, для количества экспериментов около 1000 – 3%. В случае, когда $\rho < 0{,}15$, ошибка составила менее 5 %. При одновременном выполнении условий 1) и 2) для того же числа экспериментов ошибка уменьшилась до 3,5 % и 1,5 % соответственно.

Направлением дальнейших исследований является разработка подобной методики для управляемой Марковской цепи.

Библиографический список

1. Столлингс В. Криптография и защита сетей: принципы и практика. Пер. с англ / В. Столлингс. — М.: Изд. дом «Вильямс», 2001. — 672 с.

2. Отказобезопасные информационно-управляющие системы на программируемой логике / Е.С. Бахмач [и др.] / Под. ред. Харченко В.С., Скляра В.В. — Харьков: Нац. аэрокосм. ун.-т «ХАИ», Науч.-производств. предприятие «Радий», 2008. — 380 с.

3. Охтилев М.Ю. Интеллектуальные технологии мониторинга и управления структурной динамикой сложных технических объектов / М.Ю. Охтилев, Б.В. Соколов, Р.М. Юсупов. — М.: Наука, 2006. — 410 с.

4. Шуенкин В.А. Прикладные модели теории массового обслуживания: учеб. пособие / В.А. Шуенкин, В.С. Донченко. — К.: НМК ВО, 1992. — 398 с.

Поступила в редакцию 18.05.2009 г.