УДК 004.056.5:004.052

И.А. СКАТКОВ, А.О. СМАГИНА

Севастопольский национальный технический университет, Украина

АНАЛИЗ ГАРАНТОСПОСОБНОСТИ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ СИСТЕМ НЕОДНОРОДНОГО СОСТАВА

Рассмотрены методы организации криптографической защиты человеко-машинных систем, как систем неоднородного состава, проведено их формальное описание, выделены основные структурные компоненты, рассмотрены графы переходов между ними. Предложена аналитическая модель структурной динамики на основе нестационарных дифференциальных уравнений, получено конечное решение для системы малой размерности. Приведены результаты численного моделирования.

Ключевые слова: *гарантоспособность, криптографическая защита, структурная динамика, криптостойкость, человеко-машинные системы.*

Введение

В процессе оценки состояния современных человеко-машинных систем (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. Такие системы часто становятся объектами противодействия со стороны конкурирующих структур, подвергаются действию вирусных атак, несанкционированных попыток проникновения и др. 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. Существующие методики анализа, исследования, моделирования таких систем еще не в достаточной степени учитывают вновь появившиеся угрозы информационной безопасности. Как утверждают авторы работы [2] и эта концепция далее будет развита нами: «повышение свойств информационной безопасности (целостности, конфиденциальности) приводит с одной стороны, к повышению готовности благодаря уменьшению вероятности успешных атак, а с другой, – к дополнительным затратам времени на проведение профилактических работ, что может вызвать потери готовности». В рамках данной статьи предлагается развитие методов системного анализа, ориентированных на решение задач противодействия внешним атакам на ЧМС, направленным на нарушение их нормального функционирования. Из всех первичных свойств гарантоспособности в данном случае наиболее важными представляются такие свойства, как безотказность, функциональная безопасность, целостность, конфиденциальность [3].

Будем рассматривать ЧМС как структурное единство трех основных компонент: программной (П-компонента), технической (Т-компонента) и человека-оператора (ЧО). Последний в ЧМС, как известно, может исполнять различные функции: ЛПР, оператор-исполнитель, оператор-ремонтник, эргатический резерв [4].

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. Таким образом, возникает задача построения системы защиты, которая обеспечивает требуемый уровень криптостойкости. Очевидно, что такие системы обладают недостаточ-

ной устойчивостью к атакам и не обеспечивают требуемый уровень гарантоспособности. Целью данной работы является применение диверсионного подхода к повышению гарантоспособности криптографической защиты ЧМС.

1. Формальная постановка задачи

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 ЧО. 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 КС системы. Общность рассмотрения этой задачи обеспечивается тем, что интенсивность атак и восстановления зависит от структурного элемента.

В зависимости от интенсивности восстановления криптостойкости (КС) ЧМС можно выделить три основных класса систем: 1) восстанавливаемые; 2) частично восстанавливаемые; 3) 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 КС Т-компоненты средствами П-компоненты под управлением ЧО;

– успешная атака на П-компоненту – восстановление КС средствами Т-компоненты под управлением ЧО;

– успешная атака на ключ ЧО – возможно восстановление КС как средствами Т-компоненты, так и средствами П-компоненты;

– успешная атака на ключ ЧО и П-компоненту – восстановление КС средствами Т-компоненты;

– успешная атака на ключ ЧО и Т-компоненту – восстановление КС средствами П-компоненты;

– успешная атака на П и Т-компоненты – восстановление КС средствами ЧО.

Среди ЧМС второго класса выделяют системы с восстановлением КС:

– ЧО и программной части (невосстанавливаемая техническая часть);

– ЧО и техники (невосстанавливаемая программная часть);

– программной и технической части (невосстанавливаемые функции ЧО);

– ЧО (невосстанавливаемые техническая и программная части);

– техники (невосстанавливаемые функции ЧО и программная часть);

– программной части (невосстанавливаемые функции ЧО и техническая часть).

Графы, изображенные на рис. 1, соответствуют системам неоднородного состава, состоящим из ЧО, 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 ЧО, П и Т-компонентам закрыто (ЧПТ);

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

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

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

5) S_4 – доступ к Т-компоненте закрыт, право доступ к функциям ЧО и П-компоненте получено ($\overline{\text{Ч}}\overline{\text{П}}$Т);

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

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

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

Стойкость компонент ЧМС характеризуется следующими показателями:

а) для ЧО – 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 рис. 1 (б-д) показаны графы, описывающие

ЧМС с частичным восстановлением, т.е. если не восстанавливается, например, КС Т-компоненты (рис. 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.

Рассмотрим граф, изображенный на рис. 1(б). Из состояния S_0 возможен переход в состояния S_1, S_2 и S_3. Из состояния S_2 в случае успешных атак возможен переход в состояния S_4 и S_5. Из состояния S_5 переход в обратном направлении может осуществляться только в состояние S_3. Из состояния S_3 переход возможен в состояния S_5 и S_6, вернуться в исходное состояние S_0 из S_3 невозможно, т.к. КС Т-компоненты не восстанавливается.

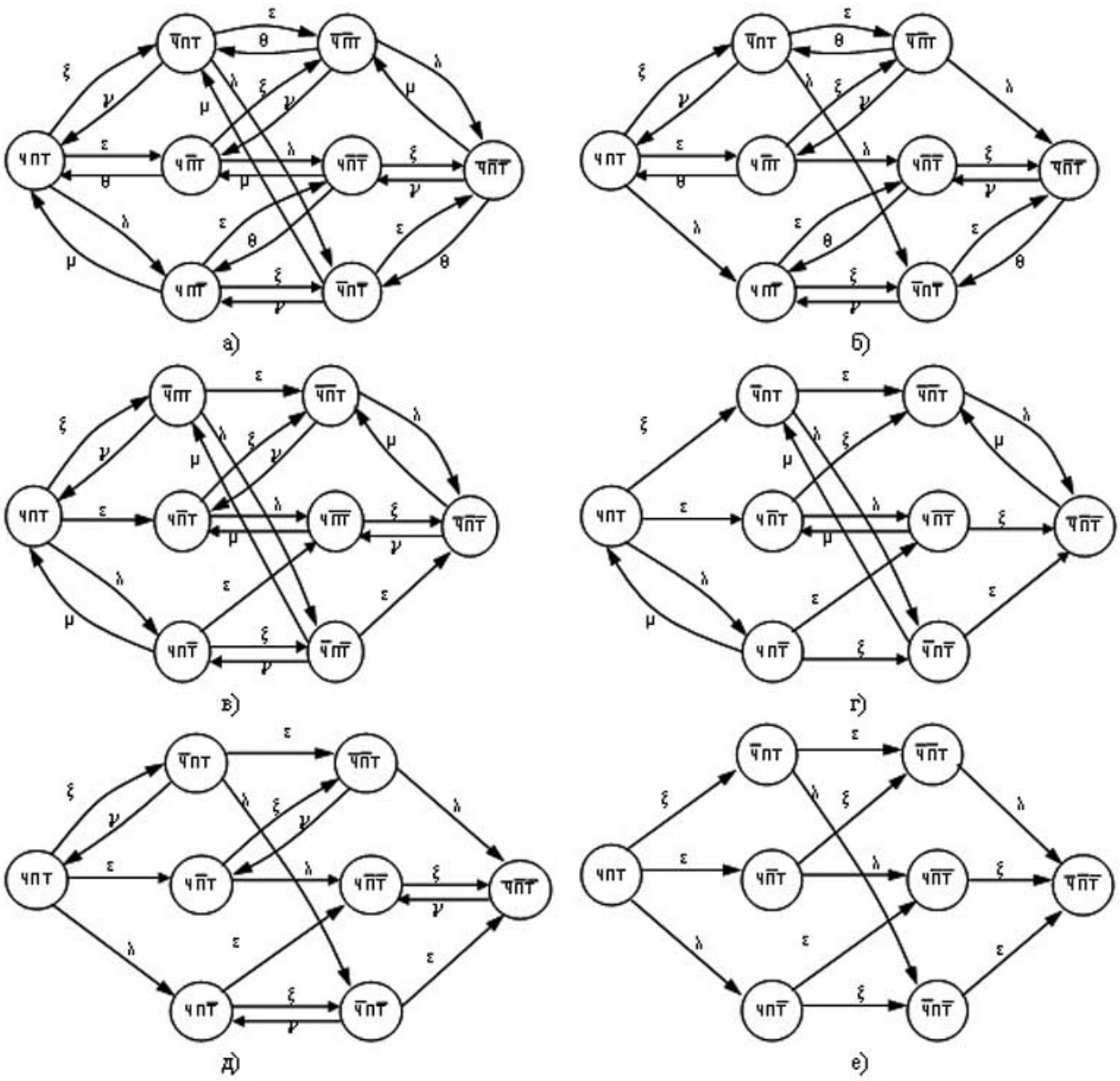

Рис. 1. Граф состояний ЧМС

а - ЧМС с полным восстановлением; б - ЧМС с невосстанавливаемой технической частью; в - ЧМС с невосстанавливаемой программной компонентой; г - ЧМС с невосстанавливаемыми ЧО и программной частью; д - ЧМС с невосстанавливаемыми технической и программной частями; е - полностью невосстанавливаемая ЧМС.

Рассмотрим фрагмент системы неоднородного состава с полным восстановлением КС (рис. 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 направ-

лены на необходимость в первую очередь получить ключ ЧО, 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.

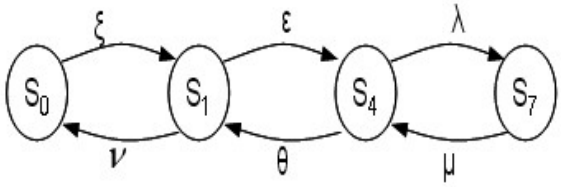

Рис. 2. Фрагмент ЧМС с полным восстановлением

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.

2. Аналитическое моделирование

Процесс структурной динамики интенсивностей атак и последующего восстановления можно описать системой нестационарных дифференциальных уравнений, которая учитывает состояния ЧПТ, $\overline{\text{ЧПТ}}$, $\overline{\overline{\text{ЧПТ}}}$, $\overline{\overline{\overline{\text{ЧПТ}}}}$:

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

На практике случаи получения полного доступа к ЧМС сравнительно редки. Поэтому вероятностью перехода в состояние S_7 можно пренебречь на данном этапе рассмотрения задачи. Далее будем рассматривать три состояния: $S_0; S_1; S_4$. Динамика переходов в этом случае описывается системой уравнений:

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

Последняя система эквивалентна линейному однородному дифференциальному уравнению третьего порядка:

$$\frac{1}{\varepsilon\xi}\frac{d^3P_{S_4}(t)}{dt^3} + \frac{\nu+\varepsilon+\theta+\xi}{\varepsilon}\frac{d^2P_{S_4}(t)}{\partial t^2} + \frac{\nu\theta+\varepsilon\xi+\theta\xi}{\varepsilon\xi}\frac{dP_{S_4}(t)}{dt} = 0$$

В предположении, что интенсивности атак ξ, ε и восстановления ν, θ для выделенного отрезка времени является постоянными, уравнение разрешимо, и на его основании можно получить функции, описывающие динамику вероятностей пребывания в выделенных состояниях. Например, для защищенного состояния S_0 и критического состояния S_4:

$$P_{S_0}(t) = C_1 + C_2\exp\left(\frac{\theta}{2}\left(A^{1/2} - \nu - \varepsilon - \theta - \xi\right)t\right) + C_3\exp\left(-\frac{\theta}{2}\left(A^{1/2} + \nu + \varepsilon + \theta + \xi\right)t\right),$$

где $A = \nu\left(\left(\dfrac{\nu+\varepsilon+\theta+\xi}{\nu}\right)^2 - \dfrac{4(\nu\theta+\varepsilon\xi+\theta\xi)}{\nu^2\theta^2}\right)$;

$$P_{S_4}(t) = C_1 + C_2\exp\left(\frac{\xi}{2}\left(B^{1/2} - \nu - \varepsilon - \theta - \xi\right)t\right) + C_3\exp\left(-\frac{\xi}{2}\left(B^{1/2} + \nu + \varepsilon + \theta + \xi\right)t\right),$$

где $B = \varepsilon\left(\left(\dfrac{\nu+\varepsilon+\theta+\xi}{\varepsilon}\right)^2 - \dfrac{4(\nu\theta+\varepsilon\xi+\theta\xi)}{\varepsilon^2\xi^2}\right)$.

В более общем случае, когда интенсивности атак и КС-восстановления являются функциями времени, решение можно получить средствами систем математического моделирования (например, MathCad или Maple).

Произвольные постоянные C_1, C_2, C_3 определяются из начальных условий.

3. Численное моделирование

Рассмотрим динамику системы полагая, что в начальный момент времени система пребывает в состоянии S_4, т.е. нарушитель получил несанкционированный доступ к обоим ключам. Так как задача является многопараметрической, что затрудняет анализ, выделим классы качественно отличающиеся друг от друга характеристиками интенсивностей атак и восстановления. Так, для одной из исследуемых нами систем, интенсивность атак принята низкой, если $\xi, \varepsilon \in [1,8; 10,7]$ и высокой, если $\xi, \varepsilon \in [10,8; 22,7]$, соответственно, интенсивности

восстановления – $\nu, \theta \in [0,8;\ 8,4]$ и $[8,5;18,3]$. Этим классам соответствуют ситуации, возникающие в процессе динамики функционирования ЧМС.

Таблица 1

Классификатор основных ситуаций, связанных с оценкой интенсивностей

Интенсивность восстановления		Интенсивность атак	
		низкая	высокая
	низкая	A	B
	высокая	C	D

Качественная оценка всех ситуаций связана с пребыванием системы в выделенных состояниях. Ситуация С является самой благоприятной, т.к. вероятность пребывания системы в критическом состоянии низкая, ситуация В – критическая, т.к. вероятность несанкционированного доступа велика.

На рисунке 3 изображены графики, показывающие динамику пребывания системы в состоянии S_4, т.к. оно описывает получение несанкционированного доступа к П-компоненте и функциям ЧО – $\overline{\text{ЧПТ}}$.

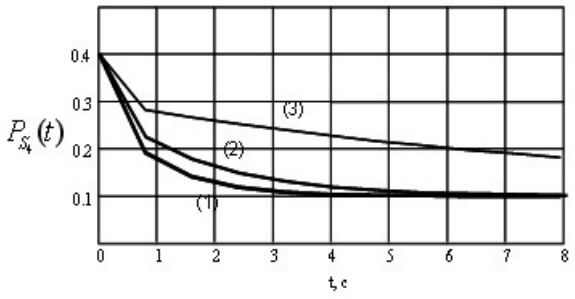

Рис. 3. Вероятность пребывания ЧМС в состоянии S_4 : (1) – ситуация С, (2) – ситуация А или D, (3) – ситуация В.

Некоторые результаты численного моделирования для ситуаций A, B, C и D, когда интенсивность атак и интенсивность восстановления возрастают; интенсивности атак возрастают, а интенсивности восстановления уменьшаются, сведены в табл. 2.

Таблица 2

Результаты численного моделирования ситуаций для состояния S_0

t_i	Классы ситуаций			
	A	B	C	D
	$P_{S_0}(t)$	$P_{S_0}(t)$	$P_{S_0}(t)$	$P_{S_0}(t)$
1	0.579	0.388	0.841	0.600
2	0.561	0.338	0.834	0.601
3	0.544	0.317	0.827	0.601
4	0.529	0.307	0.820	0.601
5	0.516	0.303	0.814	0.602
6	0.501	0.301	0.809	0.603
7	0.593	0.301	0.804	0.605
8	0.583	0.300	0.799	0.608
9	0.475	0.300	0.795	0.613
10	0.467	0.300	0.791	0.621
11	0.460	0.300	0.787	0.633
12	0.454	0.300	0.784	0.652
13	0.448	0.300	0.781	0.681
14	0.443	0.300	0.779	0.727

Результаты численного моделирования пребывания системы в состоянии S_4 сведены в табл. 3.

Таблица 3

Результаты численного моделирования ситуаций для состояния S_4

t_i	Классы ситуаций			
	A	B	C	D
	$P_{S_4}(t)$	$P_{S_4}(t)$	$P_{S_4}(t)$	$P_{S_4}(t)$
1	0.379	0.641	0.188	0.327
2	0.361	0.634	0.138	0.381
3	0.344	0.627	0.117	0.352
4	0.329	0.620	0.107	0.333
5	0.316	0.614	0.103	0.321
6	0.301	0.609	0.101	0.313
7	0.293	0.604	0.101	0.308
8	0.283	0.599	0.100	0.305
9	0.275	0.595	0.100	0.303
10	0.267	0.591	0.100	0.302
11	0.260	0.587	0.100	0.301
12	0.254	0.584	0.100	0.301
13	0.248	0.581	0.100	0.301

4. Анализ полученных результатов

Из результатов моделирования видно, что для ситуации С характерны достаточно высокие показатели пребывания ЧМС в состоянии S_0.

Рассматривая ситуацию А, которая характеризуется показателями интенсивности атак $\xi, \varepsilon \in [1,8;\ 10,7]$, и восстановления $\nu, \theta \in [0,8;\ 8,4]$, можно сделать вывод, что вероятность пребывания в критическом состоянии на малых интервалах времени достаточно высокая, что не обеспечивает защиту системы на должном уровне. Анализ ситуации на сравнительно больших интервалах времени показал, что вероятность пребывания в состоянии S_0(ЧПТ) возрастает.

Для ситуации В характерны показатели интенсивностей атак и восстановления $\xi, \varepsilon \in [10,8;\ 22,7]$ и $\nu, \theta \in [0,8;\ 8,4]$ соответственно. Анализируя показатели вероятности пребывания системы в критическом состоянии, можно сделать вывод, что система не успевает восстанавливаться после успешных атак, и переход в защищенное состояние маловероятен.

Ситуация С соответствует высокому уровню восстановления КС (интенсивность восстановления системы – $\nu, \theta \in [8,5;18,3]$) при малых интенсивностях атак ($\xi, \varepsilon \in [1,8;\ 10,7]$). Для указанного класса ситуаций характерно достаточно стабильное поведение системы на больших интервалах времени, вероятность пребывания в критическом состоянии сравнительно невелика.

Класс ситуаций D описывается высоким уровнем интенсивностей атак и восстановления ($\xi, \varepsilon \in [10,8;\ 22,7]$ и $\nu, \theta \in [8,5;18,3]$ соответственно). При моделировании указанной ситуации можно наблюдать постепенное увеличение вероятности пребывания в защищенном состоянии S_0.

Анализ результатов, полученных при моделировании различных классов ситуаций на малых интервалах времени, показал, что вероятность пребывания в защищенном состоянии наиболее высокая для класса С, затем по степени убывания вероятности – для классов D и А, и незначительная – для класса В.

При моделировании на сравнительно больших интервалах времени, можно увидеть, что вероятность пребывания в критическом состоянии уменьшается для всех классов ситуаций. Качественный анализ позволяет сделать выводы о том, что классы С и D дают высокие показатели вероятности пребывания системы в защищенном состоянии. Для класса А характерно незначительное снижение вероятности пребывания в критическом состоянии. Ситуации класса В характеризуются низкой защищенностью системы и высокой вероятностью получения к ней несанкционированного доступа нарушителем.

Заключение

Исследована способность системы неоднородного состава своевременно реагировать на атаки различной интенсивности. Предложен подход к моделированию ЧМС, который позволяет учитывать разнородность ее структурных элементов.

Предложенная структура криптографической защиты информации позволяет повысить такие свойства гарантоспособности, как информационная безопасность, целостность и конфиденциальность.

Направлением дальнейших исследований является построение программной среды поддержки принятия решений по выбору стратегий управления криптографическими ключами с использованием специальных средств и методов имитационного моделирования.

Литература

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

2. Бахмач Е.С. Отказобезопасные информационно-управляющие системы на программируемой логике / Е.С. Бахмач, А.Д. Герасименко, В.А. Головир, А.А. Сиора, В.В. Скляр, В.И. Токарев, В.С. Харченко / Под. ред. Харченко В.С., Скляра В.В. – Национальный аэрокосмический университет «ХАИ», Научно-производственное предприятие «Радий», 2008. – 380 с.

3. Жихарев В.Я. Методы моделирования и дискретной оптимизации вычислительных систем реального времени / В.Я. Жихарев, В.М. Илюшко, Л.Г. Кравец и др. – Житомир: Изд-во ЖГУ, 2004. – 494 с.

4. 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.

Поступила в редакцию 11.02.2009

Рецензент: д-р техн. наук, проф., зав. каф. В.С. Харченко, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков, Украина.

АНАЛІЗ ГАРАНТОЗДАТНОСТІ КРИПТОГРАФІЧНОГО ЗАХИСТУ СИСТЕМ НЕОДНОРІДНОГО СКЛАДУ

І.А. Скатков, А.О. Смагіна

Розглянуто методи організації криптографічного захисту людино-машинних систем, як систем неоднорідного складу, проведено їхній формальний опис, виділені основні структурні компоненти, розглянуті графи переходів між ними. Запропоновано аналітичну модель структурної динаміки на основі нестаціонарних диференціальних рівнянь, отримано кінцеве рішення для системи малої розмірності. Приведені результати чисельного моделювання.

Ключові слова: гарантоздатність, криптографічний захист, структурна динаміка, криптостійкість, людино-машинні системи.

ANALYSIS OF ENCRYPTIC SYSTEM PROTECTION DEPENDABILITY OF NONUNIFORM STRUCTURE

I.A. Skatkov, A.O. Smagina

Methods of encryptie protection organization of man-machine systems as systems of nonuniform structure are observed, their formal description is conducted, general structural components (elements) are underlined, graphs of their conversion are considered. Analytic model of structural dynamics on the basis of nonstationary differential equation is suggested, final results for small dimension systems is obtained. Results of numerical modeling is conducted.

Keywords: dependability, encryptie protection, structural dynamics, cryptographic resistance, man-machine systems.

Скатков Иван Александрович – канд. техн. наук, доц. кафедры автоматизированных приборных систем, Севастопольский национальный технический университет, Севастополь, Украина, e-mail: kvt@sevgtu.sebastopol.ua.

Смагина Анна Олеговна – ассистент кафедры кибернетики и вычислительной техники Севастопольский национальный технический университет, Севастополь, Украина, e-mail: kvt@sevgtu.sebastopol.ua.