УДК 621.396:004.621

Казакова Н.Ф. Тискина Е.О., ХорошкоВ.А.

# ПОВЫШЕНИЕ АДАПТИВНОСТИ И ДОСТОВЕРНОСТИ ВЕРОЯТНОСТНОЙ МОДЕЛИ ОЦЕНКИ ЖИВУЧЕСТИ СИСТЕМЫ ЗАЩИТЫ ШИФРОВАНИЯ

В статье рассматривается актуальность взаимоотношения отказа элемента и отказа системы.

***Введение.*** Формирование и работа многих современных сложных систем характеризуется тем, что не все ее подсистемы и элементы в одинаковой степени функционально нагружены, и не все ее элементы в процессе функционирования используются одинаково часто. В этих условиях изменяется взаимоотношение отказа элемента и отказа системы. Так, например, если элемент используется в процессе функционирования редко, то в случае его отказа даже при последовательном подключении элемента в систему, отказ системы может поступить лишь в том случае, когда этот элемент будет использоваться.

Частота использования элемента в процессе функционирования существенно влияет на ее надежность и живучесть. С учетом этого фактора нельзя описать живучесть системы только надежностью ее элементов. В литературе недостаточно внимания уделено исследованию этого вопроса.

В некоторых работах предлагается способ учета этого фактора, основанный на дискретных моделях теории графов и на методе систематических испытаний.

***Цель работы.*** В настоящей работе предлагается способ учета частоты использования элемента на основе систематической модели математического ожидания и с его помощью дано определение зависимости живучести системы от надежности ее элементов.

***Анализ научной и технической литературы*** показал, что характеристики живучести функционирования многих современных систем защиты определяется не только внутренней структурой системы, характеристиками надежности ее элементов, но и видом задач (требований), которые системы обязаны выполнять. В зависимости от вида того или другого требования к системе при его обслуживании обладает соответственно той или другой надежностью функционирования. Это объясняется тем, что каждое требование в процессе своего выполнения может использовать со своей интенсивностью (отличной от интенсивности других требований) каждый из элементов системы. При выполнении данной задачи, т.е. обслуживании данного требования, в системе могут быть задействованы только определенные элементы (вообще говоря, не все), а это значит, что система при выполнении этой задачи будет иметь уровень надежности и живучести, соответствующий такому типу задач (типу требований), который определяется степенью использования отдельных элементов системы. Возникает ситуация, когда один и тот же элемент и входит в систему в смысле надежности и живучести, и не входит в нее, т.е. в структурной схеме живучести системы наличие его является случайным в зависимости от типа обслуживаемого в данный момент времени системой требования. В этой ситуации традиционные методы расчета живучести системы защиты по надежности ее элементов не могут быть достаточно эффективными, так как с их помощью нельзя учесть указанную выше случайность. Эта задача является ***ранее нерешенной частью общей проблемы*** повышения адаптивности и достоверности вероятностной модели оценки живучести системы защиты шифрования.

Для сравнения системы защиты можно применять в качестве критерия эффективности обобщенный показатель в виде:

$$\acute{Y} = \frac{\hat{E}_{æ} \ddot{I}_{\hat{i}}}{\tilde{N}},$$

где $\ddot{I}_{\hat{i}}$ – производительность системы в обслуживании требований при идеальной надежности; $C$ – экономические затраты на обслуживание системы; $\hat{E}_{\acute{y}\acute{o}}$ – коэффициент живу-

чести системы, являющийся отношением числа состояний $\varphi$ систем, соответствующих работоспособным, по всей совокупности $\varphi_n^j$ ( $j$ – вероятность обобщенного отказа; $n$ – количество элементов): $\hat{E}_{æ} = \frac{\varphi}{\varphi_n^j}$.

***Основная часть.*** Рассмотрим один из возможных способов расчета надежности системы, когда учитывается ситуация, при которой элемент как входит, так и не входит в систему в зависимости от потока выполняемых системой задач (т.е. обслуживаемых требований).

Пусть система, состоящая из $n$ элементов, предназначена для обслуживания потока различных типов требований. Пусть $x_i$ ( $i = 1, 2, 3, ..., n$ ) – вероятность безотказной работы $i$-го элемента системы. Обозначим через $\alpha_i$ ( $i = 1, 2, 3, ..., n$ ) вероятность задействования $i$-го элемента при обслуживании данного требования из потока. В установившемся режиме функционирования системы вероятность $\alpha_i$ можно оценить как относительную частоту появления того множества типов требований, которые при обслуживании задействуют $i$-й элемент системы. Далее, через $\rho_i$ обозначим вероятность использования $i$-го элемента системы в произвольный момент времени при нормальном ее функционировании. Пусть $\tau_i^{(2)}$ – среднее время обслуживания требований, не задействующих $i$-го элемента. Нетрудно заметить, что если время обслуживания системой всех требований в среднем одинаково, т.е. если $\tau_i^{(1)} = \tau_i^{(2)}$, то вероятность использования элемента совпадает с вероятностью его задействования, т.е. $\rho_i = \alpha_i$.

Если частоты появления требований, которые задействуют $i$-й элемент и не задействуют его, одинаковы, то вероятность использования $\rho_i$ будет равна:

$$\rho_i = \frac{\tau_i^{(1)}}{\tau_i^{(1)} + \tau_i^{(2)}} + \Theta_i,$$

где $\Theta$ – управляющий параметр.

В общем случае вероятность использования $i$-го элемента в произвольный момент времени определяется как относительное время использования этого элемента за время функционирования системы, т.е. за время обслуживания требований потока [1]. Тогда, согласно этому определению,

$$\rho_i = \lim_{T\to\infty} \frac{1}{T} \int_0^T \gamma_i(t)\, dt, \qquad (1)$$

где $T$ – время работы системы, а $\gamma_i(t)$ в момент времени $t$ применяет одно из двух значений: единицу, если в этот момент $i$-й элемент используется, и нуль – в противном случае.

Используя средние характеристики, соотношение (1) можно представить в виде формулы:

$$\rho_i = \frac{\alpha_i \tau_i^{(1)}}{\alpha_i \tau_i^{(1)} + (1-\alpha_i)\tau_i^{(2)}} + \Theta_i.$$

Рассмотрим степень влияния надежности элемента на надежность всей системы. Очевидно, что в зависимости от величин вероятности $\rho_i$ надежность $i$-го элемента системы будет влиять на надежность системы существенно или не существенно [2]. Если величина $\rho_i$ малая, что соответствует ситуации, когда $i$-й элемент используется редко, то даже отказ этого понижает надежность системы только в том случае, когда $i$-й элемент будет использоваться для обслуживания требования. Исходя из этих рассуждений можно утверждать, что надежность $i$-го элемента системы (вероятность безотказной работы) представляет собой случайную величину, определенную в данный момент времени случайностью требований, которая принимает значение единицы, если элемент не используется, и значение $x_i$, если $i$-й элемент в данный момент времени используется для обслуживания требований. Поэтому, нам и для всякой случайной величины, для надежности $i$-го элемента имеет смысл рассматривать математическое ожидание. Поскольку природа случайности значения надежности элемента определяется его используемостью, то это можно интерпретировать как стохастическую связь этого элемента с другими элементами системы, ибо можно говорить о наличии этой связи (т.е. элемент используется и входит в связь с другими элементами), или о ее отсутствии (элемент не используется и не входит в связь с другими элементами, т.е. не является с точки зрения надежности системы в данный момент времени ее элементом) [1,2].

Обозначив через $\beta_i$ математическое ожидание надежности $i$-го элемента с учетом описанной выше природы случайности, можно записать:

$$\beta_i = \rho_i x_i + (1-\rho_i)\cdot 1 = 1-\rho_i(1-x_i), \qquad (2)$$

где $\beta_i$ практическая вероятность безотказной работы $i$-го элемента системы с учетом нагрузки системы и природы задач (требований), которые система должна выполнять (обслуживать). Пользуясь соотношением (2), можно по аналогии выразить надежность системы:

$$B(\vec{x},\vec{\rho}) = \prod_{i=1}^{n}\left[1-\rho_i(1-x_i)\right], \qquad (3)$$

где $\vec{\rho}$ и $\vec{x}$ – $n$-мерные векторы, компоненты которых $\rho_i$ и $x_i$ $(i=1,2,3,...,n)$. Если $i$-й элемент системы зарезервирован идентичными ему $S_i - 1$ элементами то величина (3) будет иметь вид:

$$B(\vec{x},\vec{\rho}) = \prod_{i=1}^{n}\left[1-\rho_i(1-x_i)^{S_i}\right]. \qquad (4)$$

Полученные соотношения (3) и (4) решают задачу повышения достоверности математических моделей для оценки надежности систем защиты информации.

Вторым фактором повышения адекватности и достоверности математических моделей оценивания надежности является способность описания, формализации и учета в этих моделях возможности управления надежностью. [3] Приращения надежности $\Theta$ за счет рационального управления надежностью достигается совершенствованием вариаций решения технической эксплуатации, вариаций режима технической эксплуатации, варьированием мероприятий по техническому и профилактическому обслуживанию. Вопрос о том как

часто и какие мероприятия по обслуживанию систем необходимо проводить, чтобы обеспечить их надежную работу, является одним из основных, ибо уменьшение интенсивности отказов элементов после рациональной процедуры регламентных работ зависит от уровня оптимизации этой процедуры. Уменьшение интенсивности потока отказов, изменение его вероятностной структуры ограниченного последействия может достигаться также специальными режимами внешних воздействий на систему.

Так, например, отдельные интегральные микросхемы при радиоактивном облучении резко уменьшают время их жизни. Тем не менее, проведение такой процедуры может быть оправдано, когда системой выполняется важная задача, значение которой позволяет пренебречь уменьшением времени жизни элемента за счет более строгого сохранения параметров в меньшем временном промежутке. Возникает задача об оптимальном управлении надежностью с целью оптимизации определенного критерия. Интерес представляет более частный случай этой задачи, а именно приращение надежности $\Theta$ изделия за счет управления надежностью. В случае исследования технической надежности системы защиты величина $x+\Theta$ – это надежность системы с учетом управления.

В моделях, где учитывается математическое ожидание надежности $B$, применение надежности $\Theta$ является детерминированным, поэтому как составляющее слагаемое выходит за оператор математического ожидания. Следовательно, $\beta+\Theta$ будет представлять математическое ожидание надежности системы при условии управления надежностью и случайной природы (во времени) задач, решаемых системой. Обозначив эту величину через $\tilde{B}$, математическая модель оценки надежности (2) порождает более общее выражение следующего вида:

$$\tilde{B}=1-\rho\left(1-x\right)+\Theta \tag{5}$$

или

$$\tilde{B}=\rho\left(x+\frac{1-\Theta-\rho}{\rho}\right). \tag{6}$$

**Выводы.** Разработанная модель (5) и ее модификация (обладает всеми теми же свойствами, что и ранее полученная модель (2).

### Литература


1. Гурина С.А. Живучесть систем защиты информации в условиях внешних воздействий / Гурина С.А., Егоров Ф.И., Хорошко В.А. // Захист інформації, №2, 2008. – С.69-73.
2. Гурина С.А. Создание информационных моделей систем управления защитой объектов / Гурина С.А., Егоров Ф.И., Хорошко В.А. // Вісник ДУІКТ, т. 6, №2, 2008. – С. 147-153.
3. Петров А.А. Способ формирования спецфакторов в моделях оценивания живучести систем охраны объектов / Петров А.А., Хорошко В.А. // Вісник Східноукраїнського національного університету ім. В. Даля, №8 (126), част.1, 2008. – С. 22-24.


*Статтю подано 15.10.2009*