УДК 621.31

В.С. Харченко[1], О.Н. Одарущенко[2]

[1]*Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Украина*
[2]*Полтавский национальный технический университет им. Юрия Кондратюка, Украина*

МОДЕЛЬ ИНФОРМАЦИОННО-ТЕХНИЧЕСКОГО СОСТОЯНИЯ КОМПЬЮТЕРНОЙ СИСТЕМЫ

Уточнено и формализовано понятие информационно-технического состояния (ИТС) компьютерной системы. При определении ИТС компьютерной системы предлагается учитывать состояние аппаратных, программных и информационных ресурсов.

Ключевые слова: *гарантоспособность, информационно-техническое состояние, дефект аппаратных средств, проектный дефект программных средств, проектный дефект аппаратных средств, дефект взаимодействия, операция преобразования состояния.*

Введение

Компьютерные системы, осуществляющие прием, хранение, обработку и выдачу информации, функционируют в условиях действия внутренних и внешних факторов, приводящих к нарушению их работоспособности и целостности обрабатываемой информации. Комплекс свойств системы противостоять этим факторам и обеспечить предоставление требуемых услуг (выполнение функций), которым можно оправданно доверять, называют гарантоспособностью [1]. Элементами таксономии гарантоспособности, как известно [1, 2], являются:

– угрозы (уязвимости, вторжения, дефекты, ошибки, отказы), которые могут привести к непредставлению услуг;

– механизмы отказоустойчивости (отказобезопасности, устойчивости к вторжениям), обеспечивающие устранение или снижение рисков таких угроз;

– первичные свойства гарантоспособности, характеризующие различные аспекты и степень устойчивости системы к различным типам угроз (безотказность, готовность, функциональная безопасность, целостность и др.);

– вторичные свойства, которые являются производными от первичных и более детально характеризуют составляющие гарантоспособности (например, контролепригодность для готовности).

Одним из базовых понятий, позволяющих методологически объединить элементы таксономической схемы гарантоспособности, является понятие информационно-технического состояния (ИТС). Исходная идея ИТС была сформулирована в [3], а его определение, расширяющее стандартное понятие технического состояния, дано в [4]: ИТС – это совокупность свойств и признаков как технического, так и информационного характера, присущих системе в определенный момент времени.

К числу свойств, которые должны при этом рассматриваться, относятся первичные свойства гарантоспособности, к числу признаков – множество состояний системы (исправных – неисправных, работоспособных – частично работоспособных – неработоспособных, безопасных – потенциально опасных – опасных или критических) с учетом того, что переходы между ними могут осуществляться вследствие:

– возникновения или проявления физических дефектов (ДФ) аппаратных средств;

– проектных дефектов (ДП) программных (ДПП) и аппаратных (ДПА) средств;

– дефектов взаимодействия (ДВ), которые вызываются случайными непредумышленными или предумышленными внешними воздействиями физической природы (ДВФ) (механическими, климатическими, электромагнитными, радиационными и др.) или информационными воздействиями (ДВИ) (ошибочными действиями персонала, хакерскими атаками, спамом и т.д.).

В данной статье ставится **цель** – развить понятие и дать формализованное описание ИТС с позиций одного из принципов системного подхода – принципа дополнения на основе модели «система-среда» [5].

1. Модель «система – физическая и информационная среда»

Представим модель состояний системы S(t) с учетом воздействий среды E(t) (внешних и внутренних воздействий). Вектор состояния системы в момент времени t:

$$S(t) = \{S_0(t),\ E_{int}(t),\ E_{ext}(t)\}, \qquad (1)$$

где $S_0(t)$ – работоспособное (и целостное) состояние, в котором система находится при отсутствии внутренних и внешних воздействий и которое характеризуется полным соответствием требованиям к ней, включая требования по всем составляющим гаран-

тоспособности (безотказности, функциональной и информационной безопасности); $E_{int}(t)$ – вектор внутренних воздействий, включающий воздействия, обусловленные физическими $E_{int.phs}(t)$ и проектными $E_{int.des}(t)$ дефектами:

$$E_{int}(t) = \{E_{int.phs}(t), E_{int.des}(t)\}; \quad (2)$$

$E_{ext}(t)$ – вектор внешних воздействий, включающий векторы внешних информационных $E_{ext.inf}(t)$ и физических $E_{ext.phs}(t)$ воздействий соответственно, вызывающих дефекты взаимодействия:

$$E_{ext}(t) = \{E_{ext.inf}(t), E_{ext.phs}(t)\}; \quad (3)$$

$S(t+\Delta t)$ – вектор состояния системы в момент времени $t+\Delta t$:

$$S(t+\Delta t) = \{S_{Eint}(t+\Delta t), S_{Eext}(t+\Delta t)\}, \quad (4)$$

где $S_{Eint}(t+\Delta t) = \{S_{Ehw}(t+\Delta t), S_{Esw}(t+\Delta t)\}$ – внутреннее состояние системы в момент времени $t+\Delta t$, характеризуемое состояниями его аппаратных $S_{Ehw}(t+\Delta t)$ и программных $S_{Esw}(t+\Delta t)$ средств (ресурсов); $S_{Eext}(t+\Delta t) = \{S_{Econ}(t+\Delta t), S_{Eitg}(t+\Delta t)\}$ – внешнее состояние системы в момент времени $t+\Delta t$, характеризуемое состояниями информационных ресурсов системы (их целостностью) $S_{Eitg}(t+\Delta t)$ и среды (доступностью к конфиденциальным информационным ресурсам) $S_{Econ}(t+\Delta t)$.

Реакция системы на внутренние и внешние физические воздействия проявляется тем, что система формирует ошибочную выходную информацию в данный момент времени или один из последующих моментов времени.

Реакция системы на внешние информационные воздействия проявляется тем, что нарушается внутренняя информация, циркулирующая или хранящаяся в системе, или среда (внешняя система) получает несанкционированный доступ к этой информации в данный или один из последующих моментов времени.

Допущение 1. Будем считать, что интервал времени Δt мал настолько, что общий поток внутренних и внешних воздействий, характеризуемый вектором $E(t)$ можно считать ординарным. Это не исключает возможность неординарности внутренних (вектор $E_{int}(t)$) и внешних (вектор $E_{ext}(t)$) воздействий, а также их составляющих ($E_{int.phs}(t)$, $E_{int.des}(t)$, $E_{ext.inf}(t)$, $E_{ext.phs}(t)$) в пределах интервала Δt. Следующее внутреннее или внешнее воздействие может произойти в момент времени $\Delta t_+ > \Delta t$.

Допущение 2 (*Утверждение* 1). При $t = 0$ $E_{int}(0) = \varnothing$, $E_{ext}(0) = \varnothing$, $S(0) = S_0(0)$. Такое допущение является общепринятым в теории надежности и соответствует физическому смыслу и реальной практике эксплуатации систем. В тоже время оно может быть доказано как утверждение.

Если при $t = 0$ $E_{int}(0) \neq \varnothing$ или $E_{ext}(0) \neq \varnothing$, можно условно рассмотреть поведение системы на интервале времени $\{t^* = 0, t = 0\}$, где $t^* = t - t_0$, а t_0 – продолжительность времени, в течение которого система подвергается внутренним $E_{int}(t^*)$ или внешним $E_{ext}(t^*)$ воздействиям. Всегда можно подобрать длительность интервала t_0 такую, чтобы:

– либо в его начале всегда выполнялось условие $S(t^* = 0) = S_0(t^* = 0)$ и сохранялось далее на всем интервале $\{t^* = 0, t = 0\}$ в условиях воздействий;

– либо к завершению интервала система полностью восстанавливалась бы при нарушении этого условия вследствие воздействий в момент времени $t - t_0 < t^* < t$.

Следовательно, утверждение доказано путем введения виртуального интервала времени $\{t^* = 0, t = 0\}$.

Таким образом, можно записать, что

$$S(t+\Delta t) = S_0(t) \,//\, \{E_{int}(t), E_{ext}(t)\}, \quad (5)$$

где символом // обозначен обобщенный оператор преобразования состояния $S_0(t)$ при воздействиях $E_{int}(t)$, $E_{ext}(t)$ (или сокращенно «ОПС»).

Аналогично справедливо

$$S(t) = S_0(t-\Delta t) \,//\, \{E_{int}(t-\Delta t), E_{ext}(t-\Delta t)\}. \quad (6)$$

2. Модель ИТС

С учетом (2, 3, 5) получим:

$$S(t+\Delta t) = \{S_0(t) \,//\, \{E_{int.phs}(t), E_{int.des}(t), E_{ext.inf}(t), E_{ext.phs}(t)\}\}. \quad (7)$$

Допущение 3. Будем считать внутренние $E_{int}(t)$ и внешние $E_{ext}(t)$ воздействия не зависимыми между собой по моменту времени и характеристикам воздействий. Это допущение подтверждается опытом эксплуатации, а также разной природой воздействий. При более детальном рассмотрении составляющих воздействий можно говорить о возможности в общем случае некоторой корреляции составляющих $E_{int.phs}(t)$ и $E_{int.des}(t)$, $E_{int.des}(t)$ и $E_{ext.inf}(t)$, $E_{int.phs}(t)$ и $E_{ext.phs}(t)$.

Проведем преобразование

$$S(t+\Delta t) = \{S_{tec}(t+\Delta t), S_{inf}(t+\Delta t)\}, \quad (8)$$

где

$$S_{tec}(t+\Delta t) = \{S_0(t) // \{E_{int.phs}(t), E_{int.des}(t), E_{ext.phs}(t)\}\}, \quad (9)$$

$$S_{inf}(t+\Delta t) = \{S_0(t) // E_{ext.inf}(t)\}. \quad (10)$$

Состояния $S_{tec}(t+\Delta t)$ и $S_{inf}(t+\Delta t)$ будем называть техническим и информационным состояниями соответственно. Тогда состояния $S(t+\Delta t)$ или $S(t)$ будем называть информационно-техническим состоянием системы.

При $E_{int}(t) = \varnothing$, $E_{ext}(t) = \varnothing$

$$S(t+\Delta t) = S_0(t)$$

и состояние $S(t+\Delta t)$ будем называть исправным ИТС, при котором выполняются все требования к системе.

Работоспособное (исправное или неисправное) ИТС имеет место, если при $E_{int}(0) \neq \varnothing$ или $E_{ext}(0) \neq \varnothing$, $S(t+\Delta t) = S_0(t) \vee S'_0(t)$, где $S'_0(t)$ – состояние, аналогичное работоспособному техническому состоянию, при котором выполняются также основные требования по целостности и конфиденциальности информации.

Неработоспособным ИТС $S_H(t)$ будем называть состояние, при котором не выполняется хотя бы одно из требований к работоспособности системы в части всех составляющих гарантоспособности.

3. Свойства ОПС

Исследуем свойства операции преобразования состояния //.

Ассоциативность. Операция // не обладает свойством ассоциативности, поскольку в общем случае $\{S_0(t) // \{E_{int.phs}(t), E_{int.des}(t), E_{ext.inf}(t), E_{ext.phs}(t)\}\} \neq \{\{\{S_0(t) // E_{int.phs}(t)\} // E_{int.des}(t)\} // E_{ext.inf}(t)\} // E_{ext.phs}(t)$.

Коммутативность. Очевидно, что эта операция не является коммутативной по отношению к левой и правой частям, поскольку преобразование E(t) // S(t) лишено физического смысла. Что касается свойства коммутативности операции по воздействиям, то в частном случае таким свойством могут обладать пары воздействий $E_{int.phs}$ и $E_{ext.phs}$, $E_{int.phs}$ и $E_{int.des}$, $E_{int.des}$ и $E_{ext.phs}$. Воздействия $E_{ext.inf}$ некоммутативны со всеми иными воздействиями.

Транзитивность. Свойство транзитивности для операции преобразования лишено физического смысла в силу единичности рассматриваемых состояний.

*Дистрибутивность***.** Выражения (8 – 10) постулируют свойство дистрибутивности ОПС в части относительной независимости этих составляющих ИТС в соответствии с допущением 3.

Выводы

В данной работе уточнено и формализовано понятие информационно-технического состояния. При определении ИТС компьютерной системы должно учитываться состояние аппаратных, программных и информационных ресурсов.

При этом состояния аппаратных средств и, с некоторой условностью, программных средств (вследствие необходимости поступления на входы системы определенной информации) полностью определяют техническую компоненту ИТС, а состояние информационного ресурса – его информационную компоненту.

Состояние информационного ресурса (в отличие от аппаратных и программных) включает как внутреннюю (целостность), так и внешнюю (конфиденциальность) составляющие среды или иной системы, с которой взаимодействует данная. Техническая компонента ИТС нарушается вследствие ДФ, ДПА, ДПП, ДВФ, информационная – вследствие ДВИ. Такой подход детализирует реализацию принципа дополнения в системе «КС-среда» в части определения ИТС.

Введен обобщенный оператор преобразования состояния системы (оператор воздействий) и исследованы его свойства. Фактически состояния системы (технические, информационные и ИТС), воздействия и этот оператор образуют алгебру {S, E, //}, которая является основой для общего описания поведения компьютерных систем, функционирующих в условиях внутренних и внешних угроз.

Далее следует расширить предложенную модель с учетом различных методов обеспечения гарантоспособности.

Список литературы

1. Avizienis A. Basic Concepts and Taxonomy of Dependable and Secure Computing / A. Avizienis, J.-C. Laprie, B. Randell, C. Landwehr // IEEE Trans. On Dependable and Secure Computing. – 2004. – Vol. 1, №1. – P. 11-33.

2. Харченко В.С. Гарантоспособность и гарантоспособные системы: элементы методологии / В.С. Харченко // Радіоелектронні і комп'ютерні системи. – 2006. – Вип. 5(17). – С. 7-19.

3. Харченко В.С. Гарантоздатність комп'ютерних систем: межа універсальності в контексті інформаційно-технічоного стану / В.С. Харченко // Радіоелектронні і комп'ютерні системи. – 2007. – № 8(20). – С. 8-16.

4. Отказобезопасные информационно-управляющие системы на программируемой логике / Под ред. В.С. Харченко, В.В. Скляра. – Нац. аэрокосм. ун-т «ХАИ», НПП «Радий», 2008. – 380 с.

5. Месарович М. Общая теория систем: Математические основы / М. Месарович, Я. Такахара. – М.: Мир, 1978. – 311 с.

Поступила в редколлегию 1.12.2008

Рецензент: д-р техн. наук, проф. В.М. Илюшко, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков.

МОДЕЛЬ ІНФОРМАЦІЙНО-ТЕХНІЧНОГО СТАНУ КОМП'ЮТЕРНОЇ СИСТЕМИ

В.С. Харченко, О.М. Одарущенко

Уточнено і формалізовано поняття інформаційно-технічного стану (ІТС) комп'ютерної системи. При визначені ІТС комп'ютерної системи пропонується враховувати стан апаратних, програмних і інформаційних ресурсів.

Ключові слова: *гарантоздатність, інформаційно-технічний стан, дефект апаратних засобів, проектний дефект програмних засобів, проектний дефект апаратних засобів, дефект взаємодії, операція перетворення стану.*

MODEL OF THE INFORMATIVELY-TECHNICAL STATE OF THE COMPUTER SYSTEM

V.S. Kharchenko, O.N. Odaruschenko

Specified concept of the informatively-technical state (ITS) of the computer system. At determination of ITS of the computer system it is suggested to take into account the state of vehicle, programmatic and informative resources.

Keywords: *dependability, informatively-technical state, defect of facilities of vehicles, project defect of programmatic facilities, project defect of facilities of vehicles, defect of co-operation, operation of transformation of the state.*