УДК 621.3.019.3

Н.В. СЕСПЕДЕС ГАРСИЯ*

ОЦЕНКА УРОВНЯ ЦЕЛОСТНОСТИ ГАРАНТОСПОСОБНЫХ КОМПЬЮТЕРНЫХ СИСТЕМ

*Институт проблем математических машин и систем НАН Украины, Киев, Украина

Анотація. *У статті розглянуті основні аспекти цілісності гарантоздатних комп'ютерних систем (ГКС), описані механізми та методи забезпечення цілісності ГКС, запропоновано метод кількісної оцінки рівня цілісності систем.*
Ключові слова: *цілісність, порушення цілісності, методи забезпечення цілісності, оцінка цілісності.*

Аннотация. *В статье рассмотрены основные аспекты целостности гарантоспособных компьютерных систем (ГКС), описаны механизмы и методы обеспечения целостности ГКС, предложен метод количественной оценки уровня целостности систем.*
Ключевые слова: *целостность, нарушение целостности, методы обеспечения целостности, оценка целостности.*

Abstract. *The main aspects of the integrity of dependable computer systems (DCS) are regarded in the paper; the mechanisms and methods to ensure the integrity of the DCS are described. A method of quantitative assessment of the system integrity level is proposed.*
Keywords: *integrity, loss of integrity, methods to ensure the integrity, assessment of the integrity.*

1. Введение

Широкое внедрение информационных технологий, наряду с позитивным влиянием на все стороны человеческой деятельности, привело к появлению новых угроз безопасности людей. Любая информация, которая создается, хранится и обрабатывается с помощью вычислительной техники, все больше зависит от поведения и действия людей и технических систем. Резко возросли возможности нанесения ущерба, связанные с хищением информации, так как благодаря информации о структуре и принципах функционирования системы появилась возможность воздействовать на любую систему (социальную, биологическую или техническую) с целью ее уничтожения, снижения эффективности функционирования или воровства ее ресурсов (денег, товаров, оборудования).

2. Определение понятия целостности

Для проведения анализа алгоритмов и методов обеспечения целостности необходимо привести само определение понятия *целостности гаратноспособных компьютерных систем (ГКС).*

Под *целостностью ГКС* следует понимать свойство ее компонентов и ресурсов быть неизменным (как в семантическом смысле, так и в структурном) при функционировании системы в условиях случайных или преднамеренных искажений или разрушающих воздействий.

Поскольку работоспособность и безопасность ГКС напрямую зависят от информации, которая в ГКС обрабатывается, то следует разделять целостность самой ГКС и целостность информации (рис. 1) [1].

В самом общем случае *целью целостности* является обеспечение конкретной обработки, конкретных данных в нужном формате (семантически), в определенном виде (физически), задействовав нужные ресурсы, по сигналу нужных пользователей в определенное время.

© Сеспедес Гарсия Н.В., 2013

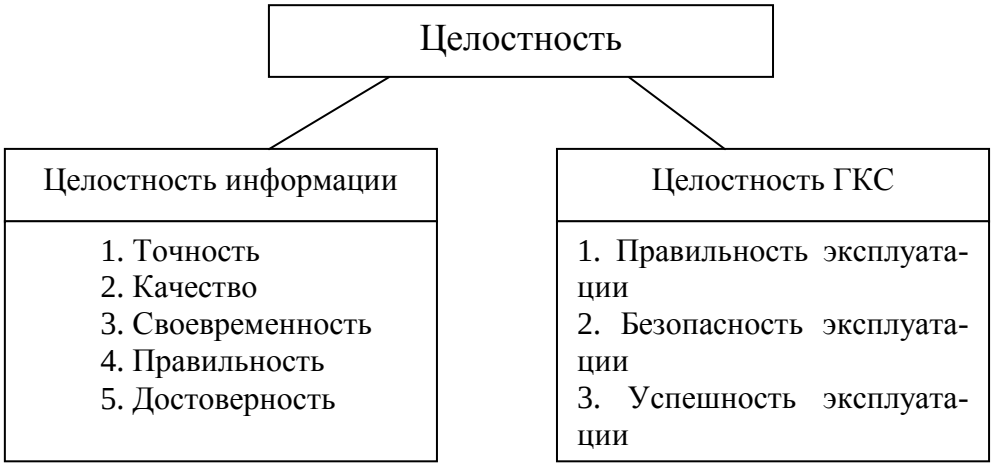

Рис. 1. Составляющие целостности системы

Целостность информации – способность средства вычислительной техники или ГКС обеспечивать неизменность информации в условиях случайного и (или) преднамеренного искажения (разрушения) [2].

Целостность ГКС с точки зрения безопасности – свойство исключать непредусмотренные изменения системы и предоставляемых услуг.

3. Причины нарушения целостности ГКС и возможные угрозы

Чтобы сформулировать некоторые более конкретные цели в вопросах целостности, необходимо определить причины и угрозы ее нарушения (табл. 1).

Таблица 1. Причины нарушения целостности ГКС и возможные угрозы

Причина нарушения целостности	Возможные угрозы
Просчеты в разработке системы. Невыявленные и неустраненные ошибки в программных и аппаратных средствах в процессе отладки и испытаний после их разработки	Некорректная работа аппаратных и программных средств. Возникновение конфликтных состояний. Реализация необратимых функций
Непрофессиональные действия персонала при взаимодействии с КС (злонамеренные/случайные)	Некорректная работа аппаратных и программных средств. Нарушения правил эксплуатации. Нарушения физической и логической целостности структур данных (уничтожение, порча информации)
Воздействия, причиненные несанкционированными пользователями или программами	Физическое уничтожение. Атака, взлом. Подмена, воровство данных. Повреждение, уничтожение данных, заражение вирусами
Старение и износ аппаратных средств	Некорректная работа аппаратных средств. Нарушения физической и логической целостности структур данных

4. Средства обеспечения целостности ГКС

Значительное место в данном вопросе занимают разработанные *модели обеспечения целостности*, позволяющие интерпретировать проблему в определенном виде, используя системный подход, что делает возможным разбиение ее на составляющие в зависимости от их функций (рис. 2) [3]. Отдельным решением представляются разного рода *активные средства обеспечения целостности* – «агенты», антивирусы, центры обеспечения безопасности, принцип действия которых основан на *семантическом анализе* действий пользователя и данных системы.

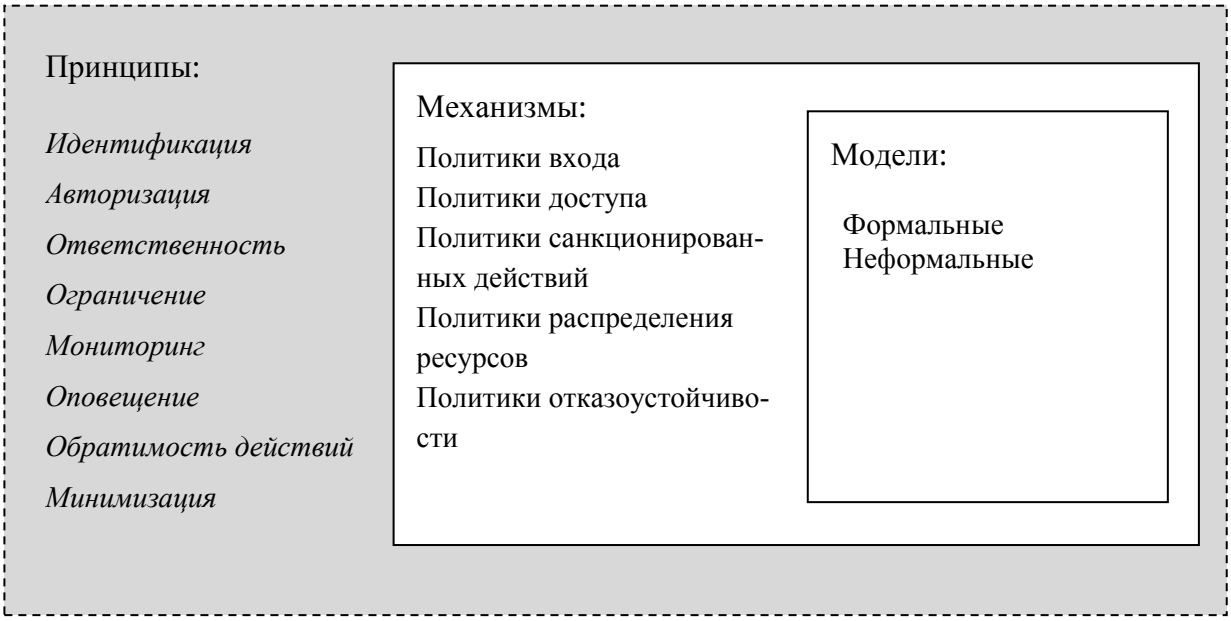

Рис. 2. Средства обеспечения целостности ГКС

5. Механизмы и методы обеспечения целостности КС

К *механизмам обеспечения целостности* относятся политики и методы, согласно которым предпринимаются определенные действия по отношению к системе и ее субъектам (табл. 2) [3]. В истоке политики и методы были в большинстве своем организационными мерами, но сейчас они представляют собой *автоматизированную систему безопасности и целостности*, реализованную либо ресурсами и программными средствами самой ГКС, либо отдельными компонентами ГКС.

Таблица 2. Механизмы и методы обеспечения целостности ГКС

Политики	Методы	
Политика идентификации и аутентификации	Идентификация и аутентификация пользователей. Аутентификация устройств. Идентификация и аутентификация объектов	
Политика санкционированных действий	Условия авторизации	Условия валидности. Количественная проверка
	Разделение полномочий	Распределение обязанностей. Административный контроль. Контроль пользователей. Согласование процессов и событий

Продолж. табл. 2

Политика распределения ресурсов	Адресация и местоопределение	Присвоение описания. Распределение пространственных имен
	Инкапсуляция	Абстракция типов данных. Строгая типизация. Домены. Роли. Передача сообщений. Шлюзы
	Контроль доступа	Возможности. Списки доступа. Метки
Политика отказоустойчивости	Контроль целостности	Передача списков. Контрольные суммы. Криптографические контрольные суммы Цепи контрольных сумм
	Обработка ошибок	Дублирование протоколов. Ручная проверка протоколов. Протоколы квитирования связи. Корректировочные коды

Политика целостности подразумевает под собой конечное множество условий, при выполнении которых санкционированные пользователи системы получают определенный доступ к информации и ресурсам ГКС. Необходимые условия задаются в виде требований и должны быть предусмотрены и реализованы в системе обеспечения целостности ГКС. Функционирование конкретной политики целостности базируется на соответствующих *механизмах целостности.* В большинстве случаев механизмы целостности могут состоять из *автоматизированных и организационных компонентов*. Автоматизированные компоненты часто являются частью основного вычислительного окружения, включая соответствующее множество процедур пользователя и администратора.

6. Оценка целостности ГКС

Общим для моделей обеспечения целостности является то, что все они направлены на введение определенных обязательных процедур анализа целостности программ, средств, ресурсов и пользователей, которые взаимодействуют с ГКС. Подход к решению вопросов целостности, основанный на построении моделей безопасности и целостности, берет свое начало з 1970-х годов, когда были заложены первые модели безопасности [4].

Предлагается универсальный подход к оценке целостности системы. Каждой метрике целостности соответствует набор критериев, по которым происходит оценка целостности ГКС (табл. 3). Набор критериев можно менять в зависимости от назначения и специфики функционирования конкретной ГКС.

Каждой метрике соответствует набор критериев оценки, количество которых равно n. Уровень исполнения критерия оценки определяется величиной $u_i \ \ (i = 1, \ldots n)$, которая находится в диапазоне значений 0÷1. Оценка уровня исполнения критерия осуществляется следующим образом:

• при полном отсутствии выполнения критерия – $u_i = 0$;

• при выполнении критерия на 10%-90% – $u_i = 0{,}1 - 0{,}9$;

• при 100% выполнении критерия – $u_i = 1$.

Таблица 3. Основные метрики целостности

Метрики целостности	Наименование критерия	Уровень исполнения критерия u_i
1	2	3
Целостность вычислительных ресурсов (ВР) – свойство исключать непредусмотренные структурные изменения системы и предоставляемых услуг	Правильность эксплуатации ВР	0–1
	Безопасность эксплуатации ВР	0–1
	Успешность эксплуатации ВР	0–1
	Способность проверять и сохранять данные	0–1
	Способность защиты от серьёзных последствий для целостности в случае ошибок	0–1
	Способность восстанавливать целостность после сбоев и ошибок	0–1
	Наличие защиты от нарушений авторского права	0–1
	Наличие функций восстановления целостности	0–1
	Наличие функций контроля целостности	0–1
	Наличие функций идентификации и аутентификации	0–1
	Наличие средств мониторинга и оповещения	0–1
	Наличие средств обработки ошибок	0–1
Целостность программных ресурсов (ПР) – свойство исключать непредусмотренные изменения программных ресурсов системы	Наличие функций в ПР по восстановлению процесса выполнения в случае сбоя операционной системы, процессора, внешних устройств	0–1
	Наличие средств восстановления процесса в случае сбоев оборудования	0–1
	Наличие возможности повторного старта с точки останова	0–1
	Наличие автоматического резервирования для сохранения текущего состояния процесса	0–1
	Наличие требований по устойчивости функционирования при наличии ошибок во входных данных, ошибок пользователя, отсутствие необходимых данных (на диске, в файле, в БД и т.д.)	0–1
	Совместимость с техническими средствами	0-1
	Совместимость с системными программными средствами	0–1

Продолж. табл. 3

	Совместимость с другим программным обеспечением, включая обмен данными (с текстовыми, графическими редакторами, БД и др.)	0–1
	Наличие устойчивости функционирования при наличии ошибок во входных данных, ошибок пользователя, отсутствие необходимых данных (на диске, в файле, в БД и т.д.)	0–1
	Возможность обработки ошибочных ситуаций	0–1
	Наличие возможности повторного старта с точки останова	0–1
Целостность информации – способность ГКС обеспечивать неизменность информации в условиях случайного и (или) преднамеренного искажения (разрушения)	Достоверность	0–1
	Точность	0–1
	Качество	0–1
	Своевременность	0–1
	Правильность	0–1
	Наличие информации о способности проверять правильность вводимой/выводимой информации	0–1
	Наличие информации о процедурах хранения данных	0–1
	Наличие тестов для проверки допустимых значений входных/выходных данных	0–1
	Наличие системы контроля полноты входных/выходных данных	0–1
	Наличие средств контроля корректности входных/выходных данных	0–1
	Наличие средств контроля непротиворечивости входных/выходных данных	0–1
	Наличие проверки параметров и адресов по диапазону значений	0–1
	Наличие обработки предельных значений	0–1
	Наличие информации о способности восстанавливаться после ошибок	0–1

Количественной оценкой метрики является усредненная оценка уровней исполнения ее критериев и вычисляется по формуле

$$L = \sum_{i=1}^{n} u_i \Big/ n . \qquad (1)$$

Уровень целостности вычислительных ресурсов L_{PC} – характеристика способности системы исключать непредусмотренные структурные изменения и предоставляемые услуги.

Уровень целостности программных ресурсов L_P – характеристика способности системы исключать непредусмотренные изменения программных ресурсов.

Уровень целостности информации L_I – характеристика способности системы обеспечивать неизменность информации в условиях случайного и (или) преднамеренного искажения (разрушения).

Если значения характеристик, вычисленных по формуле (1), L_{PC}, L_P, $L_I > 0{,}9$, то система соответствует заданным уровням целостности вычислительных ресурсов, программных ресурсов и информации.

7. Выводы

Сегодня вопрос обеспечения целостности ГКС является особо актуальным для систем *с большими массивами информации* (базами данных), а также при построении *открытых многопользовательских вычислительных систем и сред*.

Несмотря на то, что вопросы целостности систем были подняты еще в 70-х годах, остаются нерешенными вопросы *объективной оценки уровня целостности систем*, а тем более уровня целостности ГКС, к которым предъявляются особые требования по безопасности функционирования. Современные модели целостности базируются на использовании разнообразных политик и методов целостности, которые включают в себя наборы ограничений и правил того или иного порядка. По отдельному направлению осуществляется эволюция систем мониторинга и контроля целостности, представляющая собой разнообразные агенты, сканнеры и прочие активные приложения по контролю целостности информации и структуры. Разработанный подход к количественной оценке уровня целостности ГКС является универсальным и может применяться для систем самого разнообразного назначения.

СПИСОК ЛИТЕРАТУРЫ

1. Власова Л.А. Защита информации / Власова Л.А. – Хабаровск: РИЦ ХГАЭП, 2007. – 84 с.
2. Р 50.1.053-2005. Рекомендации по стандартизации «Информационные технологии. Основные термины и определения в области технической защиты информации». – М.: Издательство стандартов, 2006. – 13 с.
3. Integrity in automated information systems / T. Mayfield, J.E. Roskos, S.R. Welke [et al.] // National Computer Security Center (NCSC). – Alexandria,Virginia, 1991. – 130 p.
4. Математические основы информационной безопасности / А.П. Баранов, Н.П. Борисенко, П.Д. Зегжда [и др.]. – Орел: ВИПС, 1997. – 354 с.

Стаття надійшла до редакції 04.11.2013