УДК 621.3.019.3

Ф.М. ЦИВІЛЬСЬКИЙ, О.О. БОСКІН
Херсонський національний технічний університет

СПОСІБ ОТРИМАННЯ ОЦІНКИ ЦІЛІСНОСТІ ГАРАНТОЗДАТНОЇ КОМП'ЮТЕРНОЇ СИСТЕМИ

У даній роботі розглянуті основні аспекти цілісності гарантоздатних комп'ютерних систем (ГКС). ГКС подається як головний утворюючий чинник при проектуванні і експлуатації комп'ютерних систем. Описані механізми та методи забезпечення цілісності ГКС, запропоновано метод кількісної оцінки рівня цілісності систем. Загальна оцінка цілісності розглянута за трьома критеріями: цілісність обчислювальної інфраструкти, цілісність програмних ресурсів, цілісність інформації.

Ключові слова: цілісність, порушення цілісності, методи забезпечення цілісності, оцінка цілісності.

Ф.Н. ЦИВИЛЬСКИЙ, О.О. БОСКИН
Херсонский национальный технический университет

СПОСОБ ПОЛУЧЕНИЯ ОЦЕНКИ ЦЕЛОСТНОСТИ ГАРАНТОСПОСОБНОЙ КОМПЬЮТЕРНОЙ СИСТЕМЫ

В данной работе рассмотрены основные аспекты целостности гарантоспособных компьютерных систем (ГКС). ГКС представляется как главный образующий фактор при проектировании и эксплуатации компьютерных систем. Описанны механизмы и методы обеспечения целостности ГКС, предложен метод количественной оценки уровня целостности систем. Общая оценка целостности рассмотрена по трем критериям: целостность вычислительной инфраструктуры, целостность программных ресурсов, целостность информации.

Ключевые слова: целостность, нарушение целостности, методы обеспечения целостности, оценка целостности.

F.M.TSYVILSKYY, O.O. BOSKIN
Kherson National Technical University

INTEGRITY ASSESSMENT METHOD FOR COMPUTER SYSTEM OF DEPENDABILITY

This paper describes the main aspects of dependability integrity Computer Systems (ACS). ACS served ascreating a major factor in the design and operation computer systems.The mechanisms and methods to ensure the integrity of ACS, the method of quantitative evaluation of the integrity of the system. Overall integrity examined by three criteria: integrity computing infrastructure facilities, the integrity of software resources, the integrity of the information.

Keywords: integrity, violation of integrity, integrity methods, evaluation of integrity.

Постановка проблеми

Питання забезпечення цілісності гарантоздатних комп'ютерних систем (ГКС) є актуальним для систем з великими масивами інформації, а також при побудові відкритих комп'ютерних систем і мереж. Гарантоздатність - це здатність КС надавати необхідні послуги, яким можна виправдано довіряти. Гарантоздатність є комплексною властивістю, що включає: безвідмовність (reliability); готовність (availability); живучість (survivability); функціональну безпеку (safety); цілісність (integrity); конфіденційність (confidentiality); достовірність (high confidence); здатність до обслуговування (maintainability).

Розглянуті властивості, складові гарантоздатності, є первинними, для кожного з них можуть бути визначені вторинні властивості.

Під цілісністю ГКС (комп'ютерних мереж, алгоритмів і методів і т.п.) слід розуміти властивість її компонентів і ресурсів виключати непередбачені зміни системи та послуг при функціонуванні в умовах випадкових або навмисних спотворень або руйнуючих дій.

Для ГКС загрози порушення цілісності полягають у спотворенні або зміні неавторизованим користувачем інформації, що зберігається або передається. Цілісність інформації може бути порушена як зловмисником, так і в результаті об'єктивних впливів із сторони середовища експлуатації системи. В цілому ГКС залежить від цілісності інформації та цілісності комп'ютерної системи, яка передає і обробляє дані для користувачів.

У самому загальному випадку метою цілісності є забезпечення конкретної обробки, конкретних даних у потрібному форматі (семантично), в певному виді (фізично), задіявши потрібні ресурси, за сигналом потрібних користувачів в певний час.

Аналіз останніх досліджень і публікацій

Аналіз наукової літератури [1] з означеної проблеми засвідчує, що саме проблема порушення цілісності комп'ютерної інформаційної системи для забезпечення її гарантоздатності є головним утворюючим чинником при її проектуванні і експлуатації (рис. 1).

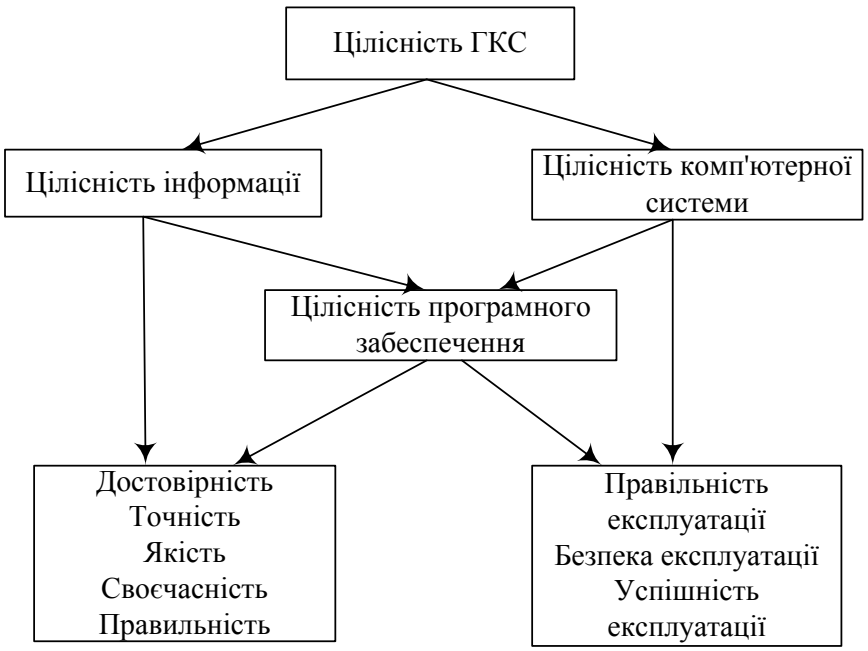

Рис. 1. Складові частини цілісності системи

Формулювання конкретних цілей в питаннях цілісності потребує визначення причин та загроз її порушення. Причини порушення цілісності ГКС і можливі загрози наведені в таблиці 1.

Таблиця 1

Причини порушення цілісності ГКС і можливі загрози

Причина порушення цілісності	Можливі загрози
Прорахунки в розробці системи. Невиявлені і не усунуті помилки в програмних і апаратних засобах в процесі налагодження і випробувань після їх розробки	Некоректна робота апаратних і програмних засобів. Виникнення конфліктних станів. Реалізація необоротних функцій
Непрофесійні дії персоналу при взаємодії з КС (зловмисні/випадкові)	Некоректна робота апаратних і програмних засобів. Порушення правил експлуатації. Порушення фізичної та логічної цілісності структур даних (знищення, псування інформації)
Вплив, завданий несанкціонованими користувачами або програмами	Фізичне знищення. Атака, злом. Підміна, викрадення даних. Пошкодження, знищення даних, зараження вірусами
Старіння і знос апаратних засобів	Некоректна робота апаратних засобів. Порушення фізичної та логічної цілісності структур даних

Формулювання мети дослідження

Мета дослідження – розробити, теоретично обгрунтувати та дослідити феномен інформаційної системи.

Загальним для моделей забезпечення цілісності є те, що всі вони спрямовані на запровадження певних обов'язкових процедур аналізу цілісності програм, засобів, ресурсів і користувачів, які

взаємодіють з ГКС. Підхід до вирішення питань цілісності, заснований на побудові моделей безпеки і цілісності, бере свій початок з 1970-х років, коли були закладені перші моделі безпеки [2].

Викладення основного матеріалу дослідження

Пропонується універсальний підхід до оцінки цілісності інформаційної системи. Кожній метриці цілісності відповідає набір критеріїв, за якими відбувається оцінка цілісності ГКС. Набір критеріїв можна змінювати в залежності від призначення і специфіки функціонування конкретної ГКС.

Кожній метриці відповідає набір критеріїв оцінки, кількість яких дорівнює n. Рівень виконання критерію оцінки визначається величиною u_i (i= 1,… n), яка знаходиться в діапазоні значень 0 – 1. Оцінка рівня виконання критерію здійснюється наступним чином:

– при повній відсутності виконання критерію – u_i= 0;

– при виконанні критерію на 10%-90% – u_i= 0,1 – 0,9;

– при 100% виконанні критерію – ui = 1.

Загальна оцінка цілісності відбувається за трьома критеріями:

1) рівень цілісності обчислювальної інфраструкти L_{PC} – характеристика здатності системи виключати непередбачені структурні зміни і надані послуги;

2) рівень цілісності програмних ресурсів L_P– ресурсів характеристика здатності системи виключати непередбачені зміни програмних ресурсів.

3) рівень цілісності інформації L_I– характеристика здатності системи забезпечувати незмінність інформації в умовах випадкового і (або) навмисного викривлення (руйнування).

Якщо значення характеристик (метрик) L_{PC}, L_P, L_I, обчислених за формулою:

$$L = \sum_{i=1}^{n} \frac{u_i}{n} \tag{1}$$

більше 0,9, то система відповідає заданим рівням цілісності обчислювальних ресурсів, програмних ресурсів та інформації.

В результаті дослідження комп'ютерної мережі у Херсонському філіалі Одеського наукового інституту медицини транспорту на підставі експертного оцінювання були отримані значення критеріїв u_i.

У табл. 2 представлено оцінювання рівнів виконання критеріїв цілісності для комп'ютерної мережі відділу автоматизації.

Таблиця 2

Оцінка метрик цілісності мережі

Метрики цілісності	Назва критерію	Критерій u_i
1	2	3
Цілісність обчислювальної інфраструкти (ОІ) - властивість виключати непередбачені структурні зміни системи та послуг (L_{PC})	Правильність експлуатації ОІ	1
	Безпека експлуатації ОІ	0,9
	Успішність експлуатації ОІ	0,9
	Здатність перевіряти і зберігати дані	0,9
	Здатність захисту від серйозних наслідків для цілісності в разі помилок	0,9
	Здатність відновлювати цілісність після збоїв і помилок	0,9
	Наявність захисту від порушень авторського права	1
	Наявність функцій відновлення цілісності	0,9
	Наявність функцій контролю цілісності	0,8
	Наявність функцій ідентифікації і аутентифікації	0,9
	Наявність засобів моніторингу та оповіщення	1
	Наявність засобів обробки помилок	0,9

Продовження таблиці 2

1	2	3
Цілісність програмних ресурсів (ПР) - властивість виключати непередбачені зміни програмних ресурсів системи (L_P)	Наявність функцій в ПР з відновлення процесу виконання в разі збою операційної системи, процесора, зовнішніх пристроїв	0,9
	Наявність засобів відновлення процесу в разі збоїв обладнання	0,9
	Наявність можливості повторного старту з точки зупину	0,7
	Наявність вимог по стійкості функціонування при наявності помилок у вхідних даних, помилок користувача, відсутність необхідних даних (на диску, у файлі, в БД тощо)	0,6
	Наявність автоматичного резервування для збереження поточного стану процесу	0,9
	Сумісність з технічними засобами	0,9
	Сумісність з системними програмними засобами	1
	Сумісність з іншим програмним забезпеченням, включаючи обмін даними (з текстовими, графічними редакторами, БД тощо)	0,9
	Наявність стійкості функціонування при наявності помилок у вхідних даних, помилок користувача, відсутність необхідних даних (на диску, у файлі, в БД тощо)	0,9
	Можливість обробки помилкових ситуацій	1
Цілісність інформації – здатність ГКС забезпечувати незмінність інформації в умовах випадкового і (або) навмисного скривлення (руйнування) (LI)	Достовірність	0,9
	Точність	0,9
	Якість	0,9
	Своєчасність	1
	Правильність	1
	Наявність інформації про здатність перевіряти правильність введеної/виведеної інформації	0,9
	Наявність інформації про процедури зберігання даних	0,9
	Наявність тестів для перевірки допустимих значень вхідних/вихідних даних	0,9
	Наявність системи контролю повноти вхідних вихідних даних	0,9
	Наявність засобів контролю коректності вхідних/вихідних даних	1
	Наявність засобів контролю несуперечності вхідних/вихідних даних	0,9
	Наявність перевірки параметрів і адрес по діапазону значень	0,9
	Наявність обробки граничних значень	0,8
	Наявність інформації про здатність відновлюватися після помилок	0,7

Результат обчислення за формулою (1) усередненої оцінки рівнів виконання критеріїв цілісності має наступний вигляд: L_{PC}= 0,9167; L_P= 0,87; L_I=0,9

Необхідно враховувати, що кожна метрика у різній мірі впливає на цілісність ГКС. Загальний сумарний рівень цілісності вирахувано за методом аналізу ієрархій (MAI) становить L_s = 0,8917. Таким чином, комп'ютерна мережа відділу автоматизації Херсонського філіалу Одеського наукового інституту медицини транспорту відповідає заданим вимогам цілісності.

Висновки

Запропонований підхід до кількісної оцінки сумарного рівня цілісності ГКС є універсальним і може застосовуватися для систем різноманітного призначення. В якості прикладу було оцінено рівень цілісності мережі відділу автоматизації Херсонського філіалу Одеського наукового інституту медицини

транспорту; остання що відповідає заданим вимогам цілісності, що в достатній мірі гарантує збереження інформації та обчислювальної інфраструктури.

Список використаної літератури

1. Чердынцева М.И., Подколзина Л.А. Методы защиты информационных систем от сетевых воздействий на примере ИС ДГТУ// Современный научный вестник. - 2013. - Т. 6. - № 2. - С. 77-81.
2. Н.В. Сеспедес Гарсия. Оценка уровня целостности гарантоспособных компьютерных систем// Математичні машини і системи, 2013, № 4. – С.204-210.
3. Зегжда Д., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2008. – 452 с.
4. Петренко, С. А. Политики безопасности компании при работе в Интернет / С.А. Петренко, В.А. Курбатов. - М.: ДМК Пресс, 2011. - 396 с.
5. Шаньгин, В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. - М.: ДМК, 2014. - 702 с.
6. Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации: Учебное пособие для вузов. / А.А. Малюк. - М.: Горячая линия -Телеком , 2004. - 280 с.
7. Чипига, А.Ф. Информационная безопасность автоматизированных систем / А.Ф. Чипига. - М.: Гелиос АРВ, 2010. - 336 с.
8. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2013. - 416 с.
9. Ярочкин, В.И. Информационная безопасность: Учебник для вузов / В.И. Ярочкин. - М.: Акад. Проект, 2008. - 544 с.