

НАДЕЖДНОСТ НА СОФТУЕРА И ПРОБЛЕМЪТ ИНФОРМАЦИОННА БЕЗОПАСНОСТ

Иванка Павлова

Университет по библиотекознание и информационни технологии

Резюме: Проблемът надеждност на софтуера е особено актуален за решаване, в това число и в контекста на информационната сигурност. Това определя обекта на настоящото изложение, което логически и структурно се базира на научни изследвания в тази област.

Ключови думи: програмно осигуряване, надеждност, информационни системи, отказ, възстановяване.

Въведение

Съвременните информационни технологии автоматизират процесите по получаване, обработка, съхраняване, предаване, представяне и използване на информация, с нужната степен на нейната безопасност. Информационната безопасност в голяма степен зависи от надеждността на техническите и програмните средства. За оценката ѝ се използват както методите на класическата теория на надеждността [3], така и специфични методи и средства, специално разработени за целта [1], [2], [4], [5], [6].

Програмното осигуряване възниква и се развива с появата и развитието на компютърната техника, цифровите технологии и интегрираните системи за комуникации. Представява специфичен интелектуален продукт, който съществено се отличава от техническите обекти, които, както е известно, се реализират с използване на едни или други физически процеси. По своята същност интегрира в себе си реализация на цели, свързани с обработването на информация чрез компютърни средства. Оказва съществено влияние върху функционалната надеждност на съответните средства и системи за обработка на информацията и управление. Поради специфичните си особености изисква отделно изясняване на проблема функционална надеждност при него, която зависи от множество фактори, като [1]:

- логически грешки, допуснати в процеса на проектиране на програмните средства и системи;

- грешки в кода на компютърните програми;
- неадекватна реакция при грешна входна информация;
- особености на структурата и общата логика на програмното осигуряване, които способстват за възникване на сбоеве и откази в определени ситуации на обработване на информацията;
- отсъствие на адекватен контрол на работата на компютърните програми.

Основните причини за грешна входна информация са:

- неправилно функциониране или отказ на сензори;
- разрушаване, самопроизволно модифициране или загуба на информацията в процеса на нейното обработване, съхраняване и предаване;
- изкривяване на информацията в комуникационните системи и мрежи в резултат на настъпили откази и сбоеве в работата им;
- грешки, допускани при въвеждане на входната информация.

Неверни изходни данни могат да предизвикат две групи въздействия върху работата на програмното осигуряване [1], [2], [3]:

- отказ или сбой в работата на информационната система, породени от факта, че обработваните данни се намират извън допустимите предели на своите толеранси;
- сбой или отказ на информационната система при изпълнение на съответна компютърна програма.

Въвеждането на информация чрез клавиатура и използване на визуален контрол се характеризира с достоверност от порядъка на $10^{-4} - 10^{-5}$ за знак. При въвеждането на графична информация точността се определя от диапазона на изменение на координатите и качеството на кодиране и въвеждане на информацията. Достижимата точност е $10^{-3} - 10^{-5}$ от диапазона на изменение на съответните координати.

Значителни грешки се допускат при въвеждането на информация от документи поради невярното им попълване – 38%; допуснати неумишлени грешки в текста – 20%; пропуснати цифри в числа – 17%. Минималното време за реакция при грешка е 0,3 – 0,5 секунди при среден темп на работа с клавиатурата 1,5 знака за секунда. Вероятността за откриване на допуснатата грешка е в границите $10^{-4} - 3 \cdot 10^{-4}$ за знак.

Съществено е влиянието на допуснати грешки в кода на компютърните програми. В литературата [1] е посочено, че в

резултат на проверка на работата на компютърни програми с обем над десетина хиляди команди за корекция може да се окажат до 30% от тях. При корекции на открити грешки в програмния код често се внасят нови такива.

Грешките в програмното осигуряване може да бъдат разделени на две основни групи – логически грешки и грешки в самия програмен код. Логическите грешки се съдържат в алгоритмите за обработване на информацията, които се реализират чрез софтуера.

Логическите грешки водят до неправилна работа на компютърните програми, независимо от качеството на програмния код. Тези грешки възникват на етапа проектиране на софтуера и могат да достигнат 70 – 80% от допуснатите грешки в процеса на създаването на софтуера. Представяват най-трудно отстраняваните грешки.

Грешките в алгоритмите често са свързани с неправилно определяне на съответните условия за обработване на информацията, с некоректна постановка на задачата и с грешки, свързани с отклонения във функционирането на софтуерните системи и комплекси.

Съществена причина за възникването на алгоритмични грешки е отсъствието на функционално пълен обем дефинирани условия за обработване на информацията. Често тези условия се доуточняват едва на етапа на самото тестване на софтуера или при открити грешки в работата му. Грешки от подобен вид са сред най-често срещаните и могат да съставляват до 70% от всички допуснати грешки при разработването на програмното осигуряване и до 30% от общото количество грешки, направени при създаването на програмните продукти.

Към алгоритмичните грешки се отнасят и тези, свързани с допуснати несъответствия при стиковането на функционалните подпрограми. Те заемат [1] до 6 – 8% от общото количество на допуснатите грешки. Обикновено са следствия от некоректност при дефинирането на задачите, свързани със създаването на програмните комплекси и системи, или са резултат от:

- неправилно дефинирани изисквания към ресурсите на компютърните системи, чрез които се реализира съответният софтуер;
- невярна оценка на времевите параметри на изпълнение на отделните групи програми на софтуерните комплекси.

На началния етап на проектиране невинаги адекватно се определя целевата функция на системата за управление като цяло

и на отделните ѝ подсистеми. Това води до необходимост от преработка на алгоритмите за обработване на информацията или от тяхната замяна с нови. В процеса на експлоатация системните грешки са преобладаващи и могат да съставляват до 80% от всички грешки в програмното осигуряване на информационните системи, свързани с управлението на едни или други обекти или процеси.

Данни за количеството грешки в алгоритмите и в кода на компютърните програми може да се получат въз основа на косвена оценка на работа им в различни условия на тестване и

експлоатация. Количеството относителни грешки $\frac{dn}{R}$, открити в програмен код с обем R за календарно време τ за тестване и корекция може да се апроксимира чрез функцията от вида [1]:

$$\frac{dn}{R} = K_1 \exp(-K_2 \tau).$$

Опитът показва, че при автономна проверка на програмното осигуряване откритите и отстранени грешки са от порядъка на $1 \cdot 10^{-6}$ грешки за команда програмен код за ден. При комплексна проверка при същите условия този показател е от порядъка на $0,2 \cdot 10^{-6} - 0,1 \cdot 10^{-6}$. При открити $0,2 \cdot 10^{-2} - 0,1 \cdot 10^{-1}$ грешки за ден на човек може да се счита, че съответната компютърна програма е пригодна за експлоатация. Стойности под $0,1 \cdot 10^{-1}$ на този показател може да се смятат за еталон за висока степен на пригодност за експлоатация на дадена програмна система.

За качествена оценка на загубите, породени от проява на възникнали грешки в програмното осигуряване на високо отговорни системи за управление [1], може да се съди по изложеното в таблица 1.

Таблица 1

Категория	Тежест на последствията	Последствия от проявата на грешката в софтуера
IV	катастрофални	Грешките с висока вероятност водят до отказ на програмното осигуряване, което поражда отказ на системата за управление.
III	критични	Грешките с висока вероятност водят до отказ на програмното осигуряване, което води до непълен отказ на системата за управление.
II	съществени	Проявилите се грешки може да предизвикат отказ на програмното осигуряване, но без значимо нарушаване на работата на системата за управление.
I	несъществени	Проявата на грешки може да доведе до намаляване на ефективността на работата на програмното осигуряване.

Надеждността на програмното осигуряване е от съществено значение за качествено обработване, съхраняване, предаване и използване на информацията в условията на използване на съвременните информационни средства, системи и технологии, което пряко комуникира с проблема информационна безопасност.

Благодарности: Докладът е изготвен с подкрепата на Министерството на образованието и науката в изпълнение на Национална научна програма „Сигурност и отбрана“, приета с РМС № 731 от 21.10.2021 г. и съгласно Споразумение № Д01-74/19.05.2022 г.

References/Литература

1. **Nachev, A. I.** Nadezhdnost na programното osiguryavane. Shumen: Universitetsko izdatelstvo „Episkop Konstantin Preslavski“, 2020.

[**Начев, А. И.** Надеждност на програмното осигуряване. Шумен: Университетско издателство „Епископ Константин Преславски“, 2020.]

2. **Nachev, A. I.** Strukturnofunktsionalna nadezhdnost na kompyutarni mrezhni. Sofia: Voенно izdatelstvo, 2002.

[**Начев, А. И.** Структурнофункционална надеждност на компютърни мрежи. София: Военно издателство, 2002.]

3. **Nachev, A. I.** Nadezhdnost na vaorazhenieto. Metodi za opredelyane na nadezhdnostta na primera na elektronните sredstva i sistemi vaorazhenie. Sofia: Balgarska akademia na naukите, 2016.

- [**Начев**, А. И. Надеждност на въоръжението. Методи за определяне на надеждността на примера на електронните средства и системи въоръжение. София: Българска академия на науките, 2016.]
4. **Nachev**, A. I. Metodika analiza i otsenki protsessov obmena informatsii v mikrokompyuternykh setyah s radioobmenom. – V: *International Journal, Information Theories and Applications*, Volume 3, Number 9, 1995, pp. 29 – 36.
- [**Начев**, А. И. Методика анализа и оценки процессов обмена информации в микрокомпьютерных сетях с радиообменом. – В: *International Journal, Information Theories and Applications*, Volume 3, Number 9, 1995, pp. 29 – 36.]
5. **Abramsan**, N. The ALOHA System – another alternative for computer communication – AFIPS Conf. Proc., 1990, v 3a, pp. 233 – 243.
6. **Data** Communication Networks Transmission, Signaling and Switching, Network Aspects, Maintenance and Administrative Arrangements. Volume VIII, CCITT Red Book, CCITT Plenary Assembly, October 8 – 19, 2014 (Malaga – Torvemolinos).

SOFTWARE RELIABILITY AND THE ISSUE OF INFORMATION SECURITY

Ivanka Pavlova

University of Library Studies and Information Technologies

Abstract: The problem of software reliability is particularly relevant to solve, including in the context of information security. This also defines the object of the present exhibition. It is logically and structurally based on scientific research in this field.

Keywords: programming provision, reliability, information systems, refusal, recovering.

About the Author

Ivanka Pavlova is a professor, doctor, vice-rector on students' affairs at the University of Library Studies and Information Technologies. Her scientific interests are in the field of automated information processing and management systems, information security.

To contact the Author: i.pavlova@unibit.bg