Method for assessing safety functions durability of the security facility of an automated spacecraft flight control system

© A.G. Andreev[1], G.V. Kazakov[1], V.V. Koryanov[2]

[1]Federal State Budget Institution the 4th Central Research Institute
of the Ministry of Defence of the Russian Federation,
Korolev town, Moscow Region, 141091, Russia
[2]Bauman Moscow State Technical University, Moscow, 105005, Russia

A significant number of risk factors affect the automated spacecraft flight control system (ASFCS). To effectively neutralize these factors, it is necessary to assess the sensitivity and stability of the information security facility of the ASFCS. For different security classes of such systems, it is necessary to define basic functional safety indicators. We rely on the notion of security functions durability, and for its evaluation we introduce strict definitions of the basic concepts: the mechanism of protection, security facility, reliability of control, sensitivity and durability of information security facility. For the security coefficient, which is an indicator of the durability of information security facility, we obtained an analytical expression. Using the standard model of the threat counteraction process, we solved the task of determining some tentative values of type 2 error probabilities for the security facility. Furthermore, we assessed the priorities of the information security facility, which enabled us to obtain a variational series of type 2 error probability values, and in certain cases to set the required values of such probabilities of the security facility. The application of the developed method makes it possible to assess the residual threat impact on the information resources of the automated spacecraft flight control system. If the residual risk is acceptable, then the stability of the protection mechanisms meets the requirements of the system's safety. Otherwise, it is necessary to use protection mechanisms with the increased durability.

Keywords*: information security, threat localization, protection mechanism, threat neutralization, threat detection, threat prevention, security facility, durability of control system, sensitivity of security facility*

REFERENCES

[1] Andreev A.G., Kazakov G.V., Koryanov V.V. *Inzhenernyy zhurnal: nauka i innovatsii — Engineering Journal: Science and Innovation*, 2016, no. 7. Available at: http://dx.doi.org/10.18698/2308-6033-2016-7-1511

[2] Borodakiy Yu.V., Dobrodeev A.Yu., Naschekin P.A., Butusov I.V. *Voprosy kiberbezopasnosti — Cybersecurity issues*, 2014, no. 2 (3), pp. 2–9.

[3] Markov A.S., Tsirlov V.L., Barabanov A.V. *Metody otsenki nesootvetstviya sredstv zaschity informatsii* [Methods for assessing the inconsistency of information secutiry facility]. Moscow, Radio i svyaz Publ., 2012, 192 p.

[4] Tsirlov V.L. *Osnovy informatsionnoy bezopasnosti. Kratkiy kurs* [Fundamentals of Information Security. A Short Course]. Rostov-na-Donu, Feniks Publ., 2008, 254 p.

[5] Polyanskiy D.A. *Otsenka zaschischennosti* [Security assessment]. Vladimir, Vladimir State University Publ., 2005, 80 p.

[6] *Rukovodyaschiy dokument. Bezopasnost informatsionnykh tekhnologiy. Polozhenie po obespecheniyu bezopasnosti v zhiznennom tsikle izdeliy*

in-formatsionnykh tekhnologiy [Guidance document. Security of information technology. The provision for ensuring safety in the life cycle of products of information technology]. Moscow, Federal Service for Technical and Export Control of Russia, 2004, 54 p.

[7] Avdoshin S.M., Saveleva A.A. *Izvestiya AIN im. A.M. Prokhorova. Biznes-informatika — News Academy of Engineering Sciences A.M. Prokhorov*, 2006, vol. 17, pp. 91–99.

[8] *Vikhman V.V., Pankov M.A. Trudy SPIIRAN — SPIIRAS Proceedings, 2014, no. 5 (36), pp. 194–205.*

[9] Varfolomeev A.A. *Zaschita informatsii s ispolzovaniem intellektualnykh kart* [Protection of information using smart cards]. Moscow, RUDN Publ., 2008, 87 p.

[10] Morozova E.V., Mondikova Ya.A., Moldovyan N.A. *Informatsionno-upravlyayushchie sistemy — Information and Control Systems*, 2013, no. 6 (67), pp. 73–78.

[11] Vasilev K.K., Glushkov V.A., Dormidontov A.V., Nesterenko A.G. *Teoriya elektricheskoy svyazi* [The theory of electrical communication]. Ulyanovsk, UlSTU Publ., 2008, 452 p.

[12] Kosolapov Yu.V. *Sposob zashchity informatsii ot tekhnicheskoy utechki, os-novannyi na primenenii kodovogo zashumleniya i kodovykh kriptosistem. Diss. kand. tekhn. nauk* [The method of protecting information from technical leakage, based on the use of code noise and code cryptosystems. Cand. eng. sc. diss.]. Rostov-na-Donu, 2009, 169 p.

[13] Pashkovskaya E.S., Pashkovskiy M.E., Barabanov V.F. *Vestnik Voronezhskogo gosudarstvennogo tekhnicheskogo universiteta — The Bulletin of Voronezh State Technical University*, 2013, no. 4, pp. 4–7.

[14] Bondar I.V., Zolotarev V.V., Popov A.M. *Modelirovanie sistem* [System modeling], 2010, no. 4, pp. 3–12.

Andreev A.G., Cand. Sc. (Eng.), Senior Research Scientist, Federal State Budget Institution the 4th Central Research Institute of the Ministry of Defence of the Russian Federation. Author of over 70 research works in the field of automated control system reliability. e-mail: kgv.64@mail.ru

Kazakov G.V., Cand. Sc. (Eng.), Assoc. Professor, Head of Federal State Budget Institution the 4th Central Research Institute of the Ministry of Defence of the Russian Federation. Author of over 70 research works in the field of automated control system reliability. e-mail: kgv.64@mail.ru

Koryanov V.V., Cand. Sc. (Eng.), Assoc. Professor, First Deputy Head of the Department of Dynamics and Flight Control of Rockets and Spacecraft, Bauman Moscow State Technical University. Author of over 40 publications in the field of ballistics simulation and dynamics of space and descent vehicles motion. e-mail: vkoryanov@bmstu.ru