метрик уязвимостей // Современные проблемы науки и образования. 2014. № 3. URL: http://www.science-edukation.ru/pdf/2014/3/344.pdf (дата обращения: 12.03.2017).

10. Белов В., Голяков А. Терминологическая база теории безопасности // Стандарты и качество. 2004. № 9. С. 48–51.

11. Быков А.А., Порфирьев Б.Н. О взаимосвязи риска с родственными понятиями и терминологии риск-менеджмента // Проблемы анализа риска. 2013. Т. 10. № 4. С. 4–10.

12. Алпеев А.С. Основные понятия безопасности // Надежность и контроль качества. 1994. № 7.

Software & Systems
DOI: 10.15827/0236-235X.120.690-698

Received 03.04.17
2017, vol. 30, no. 4, pp. 690–698

A METHODICAL APPROACH TO FORMING FUNCTIONAL REQUIREMENTS FOR A COMPUTER ATTACKS PROTECTION SYSTEM FOR AUTOMATED CONTROL SYSTEMS AND ITS SOFTWARE IMPLEMENTATION

E.B. Drobotun [1], *Ph.D. (Engineering), Doctoral Student, drobotun@xakep.ru*

[1] *Military Academy of the Aerospace Defense, Zhigareva St. 50, Tver, 170100, Russian Federation*

Abstract. One of the main stages of development and building of secured automated control systems for various purposes is the stage of forming requirements for the developed automated system including security requirements against computer attacks and other information technology impact.

Effectively developed and reasonable functional requirements for a computer attacks protection system will allow on the one hand providing the necessary level of automated system protection, on the other hand minimizing consumption of computing and human resources of the protected automated system, the amount of which is limited and finite in any automated system.

One of the possible ways to form and prove optimal functional requirements for a computer attacks protection system is using a risk-oriented approach to forming and reasoning of these requirements. The approach includes identifying the severity and probability of possible security threats against the protected automated system.

The article offers a methodical approach to formation of functional requirements for computer attacks protection systems for automated control systems. It is based on a risk assessment of information security threats in the automated system and its safe operation threats.

The application of the proposed approach will allow forming optimal functional requirements for a computer attacks protection system for automated control systems for various purposes. It will help to achieve optimal resource allocation in an automated system to ensure functioning of the computer attacks protection system.

Keywords: automated system, automated system security threat, computer attack, functional requirements, risk analysis.

References

1. Lyaskovsky V.L. *Osnovy proektirovaniya i ekspluatatsii avtomatizirovannykh sistem voennogo naznacheniya* [Fundamentals of Design and Operation of Military Assignment Automated Control Systems]. Moscow, Bauman MSTU Publ., 2016, 188 p.

2. Malyuk A.A., Pazizin S.V., Prigozhin N.S. *Vvedenie v zaschitu informatsii v avtomatizirovannykh sistemakh* [Introduction to Information Protection in Automated Systems]. Moscow, Goryachaya liniya–Telekom Publ., 2001, 148 p.

3. Galatenko V.A. *Standarty informatsionnoy bezopasnosti: kurs lektsy* [Information Security Standards: a Course of Lectures]. V.B. Betelin (Ed.). Moscow, INTUIT.RU Publ., 2006, 264 p.

4. Markov A.S., Tsirlov V.L., Barabanov A.V. *Metody otsenki nesootvetstviya sredstv zashchity informatsii* [Methods for Assessing the Discrepancy of Information Protection Means]. A.S. Markov (Ed.). Moscow, Radio i svyaz Publ., 2012, 192 p.

5. Grishina N.V. The model of a potential intruder on an object of informatization. *Izvestiya UFU. Tekhnicheskie nauki* [News of SFedU. Engineering Science]. 2003, no. 4, vol. 33, pp. 356–358 (in Russ).

6. Zhukov V.G., Zhukova M.N., Stefarov A.P. The model of the violator of access rights in the automated system. *Programmnye produkty i sistemy* [Software & Systems]. 2012, no. 2 (98), pp. 75–78 (in Russ.).

7. Drobotun E.B., Tsvetkov O.V. Building a model of information security threats in an automated control system for critical objects based on the scenarios of the violator's actions. *Programmnye produkty i sistemy* [Software & Systems]. 2016, no. 3 (29), pp. 42–50 (in Russ.).

8. *Common Vulnerability Scoring System*. Available at: http://www.first.org/cvss (accessed March 12, 2017).

9. Nurdinov R.A. Determining the probability of violation of critical properties of the information asset based on the CVSS metrics of the vulnerabilities. *Sovremennye problemy nauki i obrazovaniya* [Modern Problems of Science and Education]. 2014, no. 3. Available at: http://www.science-edukation.ru/pdf/2014/3/344.pdf (accessed March 12, 2017).

10. Belov V., Golyakov A. The terminological base of the theory of security. *Standarty i kachestvo* [Standards and Quality]. 2004, no. 9, pp. 48–51 (in Russ.).

11. Bykov A.A., Porfirev B.N. On the relationship of risk with related concepts and risk management terminology. *Problemy analiza riska* [Problems of risk analysis]. 2013, no. 4, vol. 10, pp. 4–10 (in Russ.).

12. Alpeev A.S. Basic concepts of security. *Nadezhnost i control kachestva* [Reliability and quality control]. 1994, no. 7 (in Russ.).