Литература

1. Дроботун Е.Б. Синтез систем защиты автоматизированных систем управления от разрушающих программных воздействий // Программные продукты и системы. 2016. Т. 29. № 3. С. 51–59.
2. Федоров Ю.Н. Справочник инженера по АСУ ТП: Проектирование и разработка. М.: Инфра-Инженерия, 2008. 928 с.
3. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах. М.: Горячая линия–Телеком, 2001. 148 с.
4. Основы проектирования и эксплуатации автоматизированных систем управления военного назначения; [под ред. В.Л. Лясковского]. М.: Изд-во МГТУ им. Н.Э. Баумана, 2016. 188 с.
5. Проскурин В.Г., Крутов С.В., Мацевич И.В. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах. М.: Радио и связь, 2000. 168 с.
6. Сердюк В.А. Организация и технология защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий. М.: Изд-во ВВШЭ, 2011. 572 с.
7. Шумский А.А., Шелупанов А.А. Системный анализ в защите информации. М.: Гелиос АРВ, 2005. 224 с.
8. Бородакий Ю.В., Добродеев А.Ю., Нащекин П.А., Бутусов И.В. Основной объект воздействия противника // Воздушно-космическая оборона. 2014. № 2. С. 30–37.
9. Осипова В.А. Основы дискретной математики. М.: ФОРУМ: ИНФРА-М, 2006. 160 с.
10. Поляничко М.А. Архитектура системы автоматизированного обнаружения и разрешения конфликтов программных средств защиты информации // Изв. ПГУПС. 2013. № 1. С. 39–45.

Software & Systems
DOI: 10.15827/0236-235X.118.314-319

Received 02.10.16
2017, vol. 30, no. 2, pp. 314–319

METHOD OF GENERATING SETS OF ALTERNATIVE VARIANTS OF BUILDING SUBSYSTEMS WHICH ARE A PART OF A COMPUTER ATTACK PROTECTION SYSTEM

E.B. Drobotun [1], *Ph.D. (Engineering), Doctoral Student, drobotun@xakep.ru*
E.P. Uglovsky [1], *Head of Laboratory*
I.Sh. Zamaltdinov [1], *Ph.D. (Engineering), Senior Researcher*

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

Abstract. Constructing a rational computer attack protection system for an information or automated system assumes creating a set of protection system configurations consisting of a set of separate program and hardware-software components and a further choice of a rational option of creating a computer attack protection system from the created set according to certain criteria. When generating this set, in addition to protection system compliance with necessary functional requirements, it is necessary to consider the parameters of the protected system (its structure and a multiple-level creation system), as well as software and hardware compatibility of components, and also compatibility of components with a hardware-software platform, which is the basis for the constructed protected system.

The article presents one of the possible approaches to forming a set of possible options of creating a computer attack protection system, taking into account its decomposition on three subsystem types. They are: computer attack detection subsystems, computer attack counteraction subsystems and subsystems of elimination of consequences of computer attack application.

Keywords: automated control system, computer attack, information security, protection system design, computer attack protection.

References

1. Drobotun E.B. Synthesis of protection systems of automated control systems against destroying program influence. *Programmnye produkty i sistemy* [Software & Systems]. 2016, vol. 29, no. 3, pp. 51–59 (in Russ.).
2. Fedorov Yu.N. *Spravochnik inzhenera po ASU TP: Proektirovanie i razrabotka* [Automated Process Control System Engineer's Reference Book: Design and Development]. Moscow, Infra-Inzheneriya Publ., 2008, 928 p.
3. Maluk A.A., Pazizin S.V., Pogozhin N.S. *Vvedenie v zashchitu informatsii v avtomatizirovannykh sistemakh* [Introduction to Information Protection in Automated Systems]. Moscow, Goryachaya liniya–Telekom Publ., 2001, 148 p. (in Russ.).
4. Lyaskovsky V.L. (Ed.) *Osnovy proektirovaniya i expluatatsii avtomatizirovannykh sistem voennogo naznacheniya* [Fundamentals of Design and Operation of Military Automated Control Systems]. Study guide. Moscow, N.E. Bauman MSTU Univ. Publ., 188 p.
5. Proskurin V.G., Krutov S.V., Matsevich I.V. *Programmno-apparatnye sredstva obecpecheniya bezopasnosti. Zaschita v operatsionnykh sistemakh* [Hardware-software Means of Ensuring Information Security. Protection in Operating Systems]. Study guide. Moscow, Radio i svyaz Publ., 2000, 168 p.
6. Serduk V.A. *Organizatsiya i tekhnologiya zashchity informatsii: obnaruzhenie i predotvrashchenie informatsionnykh atak v avtomatizirovannykh sistemakh predpriyaty* [Information Protection Organization and Technology: Detection and Prevention of Information Attacks in Enterprise Automated Systems]. Moscow, HSE Publ., 2011, 572 p.
7. Shumsky A.A., Shelupanov A.A. *Sistemny analiz v zashchite informatsii* [System Analysis in Information Security]. Moscow, Gelios ARV Publ., 2005, 224 p.
8. Borodaky Yu.V., Dobtodeev A.Yu., Nashchekin P.A., Butusov I.V. The Main Object of Enemy's Influence. *Vozdushno-kosmicheskaya oborona* [Aerospace Defense]. 2014, no. 2, pp. 30–37 (in Russ.).
9. Osipova V.A. *Osnovy diskretnoy matematiki* [Fundamentals of Discrete Mathematics]. Study guide. Moscow, FORUM: INFRA-M Publ., 2006, 160 p.
10. Polyanichko M.A. Architecture of the system of detection and resolution of the software security conflicts. *Izvestiya PGUPS* [Proc. of Petersburg Transport Univ.]. 2013, no. 1(34), pp. 39–45 (in Russ.).