

СИНТЕЗ АРХИТЕКТУРЫ КИБЕРБЕЗОПАСНОСТИ ДЛЯ СИСТЕМ УПРАВЛЕНИЯ АТОМНЫХ ЭЛЕКТРОСТАНЦИЙ

В.Г. Промыслов, К.В. Семенов, А.С. Шумов

Аннотация. Представлена комплексная модель кибербезопасности АСУТП. Предложен формальный метод классификации активов по уровням кибербезопасности с помощью отображения системы в виде графа и методов кластеризации. Предложен метод синтеза архитектуры кибербезопасности систем и рассмотрена его применимость для иерархических систем. Представлен пример синтеза архитектуры кибербезопасности для подсистемы АСУТП атомной электростанции в соответствии с политикой кибербезопасности МАГАТЭ и МЭК.

Ключевые слова: кибербезопасность, АСУТП, атомная электростанция, архитектура кибербезопасности, классификация, кластеризация, граф безопасности, модель «take-grant».

ЛИТЕРАТУРА

1. Менгазетдинов Н. Э., Бывайков М. Е., Зуенков М. А. и др. Комплекс работ по созданию первой управляющей системы верхнего блочного уровня АСУТП для АЭС «Бушер» на основе отечественных информационных технологий. – М.: ИПУ РАН, 2013. [Mengazetdinov, N. E., Poletykin, A. G., Zuenkov, M. A., et al. Range of works on creation on the first upper block-level I&C system for NPP «Busher» on the base of domestic information technologies. – Moscow: ICS RAS, 2013. (In Russian)]
2. ГОСТ Р МЭК 61513–2011. Атомные станции. Системы контроля и управления, важные для безопасности. Общие требования. – URL: <http://docs.cntd.ru/document/1200089290>. [IEC 61513–2011. Nuclear power plants – Instrumentation and control important to safety – General requirements for systems. – URL: <https://webstore.iec.ch/publication/5532>]
3. Бабаев Д. И., Полетыкин А. Г., Промыслов В. Г., Тимофеев М. Ю. Управление архитектурой кибербезопасности АСУТП атомных электростанций // Проблемы управления. – 2018 – № 3. – С. 47–55. [Babaev, D. I., Poletykin, A. G., Promyslov, V. G., Timofeev, M. Yu. Control of cybersecurity architecture of nuclear power plants I&C // Control Sciences. – 2018. – No. 3. – P. 47–55. (In Russian)]
4. Computer security at nuclear facilities: reference manual: technical guidance // IAEA Nuclear Security Series. – 2011. – No. 17.
5. IEC 62645(2014)/Cor.1(2015). Атомные электростанции. Системы контроля и управления. Требования к программам обеспечения безопасности для компьютерных систем. – URL: <https://webstore.iec.ch/publication/7311&preview=1>. [IEC 62645(2014)/Cor.1(2015). Nuclear power plants – Instrumentation and control systems – Requirements for security programmes for computer-based systems. – URL: <https://webstore.iec.ch/publication/7311&preview=1>]
6. Viba, K. J. Integrity Considerations for Secure Computer Systems, MTR–3153. – The Mitre Corporation, June 1975.
7. Харченко В., Скляр В., Брежнев Е. Безопасность информационно-управляющих систем и инфраструктур. – Palmarium academic publishing, 2013. – 528 с. [Harchenko, V., Sklyar, V., Brezhnev, E. The Security of Information and Control Systems and Infrastructures. – Palmarium academic publishing, 2013. – 528 p. (In Russian)]
8. Промыслов В. Г., Полетыкин А. Г. Формальная иерархическая модель безопасности верхнего уровня АСУТП АЭС // Ядерные измерительно-информационные технологии. – 2012. – Т. 4 (44). – С. 39–53. [Promyslov, V. G., Poletykin, A. G. Formal Hierarchical Security Model of I&C Upper Level System of a Nuclear Power Plant // Nuclear Measurement and Information Technologies. – 2012. – Vol. 4 (44). – P. 39–53 (In Russian)]
9. Девянин П. Н. Модели безопасности компьютерных систем. – М.: Academia, 2005. – 144 с. [Devyanin, P.N. Security models for computed-based systems. – Moscow: Academia, 2005. – 144 p. (In Russian)]
10. Denning, E. A lattice model of secure information flow // Communications of the ACM – 1976 – Vol. 19, iss. 5. – P. 236–243.

11. *Kaufman, L. and Rousseeuw, P. J.* Finding Groups in Data: An Introduction to Cluster Analysis. – NY: Wiley – 1990. – 342 p.
12. *Mirkin, B.* Mathematical Classification and Clustering. – Dordrecht-Boston-London: Kluwer Academic Publishers, 1996. – 448 p.
13. *Wood, R. T., Joseph III, R. A., Korsah, K., et al.* Classification Approach for Digital I&C Systems at U.S. Nuclear Power Plants. – Oak Ridge National Laboratory, 2012. – URL: <https://www.nrc.gov/docs/ML1209/ML120970232.pdf>.
14. *Bell, D. E., La Padula, L. J.* Secure Computer System: Mathematical Foundations // MITRE Technical Report MTR–2547, vol. 1. – MITRE Corporation, Bedford, Mass., 1973.
15. *Harrison, W. A.* Applying McCabe's complexity measure to multiple-exit programs. // Software: Practice and Experience. – 1984. – Vol. 14, iss. 10. – P. 1004–1007.
16. U.S. Nuclear regulatory commission. Research regulatory guide 5.71. Cyber security programs for nuclear facilities, January 2010.
17. *Omole* cybersecurity simulation toolkit. – URL: <https://www.omole.ws>.
18. *Bishop, M.* Computer Security: Art and Science. – Boston: Addison Wesley. – 2003. – 1136 p.

Статья представлена к публикации членом редколлегии В. В. Кульбой.

Поступила в редакцию 18.03.2019, после доработки 0.04.2019.

Принята к публикации 04.04.2019.

Промыслов Виталий Георгиевич – канд. физ.-мат. наук, ✉ v1925@mail.ru,

Семенов Кирилл Валерьевич – канд. физ.-мат. наук, ✉ semenkovk@mail.ru,

Шумов Александр Сергеевич – ✉ mau17@list.ru,

Институт проблем управления им. В.А. Трапезникова РАН, г. Москва.

SECURITY MODEL FOR INSTRUMENTATION AND CONTROL SYSTEMS FOR NUCLEAR POWER PLANTS

V. G. Promyslov[#], K. V. Semenov, A. S. Shumov

V. A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russia

[#]✉ v1925@mail.ru

Abstract. This paper presents a comprehensive cybersecurity model for process control systems. A formal method for classifying assets according to cybersecurity levels using the mapping system in the form of a graph and using clustering methods is proposed. A method for synthesizing the cybersecurity architecture of systems is proposed. The applicability of these methods for hierarchical systems is considered. An example of the synthesis of the security architecture for the subsystem of the NPP automated process control system is considered in accordance with the cyber security policy RG5.71. The Appendix describes the security graph in the take-grant model.

Keywords: cybersecurity, I&C, security architecture, NPP, nuclear power plant, classification, clustering, security graph, take-grant model.