Автоматизация в промышленности 2020. №11
www.avtprom.ru

DOI: 10.25728/avtprom.2020.11.08

О.Д. Архангельский, Д.В. Сютов, А.В. Кузнецов («Ростелеком-Солар»)

ПРАКТИЧЕСКИЕ ПОДХОДЫ К СОЗДАНИЮ ИНФРАСТРУКТУРЫ ИНДУСТРИАЛЬНОГО КИБЕРПОЛИГОНА

Обеспечение кибербезопасности АСУ и промышленной автоматики является одним из важнейших направлений в эпоху стремительного технологического развития киберфизических систем. Одним из направлений исследований в области обеспечения кибербезопасности промышленных объектов (в том числе, объектов критической информационной инфраструктуры), является проведение регулярных теоретических и практических тренировок для предупреждения, обнаружения и противодействия возможным компьютерным атакам – киберучений. Для проведения киберучений необходимо создание соответствующей инфраструктуры и методологии, позволяющих отрабатывать практические навыки обеспечения кибербезопасности без риска нанесения реального ущерба деятельности предприятия или останова технологического процесса. В статье рассматриваются основные подходы к созданию инфраструктуры для проведения киберучений, а также аспекты моделирования технологических процессов промышленных объектов в рамках формирования такой инфраструктуры.

Ключевые слова: кибербезопасность, автоматизированные системы управления, киберучения, киберполигон, информационная безопасность, киберфизические системы, полунатурное моделирование.

***Архангельский Олег Денисович** – ведущий аналитик-методолог проекта «Индустриальныйкиберполигон»,*
***Сютов Дмитрий Владимирович** – главный инженер проекта «Индустриальный киберполигон»,*
***Кузнецов Андрей Владимирович** – руководитель проекта «Индустриальный киберполигон», заместитель руководителя Лаборатории Кибербезопасности АСУТП по производству компании «Ростелеком-Солар».*

Список литературы

1. *Simon Parker.* Understanding the Physical Damage Of Cyber Attacks, URL: https://www.infosecurity-magazine. com/opinions/physical-damage-cyber-attacks
2. *Kaixing Huang, Chunjie Zhou, Yu-Chu Tian, Shuang-Hua H Yang, Yuanqing Qin.* Assessing the Physical Impact of Cyber- Attacks on Industrial Cyber-Physical Systems // IEEE Transactions on Industrial Electronics PP(99):1-1, 2018.
3. *Карантаев В.Г., Кузнецов А.В., Архангельский О.Д., Сютов Д.В.* Опыт проведения киберучений по анализу нарушений работоспособности объектов электроэнергетического комплекса в результате кибератак // Релейщик. 2020. №1 (36).

4. *Khaitan Siddhartha Kumar, McCalley James D., Liu Chen Ching (Eds.).* Cyber Physical Systems Approach to Smart Electric Power Grid. Springer. 2015.
5. *Советов Б.Я., Яковлев С.А.* Моделирование систем. М.: Высш. Шк., 2001. – 343 с.
6. *Карантаев В.Г., Кузнецов А.В., Архангельский О.Д., Сютов Д.В.* Опыт проведения киберучений по анализу нарушений работоспособности объектов электроэнергетического комплекса в результате кибератак // Релейщик. 2020. №1 (36).

Arkhangelsky O.D., Syutov D.V., Kuznetsov A.V. Practical approaches to the development of industrial cyber range infrastructure

Cyber security of control systems and industrial automatics is in focus as against the explosive growth of cyber-physical systems. Theoretic and practical trainings conducted on regular basis for preventing, detecting, and counteraction against cyber attacks is an important cybersecurity area. Cyber training requires appropriate infrastructure and methodology enabling the development of practical cybersecurity skills without process shutdown and damage enterprise operations. The paper examines basic approaches to the development of cyber training infrastructure as well as process modeling within such infrastructure.

Keywords: cybersecurity, automated control systems, cyber training, cyber range, information security, cyber-physical systems, semi-realistic simulation.