Автоматизация в промышленности 2023. №01
www.avtprom.ru

DOI: 10.25728/avtprom.2023.01.07

И.И. Лившиц (Университет ИТМО)

Ретроспектива проблемы обеспечения безопасности компонентов АСУТП

Рассмотрены подходы к оцениванию информационной безопасности компонентов АСУТП, проанализированы доступные на рынке «наложенные» решения и актуальная нормативная база в области информационной безопасности. Настоятельно рекомендуется неукоснительное соблюдение фундаментальных требований обеспечения информационной безопасности, включая подготовку необходимого числа специалистов в технических вузах и построение вертикальной «доверенной» архитектуры АСУТП в РФ. Данные меры являются ключевыми шагами на пути к достижению «цифрового суверенитета».

Ключевые слова: АСУТП, функциональная и информационная безопасность, импортозамещение, риски, аудит, оценка соответствия, цифровой суверенитет.

***Лившиц Илья Иосифович** – д-р техн. наук, проф., университет ИТМО.*

Список литературы

1. *Смирнов Е.В.* Методика оценки политической значимости угроз объекту критической информационной инфраструктуры на примере объекта инфокоммуникаций // Право. 2020. №2. С. 49-56.
2. *Новикова Е.Ф., Хализев В.Н.* Разработка модели угроз для объектов критической информационной инфраструктуры с учетом методов социальной инженерии // Прикаспийский журнал: управление и высокие технологии. 2019. № 4. С. 127-135.
3. *Щелкин К.Е., Звягинцева П.А., Селифанов В.В.* Возможные подходы к категорированию объектов критической информационной инфраструктуры // Интерэкспо Гео-Сибирь. 2019. Т. 6. №. 1.
4. *Ерохин С.Д., Петухов А.Н., Пилюгин П.Л.* Принципы и задачи асимптотического управления безопасностью критических информационных инфраструктур // Информатика. 2019. № 12. С. 29-35.
5. *Elsevier Inc.* Chapter 8 - Categorizing Data Sensitivity. In FISMA Compliance Handbook Edition: Second Edition. 2013. P. 63-78.
6. *Alan C.* NIST Cybersecurity Framework: A Pocket Guide. Ely, Cambridgeshire, United Kingdom:ITGP. 2018.
7. *Гордейчик С.В.* Миссиоцентрический подход к кибербезопасности АСУТП // Вопросы кибербезопасности. 2015. №2(10). С. 56 – 59
8. *Лившиц И.И., Неклюдов А.В.* Суверенные информационный технологии России // Стандарты и качество. 2018. № 4, 5.
9. *Лившиц И.И.* К вопросу управления уязвимостями в компонентах АСУТП // Автоматизация в промышленности. 2022. № 8. С. 12-16.
10. *Лившиц И.И.* К вопросу оценивания безопасности промышленных систем управления // Там же. 2021. № 7. С. 3-7.
11. *Лившиц И.И. И*сследование оценок защищенности промышленных систем // Там же. 2020. № 12. С. 13-18.
12. *Лившиц И.И., Зайцева А.А.* Проблемы обеспечения безопасности облачной компоненты информационных технологий // Там же. 2019. № 7. С. 10-16.

Livshits I.I. Historical overview of process control components security

The paper examines the approaches to estimating the information security of process control components, analyzes commercial "imposed" solutions and the existing guidelines in the field of information security. It strongly recommends the closes adherence to basic information security requirements including the training of the necessary number of

specialists in technical universities and the development of trustworthy vertical process control architecture in Russian Federation. These actions are the key steps on the way to attaining digital sovereignty.

Keywords: process control system, functional safety, informational security, import replacement, risks, audit, compliance assessment, digital sovereignty.