Автоматизация в промышленности 2022. №08
www.avtprom.ru

DOI: 10.25728/avtprom.2022.08.02

И.И. Лившиц (Университет ИТМО)

К вопросу управления уязвимостями в компонентах АСУТП

Приведена статистика об известных кибератаках на компоненты АСУТП и существующие меры противодействия. Отмечается, что современные подходы известных поставщиков средств защиты информации не позволяют в полной мере обеспечить приемлемый уровень защиты компонентов АСУТП по причине непринятия во внимание методов менеджмента рисков.
Для повышения уровня безопасности компонентов АСУТП предложено применять современные стандарты в области функциональной безопасности и менеджмента рисков, что позволяет ввести в оборот численные оценки заданного уровня полноты безопасности. Предложено также применять единый порядок оценки соответствия как компонентов АСУТП (например, по стандартам ГОСТ Р МЭК серии 61508 и 61511), так и предлагаемых средств защиты информации. Кроме того, настоятельно рекомендуется внести в процедуры управления уязвимостями в компонентах АСУТП современные практики менеджмента рисков (например, по стандартам ГОСТ Р ИСО/МЭК серии 31000 / 31010).

Ключевые слова: уязвимости, кибератаки, средства защиты информации, АСУТП, стандарты, функциональная безопасность, менеджмент рисков.

***Лившиц Илья Иосифович** – д-р техн. наук, профессор факультета ФБИТ, университет ИТМО.*

Список литературы

1. Livshitz I.I., Neklyudov A.V., Lontsikh P.A. IT security evaluation — “hybryd” approach and risk of its implementation // Journal of Physics: Conference Series. 2018. V. 1015. 4. P. 042030.
2. Лившиц И.И. Практика управления киберрисками в нефтегазовых проектах компаний холдингового типа // Вопросы кибербезопасности. 2020. №1(35). С. 42–51.
3. Лившиц И.И., Неклюдов А.В. Методика оптимизации программы аудитов информационной безопасности // Комплексная защита информации: Тр. XXII научно-практической конференции. Новополоцк: Полоцкий государственный университет, 2017. С. 135–139.
4. Лившиц И.И. Метод оценивания безопасности облачных ИТ- компонент по критериям существующих стандартов // Труды СПИИРАН. 2020. Т. 19. № 2. С.383–411.
5. Лившиц И.И. К вопросу обеспечения безопасности промышленных систем // Научно-технический вестник информационных технологий, механики и оптики. 2021. Т. 21, №1. С. 1–14.

Livshitz I.I. On vulnerability control in process control components

The paper presents the statistics of the detected cyberattacks against process control components and the available countermeasures. It notes that the present-day approaches of well-known vendors of information security hardware do not ensure the admissible level of process control security because risk management methods are not allowed for. To overcome this challenge, the paper proposes to apply present-day standards in the field of functional security and risk management. This will allow to apply numerical estimates of the specified safety integrity level. It also suggests to apply the unified assessment order for process controls compliance (e.g., IEC 61508 and 61511 series) and the proposed information security tools. Furthermore, the author argues for introducing present-day risk management practices (such as IEC 31000 / 31010) into the procedures of vulnerability management in process control components.

Keywords:vulnerability, cyberattacks, information security tools, process control systems, standards, functional security, risk management.