***Автоматизация в промышленности 2021. №7***
***www.avtprom.ru***

DOI: 10.25728/avtprom.2021.07.01

*И.И. Лившиц (Университет ИТМО)*

# К ВОПРОСУ ОЦЕНИВАНИЯ БЕЗОПАСНОСТИ ПРОМЫШЛЕННЫХ СИСТЕМ УПРАВЛЕНИЯ

*Проблема обеспечения безопасности для промышленных систем управления имеет давнее происхождение, в частности, первые примеры появились еще в XX веке при создании автоматизированных систем управления для объектов атомной, космической и иных отраслей. Важно, что особенностями предыдущих решений было единое архитектурное решение — не существовало раздельного определения сущностей информационных технологий и информационной безопасности. В настоящее время специалисты применяют для решения проблемы обеспечения безопасности международную экспертизу, подробно изложенную в стандартах IEC (ГОСТ Р МЭК) серии 61508 и/или 61511, а также методы обработки рисков в соответствии с требованиями стандартов ISO и ISO/IEC (ГОСТ Р) серии 31000 и/или 27005.*

*В статье предложено при обеспечении безопасности промышленных систем управления различного назначения учитывать несколько аспектов, в том числе: заданное быстродействие, методы подтверждения соответствия, формирования оценок остаточных рисков и иных исчислимых оценок. Предложено обратить первостепенное внимание на развитие подхода «от функциональности», при котором формирование и решение проблемы начинается в тот момент, когда производитель создает спецификацию на разработку промышленной системы управления, включающую требования функциональной безопасности, и далее проводит оценку по установленным и известным требованиям доверия.*

*Ключевые слова: безопасность промышленных систем управления, риск, требования функциональной безопасности, требования доверия, киберинцидент.*

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

.

**Список литературы**

*1. Лившиц И.И. А*удит информационной безопасности объектов топливно-энергетического комплекса // Энергобезопасность и энергосбережение. 2021. № 1. С. 5-12.
*2. Лившиц И.И.* К вопросу обеспечения безопасности промышленных систем // Научно-технический вестник информационных технологий, механики и оптики. 2021. Т. 21. № 1. С. 1-14.
*3. 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. N 4. P. 042030.
*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.* Практика управления киберрисками в нефтегазовых проектах компаний холдингового типа // Вопросы кибербезопасности. 2020. № 1(35). С. 42–51.

**Livshits I.I.** On the assessment of cybersecurity of industrial control systems

*Cybersecurity aspects to be allowed for in various control systems are discussed. These include specified response speed, compliance certification methods, residual risk assessment, and other measurable indicators. The paramount attention should be paid to the development of the functionality-oriented approach. This means tha the task formulation and accomplishment starts when the developer creates the specification of the future control system including functional security requirements with the subsequent assessment based on the established and known*

*confidence requirements.*

*Keywords: industrial control system security, risk, functional security requirements, confidence requirements, cyberincident.*