Автоматизация в промышленности 2020. №12
www.avtprom.ru

DOI: 10.25728/avtprom.2020.12.02

И.И. Лившиц (Университет ИТМО)

ИССЛЕДОВАНИЕ ОЦЕНОК ЗАЩИЩЕННОСТИ ПРОМЫШЛЕННЫХ СИСТЕМ

В настоящее время при организации защиты промышленных систем различного назначения наблюдаются две крайности – внедрение несовместимых средств защиты информации, не затрагивая базовую ИТ-инфраструктуру, или реализация различных режимов тотальной изоляции (например, архитектуры Zero Trust). Как следует из ежегодных аналитических отчетов мировых экспертов (IBM, MS, Group-IB, Positive Technology и др.), наблюдается постоянный рост сообщений о закрытии очередных критических уязвимостей, но проблема обеспечения безопасности промышленных систем все еще не решена. Известно, что данная проблема признана многими экспертами актуальной и важной.

Существенным негативным фактом является сохранение практики текущего раздельного оценивания двух сущностей – ИТ и ИБ, что не в полной мере обеспечивает оптимальное решение поставленной выше проблемы. В представленной работе дается краткий обзор существующих подходов оценки защищенности промышленных систем. Сформулированные рекомендации могут быть применены для совершенствования существующих и создания перспективных решений для обеспечения безопасности промышленных систем, в том числе и при обеспечении национального цифрового суверенитета.

Ключевые слова: информационная безопасность, промышленная система, менеджмент рисков, меры защиты, оценка соответствия.

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

Список литературы

1 Баранов С.Н., Соколов Б.В., Тележкин А.М., Мустафин Н.Г. Модели рисков в программных проектах // Тр. II межрегиональной научно-практич. конф. «Перспективные направления развития отечественных информационных технологий». Севастопольский государственный университет. 2016. С. 45-46.
2. Соколов Б.В., Иванов Д.А., Павлов А.Н., Слинько А.А. Имитационной моделирование живучести критических инфраструктур // Тр. VII конференции "Имитационное моделирование. Теория и практика" (ИММОД-2015). ИПУ РАН. Под ред. С.Н. Васильева, Р.М. Юсупова. 2015. С. 162-167.
3. Верзилин Д.Н., Соколов Б.В., Юсупов Р.М. Неокибернетика: состояние исследований и перспективы развития//Сб. трудов XXIII междунар. научно-практич. конф. «Системный анализ в проектировании и управлении». 2019. С. 81-98.
4. Attacks on Smart Manufacturing Systems. [Электронный ресурс]. https://documents.trendmicro.com
5. Claroty Biannual ICS Risk & Vulnerability Report [Электронный ресурс]. https://f.hubspotusercontent20.net

6. Уязвимости периметра корпоративных сетей [Электронный ресурс]. https://www.ptsecurity.com
7. Livshitz I.I., Neklyudov A.V., Lontsikh P.A. IT-Security evaluation – “Hybryd” approach and risk of its implementation. В сборнике: Journal of Physics: Conference Series. International Conference Information Technologies in Business and Industry 2018 - Enterprise Information Systems. 2018. С. 042030.
8. Лившиц И.И., Неклюдов А.В. Методика оптимизации программы аудитов информационной безопасности//Тр. XXII научно-практич. конф. «Комплексная защита информации». 2017. С. 135-139.
9. Лившиц И.И. Метод оценивания безопасности облачных ИТ-компонент по критериям существующих стандартов. SPIIRAS Proceedings. 2020. Vol. 19 No. 2. С. 383-411.
10. Лившиц И.И. Практика управления киберрисками в нефтегазовых проектах // Вопросы кибербезопасности. 2020. № 1(35). С. 42–51.
11. Костогрызов А.И., Зубарев И.Ю., Родионов В.Н. Методическое руководство по оценке качества функционирования информационных систем (в контексте стандарта ГОСТ РВ 51987). М. 2004., 352 с., 2004.
12. Костогрызов А.И. Эффективное управление рисками для критических и стратегически важных объектов РФ//ИТ-Стандарт. 2015. № 2 (3). С. 1-8.
13. Костогрызов А.И. Пути решения некоторых проблем комплексной безопасности методами системной инженерии // ИТ-Стандарт. 2017. № 4 (13). С. 5 - 12.
14. Жидков И.В., Кадушкин И.В. О признаках потенциально опасных событий в информационных системах // Вопросы кибербезопасности. 2014. №1(2). стр. 40 - 48.
15. Бойко А. А., Гриценко С. А., Храмов В. Ю. Система показателей качества баз данных автоматизированных систем//Вестник ВГУ. Серия: Системный анализ и информационные технологии. 2010. № 1. стр. 39-45.

Livshits I.I. Investigation of industrial system security assessments

Recent years have seen two extremes in the organization of industrial systems protection: the application of incompatible information security tools not affecting the basic IT infrastructure, and the implementation of various total isolation modes such as, e.g., Zero Trust architecture. Analytical reports from world experts increasingly inform about closing new critical vulnerability gaps, but the industrial systems security threat is still a challenge. An important negative factor is the existing practice of separate assessment of IT and information security. Against this background, the paper reviews the existing approaches to industrial systems security assessment. The author’s recommendations may improve the existing solutions and develop new ones for industrial systems security, in particular, to ensure the national digital sovereignty.

Keywords: information security, industrial system, risk management, protection measures, conformance evaluation.