УДК 004.056

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В АРХИТЕКТУРЕ ПРОМЫШЛЕННЫХ СИСТЕМ АВТОМАТИЗАЦИИ

Гетманюк И.Б. (ИТМО)
Научный руководитель – доктор технических наук, доцент БИТ Беззатеев С.В.
(ИТМО)

В настоящее время объекты критической инфраструктуры (КИИ) Российской Федерации (РФ), имеющие стратегическое значение для страны, обеспечиваются в значительной степени импортируемой техникой и программным обеспечением. Распоряжением правительства РФ в 2023 для обеспечения безопасности страны и ее граждан утверждён перечень направлений технологического развития до 2030 года, в который вошли технологии искусственного интеллекта, распределенных реестров, квантовых вычислений, систем связи и т.д., который был пересмотрен из-за ключевых угроз развития РФ с 2023 по 2030 годы [1].

Введение.

Критически важными для функционирования технологических предприятий КИИ являются системы автоматизации производства (кибер-физические системы — КФС). Компоненты и устройства КФС выполняют функции, необходимые для безопасной и эффективной работы процесса, но именно архитектура — логическая организация компонентов и связанной с ними инфраструктуры — часто диктует выбор этих компонентов и определяет ключевые характеристики производительности системы, такие как надежность, качество продукции, пропускная способность, масштабируемость, стоимость, защищенность информации и главное безопасность людей.

Основная часть.

Каждая КФС состоит из определенного набора элементов: процессы; сеть и линии связи; программное обеспечении и прошивки, физические устройства. Типовая архитектура строится по эталонной архитектуре Пердью, и включает в себя 5 строго вертикальных уровней (модель ISA-95) разграничивая зоны ИТ и автоматизации. Концепция промышленного Интернета вещей (IIoT) предусматривает трансформацию вертикальной архитектуры системы в горизонтально распределенную среду стирающую грань между информационными и технологическими процессами [2]. Однако одна главных концепций развития КФС — это возможность внедрять быстрые инновации, основанные на данных, в производственную деятельность предприятия с меньшими затратами, что требует преодоления ограничений, создаваемых закрытыми проприетарными системами. Крупнейшие мировые промышленные компании сотрудничают с ведущими поставщиками средств автоматизации процессов и системными интеграторами для разработки стандарта Open Group Open Process Automation Standard (O-PAS) [3]. Стандарт позволит внедрить новые цифровые инструменты Индустрии 4.0.

Выводы. Кибербезопасность является важным фактором для организаций в защите от потери доходов и репутации при нарушении безопасности информации. Архитектура КФС системы должна использовать преимущества, как существующих систем, так и технологий Индустрии 4.0, основанные на подключении к IIoT и облачных сервисах. Это играет важную роль в предотвращении повреждения продукции и оборудования или даже потенциальных катастроф, начиная от загрязнения окружающей среды и заканчивая ядерными авариями.

Список использованных источников:

1. Распоряжение Правительства Российской Федерации от 20.05.2023 г. № 1315-р «Об утверждении Концепции технологического развития на период до 2030 года» //

Официальный сайт Правительства Российской Федерации. URL: http://government.ru/docs/48570/ (дата обращения: 10.01.2024).

2. Гетманюк И.Б., Федоров И.Р., Енгалычев Р.С. ИССЛЕДОВАНИЕ МЕТОДОВ АУТЕНТИФИКАЦИИ В ПРОМЫШЛЕННОМ ИНТЕРНЕТЕ ВЕЩЕЙ. БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ = IT Security, Том 30, № 1 (2023).

3. Bartusiak R. D. et al. Open Process Automation: A standards-based, open, secure, interoperable process control architecture //Control Engineering Practice. – 2022. – Т. 121. – С. 105034.

Гетманюк И.Б. (автор) Подпись

Беззатеев С.В., д.т.н., доцент (научный руководитель) Подпись