УДК 004.056:004.896

Зайцева Надежда Валерьевна,
студентка гр. АТП-23-1, Ангарский государственный технический университет,
e-mail: nadezdazajceva29262@gmail.com
Блащинская Оксана Николаевна,
старший преподаватель кафедры АТП, Ангарский государственный технический университет,
e-mail: lin_oks@mail.ru
Деревягина Светлана Сергеевна,
доцент кафедры АТП, Ангарский государственный технический университет,
e-mail: dss-kit@yandex.ru

ОЦЕНКА РИСКОВ КИБЕРБЕЗОПАСНОСТИ АСУ ТП ПРИ ИНТЕГРАЦИИ В КОНЦЕПЦИЮ «УМНОГО ЗАВОДА»

Zaitseva N.V., Blaschinskaja O.N., Derevyagina S.S.

ASSESSMENT OF CYBERSECURITY RISKS OF AUTOMATED PROCESS CONTROL SYSTEMS DURING INTEGRATION INTO THE SMART FACTORY CONCEPT

Аннотация. В статье рассматриваются проблемы кибербезопасности автоматизированных систем управления технологическими процессами (АСУ ТП) в условиях интеграции в концепцию «Умного завода». Цифровая трансформация промышленности сопровождается конвергенцией информационных (IT) и операционных технологий (OT), что расширяет поверхность атаки и создает новые угрозы для критической инфраструктуры. Систематизированы ключевые риски, возникающие при переходе к киберфизическим производственным системам.

Ключевые слова: АСУ ТП, кибербезопасность, «Умный завод», Индустрия 4.0, критическая информационная инфраструктура.

Abstract. The article discusses the cybersecurity issues of automated process control systems (APCS) in the context of integration into the Smart Factory concept. The digital transformation of industry is accompanied by the convergence of information (IT) and operational (OT) technologies, which expands the attack surface and creates new threats to critical infrastructure. The key risks associated with the transition to cyber-physical production systems are systematized.

Keywords: automated process control, cybersecurity, Smart Factory, Industry 4.0, and critical information infrastructure.

Концепция «Умного завода» предполагает глубокую интеграцию информационных и операционных технологий, что обеспечивает новые возможности для оптимизации производства. Однако эта конвергенция коренным образом меняет ландшафт угроз для автоматизированной системы управления технологическими процессами (АСУ ТП). Подключение промышленных сетей к корпоративной инфраструктуре и внешним цифровым платформам устраняет традиционную изоляцию, открывая злоумышленникам доступ к управлению физическими процессами [1].

Ключевая проблема оценки рисков кроется в различии приоритетов: для информационных технологий (IT) главное – конфиденциальность данных, для АСУ ТП – доступность и непрерывность процесса.

Применение стандартных IT-подходов к защите промышленных систем может стать причиной отказа оборудования [2, 3].

В архитектуре «Умного завода» возникают критические зоны риска. Унаследованные контроллеры (программируемый логический контроллер) с жизненным циклом 10–15 лет не имеют встроенных механизмов защиты. Расширение поверхности атаки происходит за счет множества IoT-датчиков, часто закупаемых в обход служб информационной безопасности. Неконтролируемый удаленный доступ подрядчиков создает скрытые каналы проникновения [3].

Для минимизации рисков необходим комплексный подход, сегментация сетей с изоляцией операционных технологий (OT), контура, внедрение систем обнаружения вторжений, адаптированных к промышленным протоколам (Modbus, Profinet, OPC UA), и строгий контроль целостности системы согласно стандартам серии IEC 62443 [4].

Таким образом, безопасная реализация «Умного завода» требует перехода к адаптивной системе управления рисками, встроенной в архитектуру АСУ ТП и учитывающей их специфику.

ЛИТЕРАТУРА

1. **Айдинян А.Р., Кирсанов Д.Г.** Обеспечение информационной безопасности в производственной сети промышленного предприятия // Вестник Дагестанского государственного технического университета. Технические науки. 2025. Т. 52, № 1. С. 39–48.

2. **Кетов А.** Три ошибки руководителей служб ИБ в вопросах защиты АСУ ТП. Как их избежать? // Anti-Malware.ru. 2025. URL: https://www.anti-malware.ru/practice/methods/Three-mistakes-in-ICS-protection

3. **Генгринович Е., Половинко В., Кузнецов А.** и др. Слепые зоны реагирования в АСУ ТП // ITSec.Ru. 2025. URL: https://www.itsec.ru/articles/slepye-zony-reagirovaniya-v-asu-tp

4. ГОСТ Р МЭК 62443-3-3-2016. Сети промышленной коммуникации. Безопасность сетей и систем. Часть 3-3. Требования к системной безопасности и уровни безопасности