

УДК 004

ОЦЕНКА ПОДХОДОВ К СВЯЗИ СТАНКОВ, КОМПЬЮТЕРОВ И ИНТЕРНЕТА

Белан А.Ю., студент гр. 600 ис-2к, II курс, Кучма С.А., студент гр. 600 ис-2к,
II курс

Научный руководитель: Ващенко К.С., преподаватель
Политехнический институт (филиал) ДГТУ в г. Таганроге
г. Таганрог

Цифровая трансформация промышленности невозможна без внедрения компьютерно-интегрированных производственных систем (КИПС). В этой статье рассматривается, организация связей между станками, компьютерами и интернетом в таких системах. Проводится сравнительная оценка плюсов и минусов разных способов. Тема актуальная, потому что сейчас, в эпоху «Индустрии 4.0», от того, насколько хорошо оборудование связано между собой, напрямую зависит, насколько предприятие будет конкурентоспособным [1]. Чтобы сделать производство «умным», нужно единое информационное пространство, где станки и цифровое управление работают вместе. Без такой интеграции сложно оперативно собирать данные о работе оборудования, быстро реагировать на сбои и гибко перенастраивать производство под новые задачи.

КИПС устроена так, что все этапы производства находятся в общем информационном поле. В неё входят: сами станки (это физическая часть), компьютеры с программами (отвечают за подготовку и контроль), а также сети — локальные и глобальные, которые всё это связывают в единую систему. Благодаря такой структуре информация о состоянии каждого станка, времени выполнения операций и возможных отклонениях становится доступной для анализа в реальном времени, что позволяет оперативно принимать управленческие решения.

Главная цель, когда внедряют КИПС, — сделать производство гибким, прозрачным и более выгодным экономически [1].

Добиться этого можно только если между всеми компонентами правильно настроена связь. От того, какой способ связи выбран, зависит, как быстро предприятие реагирует на изменения рынка, насколько стабильно качество продукции и какая в итоге будет прибыль.

Если посмотреть на то, как сейчас работают предприятия, можно выделить три основных способа объединить станки, компьютеры и интернет в рамках КИПС.

Первый способ — локальный, или прямое подключение. Тут станок соединяется с компьютером напрямую через USB, RS-232 или Ethernet, но

только на время, пока передаётся управляющая программа. После передачи связь обычно разрывается.

Плюсы: дёшево, просто, не нужно покупать дорогое сетевое оборудование.

Минусы: нельзя постоянно следить за состоянием станка в реальном времени, сложно добавить ещё станки в систему, много ручной работы, не хватает данных, чтобы анализировать, насколько эффективно работает оборудование (ОЕЕ) [4]. Кроме того, при таком подходе программы приходится переносить на флеш-носители или подключать кабель к каждому станку отдельно, что занимает время и повышает риск ошибок при передаче данных. Такой вариант целесообразен для единичного производства или небольших мастерских, где отсутствует потребность в сложной аналитике.

Второй способ — сетевой, через локальную сеть. Здесь станки и компьютеры объединяются в одну сеть внутри предприятия. Это позволяет управлять оборудованием удалённо с компьютера и следить за его работой.

Плюсы: можно централизованно управлять группой станков, видеть их состояние в реальном времени, быстро передавать управляющие программы (DNC). Такая система даёт возможность гибко перенастраивать линии, следить за загрузкой и быстро замечать сбои [5].

Минусы: оборудование должно иметь сетевые разъёмы, система работает только в пределах предприятия, нужно тратить на прокладку сетей. Но для среднего бизнеса такие затраты окупаются за счёт меньшего количества простоев и роста производительности.

Третий способ — облачный, или промышленный интернет вещей (IIoT). В этом случае станки подключаются к интернету и передают данные в облачные сервисы. Управлять можно с любого устройства, у которого есть доступ в интернет [3].

Плюсы: можно удалённо получать данные с производства, автоматически собирать и хранить информацию, использовать предиктивную аналитику и машинное обучение, чтобы предсказывать поломки, управлять несколькими площадками одновременно [5].

Минусы: нужна серьёзная защита данных, каждый месяц тратишься на облачные сервисы, часто требуется дооснащать станки (ставить контроллеры), и всё работает только если интернет стабильный [2]. Особенно остро вопрос безопасности стоит для предприятий, работающих с коммерческой тайной или критической инфраструктурой, поэтому при выборе облачного решения необходимо тщательно прорабатывать меры защиты.

У каждого способа — своя сфера применения. Всё зависит от того, что важнее: функциональность или деньги. Локальный метод хоть и дешёвый, но плохо подходит для расширения. Сетевой подход чаще всего выбирают средние предприятия — он даёт хороший баланс между затратами и уровнем автоматизации. Облачный подход открывает большие возможности для работы с данными и искусственным интеллектом, но требует серьёзных

вложений на старте и высокой квалификации ИТ-специалистов для обеспечения безопасности.

При внедрении любого из этих подходов обычно сталкиваются с несколькими типичными проблемами. Первая — старое оборудование несовместимо с новыми системами. Выход — использовать промышленные шлюзы и адаптеры, которые собирают данные с датчиков. Вторая — разные протоколы передачи данных (Modbus, Ethernet/IP и другие), поэтому нужны программные коннекторы и универсальные платформы, которые переводят всё в единый формат. Третья — риски кибербезопасности: подключение к интернету увеличивает шанс, что кто-то получит несанкционированный доступ. Чтобы этого избежать, используют VPN, шифрование, делят сети на сегменты и регулярно обновляют ПО [2].

Таким образом, в ходе исследования выполнена оценка трёх основных подходов к организации связи станков, компьютеров и интернета в компьютерно-интегрированных производственных системах. Локальный подход простой, но подходит только для самых простых производств. Сетевой подход, построенный на локальной сети, даёт нужный уровень централизации и контроля для большинства промышленных предприятий. Облачный подход на базе ИИТ даёт максимум возможностей для аналитики и удалённого управления, но требует серьёзного подхода к безопасности.

Выбирать, какой вариант лучше, нужно исходя из целей предприятия, состояния оборудования и того, насколько это выгодно экономически [4]. Скорее всего, технологии промышленного интернета вещей будут развиваться дальше, облачные решения станут дешевле, и тогда они станут доступнее для малого и среднего бизнеса [3].

Список литературы:

1. Афанасьев, А. А. Индустрия 4.0: перспективы цифровизации и трансформации российской промышленности / А. А. Афанасьев // Российский журнал инновационной экономики. – 2023. – Т. 13, № 3. – С. 1427–1446. – DOI: 10.18334/vines.13.3.117880.
2. Фирсов, Д. С. Средства обеспечения сетевой безопасности АСУ ТП : выпускная квалификационная работа / Д. С. Фирсов ; Ивановский государственный энергетический университет. – Иваново, 2023. – 51 с.
3. Гнездицкий, М. А. Промышленный Интернет вещей как механизм реализации концепции "Индустрия 4.0" / М. А. Гнездицкий, Р. С. Зарипова // Научно-технический вестник Поволжья. – 2023. – № 5. – С. 193–196. – ISSN 2079-5920.
4. Кирилов, К. О. Перспективы решения проблем цифровизации российской промышленности / К. О. Кирилов // Вестник Московского университета им. С.Ю. Витте. Серия 1: Экономика и управление. – 2023. – № 2 (45). – С. 74–80. – DOI: 10.21777/2587-554X-2023-2-74-80.

5. Нигматов, Р. Р. Практические аспекты применения технологии промышленного интернета вещей на современных предприятиях / Р. Р. Нигматов // Экономика и управление в машиностроении. – 2023. – № 5. – С. 31–36.