**ЭГПА и кибер-физические системы (CPS) – «Интеллектуальные системы ЭГПА в концепции Индустрия 4.0»**

Электрогидропневмоавтоматика (ЭГПА) – междисциплинарное направление автоматизации, объединяющее электрические, гидравлические и пневматические приводы и датчики для управления промышленным оборудованием. Она опирается на принципы *мехатроники* – синергетического сочетания механики с электронными и электротехническими компонентами. В ЭГПА применяются, например, электрические двигатели и серводвигатели, гидроцилиндры и гидромоторы, пневмоцилиндры и пневмодвигатели, а также соответствующие датчики (датчики давления, положения, расхода, температуры и др.) для контроля технологических параметров. Автоматизация вообще означает применение технических средств и систем управления, позволяющих освободить человека от прямого участия в управлении процессами.

Кибер‑физические системы (CPS) – это концепция, при которой к цифровой вычислительной части «прикрепляются» физические объекты и процессы. Проще говоря, CPS – это система, в которой сенсоры и исполнительные устройства физической машины тесно связаны с вычислительным ядром и сетью, обеспечивая обмен данными между «реальным» оборудованием и цифровыми моделями. Архитектура CPS обычно включает несколько уровней: *физический уровень* (датчики и приводы), *сетевой уровень* (передача данных по промышленным сетям, протоколы связи) и *когнитивный уровень* (приложения и сервисы анализа данных, цифровые модели). На физическом уровне собираются измерения (например, давление, температура), на сетевом – данные доставляются в облако или локальный сервер, а на когнитивном – используются алгоритмы ИИ, визуализации или цифровые двойники для принятия решений и оптимизации. Интернет вещей (IoT) тесно перекликается с CPS: IoT – это концепция сети «вещей» с датчиками, связанных через интернет, то есть фактически глобальное продолжение CPS-архитектуры для подключённости устройств.

В контексте Индустрии 4.0 кибер‑физические системы играют ключевую роль, внедряя интеллект и когнитивные алгоритмы в производство[splunk.com](https://www.splunk.com/en_us/blog/learn/cyber-physical-systems.html#:~:text=Cyber,process%20of%20a%20physical%20system). CPS позволяют создавать *цифровые двойники* оборудования, прогнозировать работу механизмов и управлять сложными процессами «единой панелью», что повышает гибкость и эффективность предприятий. Например, на российских производствах уже применяются цифровые двойники газовых месторождений («Севернефтегазпром»), насосных станций и металлургических линий для мониторинга и оптимизации работы. Благодаря CPS «умная» автоматизация контролирует и анализирует оборудование в реальном времени, реализуя принципы Индустрии 4.0.

**Ключевые термины:**

**ЭГПА** (электрогидропневмоавтоматика) – направление автоматики, объединяющее электрические, гидравлические и пневматические компоненты и системы в единую систему управления.

**CPS** (кибер-физическая система) – система, интегрирующая вычислительные ресурсы с физическими устройствами и процессами, обеспечивая обмен данными между ними.

**IoT** (Internet of Things) – концепция сети передачи данных между «вещами» с встраиваемыми датчиками, позволяющая устройствам взаимодействовать друг с другом и с внешней средой.

**Мехатроника** – область науки, синтезирующая механические системы с электронными, электротехническими и компьютерными компонентами для создания «умных» машин.

**Автоматизация** – применение технических средств и систем управления, освобождающих человека от непосредственного участия в производственных процессах.

**Цифровой двойник – архитектура и компоненты**

**Цифровой двойник (Digital Twin)** – виртуальная модель физического объекта или системы, синхронизированная с ним в реальном времени. В отличие от обычной компьютерной модели, цифровой двойник не только получает данные с датчиков оборудования, но может и влиять на работу этого оборудования. Проще говоря, цифровой двойник – это «двунаправленная» связь: он непрерывно получает информацию о состоянии физической системы и при необходимости передаёт управляющие сигналы обратно для оптимизации работы. По сравнению с этим **цифровая тень (Digital Shadow)** – это «однонаправленная» копия: она собирает реальные данные, но не управляет оборудование. Например, простой цифровой двойник насосной установки содержит 3D-модель насоса и бака (физическая модель), математическую модель гидравлических процессов (модель поведения), а также поток данных с датчиков давления/расхода и HMI-интерфейс для визуализации. В архитектуре двойника можно выделить основные компоненты: физическая модель (геометрия и конструкция объекта), модель поведения (алгоритмы, описывающие динамику и характеристики), сенсорные данные (показания с датчиков реального оборудования) и интерфейс (средство визуализации или API для взаимодействия пользователя с двойником).

**Варианты реализации цифровых двойников:** существует несколько подходов. *Standalone (независимый)* – один цифровой двойник, работающий локально, без распределённого соединения. *Federated (федеративные)* – группа взаимосвязанных двойников, каждый из которых описывает часть системы. *Hybrid (гибридный)* – совмещает локальные и облачные компоненты: часть моделей и вычислений выполняется непосредственно на оборудовании (edge), а часть – в облаке. Например, двойник турбины может работать на локальном устройстве управления для быстрой диагностики, а агрегированные данные по всему цеху обрабатываются в облаке.

**Примеры кейсов:** на практике цифровые двойники создают для насосов, турбин, электромоторов и других машин. Например, цифровой двойник насосной станции сочетает модель корпуса и рабочего колеса с данными вибрации и давления, позволяя прогнозировать износ и оптимизировать режимы работы. Таким образом, цифровой двойник служит расширением традиционной автоматизации – он не только моделирует, но и предсказывает поведение оборудования.

**Протоколы IIoT: OPC UA vs MQTT**

**OPC UA** (OPC Unified Architecture) – промышленный протокол обмена данными «машина–машина» и «машина–человек». Это независимый от платформы стандарт, используемый для интеграции данных промышленных контроллеров и SCADA-систем. OPC UA позволяет описывать сложные информационные модели оборудования и обеспечивает надёжную передачу данных с сервисами обнаружения серверов (Discovery), подписки на данные (Subscription) и отслеживания конкретных «контролируемых элементов» (MonitoredItems). Клиент подключается к серверу, подписывается на нужные узлы адресного пространства, и сервер уведомляет клиента о изменении этих значений.

**MQTT** (Message Queuing Telemetry Transport) – лёгкий протокол обмена сообщениями «издатель/подписчик» для IoT-устройств. В MQTT каждая сторона работает через центральный брокер: «издатели» публикуют сообщения по темам (topics), а «подписчики» получают их, указывая интересующие темы. MQTT поддерживает три уровня качества обслуживания QoS: 0 – «доставка не гарантируется», 1 – «доставка как минимум 1 раз», 2 – «ровно 1 раз». Протокол очень лёгкий (минимальный overhead) и хорошо подходит для сетей с ограниченными ресурсами и нестабильной связью.

**Сравнение протоколов:** OPC UA и MQTT дополняют друг друга. OPC UA обладает встроенными механизмами безопасности (TLS, X.509-сертификаты, шифрование) и богатой моделью объектов, но более тяжеловесен. MQTT сам по себе очень лёгкий, но для защиты данных обычно использует TLS/VPN-соединения. OPC UA лучше подходит для традиционной автоматизации и SCADA-систем (прямое подключение контроллеров, подписки на конкретные данные), тогда как MQTT широко используется в IIoT-решениях и облачных системах (сенсоры передают данные в брокер, далее в аналитические сервисы). При необходимости гибридного подхода возможна интеграция: например, SCADA может читать данные с PLC по OPC UA, а синхронизировать агрегаты и отчёты в облаке по MQTT.

**Отказоустойчивость и кибербезопасность сетей ЭГПА**

**Отказоустойчивость** характеризует способность системы продолжать работу при отказах элементов. Ключевые параметры надёжности – **MTTF** (средняя наработка до отказа) для неремонтируемых систем и **MTBF** (среднее время между отказами) для ремонтируемых. Повышение надёжности достигается резервированием: дублированием каналов связи, контроллеров и датчиков. Например, используется двойное питание, резервные сети (двухкольцевой или ячеистой топологии) и протоколы резервирования линий связи.

Типичные топологии сетей в ЭГПА: шина (один кабель к множеству устройств, простой, но ненадёжный при обрыве), звезда (все устройства через концентратор/коммутатор, отказ одного сегмента не выводит всю сеть), кольцо (с возможностью реверсирования по второму кольцу при разрыве) и ячейчатая (mesh) (каждый узел связан с несколькими, высокая отказоустойчивость). Выбор топологии зависит от требований и бюджета: для критичных систем предпочтительны кольцевые и ячеистые сети с резервированием путей.

Кибербезопасность: важный аспект современных сетей. Используются стандартные методы защиты данных: TLS/SSL – протоколы шифрования по каналу, X.509-сертификаты – для аутентификации устройств и обеспечения надёжной передачи, VPN и VLAN – для изоляции и защиты трафика в локальных сетях. Например, OPC UA реализует TLS и цифровые подписи на уровне протокола, а MQTT обычно шифруют через TLS и расширяют по сетевым правилам. Существуют и отраслевые стандарты: ISA-99 (IEC 62443) – серия стандартов по кибербезопасности систем АСУ ТП[isa.org](https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards#:~:text=The%20ISA%2FIEC%2062443%20series%20of,between%20process%20safety%20and%20cybersecurity), определяющая уровни защиты и процессы управления доступом. Соблюдение ISA‑62443 обеспечивает комплексное управление рисками и контролями в автоматизированных системах.

**Edge-AI и предиктивное обслуживание**

**Edge-AI** – архитектура, при которой анализ данных и выводы выполняются не в облаке, а на локальных устройствах («на границе сети»). Например, датчик на насосе может сам проводить inferencing (анализ вибрационных и температурных сигналов) по обученной модели и принимать решение о необходимости сигнала тревоги или передачей только тревожных событий в облако. Это позволяет снизить задержки и нагрузку на сеть, поскольку «умный» сенсор обрабатывает «сырые» данные локально. Общая схема Edge-AI в промышленности: датчики собирают показания (вибрация, температура, ток и др.) → локальное устройство (gateway или встроенный контроллер) с AI-моделью делает быстрый анализ/классификацию → в случае необходимости передаёт в облачную систему только результаты или аномальные события для более глубокой обработки и хранения.

В **предиктивном обслуживании** (predictive maintenance) первая задача – постоянный сбор данных о состоянии оборудования. Затем применяются алгоритмы (чаще всего машинного обучения): *обнаружение аномалий* (классификация ненормального поведения), *прогнозирование* времени до отказа (регрессия), *деревья решений* и другие методы. Этапы обычно таковы: 1) сбор и очистка данных (фильтрация шумов, агрегация), 2) извлечение признаков (характеристики вибрации/температуры и т.п.), 3) построение и обучение модели на исторических данных, 4) запуск модели в реальном времени (edge или облако), 5) генерирование предупреждений о вероятном выходе оборудования из строя.

**Реальные кейсы:** в промышленности предиктивное обслуживание применяют к критическому оборудованию: насосам, турбинам, редукторам. Например, анализ вибрационных сигналов на насосах может предсказать износ подшипников задолго до фактического отказа. По данным рынка, внедрение IIoT и предиктивной аналитики может помочь промышленникам предотвратить простои оборудования и существенно повысить **OEE** (общую эффективность оборудования) – своевременное техобслуживание снижает аварийность и увеличивает время безотказной работы.

**Предобработка и визуализация данных**

Перед анализом IoT/АСУ данных необходимо очистить и нормализовать информацию. Для подавления шумов часто используют скользящее среднее (Moving Average) или медианный фильтр – они усредняют соседние точки, убирая резкие выбросы. На практике берут окно заданной длины (например, 10 измерений) и усредняют значения. После фильтрации может потребоваться нормализация данных: приведение разных величин к общему масштабу (например, [0;1] или со средним 0 и единичной дисперсией). Нормализация нужна, чтобы избежать доминирования одних признаков над другими из-за разных диапазонов изменения. Альтернативно применяют стандартизацию (приведение к Z-параметрам), особенно при использовании моделей, чувствительных к масштабу.

Далее выполняется агрегация данных – формирование усреднённых или суммарных значений по временным окнам (time window), чтобы обрабатывать большие потоки точек. Например, собирают среднее значение температуры каждую минуту вместо постоянного хранения всех замеров по миллисекундам.

Для визуализации данных есть специализированные платформы.

**ThingSpeak** – облачный IoT-сервис с графиками и API для простого мониторинга. **Grafana** – open-source панель с поддержкой множества источников (InfluxDB, Prometheus и др.), идеально подходит для real-time дашбордов с графиками времени. **Azure IoT** (Microsoft) предоставляет набор сервисов: IoT Hub для приёма данных, Time Series Insights или Power BI для визуализации и аналитики. Выбор платформы зависит от архитектуры: для автономных экспериментов подойдёт ThingSpeak, для полноценного «умного завода» – Grafana или облачные решения типа Azure, которые обрабатывают стримы данных и формируют комплексные отчёты.

**Проектирование P&I-схемы**

**P&ID** (Piping and Instrumentation Diagram) – «Трубопроводно-инструментальная схема» промышленного процесса, показывающая оборудование (насосы, баки, теплообменники и т.д.), трубопроводы и схемы управления. Схема разрабатывается на этапе проектирования и используется для планирования систем управления и управления процессом. P&ID использует стандартные обозначения ISO и ISA/SAMA для обозначения датчиков, клапанов, приводов и т.п. По стандарту ANSI/ISA S5.1 и ISO 14617 (часть 6) задаются правила идентификации измерений и обозначения устройств.

На P&ID отмечают все основные элементы технологической цепи: насосы, клапаны (задвижки, регулирующие, предохранительные), датчики давления/уровня/температуры, обменные аппараты и т.д. У каждого устройства есть «тег» (пример FIC045 – блок регулятора расхода в петле 045). Для обозначения используются принятые символы (по ISO 14617 и SAMA): кружки, квадраты, линии и сокращения (PT – датчик давления, FY – расходомер и т.д.). Разные стандарты дают таблицы этих символов (например, ISO 14617, SAMA PMC 22.1 или ISA-S5.1).

**Пример:** простейшая схема может включать насосную станцию: насос (P) перекачивает жидкость из танка (T) по трубопроводу, а в контуре установлены измерители расхода (FT) и регулирующий клапан (FV). На схеме указываются направления потока, связи датчиков с ПИД-регулятором (например, FIC – расходовой индикатор-регулятор) и место установки аварийных клапанов (RV). Для проектирования схем удобно использовать векторные редакторы (например, draw.io) с набором стандартных иконок. Главное – точно соблюдать стандарты обозначений (ISO 14617, SAMA) и чётко проставлять функциональные теги устройств.

**ПИД-регулятор в ЭГПА**

**ПИД-регулятор** реализует классический алгоритм управления:

где e(t) – ошибка (разность сигнала задания и измеренного процесса). Компоненты: пропорциональная быстро реагирует на ошибку, интегральная устраняет статическую погрешность, а дифференциальная сглаживает переход (предсказывает тенденцию изменения).

Временные характеристики системы с ПИД-регулятором включают такие параметры, как время *устоя* (перехода), *перерегулирование* (максимум выходной величины сверх установившегося значения) и *колебательность*. Увеличение обычно снижает время перехода, но увеличивает перерегулирование. Интегральный коэффициент устраняет постоянную ошибку, но делает систему более медленной, а дифференциальный помогает снижать перерегулирование и улучшать устойчивость.

**Методы настройки:** широко используются классические правила. *Метод ЧДН (Ziegler–Nichols)*: подбирают до граничных колебаний (получают

и по формулам рассчитывают , . *Метод Коэн-Куна (Cohen–Coon)* – более сложная схема для систем с запаздыванием, корректирующая недостатки Ziegler при больших задержках. Эти методы даёт начальные приближения параметров, после чего в реальных системах может потребоваться тонкая доводка.

**Пример:** при настройке ПИД-регулятора скорости насоса в Simulink можно наблюдать, как изменение , , меняет форму переходного процесса (время выхода на задачу, наличие колебаний). Повышая , мы добиваемся быстрого подъёма, но велик риск перерегулирования; добавляя , снижаем колебания; нужен для устранения смещения.

**Модуль 9: Time-Sensitive Networking (TSN) в промышленной Ethernet-сети**

**Time-Sensitive Networking (TSN)** – набор стандартов IEEE 802.1, создающий возможности для детерминированных сетей Ethernet. TSN гарантирует синхронную передачу данных с низкими задержками, что критично для автоматизации. Основные компоненты TSN: синхронизация времени (IEEE 802.1AS, основанная на протоколе PTP, обеспечивает общей тактовой частотой все устройства в сети), управление трафиком (например, IEEE 802.1Qbv – Time-Aware Shaper, планирующий временные слоты для критичных сообщений) и распределение потока (протокол резервирования Stream Reservation Protocol, IEEE 802.1Qat, который гарантирует резервацию полосы пропускания для потоков). Также есть прерывание фреймов (IEEE 802.1Qbu) – возможность «доколоть» передачу долгого не критического кадра для пропуска срочного.

TSN вводит следующие ключевые элементы: **Grandmaster Clock** (главный источник времени для всей сети), **Scheduler** (тайм-шейпер, распределяет время передачи) и **SRP** (зарезервированная полоса для потоков с высоким приоритетом). В совокупности эти механизмы обеспечивают детерминированность. По требованиям Индустрии 4.0 передачи в управлении ЭГПА должны иметь задержки менее 1 мс и джиттер менее 30 мкс (микросекунд). TSN позволяет достичь таких показателей даже в общих Ethernet-сетях, превращая их в «промышленный Ethernet» с гарантией времени доставки.

**Применение на практике:** современные коммутаторы для промышленности (например, Siemens SCALANCE или Hirschmann) поддерживают TSN. При настройке устанавливают протокол 802.1AS для синхронизации, конфигурируют таблицы временных окон (802.1Qbv) и резервирование трафика (802.1Qat). Это позволяет создавать гибридные сети, где критические управляющие команды идут по детерминированным каналам TSN, а менее важный трафик – обычным Ethernet.

**Модуль 10: PLC и SCADA vs IIoT-архитектуры**

**Традиционная архитектура** автоматизации строится по схеме: *датчики → ПЛК/РТУ → центр сбора данных (SCADA-сервер) → HMI*. Данные собираются локально, контроллеры проводят первичную обработку, а оператор через SCADA видит состояние процессов. Протоколы связи – Modbus TCP, Profinet и др. – ориентированы на надёжное детерминированное управление внутри завода. Такие системы хорошо зарекомендовали себя в простых сценариях и обеспечивают стабильность и безопасность управления.

**IIoT-архитектура:** наоборот, строится «от края к облаку»: *умные сенсоры → шлюз (gateway) → облачные сервисы → аналитика и приложения*. Протоколы – MQTT, HTTPS и другие веб-ориентированные – обеспечивают гибкий обмен данными. IIoT-фокус – на сборе больших объёмов разнородных данных (не только аварийных или операционных, но и экологических, режимных), их хранении и облачном анализе. Системы IIoT масштабируемы, легко подключают новые устройства и способны обрабатывать big data с помощью машинного обучения.

Сравнение: SCADA быстро реагирует на локальные события и предоставляет операторам удобный HMI, но часто ограничена «заводским» простором и спецификой протоколов. IIoT даёт широкие возможности интеграции (удалённый доступ через интернет, анализ больших данных, AI) и лучше подходит для предиктивной аналитики и бизнес-решений. Недостаток IIoT – потенциальные вопросы с надёжностью связи и безопасностью, а также задержки при критических задачах.

**Гибридные решения:** современные системы часто комбинируют оба подхода. Например, на заводе в реальном времени контроллеры обмениваются данными по OP UA с локальной SCADA, а часть агрегированных параметров (история работы, журналы аварий) отправляется в облачный аналитический сервис через MQTT/HTTPS. Так, инженеры получают «лучшее обоих миров» – локальное управление без задержек и глубокую аналитику в облаке. Протоколы вроде OPC UA поддерживают такую интеграцию: локальные ПЛК с OPC UA могут передавать данные в IIoT-шлюз, который конвертирует их в REST/MQTT для сервисов в облаке. Этот гибрид повышает производительность и эффективность оборудования без отказа от проверенных решений.

**Модуль 11: Big Data и аналитика в умном производстве**

**Большие данные (Big Data)** – это массивы структурированных и неструктурированных данных огромного объёма и разнообразия. Их особые свойства традиционно описывают как три «V»: *объём* (volume), *скорость* (velocity) и *разнообразие* (variety). В производстве Big Data возникают за счёт огромного числа сенсоров и систем мониторинга. Для их обработки используются горизонтально масштабируемые вычислительные решения (NoSQL-базы, MapReduce, Hadoop и т.п.). Архитектура «Data Lake» предполагает хранение всех данных (сырой и агрегированной информации) в едином хранилище, из которого выполняются ETL-процессы: извлечение, преобразование и загрузка в аналитические модели.

Для аналитики больших данных в промышленности применяются такие инструменты: Hadoop – фреймворк для распределённого хранения и обработки (использует MapReduce); Spark – платформа для быстрых вычислений «в памяти»; Elasticsearch – система индексации и поиска по большим объёмам логов и телеметрии. Они позволяют сканировать исторические записи параметров машин, выделять закономерности и строить предсказательные модели.

**Кейсы применения:** анализ данных производства помогает повышать OEE и снижать простои. К примеру, агрегирование журналов работы насосов и анализ их циклов эксплуатации позволяют выявить узкие места и неэффективные режимы, а алгоритмы машинного обучения на основе этих данных спрогнозируют, когда оборудование выйдет из стро. Используя Big Data-аналитику, компании оперативно обнаруживают аномалии (изменение вибрации, повышение температуры), вовремя проводят ТО и оптимизируют графики ремонта. В результате эффективность оборудования (OEE) растёт, так как устраняются причины простоя и сокращаются незапланированные остановки.