Круглый стол «Мир Internet вещей»

На заседании виртуального круглого стола рассмотрим экспансию Internet вещей (Internet of Things - IoT) в область промышленной автоматизации: обсудим понятие IoT, рассмотрим специфику данной предметной области, вопросы кибербезопасности, приведем примеры применений.

Ключевые слова: Internet вещей, промышленная автоматизация, идентификация, передача и обработка данных, беспроводной доступ.

Представляем участников круглого стола:

Беспалов Александр Александрович - менеджер по продукту направления «Автоматизация, промышленные устройства управления и защиты» компании Eaton в России;

Дробышевский Валерий Маликович - коммерческий директор компании «Кварта Технологии»;

Крейцер Николай Александрович - руководитель департамента разработок СпейсТим;

Кривозубов Павел Александрович - менеджер по маркетингу сегмента встраиваемых систем National Instruments (NI);

Кузин Александр Сергеевич - генеральный директор компании «Моушн Вью»;

Никишин Андрей Викторович - директор по специальным проектам департамента перспективных разработок «Лаборатории Касперского»;

Попов Сергей Игоревич - менеджер по маркетингу в России/СНГ компании Honeywell;

Хадонова Светлана Викторовна - директор по маркетингу навигационной компании СпейсТим;

Хайнрикс Бернд - управляющий директор подразделения по продвижению решений для IoT компании Cisco;

Швецов Дмитрий Петрович - руководитель технического департамента компании Прософт.

Ведущий круглого стола: Аристова Наталья Игоревна - канд. техн. наук, главный редактор журнала «Автоматизация в промышленности».

Ведущий. *В повседневной жизни современный человек уже давно привык использовать сервисы, подключенные к сети Internet. Это электронные ключи в отелях, проездные билеты, бирки на одежде в магазинах, «умные» ошейники для животных, радионяни и многое другое. Концепция IoT базируется на радиометках (для связи с окружающей средой), датчиках (собирающих информацию о параметрах контролируемого объекта), ПО (отвечающем за обработку полученной информации), встраиваемом аппаратном обеспечении (характеризуемом миниатюрными размерами, позволяющими встраивать микрочипы во всевозможные предметы обихода).*

В последнее время понятие IoT все чаще встречаются и в промышленности. Производители средств и систем автоматизации проводят презентации и конференции, описывающие Internet решения, ориентированные на производственные задачи. Так в конце мая 2015 г. компания «Кварта Технологии» провела VIII ежегодную конференцию «Встраиваемые технологии 2015». Многие участники нашего круглого стола присутствовали на этом масштабном мероприятии, объединяющей концепцией которого стала тема Internet of Things. О чем же здесь идет речь, ведь у промышленных приложений имеется своя специфика?

Пожалуйста, дайте определение понятию Internet of Things применительно к области промышленной автоматизации.

Хайнрикс Б. Строгое определение IoT применительно к области промышленной автоматизации означает, что наблюдаемые и контролируемые объекты ("вещи") не только передают информацию операторам или получают от них обратную связь, но и обладают интеллектом, достаточным для принятия решений на месте. Иными словами, сенсоры, датчики, счетчики, объекты телемеханики и т.п. обмениваются информацией друг с другом (не только с HMI или оператором), анализируют полученную информацию и на основе алгоритмов, заложенных оператором, выполняют определенные действия.

Концепция IoT применительно к промышленной автоматизации нашла свое выражение в концепции Industry 4.0. Ее родоначальником считается промышленность Германии, поддержанная феде-

Ценность Internet вещи определяется удовольствием, которое она может доставить.
Ремейк по фразе Ричард Олдингтон

ральным правительством этого государства. Industry 4.0 подразумевает, что промышленность находится на пороге четвертой волны перемен — создания так называемых «умных» фабрик (Smart Factory). "Умные фабрики" характеризуются наличием киберфизических систем: встраивание вычислительных элементов (совместно с ПО и сетевыми возможностями) в физические объекты контроля.

Беспалов А. А. В скором времени прямое информационное взаимодействие различных типов устройств и установок будет являться неотъемлемым условием функционирования практически любого производства. Такая технология называется межмашинным взаимодействием (M2M) и тесно пересекается с IoT. По сути IoT является ключевой составляющей набирающей популярность концепции Industry 4.0, которая предполагает обмен данными между всеми участниками, которые задействованы в производственной цепочке: специалистами предприятия, исполнительными компонентами, ERP-системами, роботами, продуктами и другими системами и установками. Сегодня такие предприятия принято называть «умными». В будущем продукты, изготавливаемые предприятиями, в рамках концепции Industry 4.0 должны будут «говорить» оборудованию, как, где и кем они должны быть изготовлены, для кого должны быть произведены и куда отправлены; оборудование будет автоматически перенастраиваться в зависимости от «запросов» продуктов на конвейерной ленте, а компоненты, системы управления, ERP-системы, работники предприятий и другие субъекты канала движения товара — обмениваться данными о состоянии технологических процессов, своих потребностях, состоянии товаров на этапе движения от сырья к потребителю.

Никишин А.В. Концепция Industry 4.0 предполагает оснащение промышленных агрегатов датчиками, подключаемыми к сети. Датчики отправляют информацию о состоянии узлов в центр, где данные анализируются. На основании практического опыта и данных, собранных с других устройств, принимается решение о необходимости проведения профилактических работ. В результате агрегат останавливается только тогда, когда это необходимо. Производительность растет по большому счету лишь от того, что устройство подключили к сети Internet.

Некоторые производители так и делают: оснащают свое оборудование необходимыми датчиками и контроллерами и получают рост эффективности. Но они забывают, что случилась революция, и эпоха сменилась. Нельзя так просто, без последствий подключить к Internet объект родом из «доинтернетной эры». Здесь на первый план выходят вопросы информационной безопасности.

Швецов Д. П. IoT в промышленной автоматизации — безопасное соединение того, что ранее было несоединимо. Понятие «безопасное соединение» подразумевает идентификацию устройства, коммуникационную сетевую архитектуру, способную безопасно поддерживать миллиарды устройств, за которыми стоят десятилетия инноваций и проектов мирового масштаба с использованием IP и ассоциированных протоколов безопасности.

Попов С. И. Если говорить в общем, то IoT — это сеть физических объектов, которые подключаются к Internet с помощью встроенных систем и датчиков. IoT в промышленном понимании подразумевает подключение предприятия к Internet с помощью сети различных устройств и систем автоматизации: от полевых устройств, противопожарных и аварийных систем вплоть до целой диспетчерской. По мере прогресса в области цифрового преобразования IoT в промышленности становится актуальным не столько ради постоянной связи с объектами, сколько для того, чтобы делать процессы на предприятиях более безопасными, продуктивными и гибкими.

Кривозубов П. А. Концепция IoT развивается последнее время такими семимильными шагами, что корректней было бы говорить об «Internet всего» (Internet of Everything). И разумеется сегмент промышленной автоматизации не исключение. Все то, что позволяет интегрировать промышленные технологии в единое глобальное информационное пространство, а также любые составляющие звенья, объединяющие промышленный и пользовательский IoT попадает под определение IoT в области промышленной автоматизации. Концепцию промышленного IoT нельзя рассматривать без учета двух очень важных составляющих. Это киберфизические системы и возможность оперировать большими объемами данных. Киберфизические системы — это системы, позволяющие воздействовать на физические процессы, с помощью программно-аппаратных компонентов, причем как в одну, так и в другую сторону. Большие данные — это весь поток информации, который обрабатывается киберфизическими системами, для осуществления этой связи. Совокупность этих концепций можно назвать термином IoT в области промышленной автоматизации.

Дробышевский В.М. Являясь широким термином, понятие IoT интерпретируется в зависимости от конкретного сценария и отрасли. В целом его сутью является обеспечением ощутимо новых свойств как для отдельного устройства, так и для системы в целом

на основе данных, полученных от датчиков, сенсоров и прочих источников, анализа этих данных и их применения для повышения эффективности работы. Это может относиться и к какой-то отдельно взятой системе, устройству или к целому предприятию.

Кузин А.С. Для области промышленной автоматизации концепция IoT — уже наступившее настоящее. Системы идентификации, измерения, передачи и обработки данных, системы позиционирования — все эти элементы концепции IoT уже так или иначе представлены в сфере промышленной автоматизации.

Хадонова С.В. С одной стороны, IoT — это то, что связано со встраиваемыми электронными устройствами с относительно узкой функциональностью, которые обмениваются данными через Internet. С другой, — это облачная инфраструктура, которая хранит и обрабатывает данные. Применительно к навигации и транспортной телематике IoT — это облачные M2M решения, в которых агрегируется, анализируется огромный поток навигационных данных и телематических параметров — геоданные о местоположении (координаты) объектов, данные о состоянии систем и механизмов в транспортном средстве и спецтехнике, данные о количестве топлива в топливном баке и т.д. В M2M решениях контролируется множество различных параметров, которые, в том числе считываются с CAN шины транспортного средства и передаются через облака на телематические серверы диспетчерских контрольных центров.

Ведущий. *Сформулируйте отличия концепции IoT от традиционных принципов построения промышленных систем автоматизации. Какие преимущества открывает для промышленной автоматизации новая концепция?*

Кривозубов П.А. На первый взгляд различия незначительны. Любая система автоматизации состоит из объекта автоматизации и объекта управления. Данные, которые возникают в процессе, обрабатываются и резервируются, система реагирует на контрольные точки и критические состояния либо путем управляющего воздействия, либо путем оповещения оператора. Однако отличия есть. В традиционных системах все компоненты функционируют в рамках предприятия, в связи с чем можно получить ряд проблем. Во-первых, возможности анализа данных и управления ограничены аппаратным и программным сегментом АСУТП. Все делается «на века». Отсюда вытекает вторая проблема — в случае необходимости наращивания производственной мощности производства с классической структурой модернизировать очень затратно, а зачастую и вовсе невозможно, так как это чревато полной или частичной заменой аппаратного парка предприятия, простоем производства и колоссальными убытками. В системах, работающих по концепции IoT, обработка, анализ данных, управление объектами, резервирование и другие критически важные процессы, требования к которым постоянно растут, выполняются с задействованием структур, находящихся вне предприятия, но связанных с производственным процессом по высокоскоростным проводным и беспроводным каналам связи. Такой подход делает системы IoT гораздо более гибкими и модернизируемыми, что является несомненным преимуществом подобных систем.

Дробышевский В.М. В отличие от локальных M2M сценариев IoT подразумевает два ключевых свойства — это работа с эластичной «облачной» инфраструктурой, обладающей почти безграничными возможностями по масштабированию, а также возможность подключения устройства из любого места посредством сетей беспроводного доступа. Это дает следующие преимущества:

— возможность потоковой обработки огромного объема поступающих данных без вложений в локальные серверные мощности;

— применение аналитических и серверных мощностей там, где ранее это было сделать затруднительно, например, на передвижных и удаленных объектах (главное — наличие связи, хотя бы периодически);

— существенное упрощение подключения и получения данных от множества устройств, например элементов автоматизации зданий (климат, счетчики ЖКХ, аварийные системы и т.п.), и их последующей обработки.

Беспалов А.А. С помощью IoT все участники производственной цепочки будут присутствовать в сети Internet. Это открывает возможности для целостной и адаптивной автоматизации, которая существенно повысит эффективность производственного процесса. Такая эволюция приведет к более прозрачному и эффективному производству, а также лучшей интеграции с бизнес-системами.

Гибкость производственного процесса в условиях IoT, глобально — в условиях Industry 4.0 — позволит производить каждую единицу продукта или устройства под конкретного потребителя (так называемая кастомизация) по себестоимости единицы продукции из большой партии. Это значительно поможет в ситуации, к которой сейчас стремительно движутся производители товаров потребительского рынка — максимальное удовлетворение потребностей каждого конкретного покупателя путем производства продукта с уникальными характеристиками. В совокупности с уменьшением стоимости систем управления процессом, возможным благодаря перемещению вычислений в облако, а также прогнозированию потребления, которое в свою очередь станет возможным благодаря технологиям обработки big data, это позволит изменить и удешевить всю цепочку производства и поставки продуктов или устройств.

Industry 4.0 создаст новый мир производства, в котором заказчик будет получать новую продукцию максимально быстро, причем в том виде, в котором ему хочется. Будут разработаны новые, более гибкие производственные системы, участники которых будут обмениваться информацией через Internet. Монтаж оборудования и введение его в эксплуатацию станут более оперативными. Мы получим оптимизированные системы управления, удаленный сервис и возможность обслуживания с помощью мобильных устройств. Производственные и логистические цепочки станут более «сетевыми» и значительно усложнятся, так как в рамках Industry 4.0 исчезнут производственные ограничения, обусловленные рамками одного завода или производства. Заводы начнут взаимодействовать в единой производственной сети между собой или с другими объектами, например логистическими, такими как склады, торговые магазины, либо с целыми территориальными регионами в рамках прогнозирования потребления через анализ «больших данных» и пользования Internet. Производство станет более эффективным, ожидается, что эффективность производительности труда, например, в Германии при реализации концепции Industry 4.0 может увеличиться на 30%. В итоге мы получим интеллектуальную автоматизацию на базе повсеместно интегрированных, взаимосвязанных и широко распространенных «умных» устройств, которые будут обеспечивать безотказное функционирование систем.

Швецов Д.П. По сути IoT — это более гибкая, эффективная и экономичная системная архитектура. В конечном итоге появилась бесшовная система коммуникаций для промышленного полевого ввода/вывода. Благодаря новой концепции удается достичь более высокой производительности и гибкости производства. IoT можно ассоциировать с промышленной революцией, где машинный интеллект с помощью IP будет поддерживать работу датчиков, исполнительных устройств, роботизированные комплексы, системы машинного зрения, устройства ввода/вывода через проводные и беспроводные сети. Несомненно, беспроводные устройства с поддержкой IP, включая смартфоны, планшеты и сенсоры еще шире будут использоваться в промышленной автоматизации. Благодаря поддержке IP новой версии V6 современные мощные промышленные контроллеры могут «говорить на одном языке» и реализовать больший функционал в связке с интеллектуальными датчиками с встроенными микропроцессорами. Это как минимум устранит необходимость использования промежуточного ПО, как правило, дорогого, неудобного в использовании, поддержка которого весьма затратная. В современных архитектурных решениях IoT стали более востребованы открытые беспроводные стандарты WirelessHART, ISA100 и WIA-PA и многие другие для сбора и обмена информацией, покрывающие большее пространство адресов с улучшением сетевой безопасности.

Те, кто хотят узнать, что мы думаем о всякой вещи, более любопытны, чем нужно.
Марк Цицерон

Кузин А.С. Новая концепция дает возможность максимально оптимизировать и контролировать как технологические, так и бизнес-процессы предприятий. Концепция IoT позволит увеличить скорость получения и обработки большего, по сравнению с предыдущим поколением решений, объема данных. Также системы концепции IoT позволяют уменьшить в системе рисков «человеческий фактор».

Попов С.И. В компании Honeywell промышленный IoT как концепция существует с момента появления в 1974 г. первой распределенной системы управления. Сегодня система Honeywell Experion® Process Knowledge System позволяет интегрировать различные технологические, энергетические подсистемы, а также системы безопасности. В портфеле MatrikonOPC содержится широчайший набор продуктов для связи подключаемых устройств. Фактически OPC Unified Architecture (UA) имеет все шансы стать новым стандартом для подключения устройств в мире IoT.

С возможностью подключения к Глобальной сети необходимость в сборе и анализе огромного объема информации, которая генерируется каждую секунду, становится еще более критичной. Например, программное решение Honeywell Intuition Executive собирает и анализирует большие объемы данных, обнаруживает их изменения (вариации) и преобразует их в информацию, позволяющую принимать решения. Еще одним примером служит консоль Experion Orion, которая объединяет графику и другие программные приложения РСУ в единую графическую среду, что позволяет операторам соотносить данные из разных источников.

Хайнрикс Б. В результате внедрения IoT потребителю становится доступной масса возможностей:

– информация о состоянии объектов самостоятельно поступает не только пользователю объекта, но и его изготовителю, что позволяет свести простои в работе оборудования к нулю;

– облачные технологии позволяют совместно использовать информацию о производстве с цепочкой поставщиков и улучшить показатели Just-In-Time (точно в срок);

– использование стандартных протоколов сетевого взаимодействия дает возможность применять в промышленности лучшие наработки по информационной безопасности;

– виртуализация снижает затраты на производство, поскольку позволяет смоделировать поведение объектов и перенести настройки из виртуальной модели в физическую;

– децентрализация обработки информации повышает надежность работы системы и время ее реакции;

– контроль движения и обнаружения товарно-материальных ценностей существенно снижает затраты на производство.

И это далеко не полный перечень преимуществ.

Ведущий. *Приведите практические примеры реализации концепции IoT для области промышленной автоматизации, транспорта, ЖКХ, сельского хозяйства.*

Швецов Д. П. Согласно заключению ведущих аналитиков отрасли промышленной автоматизации, в настоящее время многие компании расширяют интеграцию между системами промышленной автоматизации и корпоративными ИС, для которых IoT становится более востребованным. «Умные заводы», Industry 4.0 и «Промышленный IoT» — все эти концепции обозначают тренды развития в сфере промышленной автоматизации.

Так компания Advantech в партнерстве с Microsoft представила облако WISE-Cloud совместимое с Azure для подключения интеллектуальных устройств, разработанных и выпускаемых этой известной тайваньской компанией. Широкий перечень программных технологий уровня SCADA и MES от компании ICONICS также имеет сертифицированные коннекторы для Microsoft Azure.

Хадонова С.В. Облачные M2 M решения находят достойное место в сегменте IoT для рынка B2B. Например, в комплексной системе обеспечения безопасности пассажиров на транспорте Транспорт-Видео®, основанной на интеграции технологий ГЛОНАСС с видеонаблюдением, бортовой навигационно-связной ГЛОНАСС терминал, подключенные к нему видеокамеры и другое периферийное оборудование передают данные в диспетчерский программный комплекс.

Решение Транспорт-Видео® предназначено для повышения уровня безопасности пассажирских перевозок (включая ДТП, противоправные действия, порчу имущества и подвижного состава), а также для повышения качества перевозок (обоснованный разбор и сокращение жалоб пассажиров, сокращение сроков реагирования и разбора нештатных ситуаций, повышения культуры обслуживания пассажиров, автоматизация деятельности персонала).

В системе информирования и рекламы на пассажирском транспорте ST TransMedia® «умные» терминалы — дисплеи Digital Signage с поддержкой ГЛОНАСС, «встроенные» в автобус, обмениваются данными с облачной инфраструктурой, системой управления контентом. С помощью системы управления формируются, передаются и обновляются медиапланы в прямом эфире, производится дистанционная диагностика дисплеев, установленных в транспортное средство и т. д.

Коммерческим перевозчикам предлагается облачная услуга мониторинга транспорта ST Flagman Web®. Основа предоставления услуги — использование специализированного Web-приложения мониторинга транспорта и анализа транспортной работы.

Дробышевский В.М. В транспорте это могут быть также «умные» светофоры и системы управления трафиком; остановки, информирующие о прибытии транспорта, погоде, чрезвычайных ситуациях; системы контроля состояния автодорожного и железнодорожного полотна и подвижного состава; системы контроля скорости и видеонаблюдения; системы подобные «Эра Глонасс» и т. п. В ЖКХ — это контроль приборов учета с получением и обработкой данных в реальном времени; системы видеонаблюдения с распознаванием лиц и поведения; контроль и обслуживание лифтового хозяйства. В сельском хозяйстве — системы автоматизации теплиц, где нужно учитывать и анализировать множество факторов и не всегда есть возможность развернуть полноценные ИТ-системы; получение и обработка тахографической информации с сельхозтехники, ее ориентация в пространстве для лучшей эффективности и всевозможная телеметрия.

Кузин А.С. Системы Digital Signage, на которых специализируется компания «Моушн Вью», как элемент концепции IoT применительно к системе промышленной автоматизации реализуема, например, при организации работы логистических компаний для отображения текущего расположения и состояния транспортных средств на территории складских и/или погрузочных помещений. Создаваемая система распределенной видеотрансляции позволяет доводить до сведения персонала нужную информацию, например, с RFID-меток на транспорте, принимая и обрабатывая ее в автоматическом режиме. Другой пример — системы электронной очереди уже давно и широко используется в банковской сфере, а также активно внедряются в настоящее время в индустрии быстрого питания. Более сложные интерактивные системы, например анализ аудитории для дальнейшего использования в маркетинговых кампаниях (например, таргетированный показ рекламы), только начинают внедрятся в наиболее актуальных сферах, таких как ритейл.

Беспалов А.А. Представим шкаф управления на производстве. В шкафу управления располагается множество компонентов, которые вручную соединены между собой обычными проводами. Компания Eaton разработала коммуникационную систему SmartWire-DT, которая заменяет собой старый способ монтажа соединений в шкафу управления, позволяя сделать это примерно на 85% быстрее и легче, чем классический метод. По сути это первый шаг на пути к Industry 4.0 в рамках интеграции стандартных ис-

полнительных компонентов. SmartWire-DT уже сегодня может соединять компоненты шкафа управления, позволяя им сообщать о своем состоянии. Теперь оператору не нужно открывать шкаф, чтобы узнать о состоянии его компонентов, система сама сообщит ему об этом. Эта технология уже используется на некоторых российских предприятиях, среди которых, например, сельскохозяйственный холдинг ДАМАТЭ, где SmartWire-DT обеспечивает автоматизацию технологической линии разделки индейки. В связи с ограниченным пространством, выделяемым для размещения электрощитов управления, на заводе не было возможности использовать стандартные системы автоматизации. Решение позволило значительно уменьшить габариты шкафов управления, сократить время сборки на этапе монтажа и время тестирования системы перед запуском. По сравнению со многими коммутационными системами объем электромонтажа с помощью SmartWire-DT сокращается до 85%. Тестирование было проведено за 2,5 часа, хотя обычно это занимает до двух рабочих дней. Решение Eaton помогло не только автоматизировать линию для разделки индейки, но и свести время простоя линии к минимуму. Система универсальна и может быть использована в любой производственной сфере (автомобилестроение, пищевая, нефтегазовая и др.), которая нуждается в эффективной автоматизации.

Кривозубов П. А. Компания NI специализируется на разработке устройств класса IoT. Во-первых, это система контроля износа оборудования на предприятии Insight CM, интегрируемая в общую сеть предприятия. С помощью наших аппаратных платформ система получает данные о состоянии каждого узла, проводит диагностику, анализ и прогнозирование неисправностей. Данные обрабатываются в облачном сервере, доступ к управлению можно получить из любой точки земного шара. Помимо этого практически все устройства NI обладают возможностью интеграции в единую сеть, работающую синхронно по общему алгоритму. Это модульные платформы для высокоскоростных, многоканальных измерений PXI, платформы для построения встраиваемых систем и систем автоматизации CompactRIO и SingleBoard RIO, а также low cost платформа для построения систем сбора данных CompactDAQ. Есть множество примеров практического применения данных платформ для создания систем класса IoT. Это системы управления и автоматизации для нефтедобывающих предприятий, системы распределенного мониторинга сложных промышленных объектов, системы технического зрения и роботизированные системы, позволяющие автоматизировать целые производственные участки, системы типа «Умный дом», которые успешно применяются в области ЖКХ, или беспроводные системы сбора данных с датчиков, которые можно интегрировать в системы контроля, например в сельском хозяйстве.

Хайнрикс Б. Трансформация не происходит за одну ночь. Компании внедряют у себя те или иные элементы IoT в зависимости от сферы своей деятельности, потребностей бизнеса и от степени развития ИТ. В то же время нет ни одной компании, предлагающей полный спектр продуктов и технологий для IoT. Поэтому в настоящее время внедрение таких технологий — результат совместного труда многих производителей, системных интеграторов и заказчиков.

Среди практических примеров отметим компанию Black & Decker, реализующую контроль движения и обнаружение товарно-материальных ценностей; компанию ABB и ее современного робота YuMi; инфраструктуру порта в г. Гамбурге; виноградники в Италии и т. д.

Ведущий. *Использование сетей Internet для промышленности связано с риском угрозы кибербезопасности. Каким образом производители компонентов IoT и системные интеграторы, использующие эти компоненты, могут/должны предусмотреть эти риски и какие меры могут их снизить.*

Хайнрикс Б. Действительно, есть мнение, что использование открытых технологий Internet вместо закрытых протоколов увеличивает риск киберугроз. Однако в области Internet имеется множество наработок, связанных с обеспечением информационной безопасности. Специально для промышленной автоматизации институтом Пердью и МЭК разработаны эталонные архитектуры построения защищенной системы промышленной автоматизации, учитывающие особенности организации производства. Используя эти архитектуры и опыт производителей средств промышленной автоматизации, компания Cisco разработала ряд собственных эталонных архитектур. Например, совместно с компанией Rockwell Automation нами создана архитектура для "подключенного производства" Converged Plantwide Ethernet (CPwE) Design and Implementation Guide. Хотя в ее названии фигурирует слово "завод", заложенные в архитектуру принципы могут использоваться и в других отраслях. Более того, для отраслей ТЭК созданы архитектуры, содержащие разделы, посвященные решению вопросов информационной безопасности.

Никишин А.В. В условиях Industry 4.0 самое главное и первоочередное для производителей промышленного оборудования — признать, что новые устройства надо проектировать по-новому, с оглядкой не только на функциональную, но и на информационную безопасность. Навесить дополнительную защиту на устройство, спроектированное без учета современных реалий эксплуатации, и дорого, и сложно, а порой и невозможно. Представьте себе ситуацию, что в системе управления станком, трансформаторной подстанцией или хотя бы лифтом, обнаружена уязвимость. Скоро ли она будет закрыта? Скорее

всего эксплуатирующая организация посчитает, что у нее серьезное оборудование, до которого хакерам не добраться. Расплата может быть очень серьезной. И пока в промышленности не распространится понимание, что Internet — не просто очередной удобный инструмент, а настоящая революция, не только дающая новые возможности, но и несущая новые угрозы — ситуация с безопасностью предприятий будет неуклонно ухудшаться.

Попов С.И. Промышленный IoT до сих пор находится на ранней стадии развития. Но это не значит, что сейчас рано пытаться обеспечивать безопасность критически важных объектов, таких как производственные предприятия, НПЗ, химические заводы и т.д. Растущая угроза кибератак на промышленные объекты является мировой проблемой согласно глобальному опросу на тему кибербезопасности, проведенному компанией Ipsos Public Affairs в сентябре 2014 г. по заказу Honeywell. Две трети опрошенных полагают, что нефтегазовая, химическая и энергетическая отрасли наиболее уязвимы для кибератак. Опрос показал, что 50% взрослого населения России обеспокоены тем, что кибератаки могут нанести ущерб российской экономике. Вопрос о защите критической инфраструктуры от киберугроз должен стать приоритетным для российских компаний.

Подразделение компании Honeywell «Промышленная автоматизация» (HPS) в апреле 2015 г. представило цифровую информационную панель Industrial Cyber Security Risk Manager, предназначенную для автоматического мониторинга, оценки и управления рисками возникновения киберугроз. Решение интегрируется в системы управления нефтеперерабатывающих предприятий, электростанций и других автоматизированных производств и помогает справляться с киберугрозами, число которых стремительно растет в последнее время.

Кроме того, недавно Honeywell и Intel Security объявили о начале сотрудничества с целью предоставления заказчикам интегрированных и проверенных решений и разработки ПО, способного защитить их системы управления от вредоносных программ и ненадлежащего использования. Такой подход позволяет повысить доступность, надежность и безопасность промышленных систем управления и производственных операций

Кривозубов П.А. Для гарантии бесперебойности работы всех структур и предотвращения вмешательства стороннего кода в программы нужно обеспечивать безопасность на предприятии в виде ступенчатых систем контроля допуска и сотрудничать с ведущими компаниями в этой отрасли, чтобы получить возможность использовать их алгоритмы и ПО, направленное на обеспечение защиты информации.

Дробышевский В.М. Почти все производители, работающие в сфере IoT и компонентов для его создания, отмечают повышенные требования к безопасности таких систем, так как их внедрение сильно связано с «реальным» миром — устройства могут влиять на окружающую среду и человека. Таким образом, защита этих систем должна быть реализована одинаково качественно как в «физическом», так и в «электронном» аспекте.

Мы живем в эпоху, когда расстояние от самых безумных фантазий до совершенно реальной действительности сокращается с невероятной быстротой.
Максим Горький

Работа в этом направлении идет сразу по нескольким «фронтам». На уровне беспроводных сенсоров, устройств и шлюзов — их максимальная защита от влияния извне, дополнительная защита от уязвимостей средствами специализированных ОС и приложений. На сетевом уровне — обеспечение поддержки протоколов безопасной передачи данных в «облако», например MQTT. На уровне «облака» — это защита и сертификация ЦОДов, шифрование хранимых данных.

Уже идут работы по выработке стандартов для IoT, например, ассоциация IEEE в 2014 г. выступила с IoT-инициативой для координации действий по сертификации в этой области, результатом которой стало появление стандарта для архитектуры IoT — IEEE P2413, над которым продолжается активная работа.

Кузин А.С. Задача по обеспечению кибербезопасности была и остается камнем преткновения при внедрении любой интегрированной с Internet системы. Для обеспечения безопасности данных необходим контроль за целостностью и качеством передаваемых данных на всех этапах их прохождения: точки формирования и отправки, канала передачи, а также точки приема, обработки и хранения.

Сделать систему безопасной возможно только общими усилиями как производителей периферийных решений, разработчиками программного обеспечения, а также специалистов внедрения и обслуживания.

Крейцер Н.А. Если говорить о применении IoT устройств в интересах промышленных предприятий, то тут, как правило, возможно создание закрытой сети или Intranet сети, в которых будут применяться все те же технологии из мира IoT. Это может быть достигнуто ограничением зоны действия Wi-Fi сети, покрывающей территорию предприятия. Если территориальный охват нельзя ограничить, то можно применить технологию специфичных для сети сертификатов для авторизации доступа в Wi-Fi сеть или технологию выделенного APN плюс VPN туннеля при использовании сотовой связи в качестве канала передачи данных. Также на предприятиях, как правило, применяется межсетевое экранирование. В сово-

купности эти меры обеспечивают кибербезопасность на должном уровне.

Ситуация становится более тяжелой, если рассматривать угрозы, воздействующие на предприятие, чьим профилем деятельности является предоставление открытого сервиса с задействованием данных от IoT устройств. Оператор вынужден принимать информацию от произвольного числа и видов устройств. Ряд существующих связных технологий из сектора IoT позволяет и в этих случаях обеспечивать закрытые сети на уровне радиоканала и технологии поддержки сети, но эти решения не покрывают все возможные способы коммуникаций между IoT устройством и серверной инфраструктурой. Поэтому операторское ПО должно использовать все доступные в коммуникационной отрасли способы защиты от атак.

Если же проект предполагает хоть и открытый доступ, но от довольно ограниченного числа видов устройств, то можно адаптировать реализацию серверной платформы, поскольку циркулирующая в ней информация хорошо прогнозируема и предсказуема. В такой ситуации можно легко выявить поведение, отличающееся от типового для конкретного бизнеса, и пресечь злоупотребление. Например, если известно, что счетчик воды сообщает информацию два раза в день в конкретные промежутки времени, то универсальные системы обнаружения вторжений не потребуются.

Другой опасностью является возможность попадания информации от IoT устройства в «чужие руки». А некоторыми устройствами даже можно управлять! Для устранения этих рисков в ходе обмена информацией следует применять средства проверки подлинности сервера, а также применять цифровые подписи и шифрование. Последнее требует определенного лицензирования, поэтому нужно взвешивать соотношение между реальной степенью угрозы и способами их устранения.

Беспалов А.А. Сегодня данные стремительно «мигрируют» в облачную среду, управление все большим числом промышленных установок имеет доступ через сеть Internet, поэтому вопрос ИТ-безопасности стоит достаточно остро. Обеспечение безопасности данных промышленных систем требует тщательного подхода. Чтобы его выработать, нужно проанализировать статистику инцидентов, специфические угрозы и наиболее уязвимые точки промышленных систем. Для обеспечения адекватной защиты промышленных предприятий должны быть предприняты усилия по повышению уровня защищенности продуктов и оснащения их функциями безопасности. Это пока открытый вопрос, ответ на который сегодня ищут многие компании.

Швецов Д. П. Прежде всего, IoT позволяет широко использовать технологии OPC UA (OLE for Process Control Unified Architecture) с помощью встроенной, отлаженной и эффективной системы безопасных стандартизованных коммуникаций между первичными преобразователями, промышленными сетями и системами управления предприятий. Для решения этой проблемы можно использовать технологию туннелинга TCP, осуществляющего передачу данных через стандартный порт брандмауэра. Этот порт обычно используется для передачи данных по http-протоколу (протоколу передачи гипертекста) и поэтому он, как правило, открыт. Но для осуществления туннелинга и передачи данных требуется установка специального ПО, входящего в ОС Windows, — COM Internet Services и IIS Web-сервер (Internet Information Server). Для этих целей также очень широко используются Web-сервисы W3C (World Wide Web Consortium), разработанные для поддержки сетевых взаимодействий уровня устройство-устройство. Преимущества применения технологий IoT ради повышения эффективности и безопасности — использование стандартов ISA-99 (безопасность промышленных систем автоматизации и управления) и ISASecure EDSA — два важнейших элемента обеспечения безопасности систем. Стандарт EDSA фокусируется на безопасности встраиваемых систем и регламентирует характеристики этих устройств, а также процессы по их разработке. Встраиваемое устройство, отвечающее требованиям спецификаций ISASecure EDSA, получает соответствующую сертификацию. Сертификация ISASecure EDSA обеспечивает три уровня признания устройства, отражающих степень его безопасности.

Ведущий. *Какие Вы видите перспективные области применения решений уровня IoT для промышленности, а какие области должны быть закрыты для таких приложений?*

Беспалов А. А. Концепция IoT активно распространяется в самых разных промышленных отраслях, включая технологии интеллектуального здания и умного дома, интеллектуальные системы мониторинга окружающей среды, умные транспортные и медицинские системы. Однако есть отрасли, которым «умные технологии» необходимы в первую очередь — это авиационная и аэрокосмическая промышленности. IoT позволит устранить проблему контроля происхождения детали, появятся беспроводные системы диагностики и сбора данных для анализа и принятия решений с помощью современных технологий. Решения уровня IoT не менее актуальны для автомобильной промышленности, где могут быть реализованы системы мониторинга и механизмы взаимодействия между транспортными средствами. В телекоммуникационной отрасли использование «умных» технологий открывает возможности для объединения различных телекоммуникационных технологий с целью предоставления сервисов нового типа.

Отдельно отметим развитие «интеллектуальных» электросетей или SmartGrid. Компания Eaton понимает это, как разумное взаимодействие компонентов, которое приводит к экономии электроэнергии при ее надежном и безопасном распределении. В номенклатуре компании такие компоненты, как интеллектуальные системы среднего напряжения, решения по автоматизации, мониторинг, диспетчерское управление и сбор данных, организованные в виде самовосстанавливающейся сети с возможностью локализации поврежденного участка системы полностью в автоматическом режиме. «Интеллектуальная» сеть самостоятельно отслеживает режимы работы всех элементов системы и принимает оптимальные решения по распределению электрической энергии, предупреждению аварийных ситуаций, регулированию потоков мощности и, как следствие, повышению надежности, готовности и эффективности.

Хайнрикс Б. Прежде всего, нужно понимать, что IoT не обязывает подключать производственные линии к Internet и предоставлять свои данные в общий доступ. Технологии IoT или Industry 4.0 позволяют снизить затраты на модернизацию или внедрение системы промышленной автоматизации.

Хадонова С.В. Это технологии ближайшего будущего, консолидирующие M2 M и IoT, которые начнут массово применяться в ближайшее время. Ведь M2 M решения СпейсТим актуальны и востребованы, в том числе в концепциях «Интеллектуальных умных городов» и «Безопасных городов».

Швецов Д. П. Беспроводные сети датчиков, входящие в IoT, позволяют расширить границы систем мониторинга и управления за физические пределы, доступные с проводными соединениями. Следующий этап оптимизации процессов будет достигнут путем использования в настоящее время пока еще не задействованных данных из распределенных и локальных сетей датчиков, а также расширенных аналитических функций. Эти улучшения можно объединить в единое понятие «Промышленный Internet», которое влечет за собой более высокие требования к гарантированным скоростям обмена как в проводных сетях с детерминированным Ethernet, так и в беспроводных сетях с 802.15.4 e TSCH. 2.

Интеграция и трансформация огромных объемов информации (больших данных), повышение интеллектуальных способностей «умных машин», которые достигаются путем встроенного ПО, — вот, что способно серьезно повысить уровень «интеллектуальности» современных предприятий в соответствии с концепцией Industry 4.0.

А вот доступ к персональным данным и коммерческой информации не должен будет иметь «выход» на IoT. В лицензионных соглашениях должны быть включены требования к соблюдению положений соответствующего национального законодательства использования информации.

Дробышевский В.М. Перспективные области трудно перечислить — транспорт, медицина, торговля, сельское хозяйство, ЖКХ, энергетика, безопасность, финансы, производство — в общем, почти все. Закрытыми могут быть скорее не отрасли, а отдельные сценарии использования, например, в районах без устойчивой связи либо на объектах, где потеря связи может вызвать критические последствия. Конечно, закрытыми останутся традиционно высококритичные отрасли — это военная отрасль, космонавтика, авиация, атомная энергетика — там к внедрению подобных решений нужно подходить очень серьезно.

Попов С.И. Концепция промышленного IoT обладает потенциалом оказать существенное влияние практически на все отрасли промышленности и по всему миру. Подключенный к сети завод или предприятие дает возможность повысить качество принимаемых решений, безопасность и эффективность производства за счет улучшения взаимодействия в рамках предприятия. Использование мобильных устройств позволит существенно ускорить процесс принятия решений, предоставляя всю необходимую информацию в нужное время. “Облака” обеспечивают новым технологиям платформу для взаимодействия и помогают промышленному IoT обрести “путевку в жизнь”. Постепенно применение мобильных устройств, облачных вычислений, анализа данных окажет свое влияние на направление развития промышленной автоматизации и приведет к появлению подключенных и «умных» предприятий.

Ведущий. *Таким образом, мы выяснили, что IoT в области промышленной автоматизации — это не только и не столько встраиваемые электронные устройства, способные обмениваться данными через Internet, к которым мы привыкли в обыденной жизни. В промышленности это новая эра, называемая Industry 4.0, предполагающая обмен данными между всеми участниками, которые задействованы в производственной цепочке: людьми, роботами, исполнительными механизмами, датчиками, производственными системами, продуктами, выпускаемыми производственными линиями и т. д. Концепция IoT является базой для создания «интеллектуального» предприятия, способного выполнять операции сбора и передачи данных в центральное хранилище, отдельные операции диагностики, информировать операторов о состоянии ТП и др. И на сегодняшний день уже имеются примеры успешного использования этой концепции в реальных промышленных приложениях, в области автоматизации зданий и на транспорте. Области применения промышленного Internet в ближайшем будущем будут расширяться, а функционал Internet-решений — совершенствоваться.*

Контактный телефон (495) 334-91-30.