УДК 004.031.4

О некоторых вопросах применения технологии Интернета вещей в нефтегазовой промышленности

Фаталиев Т.Х., зав. отделом,
Мехтиев Ш.А., зав. отделом
Институт информационных технологий НАНА, г. Баку, Азербайджан

Быстрое развитие информационно-коммуникационных технологий способствовало внедрению современных датчиков, а также Интернета вещей (Internet of Things- IoT) различного назначения, оборудования для сбора данных, беспроводных сетей, коммуникационных устройств и решений для удаленных вычислений. Эта эволюция – основа структуры современных Киберфизических систем (КФС) (Cyber Physical System-CPS). КФС – это физическая и инженерная система, состоящая из многочисленных компонентов, в том числе внедренных IoT различного назначения, управляемых компьютерными алгоритмами, тесно интегрированная с Интернетом и пользователями [1]. К ним относятся такие системы, как Smart Cities, Smart Grids, Smart Factory, Smart Buildings, Smart Houses и Smart Cars, где каждый объект подключен ко всем другим объектам. Они призваны обеспечить адаптивное, гибкое и экономически эффективное функционирование. Можно предположить, что нефтегазовая промышленность в какой-то степени является фабрикой по обработке информации, что вписывается в информационно-технологическую концепцию КФС. Это большое количество устройств со встроенными сенсорами, процессорами и средствами хранения данных; интеграция, позволяющая достигнуть наибольшего эффекта путем объединения отдельных компонентов в большую систему; исключение человеческого фактора при принятии решений (human out of loop) либо дополнение способностей человека (human in the loop).

IoT по определению МСЭ-Т – это "глобальная инфраструктура для информационного общества, которая обеспечивает возможность предоставления более сложных услуг путем соединения друг с другом (физических и виртуальных) вещей на основе существующих и развивающихся функционально совместимых информационно-коммуникационных технологий" [2] и, как концепция, определяет развитие промышленности на ближайшие годы. Обязательным условием функционирования любого производства, в том числе нефтегазового комплекса в рамках этой концепции является прямое информационное взаимодействие оборудованных всевозможными сенсорами различных типов объектов, наличие интеллектуальных устройств, которые смогут передавать данные, принимать решения и взаимодействовать друг с другом.

Архитектура IoT может быть представлена четырьмя системами [3]:

1. Вещи: они определяются как уникально идентифицируемые узлы, прежде всего сенсоры (датчики), которые общаются без взаимодействия человека с использованием стандартных протоколов.

2. Шлюзы: это подключение к Интернету, безопасность и управляемость.

3. Сетевая инфраструктура, состоящая из маршрутизаторов, концентраторов, шлюзов, повторителей и других устройств, которые управляют потоком данных.

4. Облачная инфраструктура: содержит кластеры виртуализированных серверов и хранилища, которые объединены в сеть.

С момента появления и развития микропроцессоров и сетевых устройств активно изучалась возможность применения микроконтроллеров, дополненных сенсорами и механизмами, для обеспечения большей надежности, эффективности и безопасности производственных процессов в нефтегазовой промышленности (геологические изыскания, бурение, добыча, переработка, транспортировка и т.п.), так как здесь высокий уровень финансовых, экологических и гуманитарных рисков.

Так в [4] указано, что процессы обработки информационных потоков и управления в нефтегазодобывающих предприятиях происходят на трех уровнях. На нижнем уровне при помощи локально-групповых устройств осуществляется мониторинг, сбор данных с сенсоров и первичная обработка информации с целью выработки управляющих воздействий на объекты нефтегазодобычи в режиме реального времени. Замена консервативных и в большей степени ручных средств управления и мониторинга и обеспечение процессов добычи, транспортировки и переработки в нефтегазовой отрасли новыми, удобными для установки сенсорами позволяет вести непрерывный автоматический контроль за технологическими процессами, регистрировать и накапливать данные о параметрах, производить удаленную настройку. Тем самым можно повысить надежность, безопасность, энергоэффективность, влиять на экологические показатели, такие как выбросы газа, утечки и разливы первичного сырья. На следующем уровне вырабатываются решения об оптимизации процессов, определении периодичности ремонтных мероприятий для сокращения простоев и оптимизации интервалов техобслуживания узлов и агрегатов, обеспечения эффективной работы и т.д. Незапланированные простои из-за поломок оборудования, которые приводят к потере времени и финансов, можно сократить благодаря внедрению интеллектуальных систем технического обслуживания, в том числе и э-техобслуживания. Третий уровень – это уровень компании (корпорации), на котором реализуется аналитика (обработка больших данных), по результатам которой осуществляется координация действий входящих в состав компании (корпорации) предприятий и структур для

достижения общей эффективности, принимаются меры по повышению безопасности и уменьшению рисков.

Данное представление информационных потоков согласуется с архитектурно-технологической моделью IoT, в которой:

1. Сенсоры измеряют какие-либо физические параметры;
2. Микроконтроллеры обеспечивают интеллектуальность;
3. Имеется возможность коммуникации по Интернету;
4. Возможно использование облачных сервисов.

Необходимо отметить, что в облачных сервисах IoT происходит перераспределение нагрузки на туманные (fog) и мобильные (mobile) вычисления. Например, в концепции «умное месторождение» (smart field) от компании Schneider Electric [5] на основе данных от проводных и беспроводных сенсоров в режиме реального времени моделируются процессы внутри пласта и осуществляется управление добывающими нефть насосами различных модификаций. Данные сохраняются в памяти интеллектуальных контроллеров и периодически передаются в диспетчерский пункт, где обрабатываются специальными программами. За счет внедрения интеллектуальной системы сокращаются время простоев оборудования, затраты на электричество, пар, воду, а также оптимизируется весь процесс добычи.

В международной практике объекты нефтегазовой промышленности относятся к критическим инфраструктурам и, безусловно, широкое распространение IoT здесь будет зависеть от гарантий безопасности в целом как на уровне системы, так и на уровне IoT (сенсоры, съем данных, обработка, хранение и передача информации). Известные случаи аварий на объектах нефтегазовой промышленности показывают насколько уязвима структура IoT к кибератакам [6].

В рекомендации МСЭ-Т безопасность IoT предлагается решать, исходя из его трехуровневой архитектурно-технологической модели, так как потенциальные угрозы могут проявиться на каждом уровне [2].

Анализ теоретических и реальных угроз и атак на критические инфраструктуры показывает, что на каждом уровне необходимы решения по авторизации, аутентификации, защиты конфиденциальности и целостности данных [7].

Виды угроз в IoT, рассмотренные в многочисленных источниках, также могут быть реализованы злоумышленниками при реализации IoT в нефтегазовой промышленности. Например, на уровне устройств могут быть считаны значения с сенсоров, которые важны для функционирования всей системы. Открытые или не полностью устраненные проблемы безопасности в IoT можно в целом классифицировать следующим образом:

- Стандартизация для гетерогенных устройств;
- Масштабируемость;
- Конфиденциальность;

- Уязвимость программного и аппаратного обеспечения;
- Физическая безопасность устройств;
- Энергопотребление и эффективность.

Выводы. Существует множество возможных направлений дальнейших исследований в области применения и обеспечения безопасности IoT, в первую очередь из-за его постоянно растущего и всеобъемлющего характера. Согласно прогнозу «Gartner» к 2020 году к Интернету подключится 20 миллиардов объектов. Любая атака на одном подключенном узле может разрушить инфраструктуру и привести к росту связанных рисков. Чтобы гарантировать успешную реализацию и практическую полезность IoT, необходимы решения по внедрению стандартов, обеспечению качества обслуживания, конфиденциальности и надежности, управлению большими объемами данных и обеспечению эффективности.

Данная работа выполнена при финансовой поддержке Фонда Науки Государственной нефтяной компании Азербайджанской Республики – **Грант № 01 LR – НАНА, SOCAR ФН 2017**

Список литературы

1. Фаталиев Т.Х., Мехтиев Ш.А., Некоторые вопросы безопасности КФС, Актуальные проблемы информационной безопасности, III Республиканский научно-практический семинар, Баку, 8 декабря 2017 г.

2. Recommendation ITU-T, Y.2060: Overview of the Internet of things, 06/2012.[Online]. Available: https://www.itu.int/rec/T-REC-Y.2060-201206-I

3. Banafa A, Securing the Internet of Things (IoT). [Online]. Available: https://www.researchgate.net/publication/281525537_Securing_the_Internet_of_Things_IoT

4. Алиев А.И., Мехтиев Ш.А., Алгулиев Р.М., Об иерархически-распределенной системе управления и обработки информации в НГДУ / Проектирование автоматизированных систем контроля и управления сложными объектами, Харьков, 1986, с. 54-55.

5. Schneider Electric. Smart field. [Online]. Available: https://www.schneider-electric.com/en/search/smart+field

6. Critical Infrastructure. [Online]. Available: https://www.pandasecurity.com/rfiles/resources/forms/whitepapers/1611-WP-CriticalInfrastructure-EN.pdf

7. Oracevic A., Dilek S., Ozdemir S. Security in Internet of Things: A Survey, Conference ISNCC, 2017