УДК 004 **Информационные технологии**

Бабинская Екатерина Андреевна, *студент,*
Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики», г. Санкт-Петербург
E-mail: bonya93@mail.ru
Коклюхин Дмитрий Сергеевич, *студент,*
Федеральное государственное бюджетное образовательное учреждение высшего образования "Санкт-Петербургский горный университет"
г. Санкт-Петербург
E-mail: koklyuhin-dmitrii@mail.ru

ИССЛЕДОВАНИЕ СУЩЕСТВУЮЩИХ СПОСОБ ЗАЩИТЫ ДАННЫХ И ОТРАСЛЕВЫХ СТАНДАРТОВ ПРИ ИСПОЛЬЗОВАНИИ ОБЛАЧНОЙ ИНФРАСТРУКТУРЫ И УСТРОЙСТВ IOT (INTERNET OF THINGS)

Аннотация: В данной статье рассматриваются основные угрозы и способы защиты данных при их передаче от устройств IoT в облачную инфраструктуру. Рассмотрены сферы использования интернета вещей. На основании проведенного исследования выявлены механизмы защиты данных в облачной инфраструктуре.

Ключевые слова: Internet of things, облачная инфраструктура, защита данных.

Annotation: This article discusses the main threats and ways to protect data when it is transferred from IoT devices to the cloud infrastructure. The areas of use of the Internet of things are considered. Based on the study, data protection mechanisms in the cloud infrastructure are identified.

Keywords: Internet of things, cloud infrastructure, data protection.

Анализ сценариев использования устройств IoT (Internet of things) и существующих отраслевых стандартов

20 августа 2019 года Microsoft представила исследование IoT Signals, посвященное динамике внедрения Интернета вещей в компаниях из разных индустрий и стран мира [2]. Согласно его результатам, 85% организаций уже имеют как минимум один бизнес-проект в этой сфере, а к 2021 году эта цифра вырастет до 94%. При этом 88% руководителей таких проектов осознают преимущества технологии для успеха компании и ожидают 30% окупаемость инвестиций в двухлетней перспективе [1].

Среди основных целей внедрения респонденты выделили необходимость оптимизации рабочих процессов (56%), повышения продуктивности сотрудников (47%), а также общую безопасность компании (44%).

При этом несмотря на то, что 97% опрошенных беспокоит безопасность систем Интернета вещей, этот фактор не сдерживает скорость и объем внедрений. В качестве наиболее перспективных превентивных мер они выделяют: создание надежной системы аутентификации пользователей (43%), отслеживание и управление устройствами Интернета вещей (38%) и защиту их конечных точек (38%).

Сферы использования интернета вещей

В настоящее время интернет вещей используется во многих сферах, например в технологии Умный дом, в агрокультуре, в промышленности, в ритейле, в здравоохранении, в умных машинах, в носимых устройствах, технология умный город и в энергетике.

Использование IoT в нефтегазовой отрасли

Нефтегазовые предприятия уже используют мощь инструментов Big Data, а за счет использования Интернета вещей также начали повышать эффективность отрасли. С увеличением случаев использования устройств и

датчиков, Интернет вещей позволил улучшить эффективность работы агрегатов, принятие решений и управление в режиме реального времени отрасли.

Основные направления использования IoT в нефтегазовой отрасли: дистанционный мониторинг, повышение уровня безопасности и снижение рисков, управление активами в реальном времени, проверка оборудования и т.д.. Таким образом, нефтяная и газовая промышленности сокращают влияние человеческого фактора.

Существующие и разрабатываемые стандарты IoT

В настоящее время наиболее рас пространены следующие стандарты интернета вещей: NB-IoT, LoRaWAN, Signifox, ZigBee.

Стандартизированные на национальном уровне протоколы интернета вещей (IoT)NB-Fi, LoRaWAN RU и OpenUNB будут включены в проект международного стандарта совместимости систем IoT/IIoT. Такое решение было принято в ноябре 2019 года на заседании подкомитета Международной организации по стандартизации (International Organization for Standardization, ISO) и Международной электротехнической комиссии (International Electrotechnical Commission, IEC) в области интернета вещей, прошедшем в Санкт-Петербурге.

С мая 2019 года ведется разработка международного стандарта по безопасности интернета вещей – ISO/IEC 30149 Internet of Things (IoT) – Trustworthiness frameworks. Отечественный 194-ый технический комитет Росстандарта «Кибер-физические системы» получил статус соредактора [3].

Защита устройств IoT

ZigBee использует три типа ключей для управления безопасностью: главный ключ, сетевой ключ и ключ канала связи, криптографическая защита данных реализована на основе 128-битного алгоритма AES.

LoRaWAN, при активации устройства в сети, создает сессионные ключи, использующие алгоритм шифрования AES-CMAC.

Платформа «Стриж» использует следующую систему защиты данных IoTустройств:

У каждого устройства есть уникальный ключ шифрования, который хранится на самом устройстве и дублируется на сервере «СТРИЖ.Cloud»;

От базовых станций на сервер информация передаётся с помощью VPN-соединений.

Все данные зашифрованы алгоритмом XTEA-256, ГОСТ Р34.12-2015.

28 января 2020 года стало известно, что Правительство Великобритании обнародовало законопроект, направленный на защиту IoT-устройств.

Законопроект содержит три основных требования для производителей «умных» устройств. В частности, все пароли пользовательских IoT-устройств должны быть уникальными и без возможности сбросить их до «универсальных» заводских настроек; производители должны предоставить общедоступную точку контакта, чтобы каждый мог сообщить об уязвимости и рассчитывать на «своевременное принятие мер»; производители обязаны четко указать минимальный период времени, в течение которого устройства будут получать обновления безопасности в местах продаж.

Таким образом, в настоящее время стандарты интернета вещей, в большинстве случаев, используют систему защиты данных, построенную на шифровании передаваемых данных. Также некоторые стандарты используют механизмы доверительных отношений для аутентификации устройств.

Концепция построения облачной инфраструктуры

Для возможности масштабирования и эффективного управления ресурсами целесообразно использовать облачную инфраструктуру. Для облачных систем отличительной чертой является неравномерность запросов ресурсов (например, поступление сигналов с датчиков систем мониторинга в реальном времени на пульт управления для дальнейшего анализа). Основой для построения облачных систем является виртуализация.

Виртуализация — метод системы абстрагировать вычислительные ресурсы и показывать абоненту только нужные сервисы. Виртуальная машина консолидирует физические серверы и ПО. На виртуальном сервера

одновременно могут работать программы пользователей, причем под управлением разных ОС.

Облако состоит из разных уровней на которых работают разные приложения (рис.1). Самый нижний уровень IaaS — ответственен за инфраструктуру. Он предоставляет услуги по аренде вычислительных мощностей и систем хранение информации. Клиент может использовать любые операционные системы и приложения. PaaS — уровень платформы, который содержит и инфраструктуру и операционные системы и иногда с приложениями. SaaS — уровень приложений, который разрешает реализовывать приложения из облака для работы на вашем компьютере.

Рисунок 1 – Уровни облака

Таким образом, в зависимости от потребностей заказчика, устройства IoT взаимодействуют с облачной инфраструктурой на уровне платформы или приложений.

Механизмы защиты данных в облачной инфраструктуре

Механизм защиты - совокупность средств защиты, функционирующих совместно для выполнения определенной задачи по защите данных.

Механизм защиты для обычных устройств, таких как ПК или смартфоны, взаимодействующих с облачными сервисами по своей сути идентичен механизмам защиты данных, передаваемых с устройств IoT, и состоит из следующих компонентов

1. Защита устройств;

2. Защита каналов передачи данных;
3. Защита элементов облачной системы.

Основное отличие заключается в протоколах, используемых устройствами, так как для IoT устройств, в большинстве случаев, критичным является вопрос энергоэффективности.

Защита устройств осуществляется следующими способами и технологиями: защита операционной системы устройства (своевременная установка обновлений, установка антивирусной программы, включение межсетевого экрана), баз данных и других сервисов.

Защита каналов передачи реализуется на канальном и сетевом уровнях модели OSI. Обеспечение конфиденциальности на канальном уровне обеспечивают собственные устройства шифрования каналов связи, на сетевом уровне конфиденциальность обеспечивается с помощью стека протоколов IPSec.

Защита облака представляет собой взаимосвязанный комплекс защиты элементов облачной системы, таких как хостовая операционная система (которая также является устройством или группой устройств), гипервизор, хранилище, сервисов, облачных приложений и т.д.

В облачной платформе Microsoft Azure для интернета вещей предлагается следующая реализация защиты передаваемых данных от устройств IoT в облачные сервисы (см. рис 2.):

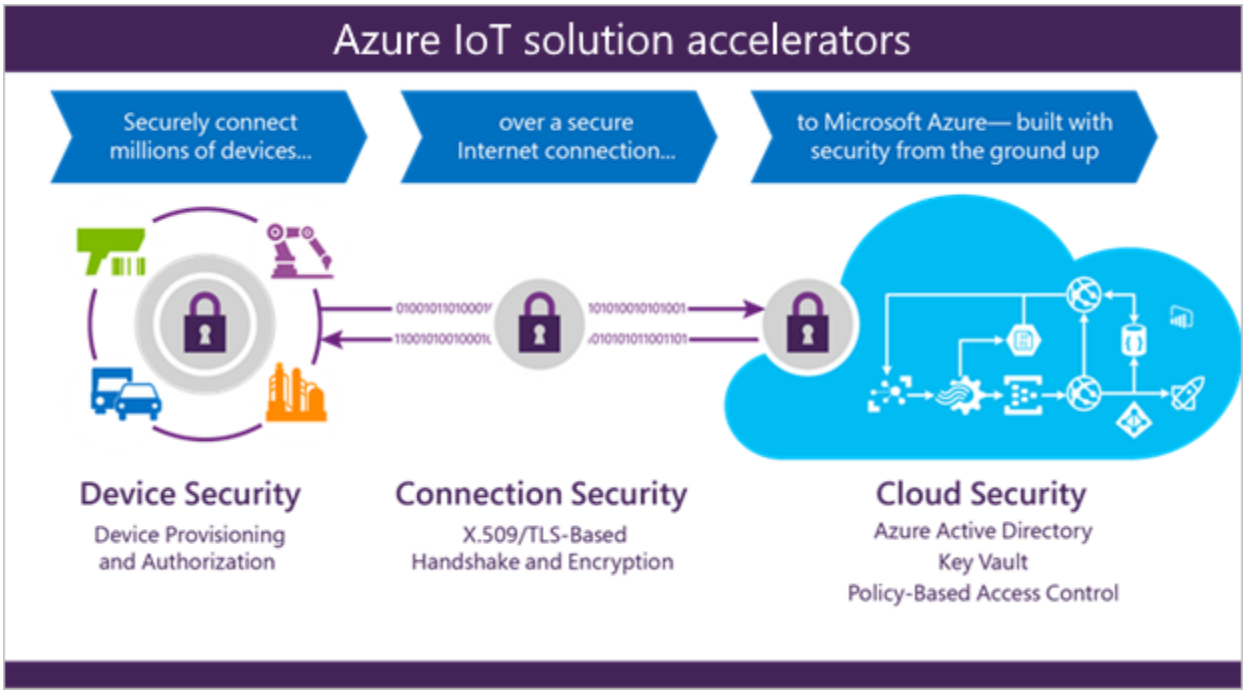

Рисунок 2. - Защита данных в Azure IoT

Защита устройств – инициализация и авторизация устройств.

Безопасность соединения – установление связи и шифрование на основе протоколов X.509 и TLS.

Защита облака:

- универсальная платформа для управления удостоверениями и обеспечения их безопасности (Azure Active Directory);
- защита криптографических ключей и других секретных данных, которые используются облачными приложениями и службами (Key Vault);
- политики управлением доступом.

Рынок интеллектуальных счетчиков 2019 года

Интеллектуальный счетчик считается одним из самых зрелых и наиболее широко принятых приложений технологии IoT сегодня. Глобальное проникновение интеллектуальных счетчиков (электричество, вода и газ) превысило 14% в 2019 году, т. е. 14% всех счетчиков теперь являются интеллектуальными счетчиками. Интеллектуальный счетчик определяется как интеллектуальная и сетевая измерительная система для ресурсов и энергии, таких как вода, газ или электричество, которая использует компьютерное

измерение, определение и контроль потребления и поставки для жилых, коммерческих и промышленных зданий.)

Расчетная установленная база интеллектуальных счетчиков (электроэнергии, газа и воды), как ожидается, превысит отметку в 1 миллиард в течение ближайших 2 лет. Чуть менее 132 миллионов интеллектуальных счетчиков (электричество, газ и вода) были отправлены по всему миру в 2018 году. Ожидается, что это число будет расти на 7% в год и превысит 200 миллионов к 2024 году.

Проведенный анализ также свидетельствует о высокой степени фрагментации рынка интеллектуальных счетчиков, обусловленной сочетанием различных региональных или страновых институциональных механизмов поддержки и регулирования, а также различными потребностями коммунальных служб в различных районах мира.

Три основных региона (Северная Америка, Европа, APAC) имеют совершенно разные характеристики и динамику рынка – здесь представлен обзор высокого уровня, включающий информацию из других регионов мира.

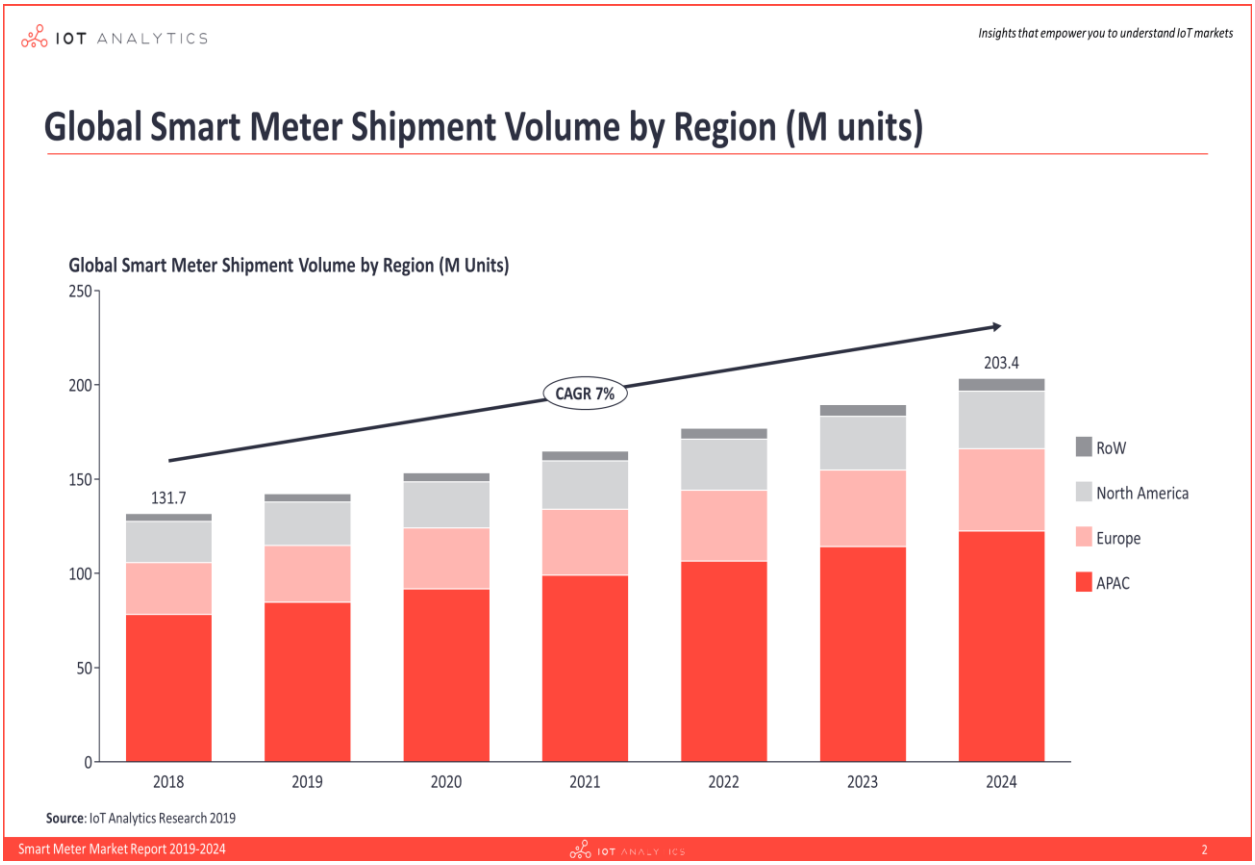

Рисунок 3 – Объемы внедрения интеллектуальных счетчиков в регионах

Северная Америка: достаточно зрелый рынок со стабильным ростом

Рынок интеллектуальных счетчиков в Северной Америке достаточно зрелый, с показателем проникновения, оцениваемым примерно в 30-40% от общего числа потребителей коммунальных услуг электроэнергии, газа и воды. И США, и Канада были ранними последователями интеллектуальных счетчиков. Сегодня многие коммунальные операторы уровня 1 в регионе развернули крупномасштабное решение для интеллектуальных счетчиков или в настоящее время находятся в процессе этого.

Европа: сильно фрагментированный рынок приближается к зрелости

В Европе рынок интеллектуальных счетчиков имеет такой же уровень принятия, как и в Северной Америке, по оценкам, около 30-40% всех потребителей коммунальных услуг. Это утверждение сравнимо с Северной Америкой, однако оно гораздо более неоднородно, с большими различиями между странами с точки зрения регулирования, диспаритета местных коммунальных рынков, а также готовности принять решения по

интеллектуальным счетчикам. В течение последнего десятилетия внедрение интеллектуальных счетчиков в регионе было обусловлено внедрением целевого показателя 80% проникновения на рынок электроэнергии к 2020 году, установленного ЕС в соответствии с планом Третьего энергопакета 2009 года. Однако прогресс внедрения не происходит так быстро, как планировалось, и в недавнем обзоре прогресса ЕС заявил, что почти 72% европейских домохозяйств и коммерческих зданий будут иметь интеллектуальные счетчики электроэнергии к 2020 году, что означает, что цель проникновения на рынок на 80% не будет достигнута вовремя.

- Ведущие страны : Италия, Швеция, Финляндия и Нидерланды уже достигли целевого показателя в 80% и ожидают 95%+ проникновение к 2020 году.
- По графику: Франция, Испания, Греция и Дания развертывание продолжается в стабильном темпе, и они, как ожидается, достигнут целевого показателя 80% к 2020 году
- Отставание от графика: прогресс в других странах был медленнее, и 80% целевой показатель не будет достигнут к 2020 году. Наиболее заметным примером является Великобритания, где различные технические и потребительские проблемы задержали развертывание и недавно убедили правительство продлить крайний срок до 2024 года.
- Не следуя плану ЕС: несколько стран, включая Германию, Бельгию и Португалию, решили не следовать плану ЕС по интеллектуальным счетчикам из-за отрицательного анализа затрат и выгод и вместо этого планируют или осуществляют выборочные развертывания.

С точки зрения счетчиков газа и воды, уровень принятия остается ниже, чем электричество, но растет быстрее. Только несколько стран в ЕС начали или планируют крупномасштабное развертывание (например, Италия, Франция, Великобритания, Нидерланды). Согласно оценкам, 40% домохозяйств и коммерческих зданий в ЕС будут иметь интеллектуальный газовый счетчик к 2020 году.

Азиатско-Тихоокеанский регион: лидирующий регион по общему объему отгрузок

Азиатско-Тихоокеанский регион на сегодняшний день представляет собой крупнейший регион на глобальном рынке интеллектуальных счетчиков, с примерно 78,1 миллиона интеллектуальных счетчиков, отгруженных в регионе в 2018 году. Это число соответствует почти 60% мирового объема отгрузок. Общее проникновение интеллектуальных счетчиков в регионе остается ниже, чем в Северной Америке и Европе, однако менее 20% потребителей коммунальных услуг оснащены интеллектуальными счетчиками. Как и в Европе, между странами существуют большие различия. В целом, счетчики электроэнергии были в основном сосредоточены в большинстве ведущих стран, в то время как счетчики газа и воды только недавно стали свидетелями увеличения тяги, хотя темпы внедрения растут медленно из-за общего отсутствия капитала для этих проектов во многих странах.

Остальной мир: рынок ранней стадии с низкой институциональной поддержкой

В остальном мире рынок интеллектуальных счетчиков в значительной степени все еще находится на ранней стадии. Большинство стран Африки, Латинской Америки или Ближнего Востока, которые либо все еще находятся в стадии пилотного проекта, либо еще не начали внедрять интеллектуальные счетчики. На сегодняшний день уровень проникновения на рынок в этих регионах составляет менее 5% от общего числа потребителей коммунальных услуг, причем наиболее распространенными являются счетчики электроэнергии, за которыми следует вода, а затем газ.

В целом, главным препятствием для внедрения интеллектуальных счетчиков в этих регионах является отсутствие финансирования и государственных инициатив, которые сыграли важную роль в развитии интеллектуального учета в других регионах с более широким проникновением. Кроме того, во многих случаях существует также проблема неадекватной инфраструктуры, основанной на устаревших технологиях и зачастую охватывающей только городские районы,

что делает внедрение интеллектуальных счетчиков все еще непосильным для многих коммунальных служб.

Библиографический список:

1. Интернет вещей, IoT, M2M, мировой рынок. [Электронный ресурс] – Режим доступа: http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9,_IoT,_M2M_(%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%BE%D0%B9_%D1%80%D1%8B%D0%BD%D0%BE%D0%BA).

2. Как Интернет вещей минимизирует убытки нефтяников/ [Электронный ресурс] – Режим доступа: https://iot.ru/promyshlennost/kak-internet-veshchey-minimiziruet-ubytki-neftyanikov.

3. Лучшие 10 IoT Стартапов 2019 [Электронный ресурс] – Режим доступа: https://iot-analytics.com/the-top-10-iot-startups-2019/.