cigré
ПОДКОМИТЕТ РНК СИГРЭ D2
Информационные системы и телекоммуникации

cigré
Российский Национальный Комитет

МЕЖДУНАРОДНЫЙ КОЛЛОКВИУМ-2017
SC D2 CIGRE
МОСКВА

20–22 СЕНТЯБРЯ 2017 ГОДА

ВПЕРВЫЕ В РОССИИ
СОСТОИТСЯ КОЛЛОКВИУМ ИССЛЕДОВАТЕЛЬСКОГО КОМИТЕТА (SC) D2 CIGRE

ПРИГЛАШАЕМ ПРИНЯТЬ УЧАСТИЕ!

- **ГЕНЕРАЛЬНЫЙ ПАРТНЕР КОЛЛОКВИУМА** ПАО «ФСК ЕЭС»
- **ПАРТНЕРЫ КОЛЛОКВИУМА** АО «НТЦ ФСК ЕЭС», АО «СО ЕЭС», подкомитеты РНК СИГРЭ А3 «Высоковольтное оборудование» и В3 «Подстанции»
- **В МЕРОПРИЯТИИ УЧАСТВУЕТ** 43 спикера из 23 стран мира
- **СРЕДИ УЧАСТНИКОВ** представители крупнейших мировых электроэнергетических компаний и ведущих производителей оборудования из России, Японии, США, Германии, Франции, Испании, Италии, Нидерландов, Швеции, Финляндии, Словении, Сербии, Южной Кореи, Индии, Бразилии, ЮАР, Китая и других

/ ЦЕЛЬ КОЛЛОКВИУМА
- Обеспечение международного обмена информацией между участниками мирового энергорынка

/ ТЕМЫ КОЛЛОКВИУМА
- Программные платформы управления распределенными энергоресурсами
- Устойчивость к киберугрозам информационных и телекоммуникационных систем в электроэнергетике
- Высоконадежная инфраструктура связи для традиционных и новых приложений в энергетике

Регистрация и подробная информация:
www.d2_rus.cigre.ru
E-mail: **colloq2017@cigre.ru**

В НОМЕРЕ

CONTENTS

ОБЩИЙ ВЗГЛЯД

BIRD'S EYE VIEW

Многогранный «Интернет вещей»
Павел Литвинов | АО «РТСофт»
4
Multifaced Internet of Things
by Pavel Litvinov | RTSoft

Embedded World 2017 – главное мировое шоу технологий для встраиваемых систем
Роман Аляутдин | АО «РТСофт»
14
Emdedded World 2017 – Leading World Embedded Show
by Roman Alyautdin | RTSoft

ВСТРАИВАЕМЫЕ КОМПЬЮТЕРНЫЕ ТЕХНОЛОГИИ

EMBEDDED COMPUTER TECHNOLOGIES

Блестящее будущее «Интернета вещей»
Норберт Хаузер | Kontron
18
A Bright Future for the Internet of Things
by Norbert Hauser | Kontron

15 лет архитектуре и аппаратной платформе ATCA: возможности использования в настоящее время
Марк Овергаард | Pentair Electronics Protection
25
ATCA and Its Hardware Platform Management at 15 Years: How Can I Use Them Now?
by Mark Overgaard | Pentair Electronics Protection

Открытые технологические платформы как глобальный тренд в области разработки систем специального назначения
Виктор Синенко | АО «РТСофт»
29
Open Technical Platforms as Global Trend in Special Purpose System Development
by Victor Sinenko | RTSoft

Универсальная вычислительная платформа «Интегро» для морского и наземного применения
Эдуард Лиманский | АО «РТСофт»
34
***Integro* Multipurpose Computer Platform for Marine and Ground-based Applications**
by Eduard Limanskiy | RTSoft

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

SOFTWARE

Создание системных сервисов в Android
Игорь Марков, Игорь Починок | НИВЦ МГУ, Auriga Inc
38
Android Based System Service Development
by Igor Markov and Igor Pochinok | MCU RCC, Auriga Inc.

ИУС ДЛЯ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ И ИНФРАСТРУКТУРНЫХ ОБЪЕКТОВ

INDUSTRIAL ENTERPRISE AND INFRUSTRUCTURE IMSs

Организация эффективного и надёжного энергоснабжения судостроительных предприятий
по материалам АО «РТСофт»
43
Organization of Effective and Reliable Energy Saving for Shipbuilding Facilities
by RTSoft materials

ИУС ДЛЯ ЭЛЕКТРОЭНЕРГЕТИКИ

Распределительные сети и Микрогрид 46
Алексей Небера, Николай Шубин | АО «РТСофт»

Долгосрочное прогнозирование динамики изменения киберугроз в энергетике методами имитационного моделирования 54
Павел Литвинов | АО «РТСофт»
Сергей Нестеров | АО «РТСофт»

POWER INDUSTRY IMSs

Distribution Networks and Microgrid
by Alexey Nebera and Nikolay Shubin | RTSoft

Long-term Forecasting of Cyber Threat Time History for Power Engineering by Simulation Modeling Methods
by Pavel Litvinov and Sergey Nesterov | RTSoft

НОВОСТИ

Новое будущее «Интернета вещей»: модули COM Express Type10 на Intel Apollo Lake 22

«Сервер-на-модуле» COM Express Type 7 на Intel Xeon для ускоренного проектирования 24

IFEC-системы РТСофт на II международном «Авиационном IT-форуме России и СНГ» 36

NEWS

A New Future of the Internet of Things: Intel Appolo Lake based COM Express Type 10 Modules

Intel Xeon based COM Express Type 7 Server-on-Module for Accelerated Engineering

RTSoft IFEC-systems at the 2nd International "Russia & CIS IT Air-forum"

РЕДАКЦИОННЫЙ СОВЕТ:

Синенко О. В. – председатель редакционного совета, генеральный директор АО «РТСофт», д. т. н.

Егоров А. А. – начальник научно-учебного Центра МАИ «Интеллектуальные системы измерений, контроля и управления в промышленности», профессор АВН РФ, к. т. н.

Золотарёв С. В. – ведущий эксперт компании «Фиорд», к. т. н.

Итенберг И. И. – генеральный директор и главный конструктор ОАО «НКБ ВС», к. т. н.

Куцевич Н. А. – технический директор АО «РТСофт», д. т. н.

Рыбаков А. Н. – технический директор АО «РТСофт»

Сюзев В. В. – зав. кафедрой, профессор МГТУ им. Н. Э. Баумана, д. т. н., лауреат премии правительства в области образования

Шагурин И. И. – заместитель заведующего кафедрой, профессор МИФИ, д. т. н.

РЕДАКЦИЯ:

Главный редактор – **Зеленова Т. И.**

ЭКСПЕРТЫ ПО НАПРАВЛЕНИЯМ:

Встраиваемые компьютерные технологии – **Якшин Ю. Н.**

Программное обеспечение – **Жданов А. А.**

ИУС для промышленных предприятий и инфраструктурных объектов – **Ханыгин А. Н.**

ИУС для энергетики – **Небера А. А.**

Ответственный за вёрстку – **Журавлева А. В.**

Подписка и распространение – **Лазарева Т. Н.**

Тираж 900 экз., цена свободная.
«Мир компьютерной автоматизации. Век XXI»
Computer Automation World
№2 (111) 2017

Издаётся с 1995 года.
Выходит 4 раза в год.

Учредитель: ЗАО «СПА»
Адрес: 105077, Москва, а/я 158
Телефон: 8 499 271-32-32
Факс: 8 495 748-68-29

mka@rtsoft.ru
www.mka.ru

Оформить подписку можно через редакцию по тел. 8 499 271-32-32

Многогранный **«Интернет вещей»**

Павел Литвинов | АО «РТСофт»

Трудно найти в наше время человека, ничего не слышавшего об «Интернете вещей» – Internet of Things (в иностранной литературе чаще всего используется акроним IoT, мы будем придерживаться русифицированной версии – ИВ). «Призрак» «Интернета вещей» бродит не только по Европе, в мировых средствах массовой информации говорят о грядущей технологической революции, которая затронет всех и изменит нашу жизнь в той же мере, как появление телевидения, персональных компьютеров или сети Интернет. Биржевая аналитика пестрит радужными прогнозами, появляются новые консорциумы по развитию и стандартизации ИВ, анонсируются новые продукты и услуги. Всё это происходит на фоне отсутствия единого мнения о том, что же такое ИВ и где его границы даже на уровне базовых определений. По мере движения от ядра – онтологии к периферии – прикладному использованию, представления расходятся сильнее и переплетаются всё причудливее, как круги на воде от брошенных камней. В настоящей статье автор попробует внести ясность в этот вопрос, путем взгляда на тематику ИВ с разных областей и под разными углами зрения. Преимуществом аналитического подхода к раскрытию темы является возможность, не навязывая субъективного мнения читателю, сформировать у него собственное представление на тему, что такое ИВ, и отношение к вопросу о его полезности и перспективах использования в самых широких областях: от частной жизни до бизнеса.

Предпосылки «Интернета вещей» M2M

Большинство источников сходятся во мнении, что непосредственным предшественником ИВ является концепция Machine-to-machine (M2M), которую образно называют «Интернетом машин». «Интернет вещей» включает в себя M2M и является дальнейшим технологическим развитием ранее заложенных идей и их маркетинговым переосмыслением. Парадигму Machine-to-machine можно представить как «сплав» возможностей, предоставляемых современными технологиями:

– беспроводные коммуникации;
– значительная вычислительная мощность в узлах, устройствах M2M;
– облачные сервисы и технологии.

Каждый из трёх компонентов вносит свой вклад в формирование ценности для потребителя и поставщика решений:

– **Беспроводные коммуникации** – существенное сокращение сроков проектирования и монтажа, возможность гибкой перенастройки, в том числе и на перспективные задачи.
– **Вычислительная мощность** в **узлах, устройствах M2M** позволяет на уровне датчиков и сенсоров использовать много недорогих устройств. От обработки «в центре» можно перейти к обработке «на месте». Движение от иерархических технологических систем и методов управления в сторону сетецентрических – также один из трендов.
– **Облачные сервисы и технологии** гарантируют максимальную гибкость и снижают не только стоимость владения, но и «порог» вхождения в новые решения.

Дополнительные блоки, которые легли в фундамент ИВ:

– низкая стоимость владения;
– минимальное энергопотребление;

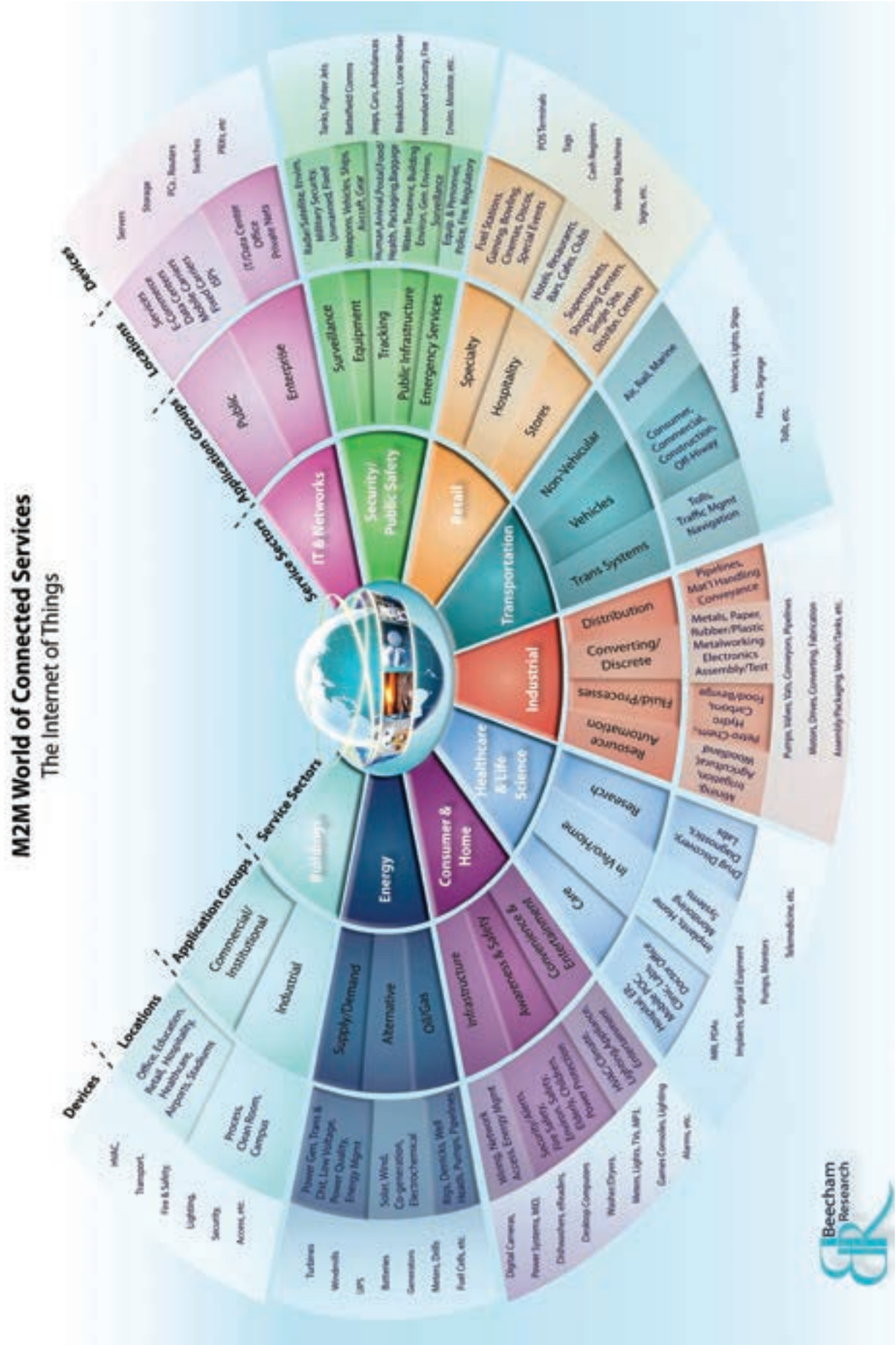


Рис. 1. Мир M2M и IoT по версии Beecham Research

– коммуникации и базовая функциональность, доступная «из коробки»;
– глобальная доступность устройств и сервисов.

На **рис. 1** приведена точка зрения компании Beecham Research. Классы приложений группируются по секторам вертикальных рынков, а в каждом из них перечисляется возможное место применения и виды устройств.

Конвергенция технологии

Среди технологий будущего, которые уже меняют или изменят нашу жизнь и деловой ландшафт на ближайшие годы, наиболее часто называют следующие:

1. Искусственный интеллект и развитие робототехники (AI).
2. Облачные технологии и сервисы (Cloud).
3. Большие данные (Big Data).
4. Интернет 3.0 (Web 3.0).
5. Аддитивные технологии (3D printing или additive manufacturing, AM).

Для первых четырёх технологий из этого списка «Интернет вещей» одновременно и движущая сила, и «бенефициар» их развития! Другими словами, ИВ в его современном понимании не существует без использования облачных сервисов, больших данных и возможностей по их интеллектуальной обработке. Новые потребительские качества и возможности появляются как сложный сплав современных трендов, причём верные пропорции для успеха найти непросто.

Немного теории

Закон Меткалфа, первоначально сформулированный 1980 году, гласит, что ценность телекоммуникационной сети пропорциональна квадрату числа подключённых пользователей системы. Уже тогда под пользователями понимались совместимые устройства, например факсимильные аппараты, телефоны и т. п. Закон отражает простой факт: количество уникальных соединений в сети с количеством узлов (n) описывается формулой n (n-1)/2. Разумеется, речь идёт о наиболее оптимистичной оценке полезности в силу объективных причин: несовместимости протоколов устройств или языкового барьера, если речь идёт о людях; захвата значительного числа ресурсов отдельными устройствами или группами пользователей – и просто для больших значений n более правильной оценкой будет пропорциональность N*log(N). Но какие бы поправки мы не вносили, очевидно, что когда счёт пойдёт на миллиарды подключённых устройств, потенциальная потребительская ценность такой сети будет огромной! **(см. рис. 2)**.

Прогнозы

Каждый продукт, потенциально способный трансформировать мир или по крайней мере наше представление о нём, находясь на ранней стадии своего жизненного цикла, вызывает ожидания в отношении потенциальных преимуществ и волнения инвесторов. Ошибки в прогнозах, с какой скоростью ИВ будет завоёвывать рынок и какое займет на нём в результате место, могут иметь непредсказуемые и дорогостоящие последствия. Дальновидные организации должны уже сейчас думать о шагах, которые необходимо предпринять на протяжении всего жизненного цикла вновь предлагаемых продуктов и сервисов. Неопределённость усиливается тем фактором, что

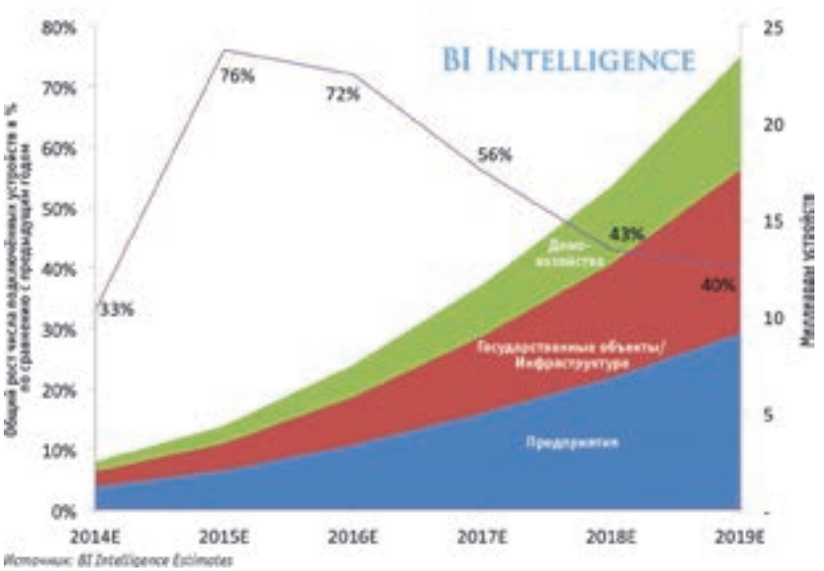


Рис. 2. Прогноз роста числа устройств в структуре секторов

парадигма ИВ вмешивается не только в понимание, но и в сами процессы жизненного цикла. На **рис. 3** отражена точка зрения компании IBM.

Изменения затронули не только количество стадий и их названия. Самым существенным отличием является то, что процессы, которые раньше выполнялись последовательно, теперь идут параллельно и зачастую одновременно.

Архитектура «Интернета вещей»

Референтная модель

Фундаментальными характеристиками «Интернета вещей» являются:

- **Взаимосвязанность**. Все устройства взаимодействуют через глобальную или локальную инфраструктуру информационного обмена.
- **Сервисы, ориентированные на устройства**. ИВ способен обеспечить семантическую согласованность между физическими объектами реального мира и их информационным представлением в виртуальном пространстве и объединить физические устройства с учётом правил и ограничений.
- **Гетерогенность**. Устройства в ИВ неоднородны по определению и могут принадлежать различным сетям и аппаратным платформам, что не является препятствием к взаимодействию.
- **Динамичность**. Состояние устройств меняется постоянно: включение и выключение, контекстная и технологическая информация, в том числе местоположение и скорость. Количество подключённых устройств также может динамически изменяться.
- **Масштабность**. Количество устройств, которые будут «общаться» и получать управляющее воздействие, в десятки раз превысит количество узлов в текущей сети Интернет. Очевидно, что количество коммуникаций, которые могут быть инициированы устройствами, радикально превысит возможное число соединений, инициаторами которых выступают люди. Поэтому на первый план выходят вопросы интерпретации данных, с целью их последующего применения.

Рис. 3. Жизненный цикл по версии IBM

Коммуникации и протоколы

С развитием сети Интернет и беспроводных технологий мы получили «коммуникации в любое время», смартфоны и планшеты позволили реализовать принцип «коммуникации в любом месте». ИВ добавляет новое измерение и третью степень свободы в пространстве коммуникаций – «коммуникации с любой сущностью», будь то компьютеры, люди или устройства. Также принципиально новым явлением становится «самостоятельный» обмен данными или информацией между устройствами различных типов.

Базовыми способами коммуникаций между устройствами могут быть следующие:

- с использованием шлюза и концентратора данных (via gateway);
- с использованием только сети передачи данных (without gateway);
- прямые соединения между устройствами (direct communication).

В части подробного описания протоколов можно порекомендовать статью «Протоколы Интернета вещей: основные сведения», опубликованную в журнале «Мир компьютерной автоматизации: встраиваемые компьютерные системы» № 1 за 2015 г. Это одно из лучших описание данной темы, которое можно найти на русском языке.

Стандарты и консорциумы

Блестящие рыночные перспективы, которые аналитики дружно обещают направлению ИВ, не позволяют компаниям самого разного размера и специализации в области информационных технологий остаться равнодушными. В одиночку и путём объединения в консорциумы они пытаются занять свою нишу и освоить это перспективное направление. В таблице представлены наиболее крупные объединения, их задачи и названия основных компаний-участников.

Практическое применение

Сценарии использования

Возможные сценарии использования парадигмы ИВ и их взаимная связь хорошо отражены на инфографике, подготовленной компанией Libelium **(рис. 4)**.

Бизнес-модель и экосистема

Чтобы лучше понять методы и способы извлечения прибыли или преимуществ от использования ИВ, необходимо определиться с несколькими справочниками. Виды спра-

Наиболее крупные консорциумы по освоению «Интернета вещей»

Консорциум	Задачи	Основные компании-участники
AllJoyn	Позволить совместимым «умным» устройствам «узнавать» друг друга, устанавливать соединения и распределять свои ресурсы и обмениваться данными вне зависимости от производителя, вида сети и используемой операционной системы.	Qualcomm + Cisco, Microsoft, LG, HTC
The Physical Web	Обеспечение возможности потребителям общаться с любым доступным «умным» устройством без предварительной загрузки и установки специализированного программного обеспечения.	Google
Industrial Internet Consortium	Проектирование и создание решений в области интеллектуальной промышленной автоматизации.	Intel, Cisco, AT&T, GE, IBM, Microsoft
Open Interconnect Consortium	Разработка коммуникационного каркаса приложений, базирующегося на индустриальных стандартах с целью установления беспроводных соединений и интеллектуального управления информационными потоками.	Intel + Atmel, Dell, Broadcom, Samsung, Wind River
Thread	Разработка нового беспроводного сетевого протокола	Google's Nest, Samsung Electronics, ARM Holdings, Freescale Semiconductor, Silicon Labs, Big Ass Fans и Yale Locks & Hardware

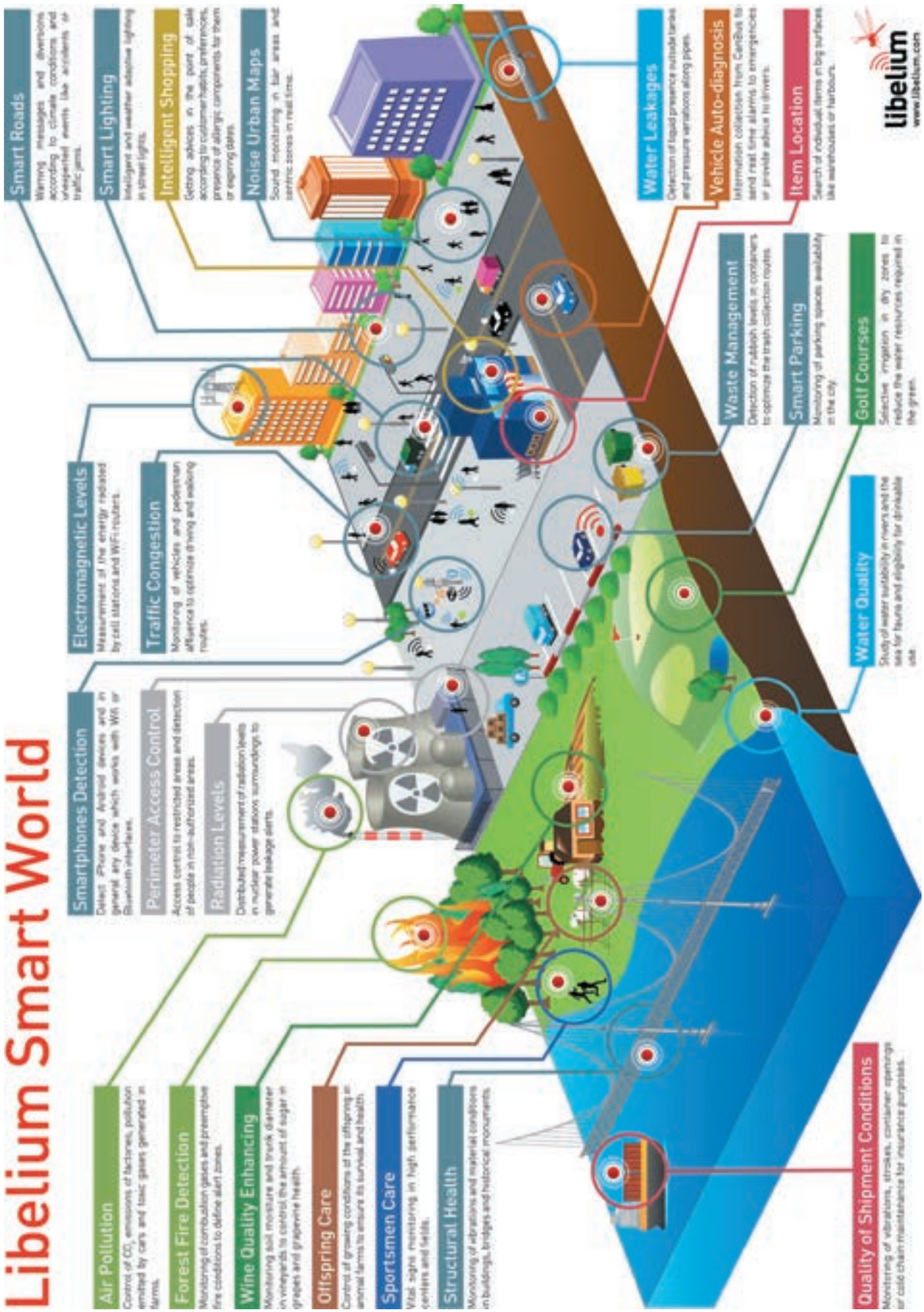


Рис. 4. «Умный» мир

вочников напрямую следуют из референтной модели, а состав может отличаться. В первую очередь определимся с конечным потребителем или заказчиком:

- Промышленность и государство (Industrial & Government Applications):
  - Умные города (Smart Cities);
  - Мониторинг окружающей среды (Smart Environment);
  - Умное водопользование (Smart Water);
  - Умный учёт (Smart Metering);
  - Безопасность и чрезвычайные ситуации (Security & Emergencies);
  - Розничная торговля (Retail);
  - Логистика и транспорт (Logistics & Transportation);
  - Производственная автоматизация и контроль (Industrial Control);
  - Сельское хозяйство (Smart Agriculture);
  - Строительство (Buildings);
  - Прогрессивное животноводство (Smart Animal Farming).
- Потребительские устройства (Consumer):
  - Домашняя автоматизация (Domotic & Home Automation);
  - Носимые устройства (Wearable Technology);
  - Электронное здравоохранение (e-Health, Healthcare).

У двух больших категорий разные драйверы развития. Если на вертикальных рынках польза от ИВ определяется наличием специфических задач (включая государственное регулирование) или нишевых проблем, не решаемых эффективно существующими технологиями, то на потребительском рынке тренд задают новые бизнес-модели, которые включают в себя формирование потребностей потребителя и создание принципиально новых услуг и возможностей.

Бизнес-модель деятельности компаний, в которую уже входит или органично может войти «Интернет вещей», можно сегментировать таким образом:

- анализ данных (Data Analysis);
- выполнение НИР и ОКР, консалтинг (Management Consulting / Research);
- облачные платформы и сервисы (Cloud Platform Service);
- производство и поставки оборудования (Hardware Producer / Vendor);
- проектирование продуктов и услуг (Product / Service Design);
- разработка аппаратного обеспечения (Hardware Development);
- разработка программного обеспечения (Software Development);
- системная интеграция (System Integrator);
- услуги и сервисы связи (End-to-end Service Provider).

Отметим также, что традиционные облачные сервисы:

- программное обеспечение как услуга (SaaS);
- платформа как услуга (PaaS);
- инфраструктура как услуга (IaaS);
- мониторинг как услуга (Maac);
- коммуникация как услуга (CaaS) – существенно сокращают время и стоимость развёртывания решений, основанных на парадигме ИВ. В этом ряду сервисов, расположенных в порядке убывания комплексности, с точки зрения заказчика, появляется ещё один, самый элементарный, присущий только ИВ, – «датчик как услуга».

На **рис. 5** приведена экосистема ИВ согласно [1].

Роли участников экосистемы (нумерация совпадает с **рис. 5**):

1. Обеспечивает возможность передачи «сырых» данных, соответствующих логике

Рис. 5. Экосистема «Интернета вещей»

и назначению устройства, оператору связи или непосредственно поставщику приложений.

2. Играет центральную роль в экосистеме ИВ и выполняет следующие функции: обеспечение доступа и интеграция ресурсов, предоставляемых другими поставщиками; поддержка и контроль сервисов инфраструктуры ИВ; размещение сервисов, в том числе для (от) других провайдеров.
3. Обеспечивает возможности интеграции и открытые интерфейсы. Наиболее типичными являются функции интеграции, хранения и обработки данных и управление конфигурацией самих устройств.
4. Использует функциональные возможности и ресурсы, предоставляемые операторами связи, платформами и самими устройствами в интересах решения задач клиента с помощью специализированных приложений.

Перебирая различные сочетания 1–4, можно получить пять базовых бизнес-моделей:

1. Весь комплекс услуг предоставляется заказчику одним провайдером (1, 2, 3, 4).
2. Устройства, услуги связи и платформу предоставляет один провайдер, а приложения – от независимого поставщика (1, 2, 3) + (4).
3. Производитель устройств снабжает их соответствующими приложениями, услуги сети и платформу предоставляет другой вендор (1, 4) + (2, 3).
4. Аналогично п. 3. – производитель является также и разработчиком платформы (1, 3, 4) + (2), оператор связи независим и выбирается заказчиком.
5. Заказчик или системный интегратор «собирает» систему из компонентов от четырёх независимых производителей (1)+(2)+(3)+(4).

Риски

Оптимизм в части перспектив ИВ сдерживается существованием разного вида барьеров, стоящих на пути этой технологии. Перечислим и кратко охарактеризуем только основные.

Новые стандарты. Нет единого стандарта на протоколы информационного обмена. Активные попытки создания идут. Существующие требуют развития или замены, так как не соответствуют новым задачам. Ситуация напоминает эпоху развития видеотехники, когда каждый консорциум развивал свои стандарты записи видеосигнала – VHS, Hi8, VHS-C, BetaMax и др. – и все они нашли свою нишу. Такое «распыление усилий» не только замедляет развитие, но и приведёт к проблемам совместимости для большинства компонентов потенциальных систем. Добавим также сравнительно медленный переход к повсеместному использованию протокола IPv6.

Стоимость. Относительно высокая стоимость каждого узла, концентраторов данных, подключение к коммуникационным сетям и (или) оплата дополнительного трафика, потребление электроэнергии, подписка на сервисы и т. д. приводит к тому, что массового появления самых эффективных, с точки зрения теории, сетей, насчитывающих десятки тысяч устройств, мы пока не наблюдаем. В большинстве потенциально чрезвычайно перспективных отраслей (например, сельское хозяйство и животноводство) сроки окупаемости пока значительные, что подталкивает потенциальных потребителей, с учётом бурного развития и переосмысления концепции ИВ, занимать выжидательную позицию.

Безопасность. Последняя в нашем списке, но самая значимая из проблем. Аспектов, по которым ИВ может отрицательно сказаться на безопасности, множество. От увеличения риска для закрытых корпоративных сетей до утечек персональных данных. Очевидно, что в промышленности использование беспроводных технологий увеличивает уязвимость. Конечно, различные производители уже готовы предложить решения, но их эффективность сильно зависит от ресурса атакующего и его мотивации. В случае значительного ресурса и высокой мотивации – гарантированной защиты пока не существует. На потребительском рынке – казуальное использование «умных» устройств, «умный дом», персональная медицина – ситуация сложней и труднопредсказуема. У людей по объективным, а

зачастую и субъективным причинам, может расти тревога в отношении возможности утраты персональной информации или вреда от излучений беспроводных устройств и т. п. Разоблачения Эдварда Сноудена, например, изменили поведение значительного числа людей, которым объективно нечего и незачем скрывать. «Синдром Сноудена» реально «ударил» по социальным сетям и некоторым производителям программного обеспечения для мобильных устройств. Справедливости ради следует отметить, что открылись новые возможности для продажи решений по защите персональной информации, включая рынок «псевдорешений».

Коммерциализация

Успешная монетизация невозможна без получения ответов на вопросы:
– кто является потребителем?
– что представляет для него ценность?
– каким образом вы планируете её создать?
– как донести эту ценность до потребителя и продать ему по разумной экономически обоснованной цене?

Новые бизнес-модели появляются как результат развития технологий и открывают широкий спектр получения прямых и косвенных доходов. Новым явлением стали многочисленные открытые сообщества разработчиков, вовлечённые не только в процессы проектирования и создания ценностей, но и в процессы их потребления. Основные модели коммерциализации для ИВ были заложены развитием традиционного Интернета.

Лицензирование. Старейшая и наиболее распространённая модель в индустрии программного обеспечения. В случае ИВ речь может идти не только о программах и сервисах, а также о данных и результатах аналитики. Их использование внутри домена приложения может быть бесплатным, плата взымается за данные, имеющие ценность для других приложений и потребителей. Это даёт совершенно уникальную возможность расширять границы приложений в соответствии с запросами клиентов.

Подписка. Одна из вариаций модели лицензирования. Плата за доступ к данным (услугам) для определённого периода времени – по сути, превращает разовые продажи продукта в повторяющиеся. При этом появляется возможность менять цены в зависимости от того, как часто и как долго клиент использует службу. Хорошая практика скидки на более долгие сроки подписки позволяет «привязывать» к себе заказчика и привлечь и аккумулировать средства на дальнейшее развитие.

Премиум-сервисы. Идея этой бизнес-модели заключается в предоставлении простых и базовых услуг бесплатно, с целью продажи более продвинутых или дополнительных функций. В этом случае рост возможен не только за счёт привлечения новых пользователей, но и повышения дохода от существующих. Если потребитель удовлетворён базовыми сервисами, он не только будет готов внести небольшую плату, чтобы получить дополнительные сервисы, но и станет рекламировать его своим друзьям и семье. Эта модель поощряет пользователей бесплатной части продукта взаимодействовать таким образом, чтобы создать спрос на дополнительные платные услуги.

Реклама. Мы уже знакомы с тем, как передовые методы бизнес-аналитики используются для контекстной рекламы и поведенческого маркетинга. ИВ даёт новые возможности, когда содержимое отображаемой рекламы будет динамически меняться в зависимости от поведения пользователя и содержания получаемых данных от сенсоров.

Генерация трафика. Бизнес-модель генерации трафика – хороший пример косвенного способа монетизации. Увеличивается шанс получения доходов от прямых бизнес-моделей, таких как электронные платежи, премиум-сервисы или реклама. Не забудем также, что весь этот трафик кем-то оплачивается, как и модернизация сетевого оборудования и каналов связи, необходимых для его прохождения.

Электронные платежи. Идея состоит в том, чтобы получить прибыль от микроплатежей от индивидуального использования наборов данных или результатов аналитики. Потребители могут произвести

платёж в любое время дня или ночи, в любой точке мира. Модель электронных платежей не новая в Интернете, но переход к микрооплатам позволит вовлечь пользователей даже с низкими доходами.

Массовая кастомизация. ИВ позволяет создавать индивидуальные продукты для каждого клиента исходя из его требований и даже предпочтений. Слишком дорогое решение для традиционного товарного производства, в случае продажи сервисов и услуг, являющихся по сути информационными, становится рентабельным и возможным.

Совместное потребление. Яркими представителями Peer-to-peer (P2P) в традиционном Интернете являются файлообменные сервисы. Модель, сложная для извлечения прибыли, используется главным образом для обмена контентом и постоянно подвергается критике правообладателей. В мире ИВ ситуация может радикальным образом измениться. Каждый легко может стать поставщиком собственного информационно-аналитического контента или просто данных от сенсоров или других устройств, который можно будет продавать или обменивать.

Мобильная коммерция. Модель быстро развивается и просто получит дополнительный импульс. Как и в случае с рекламой, возможности по точному предложению товаров и услуг, в том числе нужных «здесь и сейчас», возрастут многократно.

Заключение

Граней, на которые можно отразить парадигму ИВ, конечно, больше. Каждый месяц появляются новые исследования, которые всё глубже прорабатывают не только отдельные аспекты этой темы, но и семантические связи между ними. Если после прочтения этой статьи у читателя появится желание подумать о том, как применить новые возможности к текущим или перспективным задачам бизнеса, автор будет считать задачу выполненной. При всех сомнениях в перспективности и целесообразности использования технологий ИВ следует в первую очередь искать решение не в области замены «классических решений» – а в нахождении некоего «симбиоза» или проектирования принципиально новых систем и сервисов. Компания «РТСофт» имеет и активно развивает свои компетенции в области «Интернета вещей» и готова оказывать широкий спектр услуг в этой области – от консультационных услуг до разработки приложений и системной интеграции.

Литература

1. Recommendation ITU-T Y.2060, «Overview of the Internet of things», Geneva, 2013 г.

2. Francis daCosta, «Rethinking the Internet of Things: A Scalable Approach to Connecting Everything», © 2013 by Apress Media.

3. Fernando Almeida, Jos D. Santos and Jos A. Monteiro, «E-Commerce Business Models in the Context of Web 3.0 Paradigm», International Journal of Advanced Information Technology (IJAIT) Vol. 3, No. 6, December 2013.

4. Информация с сайтов: www.ibm.com, www.beechamresearch.com, www.libelium.com, wikipedia.org.

Павел Литвинов | АО «РТСофт»

Embedded World 2017 – главное мировое шоу технологий для встраиваемых систем

Роман Аляутдин | АО «РТСофт»

С 14 по 16 марта 2017 года состоялась 15-я выставка/конференция Embedded World, которая ещё раз ярко доказала свой лидирующий статус среди подобных мероприятий по демонстрации мировых достижений в области программного и аппаратного обеспечения для встраиваемых систем.

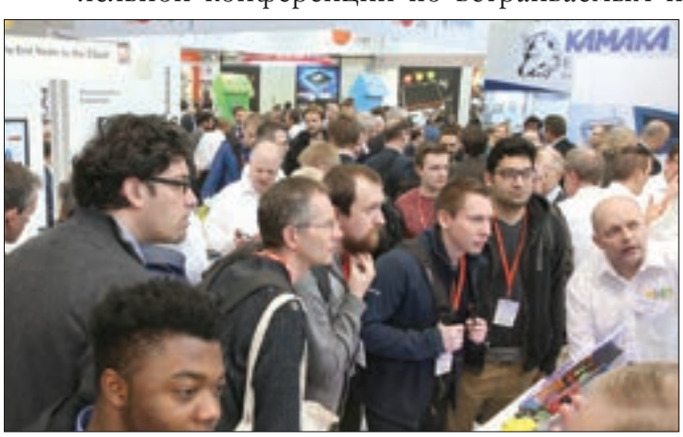
Каждый год двери Embedded World, организуемой компанией NürnbergMesse, собирают под одной крышей выставочного центра в городе Нюрнберге (Германия) сотни компаний и тысячи посетителей. 2017 год не стал исключением.

В этом году в малый, 15-летний, юбилей, число экспонентов на Embedded World стало рекордным – по официальной статистике более 1000 компаний (+8 %) из 39 стран, а количество посетителей за три дня превысило 30 000. Стенды чипмейкеров (Intel, TI, Nvidia, Imagination и др.), производителей плат и встраиваемых компьютеров (Kontron, Advantech, Adlink и др.), разработчиков операционных систем (Micrsoft, SYSGO AG, Green Hills Software и др.), средств разработки и отладки (Mathworks, IAR др.), а также производителей программных и аппаратных решений для вертикальных рынков заняли площадь 48 000 кв. м (6 залов) **(рис. 1)**.

Вырос в этом году и интерес к параллельной конференции по встраиваемым и дисплейным технологиям, что очень порадовало организаторов и профессиональное сообщество, – число прибывших экспертов выросло на 8 % и достигло 1796 чел. Основная тема конференции – «Надёжная связь в мире Embedded» (Securely Connecting the Embedded World), с фокусом на «Интернет вещей» (IoT) и «Защищённость и надёжность работы встраиваемых систем» (Security & Safety). В тематике электронных дисплеев большой интерес вызвали темы отображения информации в автомобильных приложениях, а также виртуальной и дополненной реальности (VR/AR).

Полный обзор выставки занял бы весь журнал «МКА», поэтому в данной статье хотелось бы поделиться особо яркими впечатлениями и трендами.

Automotive – одно из самых популярных слов на стендах. Продукты, относящиеся к автомобольной промышленности и к набирающему популярность рынку автономных машин (autonomous cars), были продемострированы многими компаниями – от чипмей-



керов до производителей программного обеспечения. Так, NVidia представила новую систему на модуле (SoM) Jetson TX1, которая позиционируется для использования в качестве основы в будущих системах содействия при вождении (ADAS – Advanced driver-assistance systems). Создатели наделили этот «суперкомпьютер» 256 ядрами CUDA, предназначенными для решения задач компьютерного зрения и глубинного обучения (deep learning). Предполагается, что эти технологии лягут в основу автономных автомобилей ближайшего будущего. Также были представлены оценочные (reference) платы на данной платформе, позволяющие уже сегодня разработчикам опробовать возможности новой системы на модуле. Другой чипмейкер – Renesas – представил платформу R-CAR, специальной серии SOC, разработанной для IVI (in-vehicle infotainment – системы развлечения и информирования пассажиров) и ADAS, на стенде было представлены различные демонстрации возможностей платформы как основы решений для эры автономных автомобилей. Софтверные компании также не отстают от тренда: так, значительная часть стенда QT Company была посвящена применению одноимённой библиотеки для автомобилей: приборных панелей и систем развлечений. Для того чтобы ускорить разработку подобных систем, QT выпускает новый пакет инструментальных средств (SDK) – Qt Automotive Suite – с готовыми компонентами для этой ниши и поддержкой «автомобильной» ОС QNX и Automotive Grade Linux. Так что, возможно, ваша следующая машина будет с QT на борту.

На огромном стенде Intel также нашлось место для темы Automotive: производитель встраиваемых компьютеров B-Plus представил вычислительный модуль (ECU) на чипе Intel с «классическим набором» интерфейсов – CAN, FLEXRAY – и одновременно периферией для подключения устройств компьютерного зрения. Но настоящим магнитом стенда Intel был спорткар BMW i8

Рис. 1. Стенды компаний ADlink, Kontron, Advantech, Microsoft

Рис. 2. Настоящим магнитом стенда Intel был спорткар BMW i8 и шлем дополненный реальности

и шлем дополненный реальности, который предлагалось использовать посетителям стенда. Для демонстрации технологий AR (augmented reality – дополненная реальность) инженерам Intel пришлось превратить шлем в VR (virtual reality – виртуальная реальность). Посетитель видел виртуальные машины, обгоняющие BMW i8 (наверное, это возможно будет в будущем), и при этом уже слой AR выделяет их в дорожном потоке квадратами **(рис. 2)**.

Применимость шлема сомнительна, но задачей чипмейкера было показать, что соответствующие технологии есть, а их приложение – бизнес других компаний.

Так, компания «РТСофт» представила систему дополненной реальности для пассажирского транспорта. Решение даёт возможность пассажирам, сидя в автобусе, наблюдать на экране смартфона или панели развлекательной системы видеопоток, поступающий с установленной на автобусе камеры и дополненный в виде сносок информацией об объектах вокруг – музеях, ресторанах, магазинах и так далее. Вторая отличительная особенность представленной AR-системы – возможность нанесения надписей и изображений на плоские поверхости отображаемого видео. Технология, вне всякого сомнения, найдёт рекламное и информационное применение.

Одной из тем выставки была концепция Industry 4.0. Здесь AR-технологии также были в тренде **(рис. 3)**. Предполагается, что на промышленных обьектах ближайшего будущего очки дополненный реальности либо планшет с камерой будут подсказывать инженерам информацию о деталях, узлах обьектов, выделять на изображении места возможных поломок. Сочетание AR-технологий и

Рис. 3. Традиционно в центре внимания выставок Embedded World технологии «Интернета вещей» и других аспектов Industry 4.0

Рис. 4. Стенды компаний «РТСофт» и «Лаборатория Касперского»

промышленного «Интернета вещей» сделает фабрику действительно умной.

«Интернет вещей», или IoT, уже традиционно в центре внимания подобных выставок (**рис. 3**). Особо хотелось бы отметить ажиотаж вокруг стендов TI и STMicroelectronics: на стендах обеих компаний надо было постоять в очереди, чтобы поговорить со специалистами. Огромный интерес был вызван микроконтроллерами с ультранизким потреблением и оборудованными при этом интерфейсами связи.

TI представлял экосистему msp432 и SimpleLink – микронтроллеров с ядром ARM и встроенным интерфейсом BLE, Wifi или sub1hz. Такие микроконтроллеры идеально подходят для носимых или автономных устройств. Компания STMicroelectronics представила конкурирующую экосистему вокруг микроконтроллеров STM32.

Из ярких анонсов, представленных в ходе выставки, стоит отметить создание альянса ELAA (Embedded Linux and Android Alliance), производителей встраиваемых компьютеров (Advantech и др.) и компаний с компетенциями в области разработки программного обеспечения – Canonical, «РТСофт», Witikeo и др. Целью данного обьединения обьявлена унификация Linux и Android для встраиваемых аппаратных платформ, создание модульных унифицированных программных решений для ускорения разработки «вертикальных» продуктов. В рамках анонса компании представили свои базовые решения для использования участниками альянса. Так, «РТСофт» создал унифицированную платформу управления флотом IoT-устройств с возможностью обновлений ПО по технологии OTA (Over-the-air). Представленные возможности системы вызвали неподдельный интерес (**рис. 4**, слева), так как с этой задачей встречается любой производитель IoT-устройств.

Одна из острых проблем мира «Интернета вещей» – это обеспечение безопасности. В рамках выставки компания «Лаборатория Касперского» (**рис. 4**, справа) представила свою новую операционную систему. Спроектированная для гарантированной защиты критически важной инфраструктуры, ОС хорошо подходит для применения в IoT-шлюзах, обеспечивающих связь устройств с Интернетом/Облаком.

Выставка в Нюрнберге показала огромный потенциал современных технологий и решений. Перечисленные тренды наверняка получат свое развитие и будут представлены новыми продуктами на Embedded World 2018, которая состоится в Нюрнберге с 27 февраля по 1 марта 2018 г. Ждём!

embeddedworld2018
Exhibition&Conference
... it's a smarter world

Роман Аляутдин | АО «РТСофт»

Блестящее будущее **«Интернета** вещей»

Норберт Хаузер | Kontron

В данной статье Норберт Хаузер, вице-президент по маркетингу компании Kontron, рассказывает о перспективах развития идеологии «Интернета вещей» в мире и, в частности, Германии, о проблемах, связанных с её внедрением, и об усилиях компании Kontron на этом пути.

«Интернет вещей» (Internet of Things – IoT) развивается настолько стремительно **(рис. 1)**, что ни одно современное предприятие не может пройти мимо этой тенденции. В результате цифровизации все отрасли промышленности и экономики трансформируются в единое целое. Умные устройства завоёвывают всё большее число рыночных секторов – от печатных станков до промышленных роботов, от складских помещений до ветровых электростанций. Индустрия «Интернета вещей» переживает небывалый бум, и конца ему не видно.

Это подтверждает и недавний отчёт консалтингового подразделения компании McKinsey. По его прогнозам, к 2020 году рынок «Интернета вещей» в Германии может достигнуть 23 млрд евро. Эта цифра заслуживает внимания, поскольку нынешний годовой доход от внедрения IoT в информационно-коммуникационной индустрии Германии исчисляется «лишь» 10 млрд евро. Таким образом, аналитики McKinsey ожидают удвоения в течение пяти лет – впечатляющий рост, однако стоит посмотреть на вещи и более трезво, учитывая тот факт, что по самокритичному признанию самих немецких компаний, их квалификация в IoT-сфере ещё недостаточно высока. Согласно исследованиям, проведённым по заказу немецких компаний из сферы телекоммуникаций, большинство разработчиков, начиная проектировать свои решения IoT, имеет своё собственное видение методов и технологий их создания и внедрения. Безоговорочно ясно только одно: значимость «Интернета вещей» будет расти, в особенности потому, что потенциальные выгоды, которое сулят возможности подключения к компьютерным

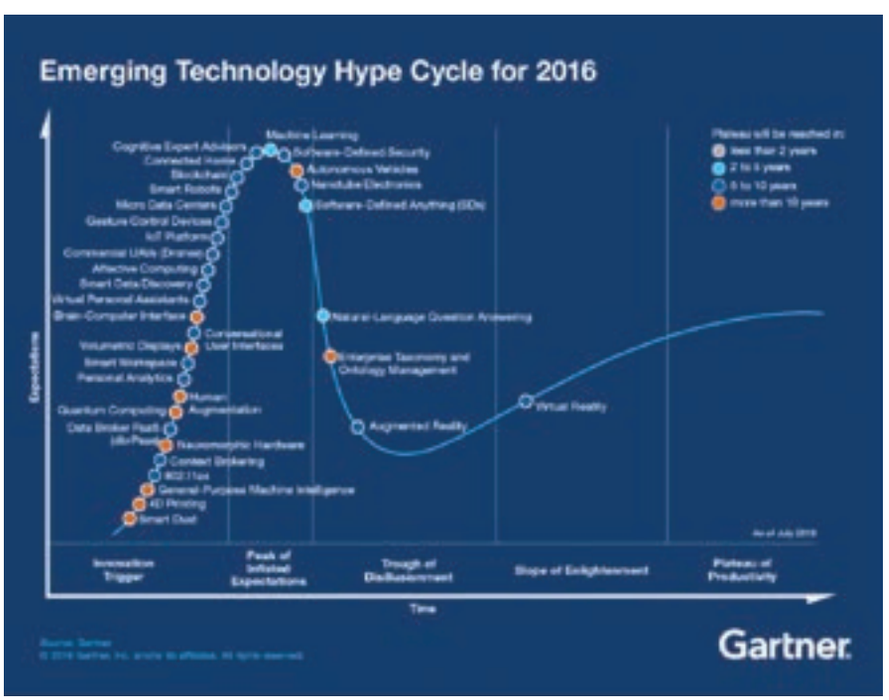


Рис. 1. График прохождения инноваций по кривой «Цикла зрелости технологий» от компании Gartner

сетям как в индустриальной, так и в потребительской сфере, реализованы недостаточно.

Kontron – одна из первых компаний, которая вносит свой вклад в реализацию программы Industry 4.0

Самая весомая доля в потенциальном доходе от IoT, согласно прогнозу McKinsey, равная порядка 9 млрд евро, приходится на сектор Industry 4.0. И, как говорит наш опыт, это действительно так. Огромное число наших заказчиков работает над проектами цифровизации производственных процессов, особенно концепции «умного предприятия» (Smart Factory). Это заставляет нас двигаться вперёд в данном направлении, считая его высокоприоритетным.

Так, концепцию «умного предприятия» штаб-квартира компании Kontron демонстрирует личным примером. Принципы Industry 4.0 мы внедрили на территории нашего предприятия в Аугсбурге **(рис. 2)**. Для этого мы полностью перепроектировали наши производственные корпуса, перегруппировали рабочие площадки и полностью заменили IT-инфраструктуру. Эти изменения позволили инженерам управлять процессами производства более эффективно, выпускать серии различных изделий в разных конфигурациях одновременно, и даже изготавливать мелкосерийные партии с минимальным периодом освоения. Установив на каждой рабочей станции по крайней мере один высокопроизводительный промышленный компьютер

Рис. 3. Промышленные компьютеры Kontron KBox Series

Рис. 2. Производственные корпуса Kontron

серии KBox **(рис. 3)**, мы предоставили нашим работникам доступ ко всей относящейся к процессу производства информации, поступающей из любого места. Это высоконадёжные и неприхотливые (благодаря безвентиляторной конструкции) миникомпьютеры, которые одновременно управляют и производственной линией. Они отслеживают процесс производства, собирают данные, непрерывно поступающие в реальном времени и используемые для контроля качества выпускаемых изделий, и автономно управляют обработкой заказов. Вся собираемая из систем информация передаётся в центральный сервер, где она обрабатывается и где любой специалист может получить к ней доступ. Таким образом, каждый работник, участвующий в процессе производства, всегда знает о текущем состоянии заказа и незавершённых в данный момент и требующих принятия решения этапах сборки.

Германия отстаёт в сфере E-Health и Smart Home

С точки зрения перспектив IoT аналитики компании McKinsey оптимистично смотрят на будущее экономики Германии в таких отраслях, как промышленное производство и автомобилестроение. Причём немецкая автомобильная промышленность, исторически инновационная, хорошо позиционируется даже в мировом масштабе. Однако в приложениях E-Health (цифровизация в области здравоохранения) и Smart Home («умный дом») Германия отстаёт. Цифровым сетям нет

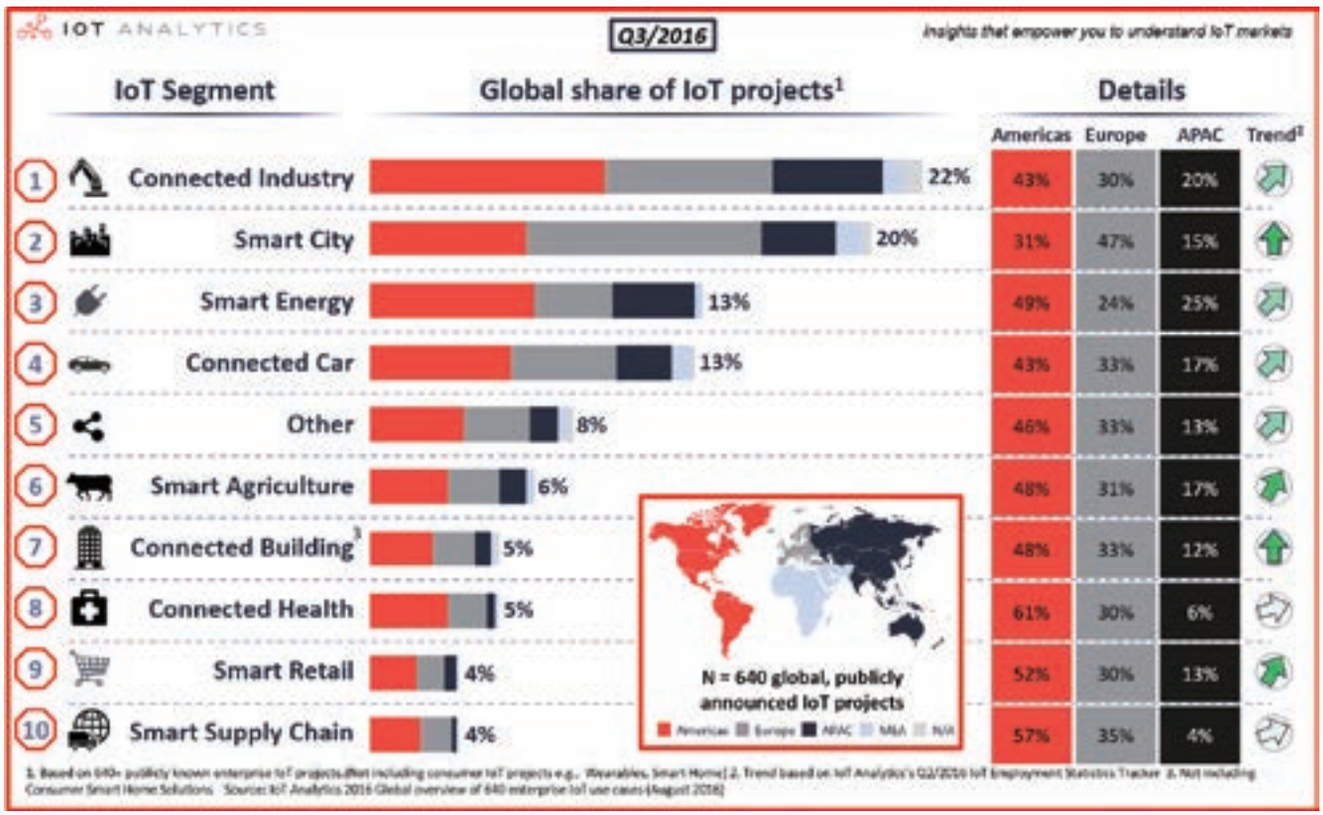


Рис. 4. Проекты «Интернета вещей» в различных прикладных сферах, в мировом масштабе

пока доверия в тех сферах, где используются конфиденциальные персональные данные. По мнению аналитиков McKinsey, чтобы завоевать такое доверие, необходима тщательная проработка соответствующих стандартов по защите информации и сохранению конфиденциальности. Эта дихотомия находит своё отражение и в отчёте *The top 10 IoT application areas – based on real IoT projects* («10 самых успешных прикладных сфер IoT») от компании IOT Analytics: Германия лидирует в сфере промышленного производства и автомобилестроения, и проигрывает в секторе E-Health и Smart Home **(рис. 4)**.

Ключ к доверию потребителей – информационная безопасность

Мы, в компании Kontron, тоже считаем, что вопрос безопасности «Интернета вещей» слишком долго сбрасывался со счетов. Это подтверждают многочисленные отчёты о крупномасштабных хакерских атаках на устройства «Интернета вещей». В одном из постов в своём блоге мой коллега Стефан Эберхардт (Stefan Eberhardt) назвал IoT «Эльдорадо для хакеров». Для по-настоящему эффективного и продуктивного принятия «Интернета вещей» в рамках всех сфер экономики вопросам IT-безопасности необходимо уделять существенно больше внимания. Это единственный способ получить шанс для завоевания доверия со стороны потребителей. А иначе в «щепетильных» областях экономики, которые связаны с личными данными, «Интернет вещей» ждёт печальная участь. Во всех наших продуктах безопасность IoT мы поставили на первое место. Как ведущая мировая компания по производству встраиваемых компьютеров, мы в качестве стандартной опции (по умолчанию) ввели во все наши продукты комплексное решение по обеспечению информационной безопасности на аппаратном уровне: Kontron Security Solution Line (см. врезку «Концепция Secure System и решение APPROTECT от Kontron: основа полной защищённости вашего приложения»). Это широкий спектр защитных мер, таких как защита IP и защита целостности информации, создание лицензий, администрирование и

трекинг, реализация модели лицензирования, а также назначение различных прав доступа. Так мы защищаем вашу критически важную информацию от киберпреступников и закладываем фундамент защищённого будущего «Интернета вещей», что позволит вам отправиться в своё собственное путешествие в мир IoT и достигнуть на этом пути успеха.

Норберт Хаузер | Kontron

Концепция Secure System и решение APPROTECT от Kontron: основа полной защищённости вашего приложения

Kontron APPROTECT – это аппаратно-программное решение, призванное обеспечить полноценную защиту создаваемых вами прикладных систем. Это комбинация двух составляющих – микросхемы аппаратной защиты всех новых продуктов Konton и программного фреймворка.

APPROTECT включает два компонента:

- аппаратный продукт компании Kontron (модуль, материнская плата, система) с встроенным чипом безопасности или с дополнительным комплектом расширения;
- программное обеспечение Kontron APPROTECT.

Это новое решение доступно для всех продуктов Kontron, где оно либо интегрировано в новые изделия Kontron на базе процессоров Intel Core и Xeon 6-го поколения и выше, а также последних поколений Intel Atom, Celeron и Pentium, либо добавляется в существующие приложения, используя специальный комплект расширения.

Аппаратно-программное решение APPROTECT — основа концепции Secure System компании Kontron. Решение APPROTECT проверено на прикладном уровне и доказало свою работоспособность. Для обеспечения всесторонней защиты прикладного ПО решение APPROTECT (чип безопасности плюс программный фреймворк) используется как дополнение к чипу TPM 2.0 (Trusted Platform Module). APPROTECT зашифровывает исходный код прикладной программы таким образом, что становится невозможной его расшифровка. Кроме того, это решение дополнено программой лицензирования (APPROTECT Licensing), которая предусматривает создание новых бизнес-моделей, таких как оплата по факту использования (pay per use), бесплатные пробные версии с ограниченным сроком действия (time based trial versions) или ограничение/расширение возможностей (enable/disable features).

Для процессоров более ранних поколений будет создан комплект расширения (upgrade kit), который обеспечит:

- защиту от копирования информации,
- защиту IP-адреса,
- защиту от расшифровки и фальсификации информации.

Кроме того, будут добавлены возможности лицензирования:

- варианты новых бизнес-моделей (комплекты средств для разработки ПО (SDK) и услуги по интеграции программного обеспечния),
- демо-версии с ограниченными возможностями: по количеству выполнений или по выбору функционала,
- базовая структура программного администрирования.

После покупки Kontron APPROTECT клиенту будет передан новой код для прошивки микросхемы защиты, которая будет установлена специалистами Kontron или самим заказчиком.

НОВОСТИ

Новое будущее «Интернета вещей»: модули COM Express Type10 на Intel Apollo Lake

Компания «РТСофт» и международный холдинг Kontron AG представляют ультрановую серию сверхкомпактных «компьютеров-на-модуле» формата COM Express mini на базе 14-нм процессоров Intel Atom, Celeron и Pentium следующего поколения (ранее известную под кодовым названием Apollo Lake). Диапазон производительности новых «компьютеров-на-модуле» COMe-mAL10 довольно широк и охватывает всю серию новейших встраиваемых процессоров Intel, готовых к использованию в рамках «Интернета вещей» (IoT): от Atom E3900 и Celeron N3350 до Pentium N4200.

Модули COMe-mAL10 поставляются как в двухъядерной, так и четырёхъядерной конфигурации.

«Компьютеры-на-модуле» COMe-mAL10 сочетают в себе современные графические технологии с высокой производительностью в энергоэффективном формфакторе COM Express mini Type10. Пользователи новых модулей получают преимущество в виде значительного прироста вычислительной мощности, впечатляющей производительности в расчёте на ватт и длительного жизненного цикла изделия, характерного для всех встраиваемых решений Kontron.

Технология Intel Time Coordinated Computing Technology, разработанная специально для «Интернета вещей» и интегрированная в модули, координирует и синхронизирует процессоры в сети IoT в пределах миллисекунды. Это не только повышает надёжность, но и обеспечивает возможность работы в инновационных приложениях с более высоким уровнем требований.

Типовые области применения новых мини-модулей COM Express – мобильные портативные устройства, блоки управления и информационно-развлекательные системы на транспорте. Мощные и при этом крайне миниатюрные модули найдут применение в средствах диагностической визуализации в медицине, приборах наблюдения и устройствах безопасности, на промышленных предприятиях, в шлюзах для «Интернета вещей», а также в иных решениях.

Кроме того, версии модулей промышленного класса, предназначенные для эксплуатации в диапазоне температур от –40 до +85°C, оснащённые модулем памяти с поддержкой ECC и рассчитанные на длительную эксплуатацию в течение нескольких десятилетий, удовлетворяют жёстким требованиям приложений в системах безопасности и транспортных средств.

Применяя COMe-mAL10 в своих проектах, разработчики могут воспользоваться всеми преимуществами обширной экосистемы x86-архитектуры и ведущего мирового встраиваемого стандарта COM Express. При помощи нового модуля можно осуществить модернизацию существующих систем без необходимости замены платы-носителя или прикладного программного обеспечения. Кроме того, клиенты могут воспользоваться услугами «РТСофт» по разработке программных и аппаратных средств, чтобы более оперативно, бюджетно и эффективно создавать свои конечные системы.

Дополнительным преимуществом для разработчиков является интегрированное в модулях встраиваемое аппаратно-программного решение для обеспечения безопасности Security Solution Approtect.

Закажите бесплатный тест-драйв!

Александр Ковалев,
директор по развитию

СДЕЛАНО В РОССИИ

прочный · легкий · тонкий · надежный

мультидисплейный · сетевой · бесшумный · бюджетный

BLOK

Российские безвентиляторные ультратонкие компьютеры высокой надежности для ответственных систем с длительным жизненным циклом в формате 19" BoxPC класса SWaP-C Premium: энергетика, оборона, транспорт

Сделано для АСУ ТП
BLOK Industrial
ЛКЖТ.466259.012ТУ

Группа 1.1-1.4.1, 2.1.1, 2.3.1
ГОСТ РВ 20.39.304
BLOK Rugged
ЛКЖТ.466259.023ТУ

- Intel Embedded Xeon/i7/i5/i3 до 3,7 ГГц
- До 32 ГБ SDRAM
- 4 x GEthernet & 6 x USB & HD Audio
- 3 x DisplayPort до 4K
- 2 x SATA III 2,5" SSD/HDD
- 2 x PSU 220 AC Auto
- 2 x mPCI Express & SIM
- 2 x RS232 с гальваноразвязкой
- Работа: -10+50°C (E1) / -40+70°C (E2)
- Удар: до 75 g
- Вибрация: 5 g/0,5-500 Гц
- MTBF: 50 000 часов
- Сертификация BLOK: ТС, ГОСТ Р
- Сертификация "РТСофт": ISO9001, ФСТЭК, Ростехнадзор
- Срок поставки: 0-16 недель

ЗА ИМПОРТОЗАМЕЩЕНИЕ ПРОГРАММА

COM Express

http://blok.rtsoft.ru

RTSoft

Не является публичной офертой, определяемой положениями Гражданского кодекса РФ.

НОВОСТИ

«Сервер-на-модуле» COM Express Type 7 на Intel Xeon для ускоренного проектирования

«РТСофт» и международный холдинг Kontron AG объявляют о выпуске высокопроизводительной модели COMe-bBD7 в продуктовой линейке «компьютеров-на-модуле» COM Express.

Модуль COMe-bBD7 обеспечивает великолепную производительность серверного уровня благодаря 16-ядерному процессору Xeon серии D-1500 и интерфейсам 10-Гбит Ethernet и PCI Express Gen.3. Теперь отечественные разработчики и OEM- производители могут в короткие сроки создавать перспективные платформы с длительным жизненным циклом для обработки массивов данных с использованием преимуществ технологий виртуализации.

Модуль разработан в формате COM Express basic (125 мм × 95 мм) в соответствии с обновлённой редакцией международного стандарта COM Express (PICMG COM.0, Rev. 3.0), в котором утверждена новая спецификация Type 7.

«Распиновка» сигналов для COM-модулей Type 7 утверждена в спецификации международного стандарта COM Express наряду с существующей спецификацией Type 6. В то время как COM-модули Type 6 предназначены для графических приложений, поддерживающих аудио- и видеоинтерфейсы, Type 7 разработаны для высокопроизводительных вычислительных платформ, не требующих поддержки графики.

Поддержка четырёх высокоскоростных интерфейсов 10-Гбит Ethernet, интерфейса NC-SI и 32 линий PCI Express в спецификации Type 7 предоставляет разработчикам богатый выбор для создания платформ серверного уровня, требующих высокой скорости передачи данных и пропускной способности сети.

COMe-bBD7 оснащён центральным процессором уровня ЦОД с производительностью от 4 до 16 ядер Intel Xeon с максимальным теплопакетом (TDP) от 25 до 45 Вт соответственно. Надёжность работы этого модуля в сочетании с поддержкой 2 портов 10-Гбит Ethernet позволяет использовать его в приложениях, где высокая производительность и сверхкомпактные размеры системы ставятся во главу угла.

COMe-bBD7 обеспечивает возможность конфигурирования линий PCI Express Gen.3 вплоть до канала PCIe x24 для высокоскоростных подключений устройств ввода-вывода. Модуль отлично сбалансирован с точки зрения процессора и памяти и поддерживает до 32 Гбайт ОЗУ DDR4 SODIMM с функцией ECC и без ECC.

Модуль Kontron COMe-bBD7 доступен также в промышленном исполнении для работы в диапазоне от –40 до +80°C, что делает его превосходным решением для приложений, работающих в жёстких условиях эксплуатации. Архитектура модуля гарантирует его совместимость с самыми различными операционными системами класса Linux, Windows Server 2008 R2 SP1/2012/2012 R2, Windows 7, 8.1, 10, а также VxWorks и QNX.

Дополнительную информацию о COMe-bBD7 можно получить на сайте, а также в офисах компании «РТСофт», стратегического партнёра холдинга Kontron в России и странах СНГ.

15 лет архитектуре и аппаратной платформе ATCA: возможности использования в настоящее время

Марк Овергаард | Pentair Electronics Protection

Стандарт ATCA (Advanced Telecommunications Computing Architecture) был принят в конце 2002 года. С тех пор в мире были реализованы миллионы ATCA-совместимых устройств на миллиарды долларов. Основная часть этих устройств была востребована индустрией телекоммуникаций. Однако область применения этого стандарта не исчерпывается одним лишь телекомом – есть и другие приложения, которые, несомненно, только выигрывают от использования архитектурных достоинств ATCA.

Что представляет собой уровень управления аппаратной платформой (HPM – Hardware Platform Management) в архитектуре ATCA? Вот краткий обзор основных элементов и функций в архитектуре ATCA HPM:

- **Управляющий модуль шасси** (Shelf Manager) (с возможным горячим резервированием) в каждом шасси для наблюдения и управления функционированием одного шасси, а также для представления этого шасси на более высоких уровнях управления.
- Логический **Системный менеджер** (System Manager) – это более высокий уровень управления в рамках архитектуры ATCA для организации работы одного или нескольких (возможно, десятков или сотен) шасси на предприятии.
- **Локальные управляющие контроллеры** (MC – Management Controller), встроенные в каждый (установленный в шасси) динамически сменный модуль (FRU – Field-Replaceable Unit) с поддержкой управления аппаратной платформой, которые представляют соответствующий FRU на более высоком уровне управления. Например, контроллеры IPMC (один из типов локальных управляющих контроллеров) представляют ATCA- платы или другие динамически сменные модули (FRU) для Управляющего модуля шасси. В то же время, модули MMC представляют модули AMC (другой тип локальных управляющих контроллеров) для соответствующего контроллера IPMC на той ATCA-плате, где установлены данные AMC- модули.
- Дублированная шина Intelligent Platform Management Bus (IPMB-0, на основе I2C) для связи между Управляющим модулем шасси и контроллерами IPMC, которые управляют динамически сменными модулями (FRU) этого шасси.
- Дублированное Ethernet-соединение для связи между платами и внешними ресурсами, предназначенное для общего контроля и управления, включая взаимодействие между **Системным менеджером** и **Управляющим модулем шасси**.

На **рис. 1** показано, что **Системный менеджер** (System Manager) может включать в себя приложения на базе интерфейса HPI (Hardware Platform Interface). Это дополнительный API-интерфейс, который был разработан консорциумом Service Availability Forum. HPI часто используется в системах ATCA в качестве интерфейса между **Системным менеджером** и **Управляющими модулями** тех шасси, которые контролирует данный **Системный менеджер**. Для поддержки таких конфигураций **Управляющий модуль шасси** может включать в себя встроенный HPI-сервер.

Также на **рис. 1** представлены основные спецификации, которые определяют ATCA и связанные с ними конфигурации. Комплект спецификаций PICMG 3.x определяет общую структуру, в том числе и аспекты управления аппаратной платформой HPM. Группа спецификаций AMC.x описывает модули AMC, которые поддерживают «горячую замену», в том числе и соответствующий HPM-уровень. В архитектуре MicroTCA модули AMC вставляются непосредственно в шасси. Эта архитектура описывается в спецификациях MTCA.x, причём управление аппаратной платформой (HPM) в данном случае основано на стандарте ATCA.

Набор спецификаций HPM.x определяет специфические возможности управления аппаратной платформой (HPM), включая обновление встроенного программного обеспечения и контроллеры IPMC, подключаемые через локальную сеть (LAN). Последняя функция позволяет контроллерам IPMC связываться напрямую по стандартному базовому ATCA Ethernet-интерфейсу в дополнение к шине IPMB-0, что обеспечивает более высокую производительность линии связи для управления (как правило, совместно с другими видами использования Ethernet-соединения).

Одна из конфигураций, основанных на ATCA HPM и отличных от PICMG, – это ANSI/VITA 46.11, системная архитектура для подключения модулей в стандарте VPX, широко используемая во встраиваемых системах для ответственных применений. Заимствуя общую архитектуру и многие аспекты ATCA HPM, стандарт VITA 46.11 ключевым образом адаптирует ATCA HPM к конкретным потребностям VPX-сообщества. Например, ни VPX, ни VITA 46.11 не поддерживают «горячую замену» модулей в работающем шасси. В настоящее время спецификация VITA 46.11 активно распространяется в растущей экосистеме VPX.

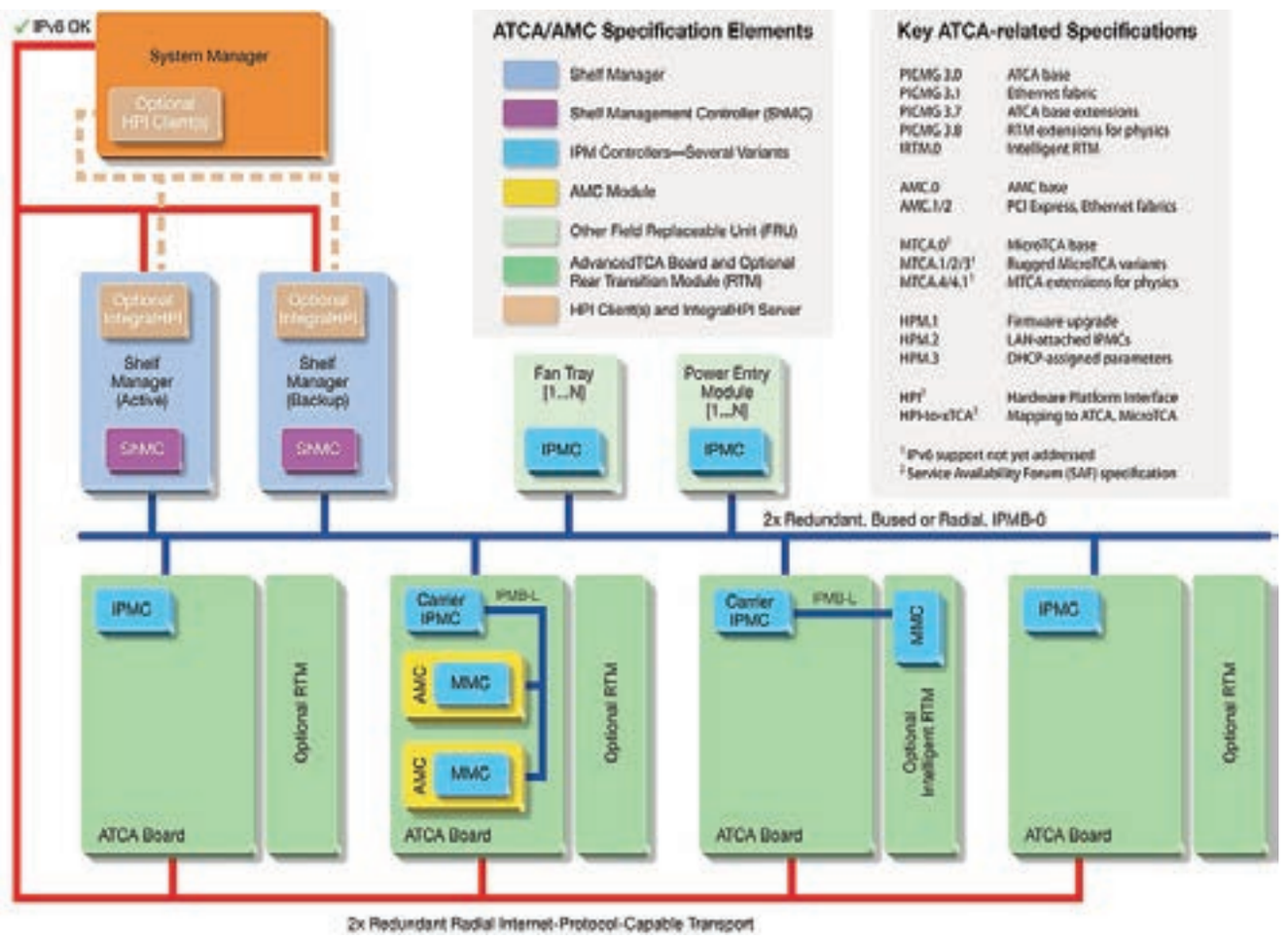


Рис. 1. Архитектура ATCA HPM и основные спецификации

Как можно использовать ATCA HPM в настоящее время

Вариант 1

Напрямую, как есть, использовать в своём проекте базовые стандартные возможности архитектуры ATCA. Высокая производительность и надёжность, высокая готовность и удобства управления в архитектуре ATCA и HPM прекрасно зарекомендовали себя во многих современных приложениях, например для военных линий связи. На основе платформы ATCA построена корабельная и дополняющая её наземная IT-инфраструктура ВМС США. В настоящее время она находится на этапе развёртывания и уже работает на десятках морских кораблей, с потенциалом развёртывания на сотнях судов. В рамках этой программы заключены контракты на миллиарды долларов.

Управление станками для производства полупроводниковых пластин, обеспечение работы серверных систем кабельного телевидения и подсистем безопасности для корпоративных сетей связи – всё это области, в которых возможности архитектуры ATCA отвечают основным потребностям рынка.

Ещё одна сфера активного внедрения решений на платформе ATCA – прикладная физика высоких энергий. Для экспериментов в этой области требуются массивные инструментальные комплексы протяжённостью в несколько километров. Решающее значение для достижения успеха в этом деле имеет высокая готовность, обеспеченная архитектурой ATCA (и также MicroTCA). В спецификации PICMG 3.8 стандартизируются основные расширения ATCA для прикладной физики высоких энергий, в то время как MTCA.4 и MTCA.4.1 играют ту же роль для MicroTCA.

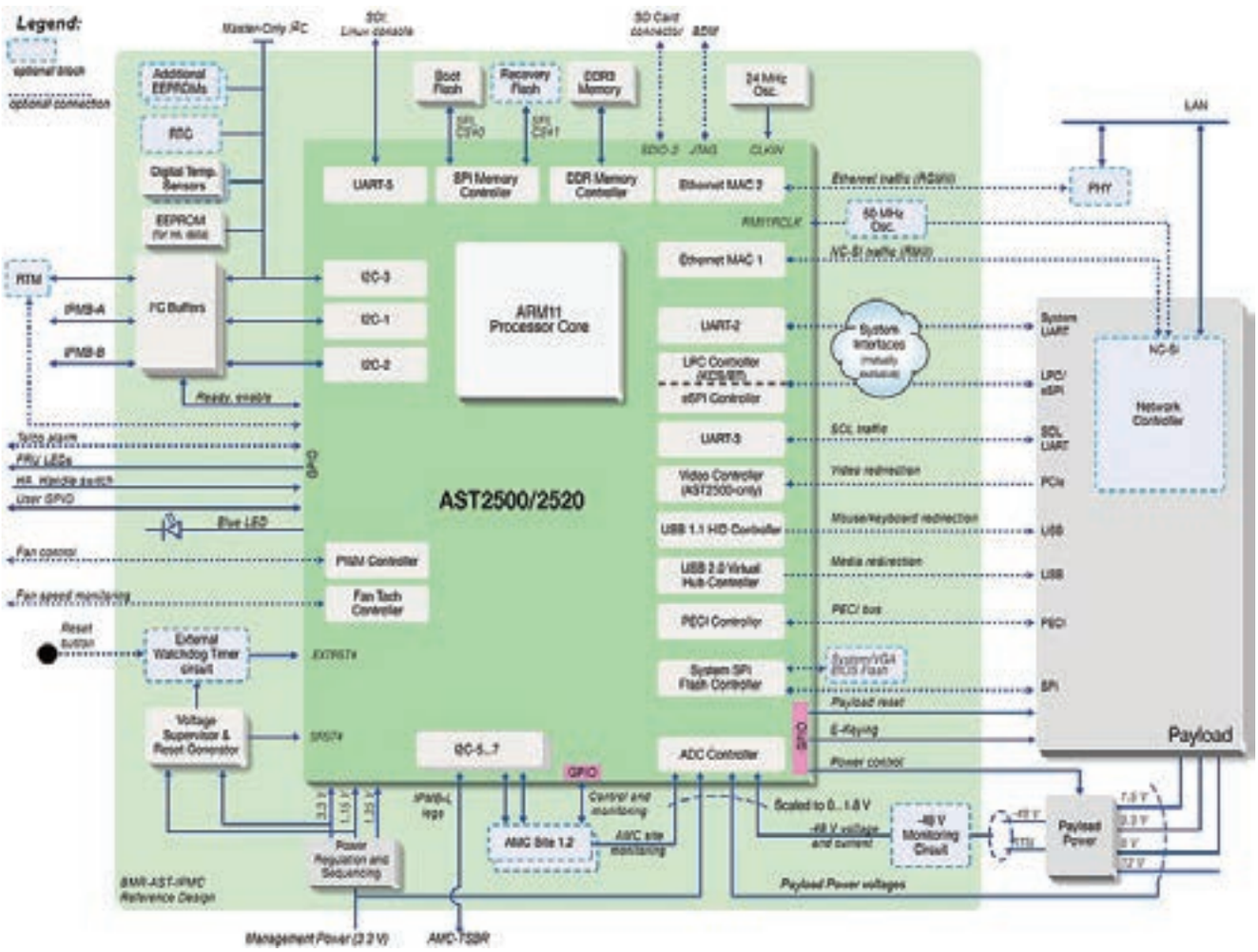


Рис. 2. Базовое техническое решение, предложенное Schroff Pigeon Point для ATCA-совместимых контроллеров IPMC

Обширная ATCA-экосистема шасси, плат (другое используемое название – блэйды, лезвия), а также сопутствующих компонентов, предоставляет поистине широкие возможности выбора аппаратуры для новых проектов.

Вариант 2

Адаптировать и расширить возможности архитектуры ATCA для удовлетворения конкретных потребностей вашего проекта. Один из ярких примеров такого подхода – Juniper (ранее BTI Systems) 7800 Series – облачная масштабируемая открытая сетевая платформа (более подробно описанная в зимнем выпуске журнала PICMG за 2013–2014 гг.). В данной архитектуре успешно поддерживается обратная совместимость с платами ATCA, а специальные слоты обладают важной дополнительной функциональностью, обеспечивающей высокоскоростную передачу данных.

На **рис. 2** показано базовое техническое решение для контроллера IPMC на основе усовершенствованного процессора, разработанного ASPEED Technologies для управления сервером. Предлагаемая схема может быть использована как на совместимых с ATCA модулях FRU, так и в расширенных архитектурах, описанных выше. Это решение доступно в виде схематики, исходного кода встроенного ПО и пользовательской документации в любом из вариантов использования или адаптации ATCA, описанных в данной статье. (Дополнительная информация представлена в журнале PICMG за апрель 2016 года).

Вариант 3

Использовать широкие возможности HPM ATCA, но при этом задать другие аспекты платформы, основываясь на особенностях вашего проекта. Можно полностью принять архитектуру управления, как показано на рис. 1 (в соответствии со спецификацией ATCA), но применить её на физической архитектуре платформы, отличной от ATCA. Например, заказная архитектура может допустить размещение и использование большего количества плат в одном шасси, чем это задано спецификацией ATCA, или может поддерживать альтернативные топологии коммуникации. В другом случае физический размер плат может быть больше или меньше размера ATCA-совместимых плат. Для некоторых компаний максимальное использование проверенной временем архитектуры управления ATCA в сочетании с проприетарными решениями позволяет существенно снизить издержки. Для компаний, выбравших этот вариант, адаптируемые компоненты управления Schroff Pigeon Point доступны для всех элементов архитектуры ATCA HPM.

Источник

http://picmg.mil-embedded.com/articles/atca-its-platform-management-15-years-can-use-now/

Марк Овергаард – архитектор и системный менеджер | Pentair Electronics Protection.

Перевели с английского
Константин Зубрилин | НИВЦ МГУ, Auriga, Inc.
Починок Игорь | НИВЦ МГУ, Auriga, Inc.

Открытые технологические платформы **как глобальный тренд** в области разработки **систем специального** назначения

Виктор Синенко | АО «РТСофт»

Квалифицированные кадры и время – безусловно, самые ценные ресурсы в проектах разработки ответственных аппаратно-программных решений. Возможность сконцентрироваться на конкретных вопросах в рамках собственной специализации – это сокращение проектных сроков и рациональное использование инженерного потенциала команды разработчиков. Один из подходов, увеличивающих таким образом конкурентоспособность и экономическую ценность создаваемых продуктов, рассматривается в данной статье.
Ключевые слова: открытые технологические платформы, встраиваемые компьютерные технологии для спецприменений, ускоренное проектирование аппаратно-программных комплексов.

Технологические платформы и расширение идеологии COTS

В современной экономике оборонно-промышленный комплекс (ОПК) – это не просто научно-производственная база обеспечения национальных вооруженных сил, но прежде всего самостоятельный наукоёмкий высокотехнологичный бизнес с высокой политической ответственностью и колоссальным экспортным потенциалом.

В 20-м веке продукция ОПК представляла собой сплав передовых достижений отраслевых научно-исследовательских и опытно-конструкторских центров и потенциала высокоточного производства, причём доля электронных компонентов и программного обеспечения в составе этой продукции постоянно возрастала. Трендом начала нового тысячелетия стало повышение добавленной стоимости наиболее продвинутых образцов вооружения и военной техники (ВВТ) за счёт использования комплексных услуг от специализированных инжиниринговых и сервисных компаний. При этом наиболее востребованы и успешны те решения и проекты, в рамках которых создаётся действительно эффективный симбиоз разработчиков и производителей ВВТ, с одной стороны, и их партнёров из области передовых информационных технологий (ИТ), с другой.

К числу подобных подходов относится хорошо зарекомендовавшая себя на российском рынке парадигма COTS (Commercial Off The Shelf) – использование готовых коммерческих продуктов «с полки», в рамках которой разработчики выбирают для своих проектов наиболее подходящие и легко интегрируемые базовые решения из числа уже имеющихся на рынке аппаратных средств модульного уровня. Построение более сложных и крупных систем, включая территориально распределённые, вполне может осуществляться по тому же принципу. Главное отличие будет состоять в переносе фокуса внимания разработчика с уровня модулей и плат на уровень устройств – базовых платформенных решений, быстро и эффективно модифицируемых архитектором под конкретную задачу.

Речь идёт о тех случаях, когда разработчики комплексов и систем «не заинтересованы в дискуссиях с ярыми приверженцами конкретных формфакторов или спецификаций, предпочитая решать свои конкретные проблемы независимо от наличия тех или иных ограничений в стандартах и специфика-

циях...» [1]. В таких обстоятельствах услуга по модификации базовой технологической платформы становится ключевым предложением партнёра по ИТ, а гибкость модификации оборудования под множество задач – существенным рыночным преимуществом для разработчика.

Платформенный подход на практике

Для наглядного представления данной концепции рассмотрим разработанную специалистами АО «РТСофт» аппаратно-программную платформу для построения специализированных вычислителей различного назначения **(рис. 1)**. В данном решении используется четыре класса устройств, выполняющих функции строительных блоков проектируемого комплекса или системы:

– блок вычислительный серверный, который предназначен для создания целевых серверных устройств с определёнными функциями (например, универсальный сервер, сервер радиолокационной информации, сервер видеоданных, сервер-коммутатор данных, сервер экрана коллективного пользования, сервер координированного управления и т. д.);
– блок вычислительный операторский, предназначенный для организации клиентских рабочих мест с развитым графическим интерфейсом и прикладным ПО (реализует различные функциональные возможности, в том числе работу с навигационными данными и картографической информацией, управление разнородными корабельными системами и агрегатами);
– блок вычислительный – хранилище данных – для обеспечения надёжного и резервированного хранения больших объёмов информации (включая видеоданные) с доступом по сетям Ethernet 1000Base-T; состоит из устройства управления памятью и устройства хранения данных;
– блок коммутационный – для организации обмена данными и командами управления с периферийными устройствами и взаимодействия смежных систем (системный мост).

Рис. 1. Один из вариантов исполнения блоков Платформы для построения специализированных устройств: серверный блок (слева сверху), операторский блок (справа сверху), коммутационный блок (справа снизу), хранилище данных (слева снизу). Возможна ускоренная кастомизация типов разъёмов, расположения внешних интерфейсов на корпусах блоков или доработка исполнения в соответствии с ГОСТ РВ 20.39.304-98 под требования конкретного проекта.

Блоки Платформы представляют собой наборы COTS-модулей в популярных стандартах встраиваемых систем CompactPCI или CompactPCI Serial (в зависимости от требований проекта и опыта заказчика) в защищённом исполнении. В аппаратной архитектуре блоков платформы традиционная для магистрально-модульных систем гибкость сочетается с повышенной стойкостью к ударным воздействиям и вибрации, пыле- и влагозащищённостью. Конструктив для всех блоков унифицирован – это «Евромеханика» высотой 4U, которая включает блок питания с различными вариантами рабочего напряжения, объединительную плату и интерфейсную панель. Устройства спроектированы с применением принудительного воздушного охлаждения, аксиального либо с забором воздуха через переднюю панель и удалением тёплого воздуха через тыльную панель, что позволяет выдерживать серьёзную тепловую нагрузку до 300 Вт.

Для сопряжения с внешними устройствами в блоках предусмотрено большое количество разнообразных интерфейсов: Ethernet 1000Base-T с возможностью замены на 10GbE,

МКИО, RS232/422/485, USB 2.0/3.0 и других. Расширение или изменение аппаратной конфигурации блоков, добавление аналоговых каналов ввода-вывода, специализированных модулей и интерфейсов может быть достигнуто за счёт применения плат с интерфейсами XMC/PMC.

Отметим, что в зависимости от предъявляемых требований возможна реализация блоков с использованием архитектуры COM Express, обеспечивающей максимальные возможности модернизации и наращивания вычислительной мощности в течение длительного жизненного цикла проектируемых устройств без необходимости изменения интерфейсов, реализованных на плате-носителе COM Express. Хотя о преимуществах такого подхода известно многим разработчикам специализированных устройств, считаем необходимым ещё раз обратить внимание на красоту заложенной в него идеи [2].

Но вернёмся к Платформе и её программному инструментарию. Поддержка функционала блоков Платформы обеспечивается пакетом базового системного программного обеспечения (БСПО) – набором библиотек под ОС МСВС и Astra Linux. С помощью БСПО разработчики могут ускоренно реализовывать функции резервирования каналов передачи данных и взаимодействия с сопрягаемыми устройствами в соответствии со специфическими синхронными и асинхронными протоколами, функции формирования исходящих и обработки входящих потоков данных, поступающих от сопрягаемых систем, а также функции обеспечения взаимодействия алгоритмов прикладного ПО с сопрягаемыми системами. В состав БСПО входят инструменты для создания оболочки программного резервирования вычислительных процессов и разнесения обработки прикладных алгоритмов и системного программного обеспечения на различные процессорные ядра или

Рис. 2. Вычислительные, серверные и коммутационные устройства – это далеко не полный перечень возможных применений аппаратно-программных средств Платформы при построении корабельных систем. Гибкий и универсальный инструментарий позволяет на манер конструктора собирать из исходных базовых блоков системы различных классов.

модули. Также с помощью этих программных средств может быть реализован мониторинг технического состояния блоков.

Для предотвращения несанкционированного доступа предусмотрено использование одного из популярных на рынке модулей доверенной загрузки, сертифицированного ФСТЭК России для применения в автоматизированных системах до класса 1Б включительно, а также по 2-му уровню контроля на отсутствие недекларированных возможностей.

Как удобство разработки способствует повышению экономической эффективности

Основное преимущество, которое получает разработчик при использовании Платформы, заключается в максимальной технологической гибкости, заложенной в её аппаратно-программный инструментарий: целевая система собирается из базовых блоков на манер конструктора **(рис. 2)**. В результате системный архитектор может сфокусировать свой инженерный потенциал на прикладных программных алгоритмах, сопряжении проектируемой системы со сторонними устройствами, контроле соответствия её параметров и логики отраслевым стандартам и внутрифирменным регламентам. При этом все действия по модификации аппаратной части блоков и доработке БСПО осуществляются поставщиком Платформы.

Примером может служить наиболее часто встречающаяся задача подобного рода – ускоренная кастомизация типов разъёмов и расположения внешних интерфейсов на корпусах блоков или доработка исполнения в соответствии с проектными требованиями по ГОСТ РВ 20.39.304-98. В программной части такие работы связаны, как правило, с адаптацией БСПО для обеспечения взаимодействия со специализированными модулями или протоколами передачи данных под популярными на рынке операционными системами семейства Linux , QNX, LynxOS и VxWorks.

Разработчики хорошо знают, что такие технологические операции на этапах проектирования и макетирования ответственных систем требуют затрат большого количества времени и внушительных объёмов финансирования. Однако наличие готового базового инструментария позволяет уйти от разработки «с нуля» и адаптировать готовые инструменты под задание на основе наработанной базы схемотехнических и программных решений. То есть, существенно сократить время и стоимость разработки на старте: так, максимальный период, который компания «РТСофт» стремится обеспечить для модификации блоков и БСПО Платформы под специфические требования, не превышает полугода. Из нашей практики мы можем отметить и другие преимущества использования инструментов Платформы – сокращение затрат на тестирование и обновление БСПО, отладку и модернизацию аппаратных средств, масштабирование системы и снижение её общей стоимости.

Особое значение платформенный подход приобретает в свете отраслевых требований к управлению жизненным циклом продукции и её обслуживанию в течение длительного периода, вплоть до 25 лет, с возможностью своевременной модернизации базовой вычислительной платформы. Довольно ёмко комплексность таких вызовов сформулирована зарубежным экспертом в области встраиваемых компьютерных технологий для спецприменений Дэвидом Пёрсли: «Производительность и надёжность имеют большое значение как для уже развёрнутых, так и для вновь разворачиваемых систем, которые должны постоянно обновляться и совершенствоваться, дабы отвечать современным требованиям в части совместного использования данных, защищённости и производительности. Например, эсминец может пережить первое крупное обновление технологий сразу после его постройки и перед спуском на воду. Его сенсоры и радарные башни навсегда останутся там, где их возвели строители, а вот компьютерные платформы и всё остальное, что подпадает под определение «бортовых ИТ», будут обновляться в промежутках между длительными походами» [3]. Здесь необходимо отметить, что работа с блоками платформы предполагает перекладку «головной боли», связанной с контролем рыночной доступности аппаратных компо-

нентов, обновления БСПО и тому подобных хлопот на плечи сервисного партнёра по информационным технологиям. Разработчик комплекса или конечной системы получает готовые к установке функционального ПО блоки устройств (что особенно ценно с точки зрения минимизации затрат при сопровождении уже поставленной продукции), проводит серию тестов – и оборудование готово к отправке хоть на Кольский полуостров, хоть на берег Южно-Китайского моря. То есть платформенный подход позволяет сохранять высокие уровни готовности, производительности и обслуживаемости систем на протяжении их жизненного цикла.

Мировые тенденции на российской почве

Стремясь идти в ногу с прогрессом, предприятия-разработчики конечных систем могут выбрать один из двух путей: накапливать компетенции в области базовых аппаратных и программных технологий, второстепенных в контексте их основной деятельности, либо использовать готовый базовый инструментарий с опорой на открытые стандарты. Последний, более рациональный и дальновидный сценарий, предполагает возрастание роли консалтинговой поддержки со стороны высокотехнологичных компаний-партнёров, позволяющей на старте разработки минимизировать риски в инженерных стратегиях развития изделия. Данная схема организации взаимодействия между предприятиями-разработчиками и изготовителями спецсистем и сервисными ИТ-компаниями, предлагающими базовые аппаратно-программные платформы в комплексе с услугами по их адаптации под требования проекта, весьма популярна в оборонной отрасли и является одним из глобальных трендов. Например, французская фирма Thales использовала многопроцессорные системы 6U VME немецкого холдинга Kontron на базе процессорных модулей POWERNODE3, PENTXM2 и PENTXM4 для создания многофункциональной РЛС Herakles и инфракрасной системы наблюдения и сопровождения Artemis для французского проекта FREMM [4].

Особенно ярко достоинства платформенного пути проявляются в проектах с несколькими предприятиями-разработчиками, где естественным образом возникает необходимость опоры на удобную для всех сторон унифицированную аппаратно-программную платформу. Так, компания General Electric Intelligent Platforms предоставляет партнёрам по североамериканскому консорциуму разработчиков перспективной авионики FACE процессорные модули 3U SBC312 и 6U SBC625 в стандарте VPX и программные средства разработки, а также соответствующее решение системного уровня FACEREF [5].

Высокую степень экономической привлекательности данного подхода для разработчиков российских систем специального назначения подтверждает опыт работы компании «РТСофт», давно и успешно участвующей в реализации такой модели на практике. Платформенный метод уже нашёл своё применение в проектах создания аппаратно-программных комплексов для информационных и управляющих систем как в наземных пунктах управления разнородными средствами, так и для управления различными корабельными системами, в том числе реального времени. Не исключено, что в условиях растущего объёма государственного оборонного заказа и повышения требований к сопровождению продукции военного назначения на всех стадиях жизненного цикла именно такие способы взаимодействия будут приводить к появлению наиболее конкурентоспособных отечественных систем специального назначения.

Литература

1. Ханер, Ирен. От коммутации к услугам: современный заказчик «тяготеет» к вендорам, способным поддерживать свои предложения услугами по разработке и интеграции готовых аппаратных платформ // Мир компьютерной автоматизации: встраиваемые компьютерные системы. – 2011. – № 6. – С. 34–35.

2. Пёрсли, Дэвид. Стратегии обновления технологий облегчают труд разработчиков военных систем // Мир компьютерной автоматизации: встраиваемые компьютерные системы. – 2012. – № 1. – С. 34–38.

3. http://www.kontron.com/applicationstorydetail/turnkey-platform-for-navy.

4. http://defense.ge-ip.com/news/ge-intelligent-platforms-joins-face-consortium-to-help-drive-innovation-and-lower-cost-for-avionics-systems/n3060.

5. http://defense.ge-ip.com/news/new-rugged-platform-from-ge-allows-face-developers-to-minimize-cost-risk-and-time-to-market/n3013.

Виктор Синенко | АО «РТСофт»

Универсальная вычислительная платформа **«Интегро» для морского** и наземного применения

Эдуард Лиманский | АО «РТСофт»

Универсальная вычислительная платформа (УВП) «Интегро» разработки АО «РТСофт» – новая отечественная аппаратно-программная платформа, предназначенная для создания различных информационно-управляющих систем надводного, подводного размещения, прибрежной инфраструктуры и предприятий судостроения.

Это универсальное решение отвечает повышенным требованиям к надёжности, адаптивности функционала, вычислительной мощности и кибербезопасности, а также высокой производительности при минимальном энергопотреблении в жёстких условиях эксплуатации.

УВП «Интегро» представляет собой линейку встраиваемых цифровых вычислительных средств для построения систем автоматизированного управления и обработки данных с повышенными требованиями устойчивости к воздействиям внешней среды.

УВП построена на основе открытого технологического стандарта и имеет модульную структуру. Вычислительные и коммуникационные характеристики позволяют применять её в качестве отдельного управляющего компьютера, строить системы с резервированием информации, формировать структуры центров обработки данных, а также создавать высокопроизводительные автоматизированные рабочие места операторов или серверы для обработки данных, в том числе больших объёмов графической информации.

Вычислительная платформа «Интегро» обладает широкими возможностями по интеграции с внешними системами, поддерживает совместимость с различными ОС (Alt Linux, Astra Linux, Windows, QNX, «Нейтрино»). Возможность интеграции с сертифицированными коммерческими средствами контроля доверенной загрузки позволяет применять её в системах с повышенными требованиями к информационной безопасности.

Предназначен для построения универсальных серверов сбора и обработки информации. Обеспечивает выполнение серверных функций средней степени нагрузки с небольшим количеством интерфейсов.

Рис. 1. УВП «Интегро» в исполнении Сервер ЛКЖТ.466259.024-021, или сокращённо КВ-021

Предназначен для построения комплексных систем управления техническими средствами. Используется в системах сбора и обработки информации с возможностью коммутации данных от высокоскоростных и специализированных низкоскоростных интерфейсов RS422/485 и МКИО (ГОСТ Р 52070-2003).

Рис. 2. УВП «Интегро» в исполнении Сервер КСУТС ЛКЖТ.466259.024-052, или сокращённо КВ-052

Все изделия УВП «Интегро» предназначены для работы в жёстких условиях эксплуатации (расширенный диапазон температур, повышенная влажность, соляной туман, механические воздействия). Они снабжены встроенной автономной системой контроля технического состояния источников питания и основных электронных модулей с возможностью подключения к внешней системе технической диагностики **(рис. 1, 2)**.

УВП «Интегро» по стойкости, прочности и устойчивости к внешним воздействующим факторам соответствует всем требованиям для аппаратуры класса 2, групп аппаратуры 2.1 и 2.3, групп исполнения 2.1.1 и 2.3.1 по ГОСТ РВ 20.39.304-98 климатического исполнения УХЛ. Стойкость изделия к неблагоприятным внешним факторам, а также применение кондуктивного (безвентиляторного) способа охлаждения позволяют строить на его базе автоматизированные системы как стационарного, так и бортового базирования. При бортовом применении платформы обеспечивается гальваническая изоляция от корпуса сигнальной общей шины устройства.

Важная особенность УВП заключается в том, что все аппаратные модули и программное обеспечение разработаны и произведены в Российской Федерации. Это позволит отечественным предприятиям строить информационно-управляющие системы мирового уровня в рамках программы импортозамещения.

Для решения индивидуальных задач компания «РТСофт» предлагает различные варианты исполнения УВП, с возможностью конфигурирования каждого конкретного изделия, адаптивного наращивания функционала, вычислительной мощности и коммуникационных возможностей конечного устройства. Гибкость адаптации под требования заказчика обеспечивает быстрое изменение конфигурации УВП и запуск изделий в производство с сохранением основных характеристик надёжности и устойчивости к внешним воздействующим факторам. Собственное производство СКБ «РТСофт» готово приступить к выпуску серийных партий изделий в кратчайшие сроки.

«РТСофт» гарантирует неукоснительное соблюдение принципов совместимости и наследуемости применяемых электронных компонентов и системного ПО, а также обеспечивает поддержку длительного жизненного цикла изделий УВП до 10–15 лет, включая гарантийный срок эксплуатации до 5 лет и послегарантийное обслуживание.

Эдуард Лиманский | АО «РТСофт»

НОВОСТИ

IFEC-системы РТСофт на II международном «Авиационном IT-форуме России и СНГ»

В декабре 2016 года АО «РТСофт» совместно с партнёром компанией ООО «СТЭК.КОМ» принял участие во II-м международном Авиационном IT-форуме России и СНГ, где представил бортовые беспроводные системы связи и развлечения (IFEC) для российских авиакомпаний и производителей самолётов.

Организатором форума стал Центр стратегических разработок в гражданской авиации (ЦСР ГА), специализирующийся на вопросах стратегического планирования в гражданской авиации.

Более 100 российских и зарубежных специалистов, включая IT-директоров, руководителей и представителей авиакомпаний, авиапортов и предприятий авиационной отрасли, среди которых Аэрофлот, «Россия», S7, Шереметьево, Домодедово, ОАК, ГСС, Росавиация, SITA и другие, приняли участие в работе форума, ставшего удобной площадкой по обмену опытом и демонстрации новых IT-решений для авиационной отрасли.

В работе форума приняли участие ведущие специалисты «РТСофт»: Александр Ковалёв, директор по развитию бизнеса, Алексей Исаев, директор направления системного ПО, и Юрий Якшин, директор по маркетингу ВКТ.

Повышенный интерес у присутствующих на форуме вызвала экспозиция «РТСофт», особый акцент в которой был сделан на готовые решения в области бортовых беспроводных систем связи и развлечения (IFE & Connectivity) на воздушном транспорте.

Участники форума могли ознакомиться и вживую, при помощи собственных мобильных устройств, протестировать работу IFEC-системы от компании Контрон. Аппаратная часть реализована на основе бортового сервера ACE Flight 4600 и двух беспроводных точек доступа Cab-n-Connect A100. Всё оборудование квалифицировано в соответствии со стандартом DO-160, обладает необходимыми сертификатами и лицензиями для использования в России и за рубежом. Программная часть была представлена в виде популярного приложения компании Axinom.

Форум показал заинтересованность представителей авиакомпаний и производителей воздушных судов в предлагаемых решениях и дальнейшем развитии сотрудничества с «РТСофт» и партнёрами компании.

АО «РТСофт» благодарит организаторов форума и своих партнёров за участие в этом уважаемом в отрасли мероприятии.

УЧЕБНЫЙ ЦЕНТР РТСофт

20 ЛЕТ УСПЕШНОЙ РАБОТЫ В ОБЛАСТИ ПРОФЕССИОНАЛЬНОГО ИТ-ОБРАЗОВАНИЯ

УЧЕБНЫЙ ЦЕНТР «РТСофт»

3500+ СЛУШАТЕЛЕЙ

40+ ПРОГРАММ КУРСОВ

15+ ТЕМ СЕМИНАРОВ

Программы учебного центра по направлениям:

- SCADA-системы и базы данных реального времени
- Системы сбора и передачи информации
- Операционные системы для встроенных и промышленных решений
- Системы управления энергоснабжением: от Microgrid до больших энергосистем
- «Интернет вещей» (IoT) и основы проектирования киберфизических систем
- Информационная безопасность АСУТП
- Индивидуальные программы обучения

По окончании обучения каждый слушатель получает удостоверение о повышении квалификации установленного образца.

ЖДЕМ ВАС В УЧЕБНОМ ЦЕНТРЕ «РТСофт»!

105264, Москва, ул. В. Первомайская, 51
+7 (495) 742-96-55, 742-96-54,
+7 (495) 967-15-05 (многоканальный)
tc@rtsoft.ru | www.rtsoft-training.ru

Лицензия Департамента образования города Москвы № 037032 от 25.01.2016 г.

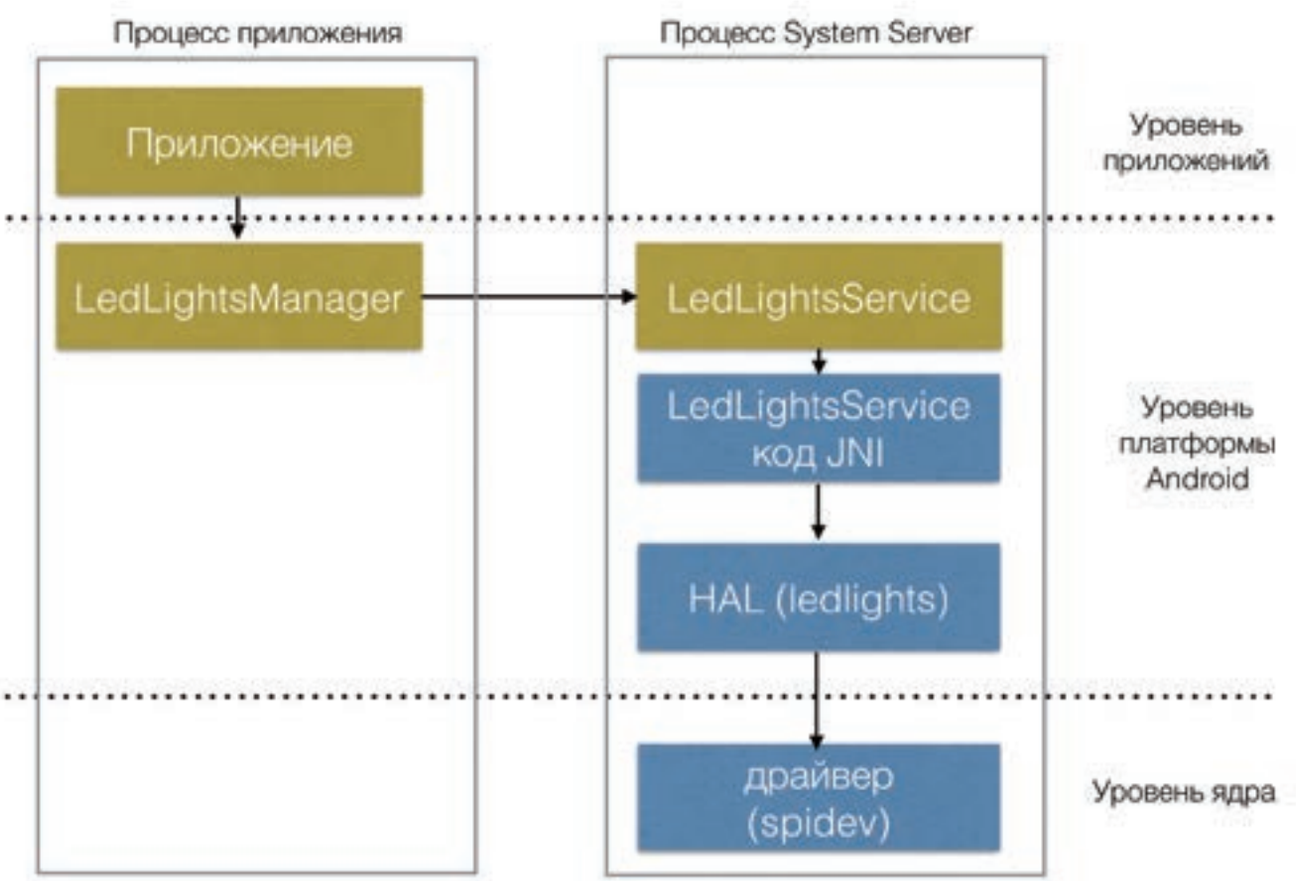
Создание системных сервисов **в Android**

Игорь Марков, Игорь Починок | НИВЦ МГУ, Auriga Inc.

При разработке собственного аппаратного обеспечения для работы с ОС Android возникает вопрос, как управлять этим обеспечением из обычных приложений. В предлагаемой статье пошагово демонстрируется процесс создания системного сервиса, позволяющий приложениям Android управлять подключённым оборудованием.

Допустим, мы хотим создать системный сервис, управляющий десятью светодиодами, подключёнными к основной плате устройства. Аппаратная конфигурация состоит из дополнительного микроконтроллера, который управляет светодиодами. Управление самим микроконтроллером осуществляется по шине SPI по заданному протоколу.

Оставим за рамками статьи аппаратную реализацию устройства, управляющего яркостью светодиодов. Достаточно сказать, что оно ожидает 11 байт по шине SPI, первый из которых – фиксированное значение 0xF0, остальные же – значения яркости 10 светодиодов в диапазоне 0 (не горит) до 100 (максимальная яркость).



Блок-схема программного управления светодиодами в ОС Android

Запрос на установку яркости проходит следующий путь (см. Рисунок):

1. Приложение вызывает метод setLights Java-объекта LedLightsManager.
2. Код этого метода вызывает «связанный» механизмом Binder метод setLights системного сервиса LedLightsService. Этот сервис находится в контексте процесса SystemServer, а не процесса приложения.
3. Код этого метода вызывает метод nativeSetLights, написанный на языке C++.
4. Этот метод, в свою очередь, вызывает функцию liblights_write, находящуюся в модуле HAL (динамически подключаемой библиотеке).
5. В свою очередь, эта функция совершает операцию ioctl над файлом "/dev/spidev0.0".

Эта операция выполняется в коде драйвера spidev, который отправляет данные по шине SPI в микроконтроллер, управляющий светодиодами.

Итак, пошаговая схема действий:

1. Создаём модуль HAL.

Модуль HAL (Hardware Abstraction Layer) – это «драйвер» устройства, работающий в пространстве пользователя (в отличие от драйверов, работающих в пространстве ядра Linux, к которым, как правило, обращается модуль HAL для работы с аппаратной частью).

Код модуля должен располагаться в каталоге *device/<производитель>/<устройство>/ledlights*. Здесь «производитель» и «устройство» заменяем на конкретные названия производителя и устройства, для которого мы создаём модуль HAL. Например, если бы мы создавали модуль для устройства Nexus 5X, то путь выглядел бы как *device/lge/bullhead/ledlights*.

В рассматриваемом случае весь код модуля HAL находится в одном файле ledlights.c и выглядит следующим образом:

```
static int spi_fd;
#define LIGHTS_NUM 10
static int liblights_write(char *buffer)
{
     char cmd[LIGHTS_NUM + 1];
     cmd[0] = 0xF0;
     memcpy(cmd + 1, buffer, LIGHTS_NUM);

     return ioctl(spi_fd, SPI_IOC_MESSAGE(1), &cmd);
}
static int ledlights_open(const hw_module_t* module, const
char* id __unused, hw_device_t** device __unused)
{
   ledlights_device_t *ledlights_dev =
(ledlights_device_t*)malloc(sizeof(ledlights_device_t));
   __android_log_print(ANDROID_LOG_DEBUG, "LEDLIGHTS", "HAL module opened");
   ledlights_dev->common.tag = HARDWARE_DEVICE_TAG;
   ledlights_dev->common.module = (hw_module_t *) module;
   ledlights_dev->common.version = LEDLIGHTS_API_VERSION;
   ledlights_dev->write = ledlights_write;
   *device = (hw_device_t *) ledlights_dev;
     spi_fd = open("/dev/spidev0.0", O_RDWR);
   return spi_fd >= 0;
}
static struct hw_module_methods_t ledlights_module_methods = {
    .open = ledlights_open
};
```

```
struct hw_module_t HAL_MODULE_INFO_SYM = {
    .tag = HARDWARE_MODULE_TAG,
    .module_api_version = LEDLIGHTS_API_VERSION,
    .hal_api_version = HARDWARE_HAL_API_VERSION,
    .id = LEDLIGHTS_HARDWARE_MODULE_ID,
    .name = "LED Lights HAL",
    .author = "Your Name Here",
    .methods = &ledlights_module_methods
};
```

Основной рабочей функцией является ledligts_write, которая отправляет команду из 11 байт по шине SPI на устройство управления яркостью светодиодов.

Функция ledlighs_open инициализирует модуль. Она открывает символьное устройство "/ dev/spidev0.0", которое представляет собой интерфейс к драйверу SPI "spidev", работающему на уровне ядра. Также эта функция инициализирует структуру ledlights_dev, заполняя, в частности, указатели на операции, которые предоставляет данный модуль. В нашем случае это одна функция ledlights_write.

Хотим обратить внимание на структуру HAL_MODULE_INFO_SYM. Она определяет идентификатор модуля HAL и указатель на ledlights_module_methods, которая, в свою очередь, содержит указатель на функцию ledlights_open. Эта структура описывает модуль HAL. Она используется при поиске модуля и для его инициализации.

Файл ledlights.c компилируется в динамически подключаемую библиотеку, модуль HAL.

Для этого необходимо добавить файл сборки Android.mk в *device/<производитель>/<устройство>/ledlights:*

```
LOCAL_PATH := $(call my-dir)
include $(CLEAR_VARS)
LOCAL_MODULE := ledlights.$(TARGET_BOARD_PLATFORM)
LOCAL_MODULE_RELATIVE_PATH := hw
LOCAL_SRC_FILES := ledlights.c
LOCAL_C_INCLUDES := hardware/libhardware
LOCAL_MODULE_TAGS := optional
LOCAL_SHARED_LIBRARIES := liblog
include $(BUILD_SHARED_LIBRARY)
```

Описание же структуры ledlights_device_t и констант LEDLIGHTS_HARDWARE_MODULE_ID и LEDLIGHTS_API_VERSION определяются в файле "hardware/libhardware/include/hardware/ledlights.h":

```
#define LEDLIGHTS_HARDWARE_MODULE_ID "ledlights"
#define LEDLIGHTS_API_VERSION HARDWARE_MODULE_API_VERSION(1,0)
struct ledlights_device {
   struct hw_device_t common;
   int (*write)(char *buffer); // buffer is 10 bytes
}
typedef struct ledlights_device ledlights_device_t;
```

Данный заголовочный файл используется также и в JNI-части системного сервиса, позволяющего управлять светодиодами.

2. Создаём системный сервис.

Этот сервис состоит из двух частей: части JNI(Java Native Interface), которая расположена в файле "com_android_server_LedLightsService.cpp" в каталоге "frameworks/base/services/core/jni", и части на языке Java.

Основные функции JNI-части:

```
static ledlights_device_t * device;
     static jint initHAL(JNIEnv *env, object clazz)
{
            hw_module *module;
            int res = hw_get_module(LEDLIGHTS_HARDWARE_MODULE_ID,
            (const hw_module_t**)&module);
            if (res == 0)
              res = module->methods->open(module, LEDLIGHTS_HARDWARE_MODULE_
              ID, (hw_device_t**)&device);
            return res;
}

static jint nativeSetLeds(JNIEnv *env, jobject jobj, jbyteArray jarr)
{
        int res = -1;
        jbyte *buf = env->GetByteArrayElements(jarr, NULL);
        if (buf) {
          res = device->write((char *)buf);
          env->ReleaseByteArrayElements(jarr, buf, JNI_ABORT);
        }
        return res;
}
```

Эти функции будут использованы из кода сервиса, написанного на языке Java.

Код сервиса frameworks/base/services/core/com/android/LedLights.java:

```
public class LedLightsService extends ILedLightsService.Stub {
     private native int nativeSetLeds(byte[] leds);
     public boolean setLights(byte[] leds) {
        if (leds.length != 10)
          return false;
        return nativeSetLeds(leds) >= 0;
     }
   }
```

Это код системного сервиса, выполняющегося в контексте процесса SystemServer. Данный процесс включает в себя десятки других системных сервисов, таких как сервис местоположения, ввода, управления WiFi, телефонией, питанием, и т. п.

Регистрация нашего нового сервиса осуществляется добавлением следующих строк в метод startOtherServices в файле "frameworks/base/services/core/com/android/server/SystemServer.java":

```
try {
     Slog.i(TAG, "LedLights Service");
     ServiceManager.addService(Context.LEDLIGHTS_SERVICE,
       new LedLightsService() );
} catch (Throwable t ) {
            reportWtf("starting LedLightsService", t);
}
```

Чтобы к сервису можно было обращаться из других процессов (приложений), создадим интерфейс к сервису в новом файле "frameworks/base/core/android/hardware/ILedLightsService.aidl":

```
package android.hardware;
/** @hide */
interface ILedLightsService
{
   oneway boolean setLights(in byte[] leds);
}
```

Этот интерфейс написан на языке Android Interface Definition Language и описывает единственный доступный метод сервиса, setLights.

Создадим также идентификатор для поиска системного сервиса. Для этого добавим в файл "frameworks/base/core/android/content/Context.java" строку:

```
public final String LED_SERVICE = "led_service";
```

3. Создаём вспомогательный класс управления сервисом.

В принципе, этого уже достаточно для того, чтобы нашим сервисом можно было пользоваться из других приложений. Но для удобства создадим вспомогательный класс LedLightsManager, который облегчит доступ к сервису.

Код класса:

```
public class LedLightsManager {
     private static LedLightsManager sInstance;
     private static ILedLightsService sServiceInstance;
     public static LedLightsManager getInstance()
     {
     if ( sInstance == null ) {
            sServiceInstance  = ILedLightsService.Stub.
asInterface(ServiceManager.getService(Context.LEDLIGHTS_SERVICE));
            if (sServiceInstance != null)
            sInstance = new LedLightsManager();
     }

     return sInstance;
     }
     public boolean setLights(byte[] leds) {
       try {
       return sServiceInstance.setLights(leds);
     } catch (RemoteException e) {
```

```
            return false;
            }
        }
    }
```

Класс расположен в файле "frameworks/base/core/android/app/LedLightsManager.java".

Стандартный способ в ОС Android для получения объекта для доступа к системному сервису из обычного приложения это вызов Context.getSystemService(<идентификатор_сервиса>);

Для того чтобы обеспечить возможность получать наш объект класса LedLightsManager таким образом, добавим следующие строки в секцию static в файле "frameworks/base/core/android/app/SystemServiceRegistry.java":

```
registerService(Context.LEDLIGHTS_SERVICE, LedLightsManager.class,
          new CachedServiceFetcher<LedLightsManager>() {
               @Override
                 public LedLightsManager createService(ContextImpl ctx) {
                    return LedLightsManager.getInstance();
               }
          });
```

4. Собираем прошивку.

Подготавливаем проект к сборке следующей последовательностью команд:

```
. build/envsetup.sh
lunch
make -j40 update-api
```

После этого, соберём проект AOSP командой "make -j40". Обновим прошивку устройства одним из двух методов:

1. Перегрузим устройство в режим fastboot командой "adb reboot bootloader". Запишем собранный образ system.img в раздел system: "fastboot flash system system.img; fastboot reboot".
2. Либо обновим содержимое раздела system командами "adb root; adb shell stop; adb remount; adb sync; adb shell start".

Так как появились изменения в системном интерфейсе (API), то соберём Android SDK командой "lunch sdk-eng; make -j40 sdk". При использовании собранного таким образом SDK будут доступны константа Context.LEDLIGHTS_SERVICE и класс LedLightsManager.

5. Создаём приложение.

После обновления прошивки, светодиодами можно управлять из любого приложения. Достаточно использовать следующий код в любом классе, производном от Activity или Service:

```
LedLightsManager manager = getSystemService(LEDLIGHTS_SERVICE);
manager.setLights(new byte[] {100, 0, 0, 0, 100, 100, 0, 0, 0, 100});
```

Игорь Марков | НИВЦ МГУ, Auriga Inc.
Игорь Починок | НИВЦ МГУ, Auriga Inc.

Организация эффективного и **надёжного энергоснабжения** судостроительных предприятий

По материалам АО «РТСофт»

Любое предприятие судостроительного комплекса тратит огромное количество электроэнергии на освещение цехов, верфей и доков, на обеспечение работы специального профессионального электрооборудования и грузоподъемных механизмов, а также отопление, водоснабжение и другие производственные нужды. Поэтому снижение затрат на закупку электроэнергии становится одним из важнейших факторов рентабельной работы как крупных кораблестроительных корпораций, так и небольших заводов. Одна из реальных возможностей не только снизить производственные потери и улучшить качество электроэнергии, но и заработать на её правильном перераспределении – внедрить одно из новейших решений по управлению локальной энергосистемой предприятия.

Информационно-управляющая система, разработанная в компании «РТСофт», обеспечивает координированное управление составляющими энергосистемы предприятия. Оптимизация электроснабжения происходит за счёт двух факторов: обеспечения управляемого снижения потребления и уменьшения затрат на закупку электроэнергии. С помощью решения, предлагаемого «РТСофт», осуществляется управление различными элементами локальной энергосистемы, а именно: накопителями энергии, интегральными нагрузками (вентиляция, кондиционирование, газоудаление, дымоудаление), собственной генерацией, возобновляемыми источниками энергии. Таким образом, обеспечивается контроль потребления энергии из внешней энергосистемы. Например, в периоды времени, когда энергия дорогая, система подключает использование собственной генерации или разряжает накопители, а при снижении цены – увеличивает использование внешней энергии, как для обеспечения производства, так и для зарядки накопителей **(рис. 1)**. Кроме этого система позволяет прогнозировать нагрузку электрической сети. Возможность прогнозирования позволяет в часы пиков потребления в требу-

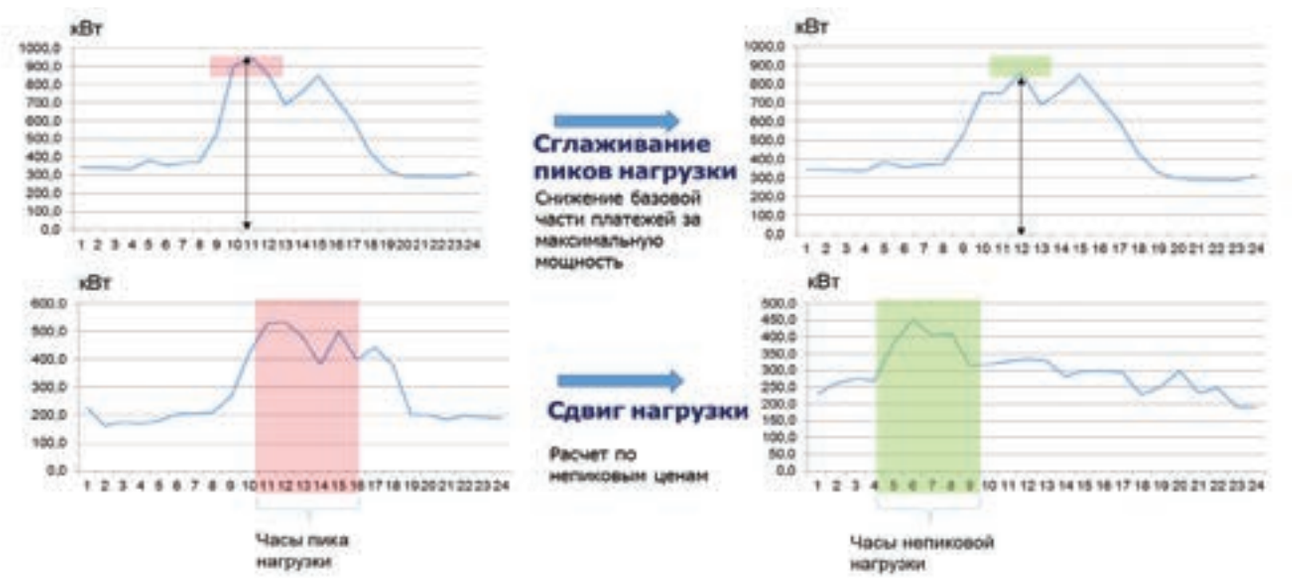


Рис. 1. Сглаживание пиков нагрузки и сдвиги нагрузки во времени

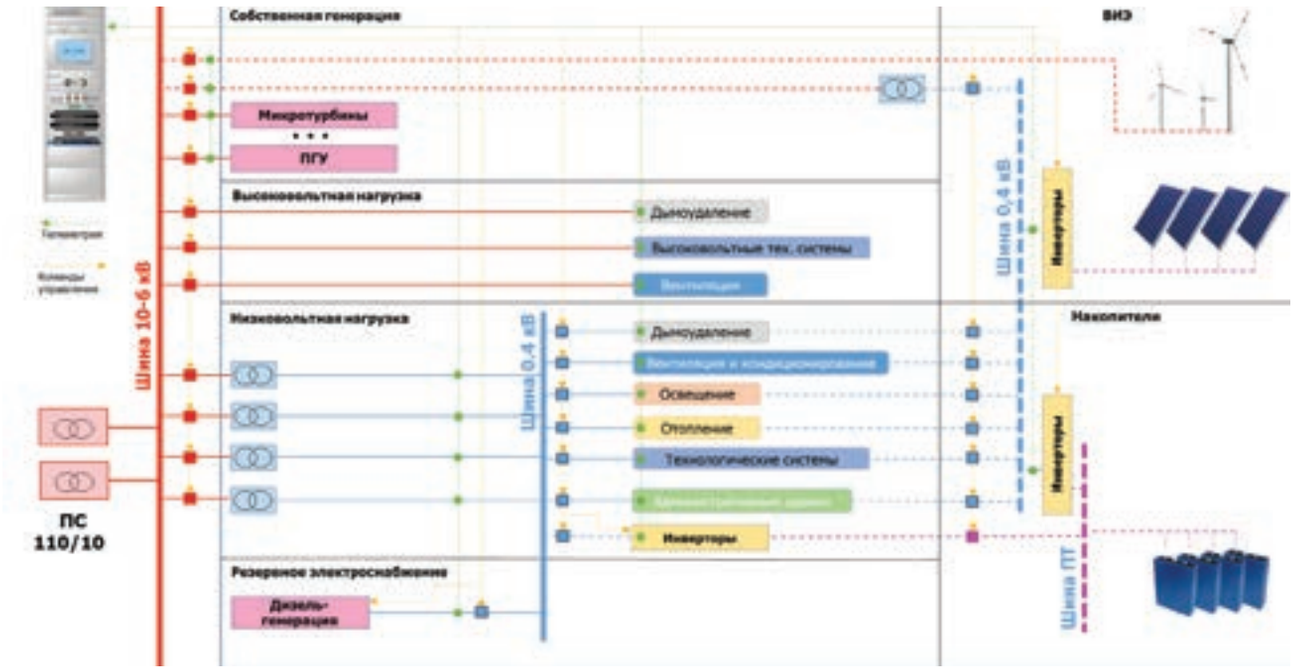


Рис. 2. Примерный вариант системы электроснабжения модернизированного предприятия

емый момент подключить накопитель электроэнергии или собственную генерацию и сгладить таким образом пик нагрузки. Сглаживание пиков потребляемой из внешней сети мощности позволяет избежать перегрузок электросетевого оборудования, а также необходимости оплаты потреблённой сверх меры мощности электроснабжающей организации по более высокому тарифу.

Предприятия, у которых одновременно задействовано множество производственных процессов, например используются мощные электрические двигатели и сварочное оборудование, часто испытывают проблемы с качеством электроэнергии, такие как просадка напряжения при пуске мощных агрегатов, высокие гармоники при сварных работах. Решение позволяет за счёт эффективного управления устройствами компенсации напряжения и реактивной мощности снижать количество внутренних отключений и, соответственно, снижать уровень износа электрооборудования. Кроме того, производство может обеспечить себе дополнительный доход за счёт участия в программе ценозависимого потребления, которая сейчас активно развивается Системным оператором.

Помимо системы управления, компания «РТСофт» предлагает сервисы, в рамках которых можно, с одной стороны, провести анализ проблем электроснабжения предприятия и получить ответ на вопрос, какие средства могут справиться с этими проблемами. Для этого создаётся виртуальная модель энергосистемы, которая показывает, как энергосистема предприятия функционировала до модернизации и как будет работать после внедрения решения. Используя моделирование, можно понять, какое оборудование следует установить дополнительно. С другой стороны, моделирование позволяет просчитать экономический эффект от использования информационно-управляющей системы и выбранного оборудования. В результате могут быть определены капитальные и эксплуатационные расходы на систему в целом и спрогнозирован срок окупаемости, что актуально для менеджмента компании, принимающего управленческие решения.

Решение имеет модульную архитектуру и очень хорошо масштабируется, что позволяет подобрать набор функций системы в соответствии с потребностями клиента. Программное обеспечение, используемое в решении, – полностью российская разработка. Компания «РТСофт» обладает всей кодовой базой решения, что даёт возможность дорабатывать его под индивидуальные требования заказчика.

По материалам АО «РТСофт»

Распределительные сети и Микрогрид

Алексей Небера | АО «РТСофт»
Николай Шубин | АО «РТСофт»

SmartGrid, MicroGrid, возобновляемые источники энергии, синхронизированные векторные измерения – самые обсуждаемые темы в электроэнергетическом мире. На стыке этих новейших энергетических технологий и зарекомендовавших себя современных энергосистем при непосредственном участии потребителей на наших глазах рождается электроэнергетика будущего. Пока не до конца понятно – чем закончится эта встреча хорошего и нового. Приведёт ли она к очередной научно-технической революции и радикальным изменениям привычного энергетического уклада или новейшие технологии будут незаметно поглощены эволюцией развития? Предлагаемая статья не даёт ответа на этот вопрос, в ней обсуждаются конкретные проблемы и возможности трансформации фрагментов современных распределительных сетей в малые распределённые энергосистемы – в MicroGrid (Микрогрид).

Введение

Тенденции развития электрических распределительных сетей (РС) определяются изменяющимися потребностями общества и находятся в зависимости от прогресса электроэнергетического оборудования, технологий потребления электроэнергии, коммуникационных технологий и разнообразных условий территории (климатические, экологические, стеснённость и др.).

Характерные для современного общества потребности и объективные условия, такие как:

- желание людей жить за пределами перегруженных и экологически загрязнённых мегаполисов;
- стремление администраций к выносу промышленности и её инфраструктуры из центра городов и вообще за пределы городской черты;
- рост электровооружённости домашних хозяйств и культурно-спортивно-развлекательных предприятий;
- повышение требований к сокращению времени на технологическое присоединение новых потребительских электроустановок к сети (принцип «время не ждёт»);
- дороговизна и объективно медленные (относительно динамичных потребностей бизнеса) темпы строительства электрических сетей – в совокупности с такими факторами, как:
  - постоянное повышение КПД и встречное снижение себестоимости малой электро-, ко- и тригенерации;
  - расширяющееся рыночное предложение оборудования для возобновляемых источников энергии (ВИЭ) и малой генерации при одновременном росте интереса к этой теме потребителей электроэнергии (потенциальный спрос);
  - наличие в ряде регионов источников относительно дешёвого топлива –

являются движущими силами (драйверами) трансформации существующих РС в относительно независимые **распределённые энергосистемы (РЭ)**, допускающие возможность свободного синхронного присоединения к ним разнообразной малой генерации.

Открытый, постоянно пополняемый список возможных видов малой генерации включает в себя топливные элементы, ветровые турбины, фотоэлектрические и нагревательные солнечные системы, гидравлические, геотермальные и газопоршневые установки, микротурбины, работа-

ющие на газе, в том числе на биотопливе, и другие. В отличие от огромной ЕЭС России и других больших энергосистем, относительно небольшие по мощности РЭ не могут нормально функционировать без двух дополнительных компонентов:

- **накопителей энергии**, способных быстро и точно нейтрализовать небалансы активной и реактивной мощности;
- **системы автоматического управления (САУ)**, обеспечивающей живучесть распределённой энергосистемы на всём множестве схемно-режимных ситуаций, включающем нормальные, ремонтные, аварийные и послеаварийные режимы.

Небольшие автоматически управляемые РЭ, обладающие чёткими территориальными границами, получили название **микрогридов** (МГ). В одной из первых публикаций, посвящённой обсуждаемой теме, – «White Paper on Integration of Distributed Energy Resources. The CERTS MicroGrid Concept» [1], МГ определяется как агрегированное множество нагрузок и микроисточников, управляемых как единая система, производящая электро- и теплоэнергию, обеспечивающая надёжность и безопасность локального потребления. Таким образом, первоначально термин МГ обозначал полностью изолированную локальную систему электроснабжения. В современной трактовке **МГ – это группа распределённых нагрузок потребления и различных энергетических ресурсов – источников и накопителей энергии (электро-, тепло-), объединённых электрической сетью переменного и/или постоянного тока в рамках определённых границ, действующая и воспринимаемая операторами больших энергосистем и центров управления сетями как единый управляемый объект, который можно свободно подключать/отключать к/от электрической сети общего назначения.** При отключении от энергосистемы МГ должен продолжать надёжное и безопасное энергоснабжение своих внутренних потребителей в автономном (островном) режиме с соблюдением нормативных требований к качеству электроэнергии.

Пример МГ приведён на **рис. 1**.

Особенности функционирования и Требования к микрогриду

Наиболее близкими предшественниками МГ являются широко применяемые схемы электроснабжения предприятий с системами гарантированного питания (СГП). Современные СГП работают по логике *или*, при которой электрическое питание либо полностью обеспечивается от сети энергосистемы,

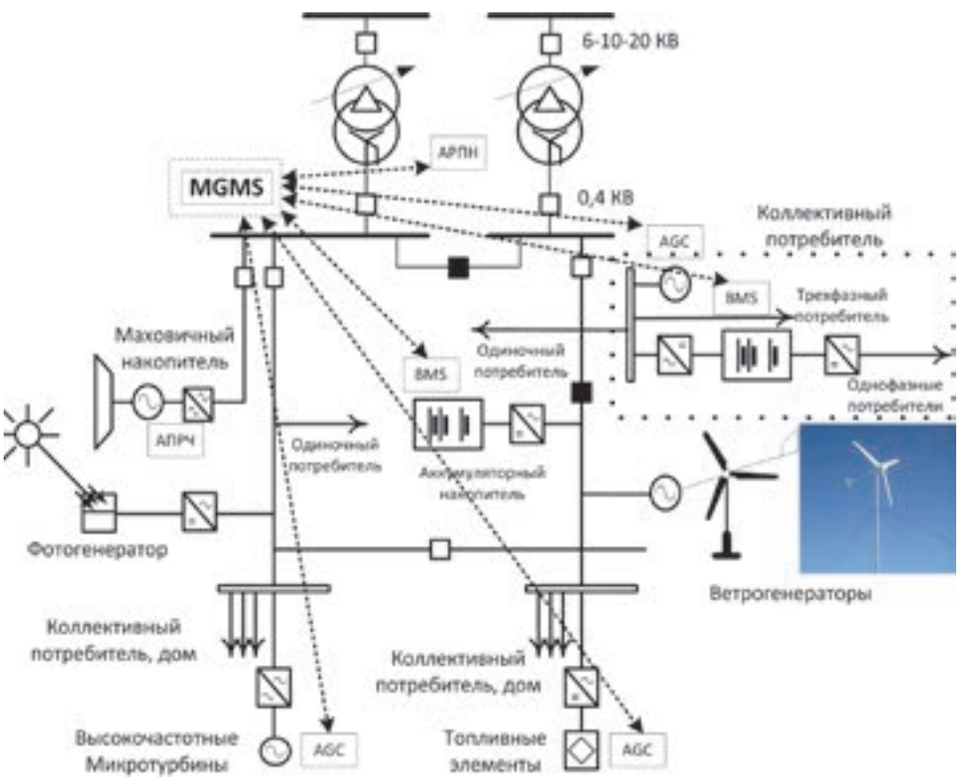


Рис. 1. МГ на напряжении 0,4 кВ

либо – частично или полностью – от внутреннего независимого источника энергии. Таким образом, СГП предназначены для кратковременного частичного замещения основного источника питания на резервный. МГ же, согласно замыслу, разрабатываются для длительной синхронной работы с большой энергосистемой в целях достижения более экономичного и надёжного энергообеспечения внутренних потребителей. Обозначенное существенное различие в предназначении не означает, однако, гигантской технологической дистанции жду СГП и МГ. Для перехода от СГП к МГ требуется решить всего лишь две принципиальные проблемы:

1. Необходимо обеспечить физическую возможность синхронной работы внешней сети и внутренних источников энергии при сохранении способности внутренних источников справляться с заведомо несимметричной и неравномерной во времени потребительской нагрузкой при выделении МГ на автономную работу.
2. Требуется обеспечить экономичность продолжительной работы внутренних источников МГ.

Экономичность внутренних источников микрогрида

Электрический КПД современных газопоршневых установок и газовых микротурбин мощностью от единиц до нескольких сотен киловатт достигает соответственно 43 и 30–33 %, что делает их соизмеримыми по энергоэффективности с газовыми энергоблоками большой энергетики. Это обстоятельство создаёт экономические предпосылки для развития потребительской распределённой генерации. Однако на практике обеспечить экономичную и надёжную работу МГ оказывается не так просто. Дело в том, что при выделении на островной режим генераторы МГ должны питать сильно неравномерную, меняющуюся во времени, нагрузку потребителей **(рис. 2)**. В больших энергообъединениях, крупнейшим из которых является синхронная Зона ЕЭС России, диапазон суточного хода потребления составляет около 20 % от его максимального значения. В РЭ соотношение максимальных и минимальных суточных нагрузок значительно выше – может составлять 3-4 раза и более. Это обстоятельство определяет специфические условия работы генерации внутри МГ.

В современных схемах с СГП «спасаемая» нагрузка потребления полностью ложится на единственный резервный источник (на рис. 2 вариант выбора состава оборудования 1). Очевидно, что в этом случае большую часть времени, кроме кратковременных режимов максимального потребления, питающий генератор будет работать со значительной недогрузкой, то есть неэкономично – в зоне низких КПД. Более того, если на острове имеются двигатели, то для обеспечения нормального режима их пуска или самозапуска потребуется ещё большее завышение мощности резервного генератора, что приводит к ещё большему снижению энергоэффективности.

Повышения экономичности МГ можно добиться путём разукрупнения генерации, а именно: вместо одного источника, покрывающего всё электропотребление, в МГ использу-

Рис. 2. Профиль нагрузки потребления и состав включённого генерирующего оборудования

ется множество мелких. В этом случае общая потребность в мощности обеспечивается более точно и экономично за счёт оптимального выбора состава включённого генерирующего оборудования (ВСВГО), реализуемого в САУ МГ (или MicroGrid Management System – MGMS). На **рис. 2** график включённой генерирующей мощности, формируемый MGMS, представлен вариантом выбора состава оборудования 2 (чёрный пунктир). Автоматическая технология ВСВГО должна включать в себя подсистемы:

- прогноза профиля энерго- и электропотребления;
- определения необходимого резерва мощности, учитывающего:
  - пропускную способность сети МГ;
  - готовность к работе, запасы топлива и допустимую скорость набора/сброса нагрузки на управляемых источниках генерации;
  - вероятные аварийные отключения источников генерации и/или сетевых элементов (принцип N-k).

Уместно добавить, что разукрупнение внутренней генерации МГ способствует не только повышению экономичности, но в ещё большей мере – обеспечению допустимых отклонений частоты при вероятных аварийных отключениях отдельных внутренних источников генерации.

При наличии существенной суточной волатильности рынка электроэнергии, заключающейся в значимом изменении рыночной цены на электроэнергию внутри суток, дополнительный вклад в повышение экономичности работы МГ может внести технология управления спросом (ТУС). Так, при существующем уровне рыночных цен на электроэнергию порядка 1500 руб./МВтч и суточной дифференциации цен (макс.–мин.)/мин. = 40 % годовая экономия от перемещения одного МВтч электроэнергии из пиковой зоны графика суточных цен в провальную даёт при покупке электроэнергии экономию на 1,5 миллиона рублей [2].

Особенности поведения потребления РЭ не исчерпываются одним только большим диапазоном суточного изменения профиля потребления. Сложности в управлении балансами мощности и режимами в МГ создают также:

- большой размах нерегулярных колебаний потребления;
- включение в состав МГ резкопеременной генерации на возобновляемых источниках энергии (ВИЭ), подверженной влиянию случайных метеорологических факторов;
- существенную несимметричность нагрузки и других параметров режима;
- искажение синусоидальности формы переменного напряжения и токов.

Преодоление технических проблем внутренней сети микрогрида

Нерегулярные колебания и интеграция ВИЭ генерации

Нерегулярные колебания потребления активной и реактивной мощности – явления по своей физической сути случайные, то есть величины непредсказуемые. Это означает, что их подавление в режиме планирования графика генерации принципиально невозможно. Если не предпринимать специальных технических и экономических мер, нерегулярные колебания нагрузки МГ будут напрямую транслироваться на такие показатели качества электроэнергии, как частота и уровни напряжения. Такими специальными техническими средствами, эффективно поддерживающими нормальное качество электроэнергии по частоте и уровням напряжения в больших энергосистемах, являются локальные (ОПРЧ – общее первичное регулирование частоты и НПРЧ – нормированное первичное регулирование частоты) и централизованные системы регулирования частоты и мощности. Однако в условиях МГ скорости реакции силовых агрегатов, управляемых такими системами, будут недостаточны для нейтрализации повышенного уровня нерегулярных колебаний. По этой причине компенсация нерегулярных колебаний балансов мощности и напряжения в МГ обеспечивается в темпе процесса быстродействующими динамическими компенсаторами, силовая электроника которых мобильно использует возможности различных накопителей энергии: маховичных, аккумуляторных, суперконден-

саторных и конденсаторных. Обеспечение согласованной работы разнообразных систем регулирования генерации и потребления МГ, включая быстродействующие системы управления накопителями энергии, – ещё одна важная функция MGMS (наряду с функцией ВСВГО). Специфика и подходы к моделированию работы систем смешанного локально-централизованного управления частотой в МГ при их выделении на изолированную работу освещены в [3].

Кроме быстрого и качественного управления балансами мощности, использование накопителей энергии позволяет также дополнительно повысить экономичность работы МГ за счёт снижения включённой управляемой генерации МГ и прохождения экстремальных нагрузок (пики и минимумы) за счёт накопленной или сохраняемой энергии. На **рис. 2** график включённой генерирующей мощности, формируемый MGMS при наличии накопителей, представлен вариантом выбора состава оборудования 3 (красная ступенчатая пунктирная линия).

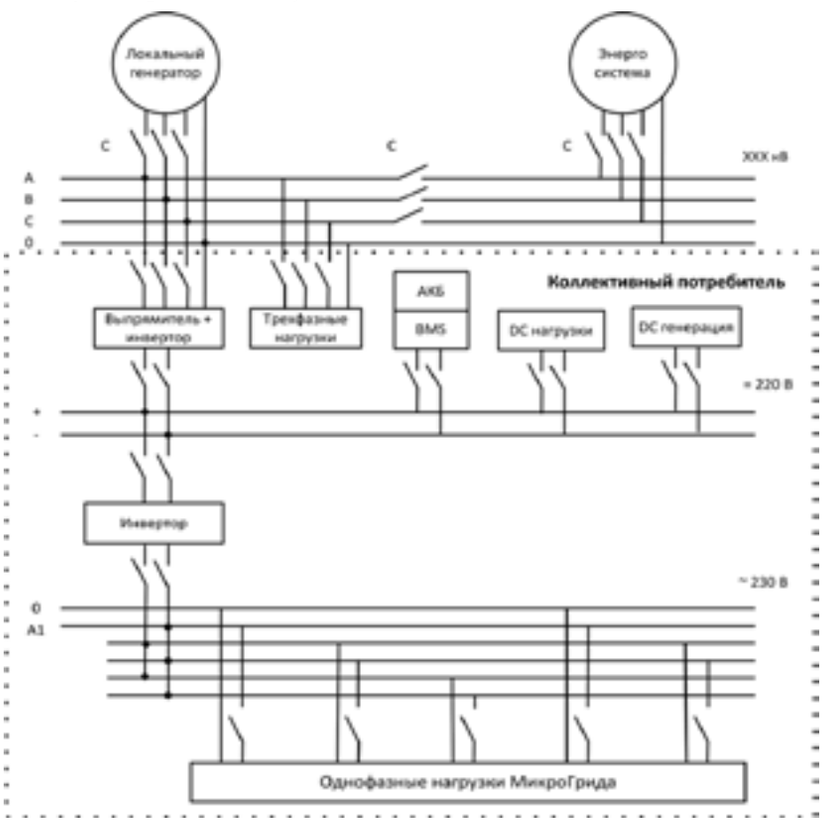


Рис. 4. Пример схемного решения по отделению сети постоянного тока и однофазных нагрузок переменного тока некого коллективного потребителя от основной сети МГ, изображённой на рис. 1

В то же время стабилизирующего эффекта от разукрупнения источников генерации и создания системы смешанного локально-централизованного регулирования режима (в составе MGMS), воздействующей на источники и накопители энергии, может оказаться недостаточно. В этой связи для окончательного преодоления проблем с нестабильностью частоты и напряжений при работе МГ в островных режимах к регулированию необходимо привлекать потребителей энергии. В первую очередь целесообразно обеспечить качественную настройку таких традиционных средств аварийного регулирования частоты (АРЧ), как автоматическая частотная разгрузка (АЧР), дополнительная аварийная разгрузка (ДАР) и частотное автоматическое повторное включение (ЧАПВ). При проектировании и настройке средств АРЧ необходимо учитывать как внешние требования, транслируемые на МГ со стороны Системного оператора, так и внутренние схемно-режимные условия, которые в разных МГ могут иметь существенные индивидуальные особенности. В этой связи потребуется тщательное моделирование режимов внутренней сети МГ с учётом меняющейся частоты и электромеханических процессов.

Другие серьёзные вызовы генерации МГ формируются несимметричностью и нелинейностью нагрузок и других параметров режима сети переменного тока.

Несимметрия и несинусоидальность

Сети низкого напряжения, ввиду большого количества относительно случайно включаемых/отключаемых однофазных нагрузок, являются естественными производителями несимметрий и несинусоидальностей.

Никакое, даже самое тщательное, статическое распределение этих нагрузок между фазами принципиально не может противостоять динамическому нарушению равенства нагрузки

фаз, вызывающему соответствующую несимметричность параметров электрического режима. В то же время для обеспечения надёжной работы и предотвращения сокращения сроков службы трёхфазных электрических машин (генераторы и двигатели) требуется ограничивать разность токов в фазах 10-ю процентами. В режимах с изолированной нейтралью, а именно в таких режимах эксплуатируются электрические генераторы, проблемы создаются так называемыми токами обратной последовательности, вызывающими в машине ряд нежелательных явлений, и делают режим работы машины тяжёлым [4]. В частности, наличие обратной последовательности в магнитном поле статора вызывает:

- излишние потери в роторе (особенно в неявнополюсных машинах), вызванные индуцированными токами двойной промышленной частоты, и его нагрев, сопровождаемый также снижением КПД машины (высокие температуры ротора способны вызывать в нём опасные деформации, что резко повышает вероятность повреждения изоляции обмотки возбуждения);
- повышенную вибрацию машины, появляющуюся в результате взаимодействия магнитных потоков возбуждения и обратной последовательности статора, а также – поля прямой последовательности статора и поля токов двойной частоты ротора (при этих воздействиях на ротор и статор действуют знакопеременные вращающие моменты и тангенциальные силы, пульсирующие с частотой 100 Гц);
- искажение симметрии напряжений. В результате различности падений напряжений в фазах напряжения более загруженных фаз будут несколько ниже, в менее загруженных – выше. Несимметрия напряжений ухудшает условия работы приёмников, в особенности асинхронных и синхронных двигателей.

Высшие гармоники тока могут вызывать опасные резонансные явления, если цепи обмоток статора работают на емкостную нагрузку, формируемую, например, электрическими ёмкостями кабельных линий электропередачи. В результате резонанса напряжений на зажимах обмотки статора возникают напряжения повышенных частот, которые могут превышать номинальные напряжения во много раз и приводить к преждевременному повреждению изоляции машины.

Эффективной формой борьбы с резонансами напряжений в большой энергетике считается применение мощных успокоительных (демпферных) обмоток. Например, демпферные обмотки уникальных мощных гидрогенераторов, работающих на длинные линии передачи (емкостной характер нагрузки), позволяют выровнять сверхпереходные сопротивления генераторов по продольной и поперечной осям, вследствие чего токи остаются синусоидальными и опасность резонансных перенапряжений исчезает.

К сожалению, демпферные обмотки не устанавливаются на малые электрические машины. Поэтому для МГ требуется найти свои методы борьбы с несинусоидальностью.

Радикальным способом преодоления проблем несимметричности параметров режимов и несинусоидальности формы кривых переменных токов и напряжений является физическое отделение трёхфазной генерации от заведомо несимметричных и нелинейных нагрузок. На **рис. 3** приведён пример схемного решения по отделению сети постоянного тока и однофазных нагрузок переменного тока некого коллективного потребителя от основной сети МГ, изображённой на **рис. 1**. Такая схема обеспечивает надёжную изоляцию трёхфазной сети от любой несимметрии и несинусоидальности. Недостатком этой схемы является то, что присутствующие в ней выпрямители и инверторы имеют не стопроцентный КПД. Потери в преобразователях составят около 10 %.

Другие способы борьбы с нарушениями показателей качества электроэнергии предусматривают использование быстродействующих регулируемых компенсирующих устройств: источников реактивной мощности и кондиционеров или динамических компенсаторов искажений напряжений (ДКИН).

Заключение

Потребность общества в расширении жизненного пространства за пределы перегруженных мегаполисов, повышение требований бизнеса к сокращению времени на технологическое присоединение к сетям, дороговизна и объективно медленные темпы строительства электрических сетей, наличие в РФ территорий со стеснёнными условиями, а также удалённых территорий, в том числе с экстремальными климатическими условиями, которые нуждаются в быстром и эффективном развитии, – могут послужить поводом к созданию новой сущности в электроэнергетике – распределённым энергосистемам и, в частности, МГ.

Ввиду особенностей физических процессов, происходящих в сетях среднего и низкого напряжения, МГ не могут быть созданы путём простого присоединения распределённой генерации к существующим РС. МГ – это инновационная технология, предусматривающая создание умной системы автоматического управления (MGMS), взаимодействующей с умными управляемыми энергоустановками генерации и потребления.

Поскольку МГ включает в себя множество разнородных внутренних энергетических источников, управляемых электроустановок потребителей, накопителей энергии и к тому же сам подключён к источникам внешнего электроснабжения, MGMS должна в темпе реального времени решать и технические, и экономические задачи. Технические задачи – по регулированию частоты и напряжения; по обеспечению устойчивости. Экономические задачи – по оптимальному динамическому распределению нагрузки между всеми управляемыми ресурсами.

Наличие интеллектуальной контролирующей, анализирующей, оптимизирующей и управляющей MGMS, наряду с появлением линий электропередачи с двухсторонним питанием, определяет основное отличие МГ от современных РС, внутренних электрических сетей домов и предприятий.

Появление МГ – это значимое явление на современном этапе развития электроэнергетики. МГ позволят:

1. Преодолеть нарастающую стихию неуправляемости режимов в сетях среднего и низкого напряжения. Действительно, МГ проектируются и формируются как агрегаты распределённых нагрузок и генерации, воспринимаемые Операторами энергосистемы и рынка как единые (виртуальные) объекты управления, обладающие внутренним порядком.
2. Усилить конкуренцию «снизу». Причём МГ позволяет не только усилить конкуренцию на площадке генерации, но и распространить конкуренцию в электроэнергетике на электрические сети.

МГ могут найти активное применение в стеснённых условиях мегаполисов, в отдалённых регионах России, в первую очередь в Сибири и на Дальнем Востоке. В регионах, где отсутствует централизованное электроснабжение, на территориях, расположенных вдали от крупных населённых пунктов, на объектах добывающей промышленности, в туристических центрах, на военных объектах и прочих.

Литература

1. Robert Lasseter, Abbas Akhil, Chris Marnay, John Stephens, Jeff Dagle, Ross Guttromson, A. Sakis Meliopoulous, Robert Yinger, and Joe Eto, «White Paper on Integration of Distributed Energy Resources. The CERTS MicroGrid Concept», LBNL-50829, 2002 г.

2. А. С. Бердин, О. Д. Молчан, Н. Г. Шубин, «Об участии потребителей в новом типе управления энергосистемой», журнал «Энергетика и ЖКХ Урала», июль 2013.

3. A. Madureira, C. Moreira and J. Pe as Lopes, «Secondary Load-Frequency Control for MicroGrids in Islanded Operation», 2005 г.

4.Вольдек А. И., «Электрические машины», 3-е издание, переработанное, издательство «Энергия», 1978 г.

Алексей Небера | АО «РТСофт»
Николай Шубин | АО «РТСофт»

RTSoft | ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ И СРЕДСТВА АВТОМАТИЗАЦИИ

БЕЗОПАСНОСТЬ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИХ СИСТЕМ

ПРОГРАММНЫЙ КОМПЛЕКС СРЕДСТВ ЗАЩИТЫ

ПЛАТО-РТ

Предназначен для организации защищенной обработки конфиденциальных данных на объектах критически важных информационно-управляющих систем

// МОНИТОРИНГ ЗАЩИТЫ СЕТИ
// МОНИТОРИНГ ЗАЩИЩЕННОСТИ УЗЛОВ И ПРИЛОЖЕНИЙ
// МОНИТОРИНГ ИНСТАЛЛЯЦИЙ И ОБНОВЛЕНИЙ

ЭЛЕКТРОЭНЕРГЕТИКА | АТОМНАЯ ПРОМЫШЛЕННОСТЬ | НЕФТЕГАЗ | МЕТАЛЛУРГИЯ | ТРАНСПОРТ | ВПК (СПЕЦПРИМЕНЕНИЯ)

АО «РТСофт»
105037, Москва, ул. Никитинская, д. 3 | тел.: +7 (495) 967-15-05 | e-mail: rtsoft@rtsoft.ru | www.rtsoft.ru

Долгосрочное прогнозирование динамики изменения киберугроз **в энергетике методами** имитационного моделирования

Павел Литвинов, Сергей Нестеров | АО «РТСофт»

В настоящей статье рассмотрены способы применения методов имитационного моделирования как инструмента оценки защищённости и оптимизации затрат на мероприятия по обеспечению киберзащиты. Выполнено описание модели, позволяющей оценивать динамику изменения угроз для объектов электроэнергетики на ближайшие десять лет. Приведён пример расчёта для сценария, который авторы считают достаточно вероятным.

1. Введение

Задача обеспечения кибербезопасности АСУ ТП и комплексов релейной защиты и автоматики в силу объективных причин приобретает всё большее значение [1]. Сегодня процессы производства, передачи и распределения электроэнергии существенно зависят от информационных систем, включая и сети передачи данных. Появление и развитие интеллектуальных электроэнергетических систем (ЭЭС) ведёт к централизации контроля и управления, что порождает качественно новые угрозы и риски, поскольку совсем недавно эти функции выполнялись локально и децентрализованно. Такие понятия, как «киберпреступность» и «кибервойны», уже перекочевали со страниц фантастических произведений в ленты новостей.

Очевидно, что устройства и объекты электроэнергетики – чрезвычайно привлекательные цели для атак злоумышленников – как в силу величины прямого ущерба (от возможного повреждения первичного оборудования), так и косвенного (от нарушения энергоснабжения). При этом колоссальный массив уже разработанных стандартов и рекомендаций по информационной безопасности, а также существующих программно-технических средств, предназначенных для построения систем информационной защиты, требует изучения и переосмысления применительно к нашей задаче – защите РЗА и АСУТП подстанций. Прямое следование рекомендациям этих стандартов нецелесообразно, а зачастую и невозможно, поскольку изначально они разрабатывались для защиты и обеспечения информационной безопасности других систем.

В настоящей статье будут изложены общие подходы, позволяющие математически обоснованно построить проекцию основных положений из стандартов, посвящённых вопросам информационной безопасности, на нашу предметную область. Приведена методика построения имитационной модели, показаны первые результаты моделирования и сделанные из них выводы.

2. Постановка задачи

В настоящее время сокращение операционных расходов и увеличение выручки за счёт предоставления новых сервисов возможно главным образом благодаря использованию следующих передовых технологий [2]:
– адаптивная защита,
– распределённая генерация,
– цифровые и гибридные подстанции,

– renewables,
– trigeneration,
– Smart Grid,
– Smart metering,
– Demand response,
– Virtual power plants,
– Smart building.

В этой ситуации для обеспечения необходимого запаса устойчивости необходимо не только иметь намного больше информации от всех узлов энергосистемы, но также и координировать действия значительно большего числа центров управления ЭЭС. Рост уязвимости подобных систем к кибератакам компенсируется использованием новых технологий и средств защиты. Как и в историческом процессе «соревнования» брони и оружия, абсолютного победителя не будет и здесь, потому что на каждом витке технологической спирали будут совершенствоваться способы нападения и изыскиваться адекватные им средства защиты.

С практической точки зрения при планировании технических и организационных мероприятий по обеспечению информационной безопасности возникает оптимизационная задача минимизации затрат при максимальном снижении допустимых рисков и недопущении рисков критических. Оговорка про критические риски является важным граничным условием. В бизнесе невозможно компенсировать все риски, потому что такая линия поведения сделает вашу продукцию и услуги неконкурентоспособными, поэтому какие-то из рисков необходимо осознанно принять. Зачастую допустимо принятие даже части критических рисков. Главное – не допустить катастрофических рисков, при которых возникает прямая опасность для жизни людей или угроза потери бизнеса.

Состав и необходимость дополнительных затрат на оборудование и организационно-технические мероприятия по обеспечению кибербезопасности зависят от адекватности модели угроз и правильности расчёта рисков. Понятие риска относится к многомерным категориям, но в инженерном смысле и применительно к задаче анализа «риск» – это вероятность, умноженная на последствия. В нашем случае, когда речь идёт о киберугрозах, оба этих множителя неизвестны и могут быть оценены лишь приблизительно. В части оценки вероятности мы не можем полагаться на статистику – надёжной статистики применительно к конкретным системам просто не существует в силу ряда объективных и субъективных причин:

– не все инциденты фиксируются, а тем более попадают в открытые отчёты;
– не всегда есть возможность достоверно установить связь технологических сбоев с действиями хакеров, в «продвинутых» атаках обязательным является этап сокрытия следов проникновения;
– потенциально самые опасные атаки реализуются редко или вообще пока не были зафиксированы (по существующей статистике от начала распространения продвинутых вирусов до их обнаружения проходят годы);
– вероятность успешной атаки пропорциональна мотивации и ресурсу нарушителя, что, в свою очередь, является функцией времени и значительного количества событий, которые ещё не произошли и не могут быть достоверно предсказаны.

Что касается оценки ущерба (последствий), то здесь ситуация ещё сложнее. Все энергетические объекты являются сложными системами, поэтому нарушение функционирования любого элемента закономерно отражается на остальных элементах. В силу отсутствия знания о способах и видах будущих атак степень их влияния на другие элементы предсказать сложно. Ещё больше затрудняет оценку тот факт, что в энергетическом секторе сбои могут вызвать каскадный эффект и/или эффект домино – когда проблемы в одной подсистеме незамедлительно или с небольшой задержкой приводят к сбою в зависимых/смежных подсистемах. Нарушение в энергетической инфраструктуре одной страны или региона может спровоцировать развитие каскадного эффекта в такой степени, что в результате пострадает инфраструктура других стран [3].

Безопасность – комплексное и многофакторное понятие, способов атаки и потенциальных уязвимостей – множество и потенциальные злоумышленники будут использовать любое слабое место. Одним из лучших способов достижения пропорциональности и

сбалансированности инвестиций для решения сложных организационно-технических задач является декомпозиция на более простые задачи. С точки зрения математики возможно последовательное применение параллельно-последовательной декомпозиции, а применительно к простым функциям – построение их суперпозиции. В рекомендациях NIST (National Institute of Standards and Technology) «Framework for Improving Critical Infrastructure Cybersecurity» [4] содержится детальное описание процесса такого дробления функций на категории и подкатегории.

Обоснованный способ определения необходимых для моделирования агентов можно заимствовать из стандарта ISO/IEC 27032:2012 «Guidelines for cybersecurity» [5]. Совершенно аналогичную систему понятий безопасности и их взаимосвязи с точностью до тонкостей перевода содержит ГОСТ Р ИСО/МЭК 15408-1- 2012.

Вышеупомянутый стандарт вносит важное расширение в общую модель риска, представляя вероятность как суперпозицию «угроз» и «уязвимостей».

В предметной области менеджмента рисков существует по крайней мере 31 метод, рекомендуемый для поддержки процесса оценки риска [6]. Все эти методы имеют различную применимость и эффективность на разных стадиях процесса: идентификации рисков, анализа последствий, анализа вероятностных характеристик, сравнительных оценок и уровня риска. Применительно к задаче построения модели угроз на начальном этапе идентификации опасностей и риска для людей, оборудования и окружающей среды эффективно использование методологии исследования опасности и работоспособности (HAZOP – Hazard and Operability Study). Сравнительная оценка риска может быть получена моделированием методом Монте-Карло, который является хорошим способом оценки влияния неопределённости параметров системы в широком диапазоне ситуаций, особенно если характер распределения переменных (равномерный, треугольный, нормальный или логарифмический) известен заранее из аналогичных процессов, физического смысла и т. п. Практические рекомендации по использованию этих и других методов можно найти в [7].

Сегодняшняя реальность такова, что даже требования регуляторов не позволяют разработать чёткий план действий по усилению защиты на долгосрочную перспективу. Применительно к нашей предметной области существующие требования:

– не гармонизированы,
– недостаточно конкретны,
– оторваны от технологической специфики,
– неполны или избыточны (не всегда актуальны текущим угрозам),
– а самое главное, не содержат этапности.

Очевидно, что невозможно обеспечить полное выполнение всех требований и рекомендаций в масштабах ЕЭС. Если речь идёт об обеспечении надёжности энергоснабжения, то риски порождаются не только и не столько хакерскими атаками. Это могут быть и выход из строя оборудования или каналов связи вследствие низкой технической надёжности или износа, ошибки настройки и эксплуатации, недостаточный опыт и квалификация персонала, уход специалистов и т. п. При очевидной лимитированности ресурсов требуется «балансировка» расходов между этими направлениями. Никто не доказал, что именно хакеры сейчас – наша главная проблема и угроза надёжности. Отсутствие обоснованных прогнозов порождает неуверенность и, возможно, лишние расходы. С целью оценки динамики угроз во времени и была построена модель.

3. Имитационная модель

3.1. Текущее состояние вопроса

Тема потенциала использования агентного моделирования энергетических систем в контексте кибербезопасности давно обсуждается в научном сообществе. Можно рекомендовать работы зарубежных [8] и российских авторов [9], каждая из статей содержит обширный список литературы для знакомства с историей и текущим состоянием вопроса.

Несмотря на многолетний опыт исследований, отдельные положительные результаты и очевидную полезность, методы имитационного моделирования вопросов информаци-

онной безопасности в силу ряда объективных и субъективных причин [10] не получили широкого практического применения.

3.2. Оценка изменения рисков во времени через динамику изменения количества киберугроз, числа устройств, мероприятий по защите, вероятности наличия уязвимостей и предполагаемого профиля злоумышленника

Далее предлагается описание и результаты выполнения расчёта на разработанной авторами имитационной модели (рис. 1) прогноза количества взломов устройств РЗА на ближайшие 10 лет в разбивке по месяцам, построенной с применением метода системной динамики. На этапе проработки концепции модели было принято решение использовать программное обеспечение AnyLogic, тем более что, в силу относительной простоты первого этапа моделирования, достаточно возможностей бесплатной версии Personal Learning Edition.

3.2.1. Параметры модели

Ниже приведён список параметров, использованных для масштабирования и первоначальной настройки модели:

– HackerAtBegining = 50 – первоначальное количество злоумышленников, включая и инсайдеров;

– DeviceAtBegining = 20 000 – первоначальное общее количество устройств, подверженных взлому;

– VulnerabilitiesAtBeginning = 0,4 – первоначальная доля устройств, имеющих уязвимости любого рода: от ошибок в реализации и/или закладок производителей до слабых паролей администратора;

– CrackProbabilityFactor = 0,00001 – фактор вероятности успешного взлома.

3.2.2. Табличные функции

Нижеперечисленные табличные функции были использованы для того, чтобы задать прогнозное развитие событий на ближайшие 120 месяцев. Желаемая форма кривой и коэффициенты задавались в отдельных точках, для вычисления остальных значений в модели использовалась интерполяция. Вид интерполяции (ступенчатая, линейная или сплайн)

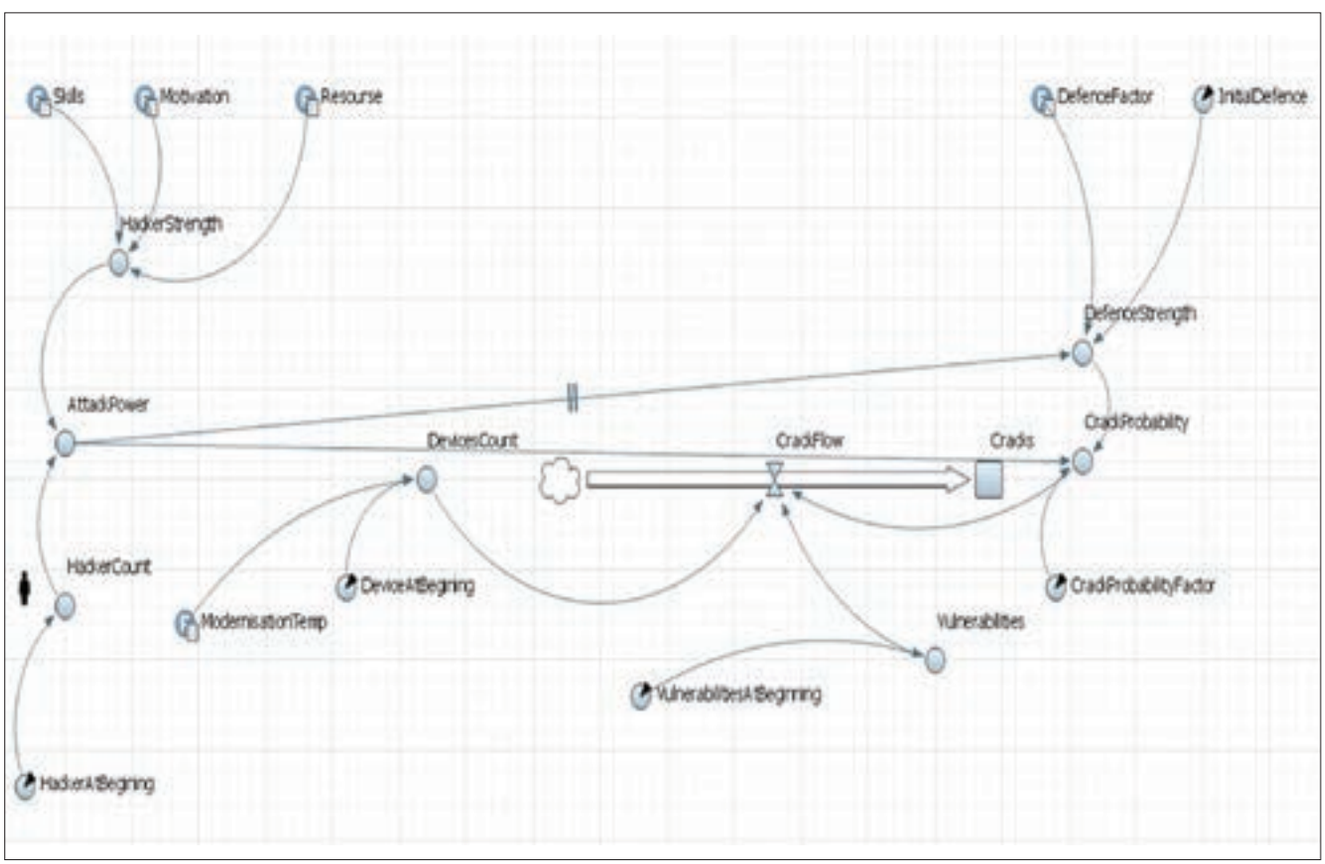


Рис. 1. Динамическая диаграмма

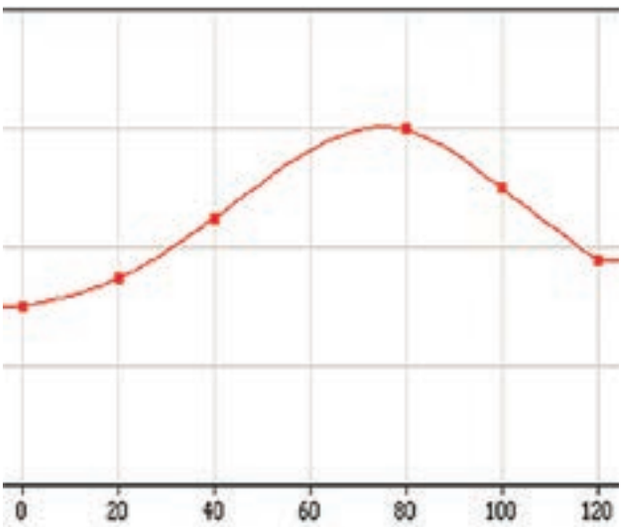


Рис. 2. Опыт хакера

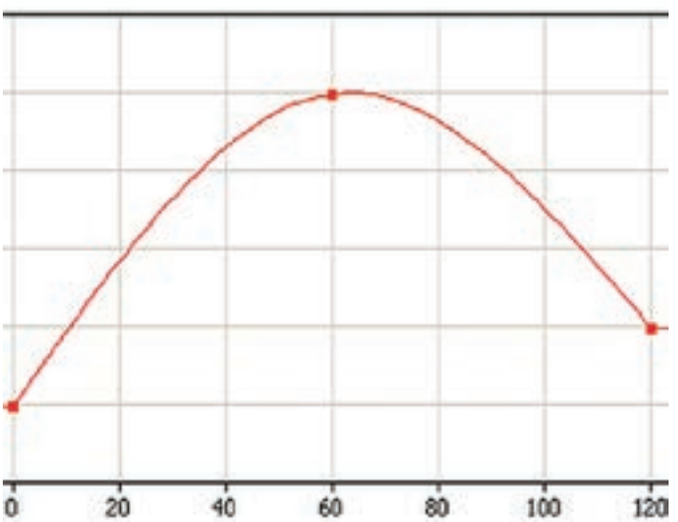


Рис. 3. Мотивация злоумышленника

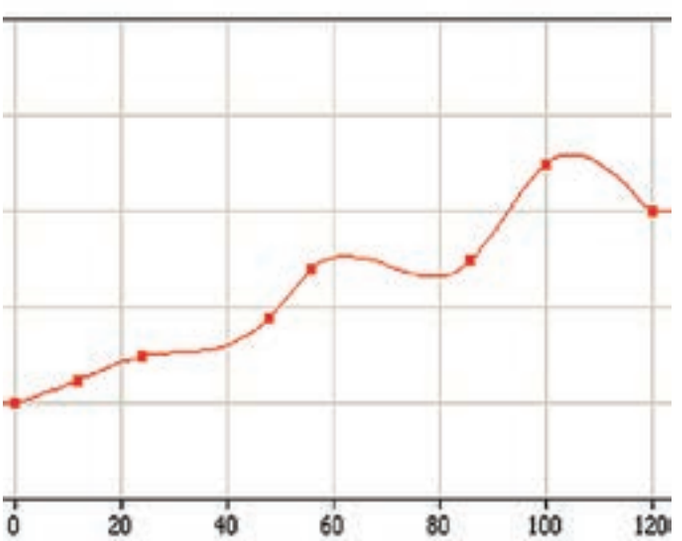


Рис. 4. Доступный хакеру ресурс

выбирался в зависимости от логического смысла коэффициента.

Здесь и далее осью абсцисс является линия времени. Значения – количество месяцев, прошедших от даты расчёта. При отсутствии обозначений на шкале по оси ординат максимальное значение равно единице.

- Skills – усреднённый опыт хакера **(рис. 2)**,
- Motivation – мотивация злоумышленника **(рис. 3)**,
- Resourse – доступный ему ресурс, включая время на подготовку атаки **(рис. 4)**,
- DefenceFactor – усилия, предпринимаемые собственниками энергообъектов в части информационной безопасности **(рис. 5)**,
- ModernisationTemp – прогнозное увеличение количества устройств. Предполагался 5-кратный рост количества устройств, потенциально уязвимых для атак **(рис. 6)**.

В сложных случаях, когда не было возможности опереться на статистические данные и прогнозы, использовалось декомпозиция. Например, усреднённая сила атаки (HackerStrength) вычислялась как суперпозиция трёх значений: опыта хакера (Skills), его мотивации (Motivation) и ресурса, который он может привлечь (Resourse). Гипотезы по оценке и прогнозированию каждой из этих величин строить значительно проще.

3.2.3. Динамические переменные

HackerStrength – сила потенциальной атаки **(рис. 7 с формулой 1)**

Формула 1 предполагает суперпозицию, о которой говорилось выше, и монотонный слабый рост во времени от базового значения.

HackerCount – количество активных злоумышленников **(рис. 8 с формулой 2)**.

Также предполагается медленный рост во времени, но основной вклад даёт ограниченное снизу непрерывное распределение хи-квадрат. Использование распределения даёт также возможность впоследствии применить метод Монте-Карло.

AttackPower – мощность потока атак **(рис. 9 с формулой 3)**.

DevicesCount – количество устройств **(рис. 10 с формулой 4)**.

DefenceStrength – усилия, направленные на защиту объектов **(рис. 11 с формулой 5)**.

В **формуле 5** значения коэффициента предполагаются пропорциональными соответственной табличной функции, но с существенным дополнением. После мощных атак (AttackPower>200) на короткое время вносится поправка на значительное увеличение защищённости. Предполагается, что это будет результат последующих оперативных организационно-технических мероприятий, например таких как запрет на дистанционную смену уставок и т. п.

Vulnerabilities – доля уязвимых устройств **(рис. 12 с функцией 6)**.

Функция 6 моделируется как периодическая с увеличивающимся периодом, слабо затухающая во времени. Периодичность моделирует смену поколений оборудования и/или совершенствование технологий хакерских атак.

CrackProbability – вероятность взлома **(рис. 13 с формулой 7)**.

Формула 7 отражает очевидную пропорциональность вероятности взлома мощности атак и обратную пропорциональность усилиям по защите.

3.2.4. Поток и накопитель

CrackFlow – количество взломанных устройств на данном шаге **(рис. 14 с формулой 8)**.

Cracks – суммарное количество успешных взломов нарастающим итогом **(рис. 15 с формулой 9)**.

Итогами моделирования являются диаграммы (CrackFlow) в разбивке по месяцам и (Cracks) – нарастающим итогом.

3.3. Интерпретация результатов моделирования

Был рассмотрен достаточно консервативный сценарий постепенного движения к безопасности на фоне 5-кратного увеличения числа устройств и роста числа атак. При этом число успешных взломов при очевидных колебаниях имеет тенденцию к снижению. К полученным абсолютным значениям надо относиться со скептицизмом, поскольку их величина зависит от параметров, выбранных эмпирическим путем. Нас в первую очередь интересовало поведение кривой, а не амплитуда значений.

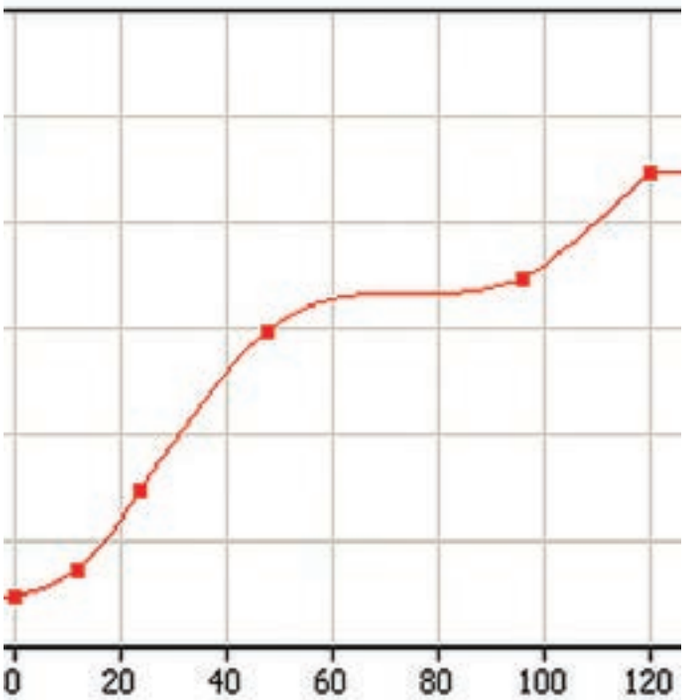


Рис. 5. Усилия по защите объектов

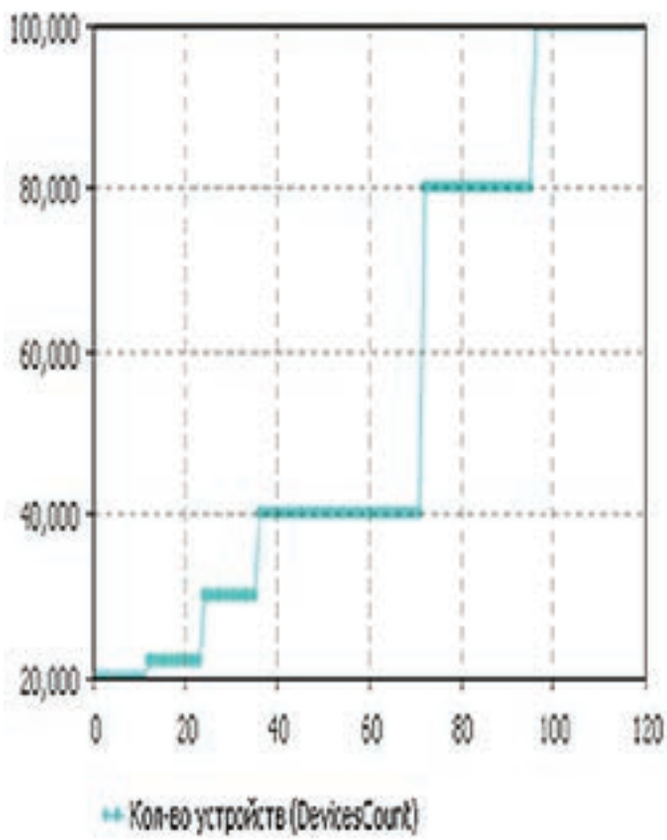
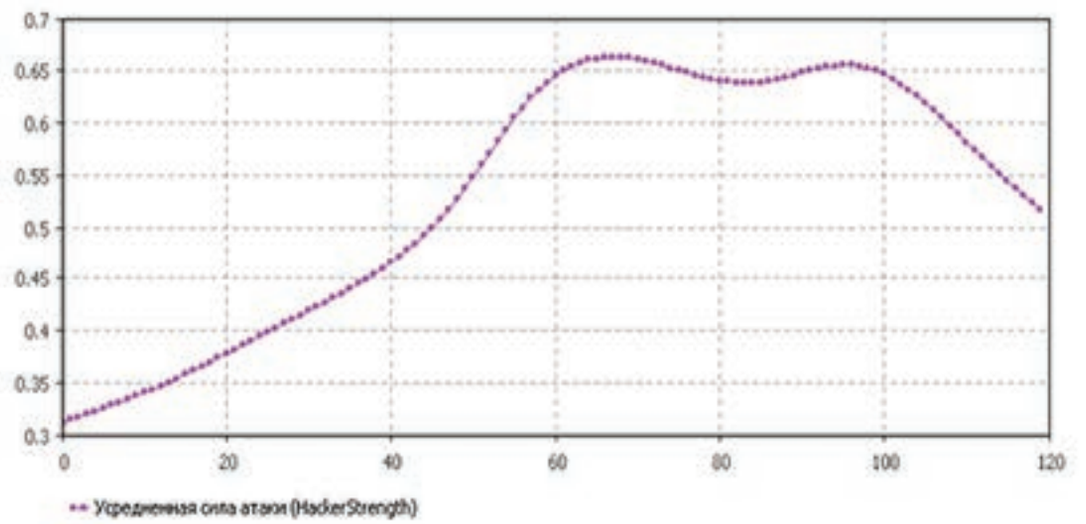
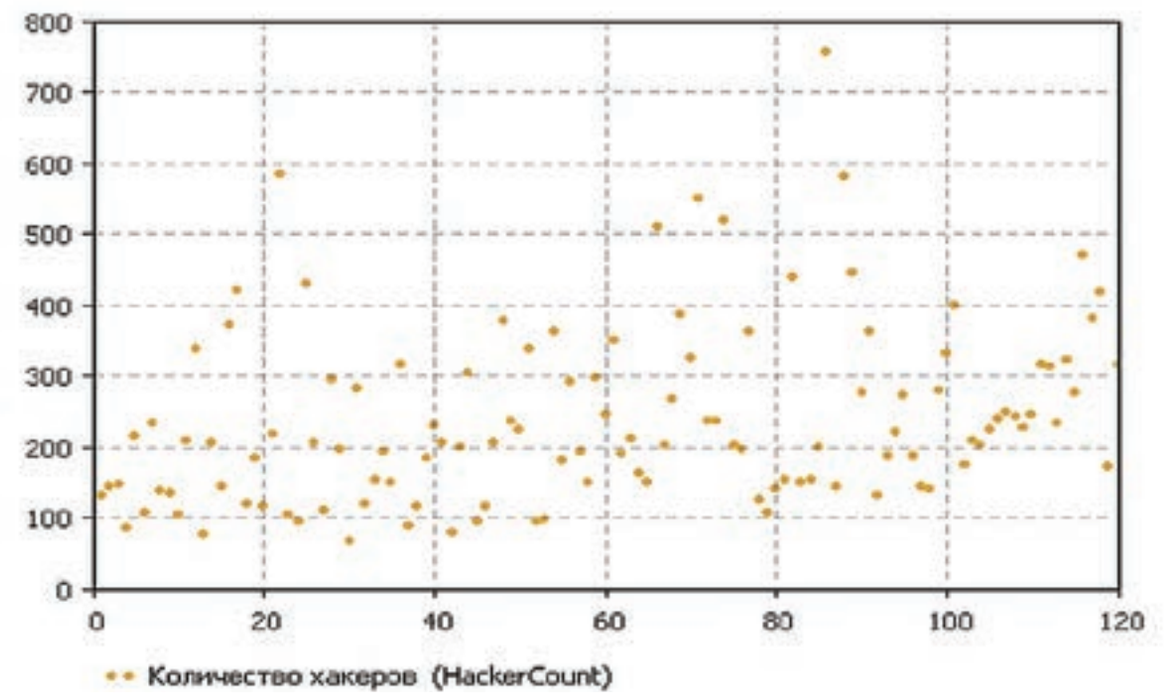


Рис. 6. Прогнозное увеличение количества устройств



$$HackerStrength = 0{,}001 \times time() + Skills(time()) \times Motivation(time()) \times Resourse(time()) + 0{,}3 \quad (1)$$

Рис. 7. Сила потенциальной атаки



$$HackerCount = HackerAtBegining \times (0{,}5 + chi2(3)) + HackerAtBegining \times time()/50 \quad (2)$$

Рис. 8. Количество злоумышленников

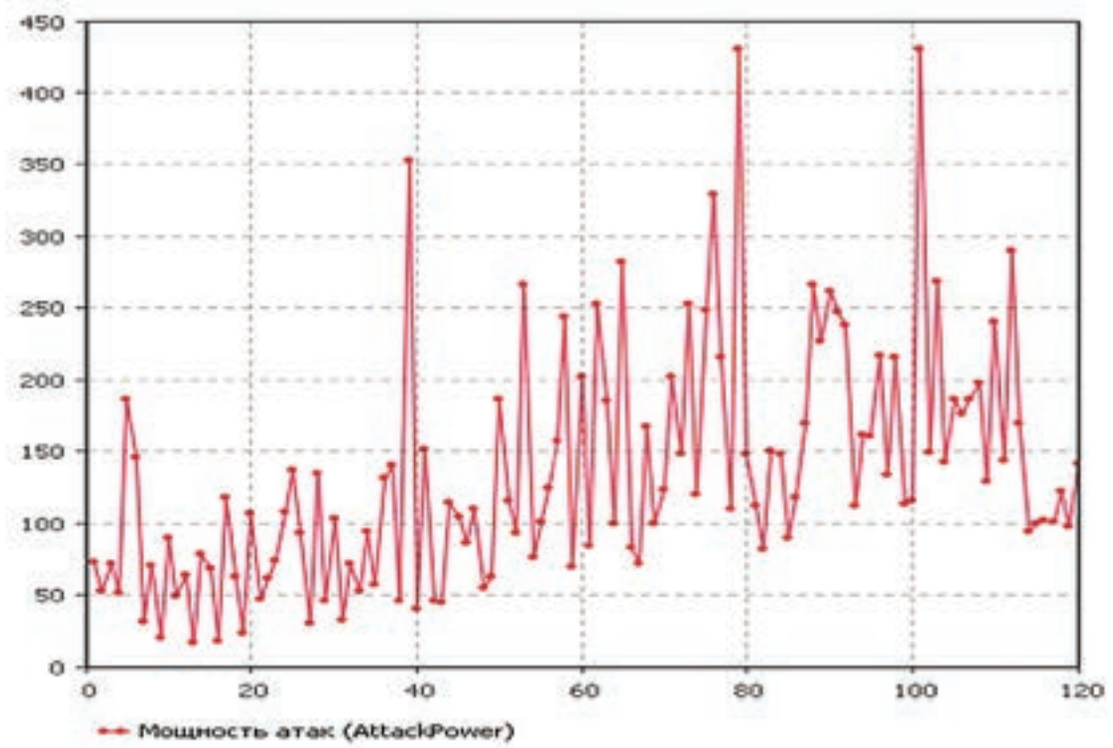
Полученные результаты можно интерпретировать следующим образом:

– В ближайшие 10 лет при сохранении текущих трендов риски существенно не вырастут (говоря языком публицистики, «кибер-армагеддон» откладывается).

– Сейчас и в ближайшие два года мы находимся в достаточно рискованной зоне. Хорошим решением было бы выполнение простых и относительно дешёвых организационно-технических мероприятий, включая обучение персонала, результатом чего будет существенное снижение рисков.

3.4. Планы по развитию модели

Очевидным способом развития модели с целью учёта большего количества влияющих

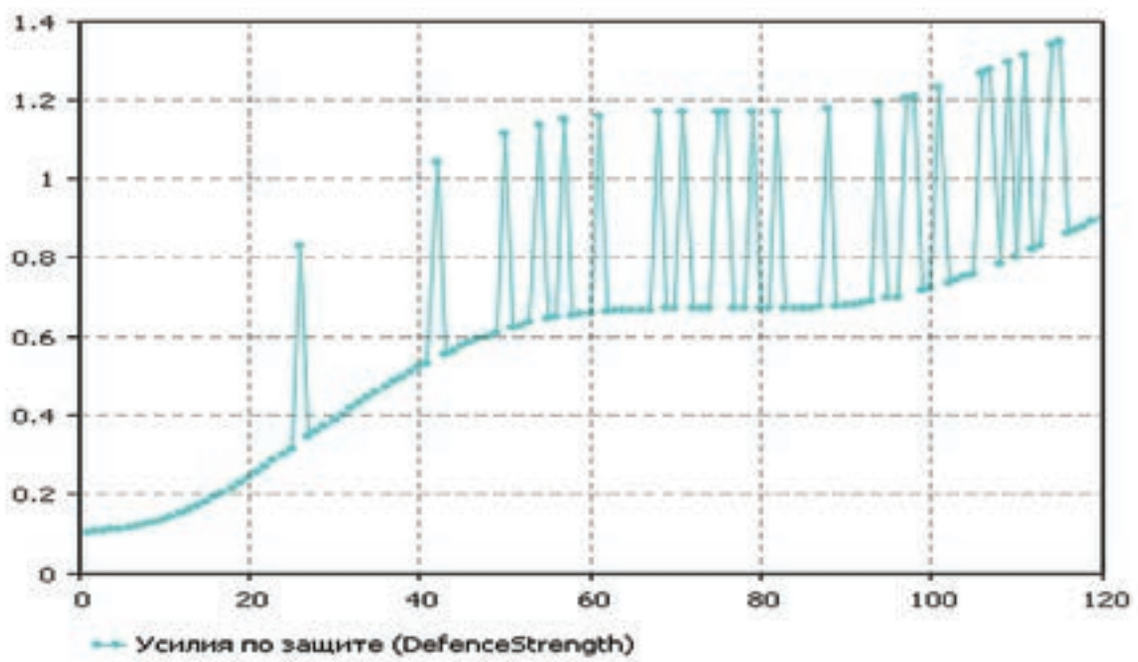


$$AttackPower = HackerStrength \times HackerCount \quad (3)$$

Рис. 9. Мощность потока атак

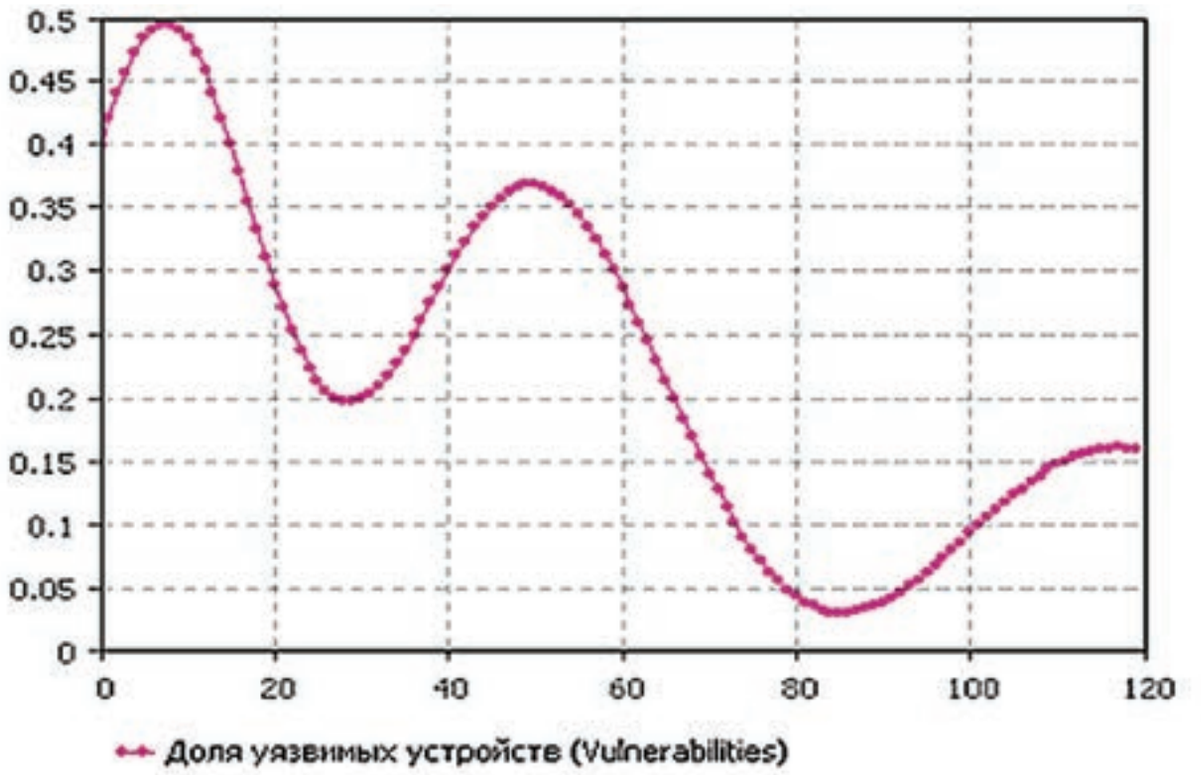
$$DevicesCount = DeviceAtBegining \times ModernisationTemp(time()) \quad (4)$$

Рис. 10. Формула расчёта количества устройств



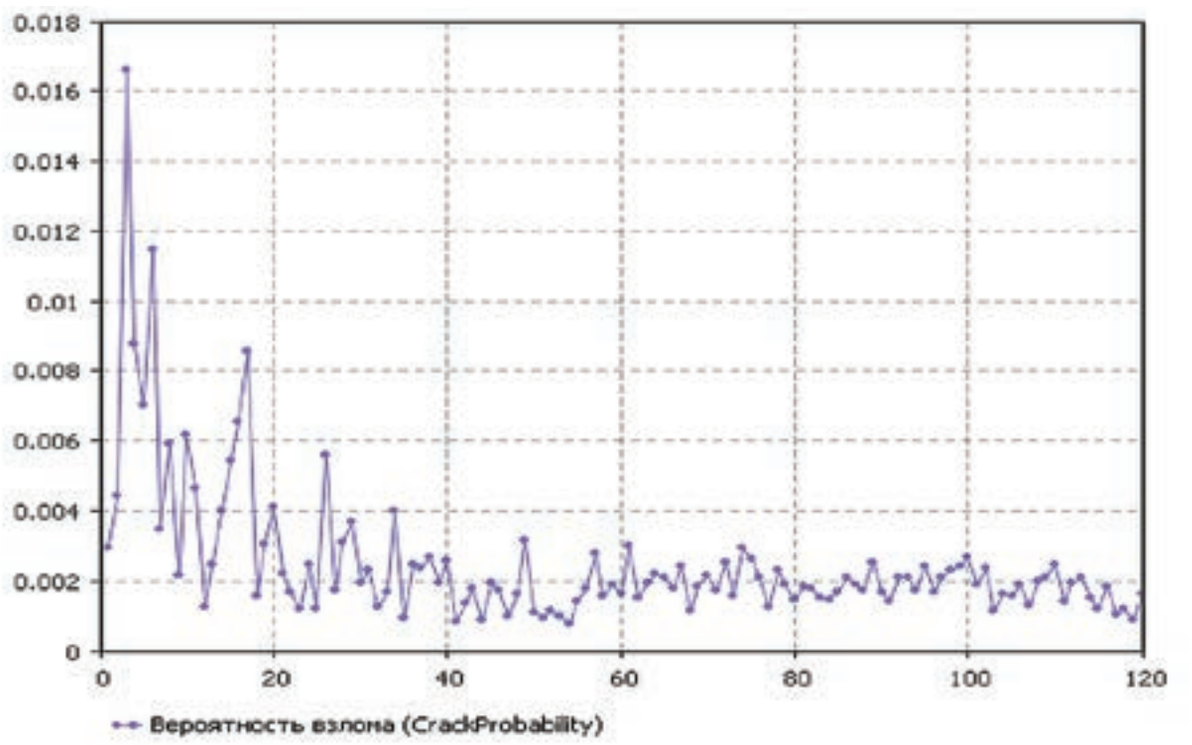
$$DefenceStrength = InitialDefence \times DefenceFactor(time())+0,5 \times (AttackPower>200?1:0) \quad (5)$$

Рис. 11. Усилия по защите



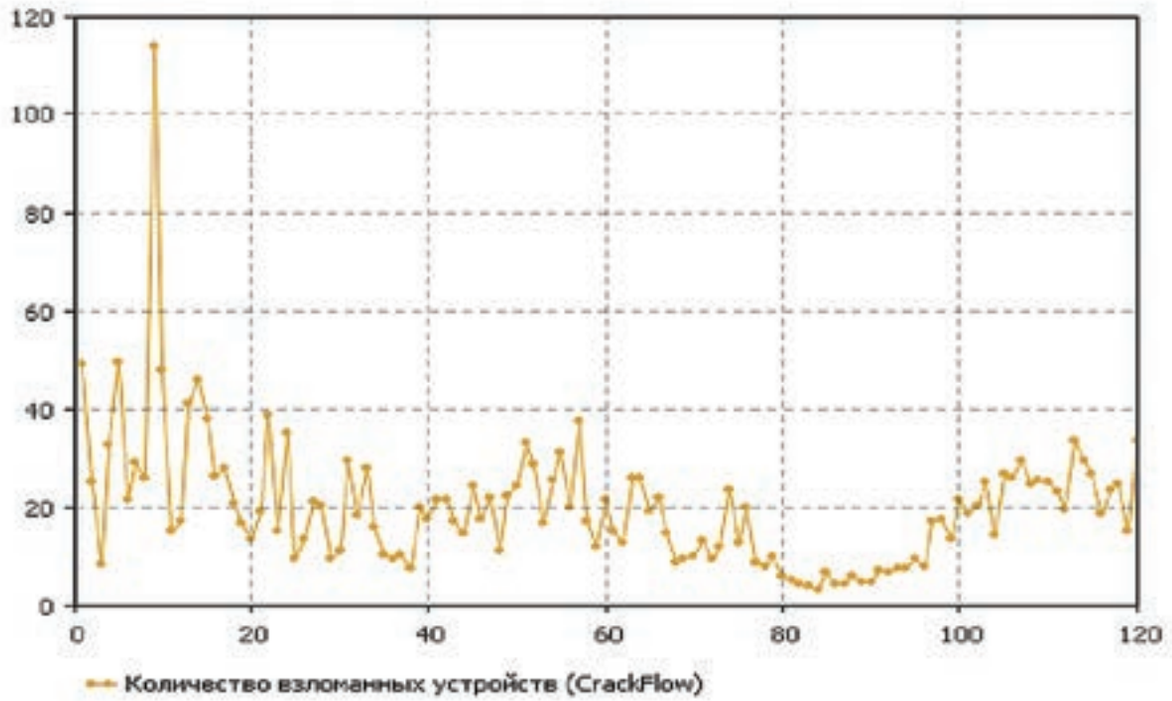
$$Vulnerabilities = VulnerabilitiesAtBeginning \times (1+0{,}3 \times \sin(time()/(5+0{,}03 \times time()))) - 0{,}003 \times time() \quad (6)$$

Рис. 12. Доля уязвимых устройств



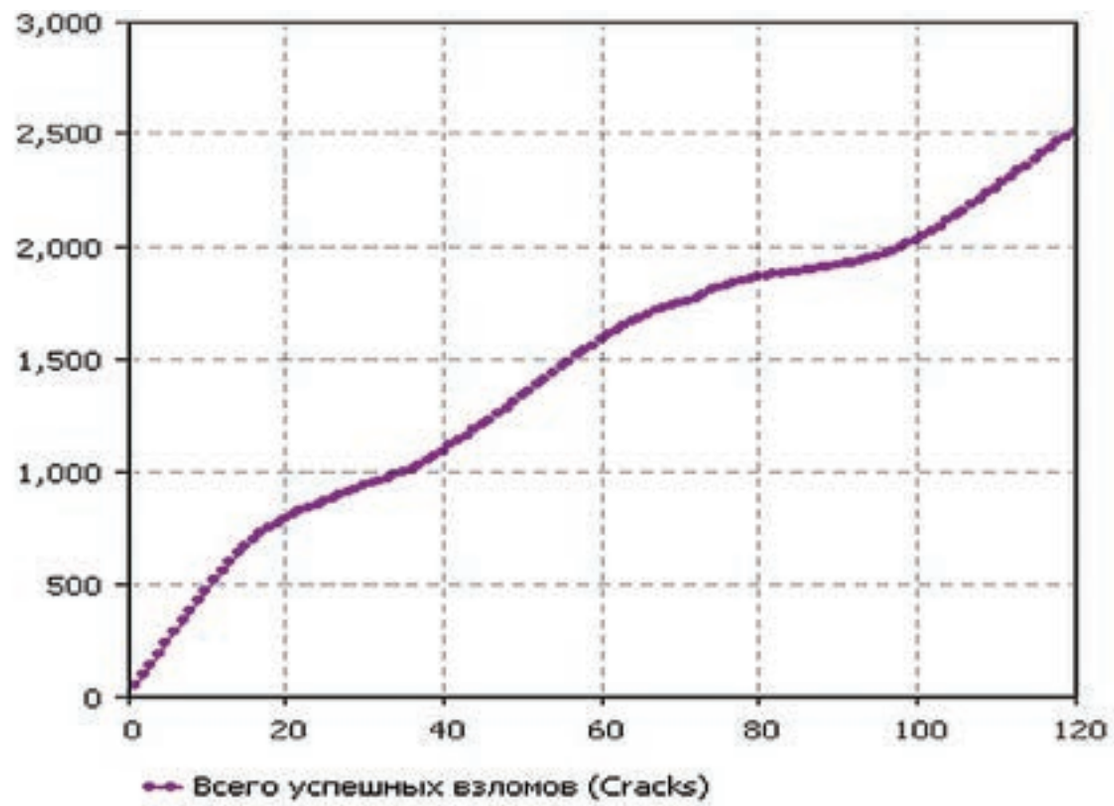
$$CrackProbability = (CrackProbabilityFactor \times AttackPower)/DefenceStrength \quad (7)$$

Рис. 13. Вероятность взлома



$$CrackFlow = DevicesCount \times Vulnerabilities \times CrackProbability \quad (8)$$

Рис. 14. Количество взломанных устройств на данном шаге



$$d(Cracks)/dt = CrackFlow \quad (9)$$

Рис. 15. Всего успешных взломов нарастающим итогом

факторов является переход к агентному моделированию. Сейчас мы рассматриваем уже усредненный портрет «хакера» или «устройства» как функцию времени. Создавая достаточное число агентов и устанавливая характеристики и правила взаимодействия для каждого из них в каждый момент времени, мы можем получить новые, совсем не очевидные зависимости.

Следующим шагом было бы параллельное использование и учёт отдельных факторов через дискретно-событийное моделирование. Например, таких как ввод в работу Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА) [11] или скорое принятие поправок в УК РФ, предусматривающих наказание за попытку взлома объектов критической инфраструктуры.

Перспективным также представляется использование наработок шведского Royal Institute of Technology [12], где с целью упрощения моделирования предприняли попытку создать специализированный язык – Cyber Security Modeling Language (CySeMoL). Язык не получил широкого распространения, но, по замыслу авторов, позволял формально описать 59 видов атак, 58 типов защиты для 23-х разновидностей активов и установить отношения между этими сущностями.

4. Заключение

В настоящей работе исследованы различные способы и продемонстрированы подходы, позволяющие успешно применить методы имитационного моделирования как инструмент оценки защищённости и оптимизации затрат на мероприятия по обеспечению киберзащиты.

1. Выполнено описание модели, позволяющей оценивать динамику изменения угроз для объектов электроэнергетики на ближайшие десять лет. Приведён пример расчёта для сценария, который авторы считают достаточно вероятным.
2. Даны рекомендации по применимости имитационного моделирования и предложения по развитию существующей и созданию новых моделей с учётом информации, доступной в научных публикациях на эту тему.
3. Поставлены вопросы, требующие дальнейшего изучения и обсуждения, намечены пути совершенствования модели.

Литература

1. «Концепция развития релейной защиты и автоматики электросетевого комплекса», Приложение №1 к протоколу Правления ОАО «Россети» от 22.06.2015 № 356пр

2. Г. С. Нудельман, ОАО «ВНИИР», ИК B5 РНК СИГРЭ, «Обобщение мировых тенденций развития техники и технологий в области релейной защиты и автоматики», 2015.

3. OSCE. Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace. 2013.

4. National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity. 2014.

5. ISO/IEC 27032:2012(E). Information technology — Security techniques — Guidelines for cybersecurity. 2012.

6. ГОСТ Р ИСО/МЭК 31010. Менеджмент риска. Методы оценки риска. 2011.

7. Pavel Fuchs, Jan Kamenicky, Tomas Saska, David Valis, Jaroslav Zajicek. Some Risk Assessment Methods and Examples of their Application. б.м.: Technical University of Liberec, 2011.

8. Paranjape, Raman. "Agent-Based Modeling of Power Systems Infrastructure Cyber Security". World Academy of Science, Engineering and Technology International Journal of Social, Behavioral, Educational, Economic, Business and Industrial Engineering, 2013 г., T. Vol:7, No:8.

9. Д. И. Котенко, И. В. Котенко, И. Б. Саенко. Методика итерационного моделирования атак в больших компьютерных сетях. Труды СПИИРАН. 2012 г., Вып. 4(23).

10. Павел Литвинов, «Имитационное моделирование вопросов информационной безопасности как инструмент оценки защищённости и оптимизации затрат», МКА №2/2016

11. Указ Президента Российской Федерации от 15 января 2013 г. N 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» и «Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации», утвержденная Президентом РФ 12.12.2014 № К 1274.

12. A Manual for the Cyber Security Modeling Language. Hannes Holm, Mathias Ekstedt, Teodor Sommestad, Matus Korman. Stockholm: Department of Industrial Information and Control Systems, Royal Institute of Technology, 2014.

Павел Литвинов | АО «РТСофт»
Сергей Нестеров | АО «РТСофт»