Лицензия на образовательную деятельность № 037032
Департамента образования г. Москвы

ЧУ ДПО «УЦ РТСофт»

Расписание учебных курсов на II квартал 2016 г.

Учебный Центр РТСофт

Наименование	Дата начала	Дата окончания
SCADA-система InTouch 2014R2	19.04.2016	22.04.2016
ПТК SMART-SPRECON	25.04.2016	29.04.2016
Инструментальная платформа ПЛАТИНУМ-РТ	25.04.2016	29.04.2016
Использование программного обеспечения PowerFactory для расчета аварийных режимов сети, ТКЗ, моделирования и анализа работы РЗА	25.04.2016	27.04.2016
Регистратор переходных режимов SMART-WAMS 2	26.04.2016	28.04.2016
Анализ и оптимизация режимов распределительной сети на базе ПК PowerFactory	28.04.2016	29.04.2016
Использование программного обеспечения PowerFactory для расчета режимов электрических сетей и систем	04.05.2016	06.05.2016
Устройство сбора данных SMART-КП Электра	04.05.2016	06.05.2016
SCADA-система CITECT	10.05.2016	13.05.2016
ПТК SMART-SPRECON	16.05.2016	20.05.2016
SCADA-система SPRECON-V460	16.05.2016	20.05.2016
SCADA-система InTouch 2014R2	24.05.2016	27.05.2016
ПТК SMART-SPRECON	30.05.2016	03.06.2016
Контроллер Sprecon-E-C	30.05.2016	03.06.2016
Использование программного обеспечения PowerFactory для расчета режимов и устойчивости электрических сетей и систем	06.06.2016	10.06.2016
Регистратор переходных режимов SMART-WAMS 2	06.06.2016	08.06.2016
LynxOS - операционная система жесткого реального времени	07.06.2016	10.06.2016
SCADA-система CITECT	14.06.2016	17.06.2016
Хранилище данных Wonderware Historian	15.06.2016	17.06.2016
Развертывание CitectHistorian и создание отчетов	15.06.2016	17.06.2016
Инструментальная платформа ПЛАТИНУМ-РТ	20.06.2016	24.06.2016
Общий курс по SCADA-системам	20.06.2016	24.06.2016
Настройка и эксплуатация ЦППС SMART-FEP	21.06.2016	24.06.2016
SCADA-система InTouch 2014R2	21.06.2016	24.06.2016
Анализ и оптимизация режимов распределительной сети на базе ПК PowerFactory	27.06.2016	28.06.2016
Использование программного обеспечения PowerFactory для расчета аварийных режимов сети, ТКЗ, моделирования и анализа работы РЗА	29.06.2016	01.07.2016

105264, Москва,
ул. Верхняя Первомайская, д. 51
ЧУ ДПО «УЦ РТСофт»

тел.: (495) 742 96 55, 742 96 54
факс: (495) 742 65 66
e-mail: tc@rtsoft.msk.ru
http: //www.rtsoft-training.ru

OpenSystems Publishing

МИР КОМПЬЮТЕРНОЙ АВТОМАТИЗАЦИИ • COMPUTER AUTOMATION WORLD

В НОМЕРЕ

CONTENTS

ВСТРАИВАЕМЫЕ КОМПЬЮТЕРНЫЕ ТЕХНОЛОГИИ

EMBEDDED COMPUTER TECHNOLOGIES

Промышленные ПК для операторных: российские или импортные? низкошумные или безвентиляторные?
Олег Холодный, ЗАО «РТСофт»
4
Industrial PCs for Operating Rooms: Domestic or Foreign? Low-noise or Fanless?,
by Oleg V. Kholodnyi, RTSoft

Обзор алгоритмов охлаждения в системах AdvancedTCA
Владимир Павлов, Сергей Жуков, Игорь Починок, Auriga Inc., НИВЦ МГУ
9
Cooling Algorithms for AdvancedTCA Systems Overview,
by Vladimir Pavlov, Sergey Zhukov and Igor Pochinok. Auriga Inc. and MSU RCC

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

SOFTWARE

«Интернет вещей» и стандарты беспроводной связи
Сис Линкс (Cees Links), Greenpeak technologies
17
Wireless Communication Standards for the Internet of Things,
by Cees Links, GreenPeak Technologies

За пределами границ
Герард Хольцман (Gerard I. Holzman), NASA/JPL
23
Out of Bounds,
by Gerard I. Holzman, NASA/JPL

ИУС ДЛЯ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ И ИНФРАСТРУКТУРНЫХ ОБЪЕКТОВ

INDUSTRIAL ENTERPRISE AND INFRASTRUCTURE IMSS

Комплекс магнитного управления плазмой информационно-управляющей системы установки «Токамак Т-15»
Г. С. Кузьмина, Ю. Я. Моцкин (ЗАО «РТСофт»), М. М. Соколов, Р. Р. Хайрутдинов, П. П. Хвостенко (НИЦ «Курчатовский институт»),
27
Plasma Magnetic Control Complex of TOKAMAK T-15 Management Information System,
by G. S. Kuzmina and Yu. Ya. Motskin, RTSoft, M. M. Sokolov, R. R. Khayrutdinov and P. P. Khvostenko, NRC «KURCHATOV INSTITUTE»

Реализация задач сбора, консолидированной обработки и доступа к разнородным источникам данных
К. Б. Здирук, В. Ю. Синенко, А. Н. Ханыгин, ЗАО «РТСофт»
33
Heterogeneous Data Acquisition, Consolidated Processing and Access Implementation,
by K. B. Zdiruk, V. Yu. Sinenko, and A. N. Khanygin, RTSoft

ИУС ДЛЯ ЭЛЕКТРОЭНЕРГЕТИКИ

POWER INDUSTRY IMSS

СИГРЭ: Информационные системы и телекоммуникации для электроэнергетики – актуальные проблемы и задачи 2014–2016 годов
А. Р. Вериго, В. И. Чехов, ЗАО «РТСофт»
38
SIGRE: Power Industry Information Systems and Telecommunications – 2014–2016 Problems and Tasks,
by A. R. Verigo and V. I. Chekhov, RTSoft

Имитационное моделирование вопросов информационной безопасности как инструмент оценки защищённости и оптимизации затрат
Павел Литвинов, ЗАО «РТСофт»
43
Information Security Simulation Modeling as a Tool of Cost Security and Optimization Evaluation,
by Pavel Litvinov, RTSoft

«РТСофт» на конференции PTC LiveWorx Europe 2015
Павел Литвинов, Сергей Нестеров, ЗАО «РТСофт»
54
RTSoft at PTC LiveWorx Europe 2015 Exibition and Conference,
by Pavel Litvinov and Segrey Nesterov, RTSoft

Основные тенденции развития Smart City
Анна Шихина, ЗАО «РТСофт»
57
Smart City Main Trends,
by Anna Shikhina, RTSoft

НОВОСТИ РЫНКА
8, 13–16, 26, 32, 42
MARKET NEWS

Редакционный совет:

Синенко О. В. – председатель редакционного совета, директор НП «Вера+», 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 ЗАО «РТСофт», д.т.н.

Рыбаков А. Н. – технический директор ЗАО «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 электроэнергетики – Небера А. А.

Ответственный за вёрстку – Белов И. В.

Подписка и распространение – Лазарева Т. Н.

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

Тираж 900 экз., цена свободная.

Перспективные информационные технологии для встраиваемых систем, информационных и информационно-управляющих систем в промышленности и энергетике

«Мир компьютерной автоматизации»
Computer Automation World
№ 1 (108) 2016

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
E-mail: mka@veraplus.msk.ru,
URL: www.mka.ru

Олег Холодный, ЗАО «РТСофт»

Промышленные ПК для операторных: российские или импортные? низкошумные или безвентиляторные?

Управление воздушным движением, управление на ЖД-переездах, контроль технологических процессов на верхних уровнях управления атомных электростанций – вот далеко не полный перечень приложений с высокой ответственностью, где роль оператора очень важна для обеспечения комплексной безопасности. Здесь критично всё, начиная от надёжного функционирования аппаратного и программного обеспечения и заканчивая комфортом специалистов, от которых зависит принятие верных решений. Известный факт: человеку легче сконцентрироваться, когда его ничто не отвлекает. Концепция «тихая операторная» сама по себе не нова и в последнее время набирает популярность во всё большем количестве отраслей промышленности. Развитию этой концепции, в частности, способствуют перспективные российские и зарубежные разработки встраиваемых компьютерных платформ с низкошумным и полностью безвентиляторным отводом тепла.

На рынке промышленных приложений существует актуальный тренд, состоящий в стремлении сделать труд операторов и диспетчеров, принимающих ответственные решения, максимально комфортным. Речь в данном случае идёт о том, что в помещении, где работает оператор, количество факторов, мешающих его качественной работе, должно быть сведено к нулю. Ошибки в таком процессе могут стоить недопустимо дорого. Если переводить данную тему в плоскость использования компьютерного оборудования на местах, то здесь очень важно отметить необходимость в надёжном функционировании, высокой эргономичности и простоте в эксплуатации, а также позаботиться о том, чтобы шум, издаваемый техникой во время работы, не превышал допустимые или «комфортные» нормы. В этой связи появилась и получила своё логическое развитие концепция «тихой операторной», упор при построении которой ставится на обеспечение минимального уровня шума при работе сложного аппаратного обеспечения.

Существуют два основных подхода, которые позволяют снизить уровень шума на уровне системы, – это использование сбалансированных вентиляторных конструкций, качественно работающих на высоких оборотах, либо более дорогой, но профессиональный сценарий, который предполагает полностью кондуктивный отвод тепла для вычислительных и графических подсистем, а также для подсистемы питания. В России широко представлены встраиваемые вычислители, которые выполнены как по первому, так и по второму принципу, причём среди них можно выделить и отечественные, и зарубежные продукты. Какой подход и страну происхождения выбирать разработчику, дело сугубо индивидуальное и, как покажет материал ниже, может зависеть от различных факторов.

Низкошумные серверы KISS приняли российское гражданство

Торговая марка низкошумных стоечных компьютеров KISS (Kontron Industrial Silent Server) давно известна не только в России, но и во всём мире. Данные компьютеры берут своё начало на производственных мощностях холдинга Kontron AG и сегодня стоят на одной «торговой полке» с такими известными производственными гигантами, как Siemens, Beckhoff, GE, B&R. Промышленным ПК KISS удалось завоевать своего покупателя исключительными особенностями, которые были положены в основу этих систем немецкими разработчиками профессионального встраиваемого железа. KISS вобрали в себя опыт нескольких лет разработки не одного десятка щепетильных R&D-инженеров, который получил отражение в глобальных проектах в сферах нефтегаза, энергетики, транспорта и многих других отраслях и позволил KISS стать широ-

ко узнаваемым в узких кругах системных инженеров. Размах мировых проектов с использованием этих систем внушителен, а на производственных конвейерах сегодня выпускаются десятки, а то и сотни тысяч таких машин в год.

Российские реалии, а точнее сегодняшняя политика государства в области импортозамещения, диктует свои правила и ставит под сомнение использование стоечных ПК зарубежного производства по крайней мере для крупных государственных проектов. Это, с одной стороны, открывает дополнительные бизнес-возможности для российских производителей, но с другой стороны – заставляет системных интеграторов пользоваться продуктами, которые произведены с использованием невыверенных и неотточенных технологий сборки, где при выборе базовых комплектующих предпочтение отдаётся азиатским вендорам прежде всего из соображений меньшей себестоимости. В результате системным интеграторам приходится использовать продукты с заведомо худшим качеством, сниженным жизненным циклом, которые менее удобны в эксплуатации, не говоря уже о внешнем виде, сравнимом по грубым меркам с «постсоветским».

В условиях ограниченного импорта разумный подход в предложении рынку качественного продукта видится в локализации высокотехнологичного производства промышленных компьютеров известной мировой марки в России. По этому пути и пошла компания «РТСофт», имея многолетний опыт сотрудничества с холдингом Kontron AG, обученных системных архитекторов и обладая полной производственно-технологической картой от партнёров Kontron AG. Известная марка KISS теперь производится на собственных мощностях, расположенных в наукограде Черноголовке. На текущий момент каналы продажи компании «РТСофт» могут предложить почти полную линейку сертифицированных промышленных ПК KISS российского производства. Российские KISS сегодня – это не только защита от санкций, недобросовестных и некачественных поставщиков, но и будущий задел в производстве отечественных конкурентоспособных систем.

Отечественный BLOK санкциям

Там, где определённый уровень локализации и использование зарубежных продуктов не позволяют решить поставленные производственные и проектные задачи российских системных интеграторов, «РТСофт» готов предложить свою собственную разработку – промышленный безвентиляторный компьютер BLOK (рис. 1), который просто идеален для организации операторных нового поколения. Идеален он по ряду причин, которые будут более подробно освещены в данном разделе.

BLOK не является предметом «отвёрточной» сборки, а представляет собой полноценный проект НИОКР по разработке российской электронной аппаратуры. Разработка данного устройства велась с использованием самых современных стандартов встраиваемой компьютерной техники, достижений в области сетевых и мультимедийных интерфейсов, а также благодаря современным системам проектирования и производства точной 3D-механики. BLOK производится в России на основе полного комплекта КД и имеет максимальную защищённость от действий поставщиков и производителей компонентов, так как все критически важные части системы имеют полные альтернативы.

В качестве компьютерного ядра устройства BLOK используется модуль, который выполнен в международном стандарте COM Express. Для справки: COM Express сегодня – **номер один** по темпам роста на мировой площадке встраиваемых компьютерных архитектур. Эта технология очень популярна в мире, и производством модулей в данном стандарте занимаются более ста международных компаний, включая российские. Не будет лишним сказать, что данную технологию взяла на вооружение российская компания «МЦСТ» и уже выпускает свои первые модули COM Express на базе собственных процессоров «Эльбрус». Эта важная особенность промышленного компьютера BLOK позволит ему в будущем не только масштабировать собственную производительность, используя ядра на Intel Atom Bay Trail или Intel Core 6th Skylake, но и применять в качестве ядра модули COM Express с российскими процессорами. Благодаря возможности масштабирования по процессорному ядру, жизненный цикл продукта BLOK не ограничен поддержкой на рынке в течение 5–7 лет, а может быть расширен до более длительного. Этот факт очень важен для долго-

Рис. 1 Промышленный безвентиляторный компьютер BLOK, разработки компании «РТСофт»

срочных спецпроектов, проектов в области атомной энергетики и в нефтегазовом секторе.

Полностью безвентиляторное охлаждение, развитая подсистема ввода-вывода, высокие мультимедийные возможности, подсистема RAID, дублирование питания – вот далеко не полный набор перспективного изделия BLOK, который делает его идеальным для построения современных полиэкранных бесшумных рабочих станций для операторов и диспетчеров. Девиз этого устройства – «поставил... и забыл».

Локальный оперативный сервис и гарантия

Опытные системные интеграторы, готовые поставить часть своей профессиональной судьбы на то или иное оборудование, просто обязаны позаботиться об уровне сервиса и качестве поддержки от поставщика/производителя, которую им обязательно придётся проверить на себе при реализации более или менее крупных проектов. Например, при взаимодействии с крупным мировым OEM-производителем проблемы могут возникнуть с обратной связью либо с полным отсутствием таковой. Российские компании, реализующие небольшие проекты в объёмах до 1000 компьютеров в год, не представляют особого интереса для массового производителя. В таких случаях бывает сложно договориться о доработках БИОС, реализации дополнительной схемотехники, дополнительной доработке механики и т. д.

Далеко не многие производители, а уж тем более поставщики, могут оказывать длительную гарантийную поддержку продукту. В самых стандартных случаях этот срок не превышает одного года. Мировая практика показывает, что более длительную поддержку, как правило, гарантируют производители, обладающие внушительной системой качества на предприятии, отработанной производственной технологией, производящие изделия с тщательно выверенной компонентной базой и комплектующими, имеющими большие показатели параметра наработки на отказ (MTBF – Mean Time Between Failures). Именно этими тремя принципами руководствуется компания «РТСофт» при разработке, производстве и сборке продуктов KISS и BLOK. Каждая итерация выбора компонентной базы, проектирования, входного контроля, производства, наладки и многих других этапов создания изделия контролируется профессионалами своего дела на местах. Такой тщательный подход гарантирует заказчикам качественное и профессиональное исполнение продуктов, которое подтверждается расширенной гарантией до трёх лет.

Гарантийная поддержка очень важный фактор, но ещё большую значимость она приобретает в совокупности с компетентной и качественной технической поддержкой по продуктам и возможностями производителя делать определённые доработки – другими словами, кастомизировать готовый продукт под требования заказчика. Близость производителя, расположенного в России, даёт абсолютные преимущества в этой части. Заказчикам «РТСофт», например, доступна модификация готового продукта даже в самых крохотных партиях от 50–100 шт. Вопрос в данном случае не ограничивается кастомизацией аппаратной части, поскольку у «РТСофт» имеется достаточно большой и профессиональный ресурс для работы с системным ПО. Если говорить более понятным языком, это большой штат программистов международного уровня, владеющих технологиями разработки драйверов (BSP-пакетов) под широкий класс операционных систем.

Профессионализм на местах, возможность доработки, качество производства и локальная длительная поддержка позволяют KISS и BLOK иметь неоспоримые преимущества для российского пользователя, профессиональный интерес которого лежит в эффективной и качественной реализации серьёзных проектов.

Немного о KISS

Весьма удобны с точки зрения организации АРМ операторов и диспетчеров те модели KISS, в названии которых присутствует слово «short», означающее уменьшенную глубину. Одной из новых систем этого типа является KISS 1U Short KTQM87 (рис. 2). Благодаря высоте 1U и глубине 350 мм, данное изделие способствует более плотному размещению оборудования. Система имеет три порта DisplayPort, четыре порта USB 3.0 и допускает гибкое конфигурирование и модернизацию в соответствии с требованиями заказчика. В двумерных и трёхмерных приложениях интегрированное графическое ядро Intel HD Graphics с поддержкой функций DirectX 11.1, Open GL 4.0 и Open CL 1.2 демонстрирует производительность уров-

Рис. 2. Внешний вид модели KISS 1U Short KTQM87, оснащённой высокопроизводительными процессорами Intel Core i3/i5/i7 четвёртого поколения и имеющей уменьшенную глубину

ня дискретных видеокарт. Малошумный промышленный компьютер KISS 1U Short KTQM87 базируется на четвёртом поколении процессоров Intel Core i3/i5/i7 с тактовыми частотами до 3,8 ГГц. В комбинации с чипсетом Intel QM87 и памятью DDR3 объёмом до 32 Гбайт это обеспечивает покрытие широкого диапазона требований по производительности. Компьютер KISS 1U Short KTQM87 может работать под популярными операционными системами Windows 7, Windows Embedded Standard 7 (32- и 64-разрядная), Windows 8 и Linux. Слот PCI Express x16 позволяет создавать специализированные конфигурации с использованием плат расширения на основе открытых стандартов. Благодаря восьми портам USB 2.0 (6 сзади, 2 спереди) и трём портам Gigabit Ethernet, компьютер KISS 1U Short KTQM87 обладает богатыми возможностями подключения к периферийным устройствам и сетям. Упрощающая обслуживание технология Intel AMT 7.0 способствует повышению готовности системы и снижению затрат. Помимо внутреннего ударозащищённого отсека в 2,5 дюйма имеются доступные с фронтальной стороны отсек 3,5 дюйма и привод DVD Slim. Поддержка 6-гигабитной версии технологии SATA обеспечивает высочайшую скорость взаимодействия с дисками, а возможность установки опциональной подсистемы Kontron KISS Stor Slim RAID 1 с двумя 2,5-дюймовыми дисками в конфигурации RAID 1 с возможностью «горячей» замены позволяет повысить степень защиты данных. Средняя наработка на отказ (MTBF) для KISS 1U Short KTQM87 составляет 30 000 часов. Изделие имеет класс защиты IP20, выдерживает удары силой до 15 g и рассчитано на работу при температурах от 0 до +45 °С.

Рис. 3. Пример работы платформы BLOK с 3–мя дисплеями

Немного о BLOK

Типовой вариант поставки BLOK базируется на комбинации из процессора Intel Core 5 Haswell (2 ядра, частота 1,6 ГГц) и чипсета Intel Mobile Q87. Компьютер может быть оснащён памятью DDR3L-1600 объёмом до 16 Гбайт и двумя твердотельными либо жёсткими дисками формата 2,5 дюйм. Для подключения внешних устройств доступны два последовательных интерфейса,

BLOK в лаборатории «Интернета вещей»

Промышленный компьютер BLOK (blok.rtsoft.ru) российской компании «РТСофт» был выбран корпорацией Intel для участия в открытии московской лаборатории «Интернета вещей» (Internet of Things – IoT), состоявшегося 30 июня 2015 г. в Москве. В постоянной экспозиции лаборатории компьютер BLOK фигурирует в составе программно-аппаратного комплекса «Монтрек», адресованного предприятиям, имеющим собственный парк транспортных средств и желающим наладить их эффективный онлайн-мониторинг (см. фото). Разработанная специалистами «РТСофт» мониторинговая система «Монтрек» не имеет мировых аналогов и способна обеспечивать рентабельное функционирование на обширных территориях нашей страны, где не работают обычные средства коммуникации. Достигается это за счёт нового, революционного подхода к принципам слежения за объектами. Система позволяет организовать непрерывный контроль транспорта и производственных объектов с удалённым управлением логистикой и технологическими процессами. Её основная область применения – контроль перемещения транспортных средств в удалённых и труднодоступных районах, в том числе вне зон покрытия мобильной связи. Система «Монтрек» служит наглядным примером того, как промышленные компьютеры BLOK помогают при создании современных операторских приложений в самых различных сферах, включая такие новые и бурно развивающиеся сегменты рынка, как «Интернет вещей».

Промышленный компьютер BLOK в составе системы «Монтрек» на открытии московской лаборатории «Интернета вещей»

четыре порта Gigabit Ethernet, шесть портов USB 3.0/2.0 и три графических интерфейса (3 DisplayPort либо 2 DisplayPort + 1 DVI-D), а также звуковые вход и выход. Возможности расширения включают слот SIM-карты и два слота Mini PCI Express с поддержкой модулей Wi-Fi.

В базовой конфигурации платформа BLOK способна осуществлять вывод изображения на три дисплея в разрешениях до 4K с параллельной передачей аудио (рис. 3). Эта особенность имеет большое значение в контексте задач визуализации, оснащения операторских и организации автоматизированных рабочих мест. Безвентиляторный дизайн, обеспечиваемый малым тепловыделением процессора Intel Core 5 Haswell (не более 25 Вт), повышает надёжность системы и делает её полностью бесшумной. К характеристикам надёжности следует отнести также резервированный блок питания 220 В/50 Гц. Средняя наработка на отказ (MTBF) для BLOK превышает 150 000 часов (более 7 лет). Базовая конфигурация рассчитана на использование при температурах от –10 до +55 °С, весит 4,4 кг и имеет габариты 44 мм (1U) × 415 мм (19") × 200 мм. Производитель обладает лицензиями TUV ISO 9001-2008, ФСТЭК, Ростехнадзора и ФСБ. Продукт сертифицирован по ГОСТ Р и ТС. По умолчанию для BLOK доступны операционные системы Windows 7, Window 8, Windows Embedded Standard 7, Windows Embedded 8 Standard и Linux. Возможна адаптация других ОС, а также изменение характеристик питания, расширение температурного диапазона, усиление механических свойств, повышение класса защиты IP, проведение специсследований, спецпроверок и приёмки заказчика.

Напоследок

Промышленные компьютеры типа BLOK и KISS – это яркий инструментарий, который позволяет системным интеграторам разрабатывать бесшумные диспетчерские и операторные пункты, шлюзовые и вычислительные узлы нового поколения. Причём делать это на основе самых современных процессорных архитектур, коммуникационных возможностей и технологий отвода тепла. Российские низкошумные и бесшумные промышленные ПК высокой надёжности в будущем обязательно станут неотъемлемой частью высокотехнологичных и безопасных диспетчерских пунктов и станций оператора, которые занимаются управлением сложных технологических объектов, систем транспорта, коммуникаций и многих других.

ЗАО «РТСофт»
www.rtsoft.ru
pr@rtsoft.ru
тел. 8-495-967-1505

Новости рынка

«РТСофт» – лауреат премии в области импортозамещения «Приоритет–2015»!

Компания «РТСофт» стала лауреатом Национальной премии в области импортозамещения «Приоритет-2015» в номинации «Связь и информационные технологии», представив на конкурс отечественный безвентиляторный компьютер BLOK.

Национальная премия «Приоритет-2015» – ежегодный конкурс, предназначенный для поддержки и поощрения компаний, продвигающих на рынке конкурентоспособные товары, услуги и технологии собственного производства. Импортозамещение в условиях стратегических глобальных вызовов на сегодняшний день – важнейшая задача экономической безопасности и экономического развития России.

Конкурс – первый и пока единственный по-настоящему масштабный смотр самых современных и эффективных компаний России, их флагманских товаров и услуг. «РТСофт» стал одной из трёх компаний-лауреатов в номинации «Связь и информационные технологии», представив свою инновацию – бесшумный промышленный компьютер высокой надёжности BLOK. Он разработан и произведён компанией «РТСофт» по программе импортозамещения и был выбран комиссией из большого числа конкурсантов.

Сферы применения – локальный и удалённый мониторинг объектов в атомной энергетике, промышленности, авиации, системах специального назначения и в транспортной отрасли.

«BLOK дружелюбен, понятен, прост, надёжен и эффективен, – говорит технический директор «РТСофт» Алексей Рыбаков. – Мы сделали его для многолетней круглосуточной работы с минимальными затратами на обслуживание на базе самых современных идей и технологий».

Подробности – на сайте «РТСофт» по адресу: blok.rtsoft.ru.

Владимир Павлов, Сергей Жуков, Игорь Починок, Auriga Inc., НИВЦ МГУ

Обзор алгоритмов охлаждения в системах AdvancedTCA

Одна из важных задач управления в системах AdvancedTCA – адекватное охлаждение шасси и работающих в нём модулей. Существующие алгоритмы охлаждения используют разные подходы для нахождения необходимого баланса между двумя взаимоисключающими задачами – достаточного охлаждения системы и минимизацией производимого вентиляторами шума, а также потребления ими энергии. Это алгоритмы, основанные на анализе окружающей температуры, адаптивные алгоритмы и смешанные. Все они работают в рамках парадигмы зонного охлаждения, принятой в стандарте AdvancedTCA.

Неуклонное повышение производительности процессоров приводит к росту тепловыделения в геометрической прогрессии. Если в 2002 году спецификация AdvancedTCA допускала только 200 Вт тепловыделения на встраиваемый модуль, то на текущий момент многие модули выделяют уже 300 Вт. Последнее поколение модулей AdvancedTCA рассеивает свыше 400 Вт, а следующие поколения модулей для телекоммуникационного рынка будут иметь больший формфактор и смогут производить до 2 кВт на модуль.

Одна из важных задач управления в системах AdvancedTCA – адекватное охлаждение шасси и работающих в нём модулей. Как правило, в таких системах используется воздушное охлаждение за счёт обдува вентиляторами, и управляющий модуль регулирует скорость вращения вентиляторов. При этом управляющий модуль должен не только обеспечивать достаточное охлаждение системы, но и выполнять требования по минимизации производимого вентиляторами шума и потребления ими энергии. Существующие алгоритмы охлаждения используют разные подходы для нахождения необходимого баланса между этими взаимоисключающими задачами.

Требования к алгоритму охлаждения в спецификации AdvancedTCA

Спецификация AdvancedTCA допускает максимальную температуру окружающей среды +40°C. В чрезвычайных ситуациях системы ATCA могут выдерживать температуру окружающей среды до +55°C на некоторый (до 96 часов) период времени.

В нормальных рабочих условиях скорость вентиляторов должна регулироваться в соответствии с состоянием элементов шасси, установленных в шасси модулей и температурой окружающей среды. Для достижения оптимальной скорости вентиляторов могут использоваться алгоритмы, использующие данные от сенсоров, измеряющих температуру входящих и исходящих потоков воздуха, а также данные от установленного в шасси оборудования. Скорость вентиляторов может быть увеличена или уменьшена по достижении определённых условий, внутренних или внешних. Однако она должна сохраняться настолько низкой, насколько это возможно для минимизации производимого вентиляторами шума и потребления ими энергии.

С этой же целью спецификация AdvancedTCA предусматривает возможность *зонного* охлаждения, которое позволяет контролировать работу каждого блока вентиляторов и состояние охлаждаемых им модулей независимо друг от друга.

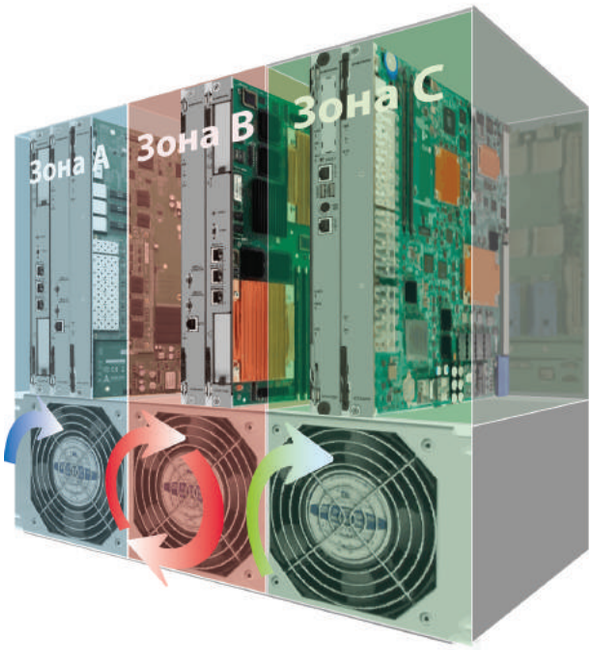
Когда управляющий модуль получает температурное событие, он должен нивелировать его последствия: ускорить вращение вентиляторов для увеличения воздушного потока или включить иную охлаждающую систему и, если это не решает проблему, уменьшить потребляемую мощность перегретого модуля. Если температурное событие критическое, то есть угрожает работоспособности самого шасси, управляющий модуль должен выключить перегретый модуль, а при необходимости все модули и само шасси. При возвращении системы в нормальное состояние управляющий модуль дол-

жен вновь включить модули и шасси, установить оптимальную скорость вращения вентиляторов. Способы достижения этих требований, равно как и алгоритмы работы системы охлаждения, являются прерогативой производителей и могут быть ключевым отличием одних систем AdvancedTCA от других.

Для оценки режима функционирования системы охлаждения определены следующие состояния:

– *нормальное* (normal), когда ни один сенсор в системе не пересёк определённых пороговых значений (например, для модуля сетевой маршрутизации, от 0 до +74°C);
– *горячее* (minor alert, non-critical state), если значение хотя бы одного сенсора превышает нижний порог, но не пересекает верхнего порога, определённых для этого состояния (например, для вышеуказанного модуля, от +74 до +84°C);
– *перегрев* (major alert, critical state), если значение хотя бы одного сенсора превышает нижний порог, но не пересекает верхнего порога, определённых для этого состояния (например, для того же модуля, от +84 до +94°C);
– *критическое* (critical alert, non-recoverable state), если значение хотя бы одного сенсора превышает порог, определённый для этого состояния (например, для того же модуля, выше +94°C).

Состояние системы охлаждения определяется по показаниям температурных сенсоров, размещаемых как в самом шасси, так и в устанавливаемом в этом шасси оборудовании. Изменение состояния происходит при пересечении показаниями датчиков определённых выше пороговых значений. Следует отметить, что пороговые значения температуры для определения состояния системы зависят от места установки сенсоров и задаются производителем оборудования в соответствие с собственными техническими требованиями.



Пример разбиения шасси на зоны охлаждения

Основная цель общей стратегии управления системой охлаждения – это сохранение нормального состояния системы при удерживании минимально возможной скорости вращения вентиляторов. Для достижения этой цели используются различные подходы.

Зонное охлаждение в стандарте AdvancedTCA

В настоящее время стандарт AdvancedTCA поддерживает *зонное* охлаждение. Использование механизмов зонного охлаждения позволяет управляющему модулю контролировать работу каждого блока вентиляторов и состояние охлаждаемых им модулей независимо друг о друга.

Данная возможность обеспечивается наличием специальной записи в наборе информации о шасси (Shelf FRU Information), в которой описывается соответствие между блоками вентиляторов и охлаждаемыми ими модулями. В результате шасси разбивается на некоторое количество *зон охлаждения.* Каждая из зон представляет собой множество вентиляторов и модулей, которые охлаждаются именно этими вентиляторами. Управляющий модуль реализует алгоритмы охлаждения отдельно и независимо для каждой зоны. По умолчанию (если информация о зонах отсутствует в наборе информации о шасси) шасси представляет собой единую зону охлаждения, где все блоки вентиляторов отвечают за охлаждение всех модулей в системе.

Каждая зона охлаждения оснащена собственными температурными сенсорами входящего и исходящего потоков воздуха. На основании показаний этих сенсоров, а также сенсоров на установленных модулях осуществляется оценка состояния данной зоны и выполняются действия в рамках стратегии управления системой охлаждения для данной зоны: увеличивается или уменьшается скорость вращения вентиляторов, производится выключение перегретых модулей и т. д. Пример разбиения шасси на зоны охлаждения приведён на рисунке.

Использование зонного охлаждения позволяет оптимизировать функционирование системы охлаждения, уменьшить её энергопотребление и уровень шума.

Алгоритмы, основанные на анализе окружающей температуры

Алгоритмы, основанные на анализе окружающей температуры, используют табличную функцию температуры для получения требуемой скорости вращения вентиляторов (см. таблицу). Такие алгоритмы наиболее просты в реализации и в системах AdvancedTCA исторически стали использоваться раньше других.

В нормальном состоянии модуль управления анализирует показания температурных датчиков входящих и исходящих потоков воздуха. Как правило, на входящий и исходящий потоки устанавливается несколько датчиков.

Для определения температуры окружающей среды используются сенсоры входящего потока. Датчики исходящего потока помогают оценить эффективность функционирования системы охлаждения, а также используются для определения состояния системы.

В качестве температуры окружающей среды принимается либо среднее, либо медианное значение показаний датчиков входящего потока. В качестве дополнительной меры для исключения ошибок может производиться проверка на расхождение показаний датчиков. Например, если показания какого-либо сенсора отличаются от показаний остальных сенсоров более чем на 10° С, эти показания исключаются из расчёта как ошибочные.

Как уже было написано выше, основная цель общей стратегии управления системой охлаждения – это сохранение нормального состояния системы при удерживании минимально возможной скорости вращения вентиляторов. В алгоритмах, основанных на оценке температуры окружающей среды, ответственность за минимизацию скорости вентиляторов возлагается на составителя таблицы-функции скорости вентилятора от температуры. При этом сам алгоритм оказывается проще в реализации, что ранее было актуально для систем со слабыми вычислительными ресурсами.

Пример таблицы–функции скорости вентилятора от температуры окружающей среды

Температура входящего потока, °С	Скорость вентилятора, уровень	PWM-сигнал [%]	Целевая скорость воздушного потока, м3/ч
T < -5	5	33	
-5 ≤ T < 0	6	40	
0 ≤ T < 20	7	47	520
20 ≤ T < 25	8	53	
25 ≤ T < 28	9	60	
28 ≤ T < 31	10	67	
31 ≤ T < 34	11	73	
34 ≤ T < 37	12	80	
37 ≤ T < 40	13	87	
40 ≤ T < 42	14	93	
T ≥ 42	15	100	1100

Адаптивные алгоритмы охлаждения

Эти алгоритмы используют адаптивный подход к управлению скоростью вращения вентиляторов.

Когда система работает в *нормальном* режиме, то есть показания температурных датчиков не превышают определённых пороговых значений, нет необходимости увеличивать скорость вращения вентиляторов. Более того, в *нормальном* режиме система охлаждения периодически уменьшает скорость вращения, пока она не достигнет определённого минимального значения или пока система не выйдет из *нормального* режима, когда показания одного или нескольких температурных сенсоров начнут превышать пороговые значения. Шаг уменьшения скорости вращения вентиляторов и период времени, по истечении которого происходит уменьшение скорости, являются конфигурируемыми параметрами и могут варьироваться в различных реализациях систем охлаждения. Минимальная скорость вращения вентиляторов также конфигурируемый параметр, однако его значение может изменяться как в сторону увеличения, если система начинает перегреваться, чтобы избежать дальнейшего повышения температуры, так и в сторону уменьшения, если система длительное время находится в *нормальном* режиме.

Таким образом, происходит адаптация системы управления охлаждением к условиям окружающей среды.

Считается, что система охлаждения работает в *аномальном* режиме, если показания по крайней мере одного температурного датчика в системе превышают предел *нормального* состояния.

В *горячем* состоянии *модуль управления* с заданной периодичностью увеличивает скорость вращения вентиляторов, пока система не вернётся в *нормальный* режим функционирования.

Если показания хотя бы одного сенсора указывают на *перегрев*, *модуль управления* устанавливает максимальную скорость вращения вентиляторов и начинает периодически уменьшать подачу питания на установленные в шасси модули, если это возможно, но не выключает их.

В *критическом* состоянии *модуль управления* устанавливает максимальную скорость вращения

вентиляторов. Если *критическое* состояние вызвано перегревом какого-либо установленного в шасси модуля, выключается только этот модуль, в противном случае выключаются все модули, установленные в шасси. В зависимости от конфигурации *модуля управления* после возврата системы в *нормальное* состояние, выключенные ранее модули либо включаются автоматически, либо для их включения требуется вмешательство оператора.

Модуль управления время от времени изменяет минимально допустимую скорость вращения вентиляторов во избежание колебания системы охлаждения между *нормальным* и *аномальным* состояниями. Выход системы из *нормального* в *аномальное* состояние означает, что текущая скорость вращения вентиляторов не обеспечивает эффективное охлаждение шасси. В этом случае *модуль управления* увеличивает минимально допустимую скорость вращения вентиляторов с тем, чтобы исключить в последующем возможность уменьшения скорости до неэффективного значения. Таким образом, после нескольких колебаний системы между *нормальным* и *аномальным* состояниями устанавливается минимально возможная скорость вращения вентиляторов, при которой обеспечивается достаточно эффективное охлаждение системы для её функционирования в нормальном режиме.

Чтобы учесть возможные изменения тепловой нагрузки в шасси за достаточно длительные периоды времени, предусматриваются дополнительные меры. Если система стабильно функционирует в нормальном режиме определённый период времени (например, 1 час), минимально допустимая скорость вращения вентиляторов уменьшается, с тем чтобы скорость вращения вентиляторов могла быть уменьшена до нового предельного значения. Если тепловая нагрузка в шасси уменьшится, периодическое уменьшение минимально допустимой и актуальной скоростей вращения вентиляторов будет продолжаться. В противном случае система вновь перейдёт в *аномальное* состояние, запустив процесс стабилизации системы охлаждения, как это описано выше.

При использовании зонного охлаждения описанные алгоритмы работают отдельно для каждой зоны. Так, например, скорость вращения вентиляторов устанавливается отдельно для каждой зоны и в случае *критического* состояния зоны выключение модулей ограничивается пределами зоны.

Настройка адаптивных алгоритмов для конкретных систем производится изменением порогов температурных сенсоров шасси и внутренних параметров алгоритма. Для модулей настройка порогов температурных сенсоров обычно не требуется, так как модули, как правило, поставляются с уже правильно предустановленными параметрами сенсоров.

Смешанные алгоритмы

В последнее время появились смешанные алгоритмы, которые в основе своей содержат табличный метод определения скорости вращения вентилятора, но в дополнение к таблице используют специальный корректирующий параметр, который прибавляется к скорости вращения вентилятора, полученной из таблицы. Значение этого корректирующего параметра адаптируется к состоянию системы охлаждения, то есть может увеличиваться или уменьшаться, принимая даже отрицательные значения. Таким образом, достигается основная цель общей стратегии управления системой охлаждения.

В общих чертах данный алгоритм выглядит следующим образом:

- Получить актуальный список датчиков, показывающих температуру входящего потока воздуха, и вычислить температуру окружающей среды (медиана, среднее арифметическое).
- Для системы, находящейся в *нормальном* состоянии:
  - уменьшить значение корректирующего параметра, если истёк период стабильного режима работы для корректирующего параметра и значение корректирующего параметра больше его минимально допустимого значения;
  - уменьшить значение минимально допустимого значения корректирующего параметра, если истёк период стабильного режима работы для минимально допустимого значения корректирующего параметра и его значение в допустимых пределах;
  - установить новую скорость вращения вентиляторов.
- Для системы, находящейся в *аномальном* состоянии (то есть показания по крайней мере одного температурного датчика в системе превышают предел *нормального* состояния):
  - установить максимальную скорость вращения вентиляторов;
  - увеличить значение корректирующего параметра, если оно не превышает максимально допустимого значения;
  - увеличить значение минимально допустимого значения корректирующего параметра, если оно не превышает максимально допустимого значения и если с момента последнего умень-

шения значения корректирующего параметра или перехода системы в *нормальное* состояние прошло определённое в конфигурации системы время.

Таким образом, приведённый выше алгоритм сочетает в себе как табличный метод определения скорости вентиляторов, который позволяет настроить работу конкретного оборудования для различных температурных условий, так и адаптивный метод, который обеспечивает возможность более гибкого достижения основной цели системы охлаждения.

Заключение

Рассмотренные алгоритмы работы систем охлаждения, применяемых в системах AdvancedTCA, показывают разные подходы производителей телекоммуникационного оборудования к решению проблемы отвода выделяемого при работе тепла и выполнению требований по минимизации производимого вентиляторами шума и потребления ими энергии.

Алгоритмы, основанные на анализе окружающей температуры, не универсальны, настраиваются под определённое оборудование, но имеют более простую реализацию.

Адаптивные методы более универсальны и могут применяться для любого оборудования, однако могут требовать настройки пороговых значений температурных сенсоров для учёта особенностей конкретной системы.

Смешанные алгоритмы позволяют производить более точную адаптацию системы охлаждения к определённым видам оборудования, сохраняя при этом гибкость адаптивного метода.

Литература

1. PICMG Advanced Telecommunication Computing Architecture (AdvancedTCA) Base Specification. Revision 3.0. http://www.picmg.org

2. Pigeon Point Shelf Management Mezzanine (ShMM) Shelf Manager Software Architecture. Technical Specification. http://www.pigeonpoint.com

3. With Thermal Dissipation Up, Will Cooler Heads (Up) Thinking Prevail? By Christian Ganninger // EMBEDDED SYSTEMS ENGINEERING, http://eecatalog.com/atca/2015/02/26/with-thermal-dissipation-up-will-cooler-heads-up-thinking-prevail/

Новости рынка

«РТСофт» ставит правильный BLOK

Компания «РТСофт» запустила в серию новое поколение ультракомпактных бесшумных отечественных встраиваемых компьютеров серии BLOK. Машины предназначены для создания широкого спектра решений при построении ответственных эргономичных систем с длительным жизненным циклом в атомной энергетике, в управлении воздушным движением, на транспорте, в специальных сегментах экономики. Компьютеры BLOK прекрасно подходят для создания сетевых мультимедийных человеко-машинных интерфейсов, в качестве встраиваемых компактных серверов, бортовых машин и коммуникационных шлюзов.

Компьютеры BLOK обеспечены высоким уровнем сертификационной и лицензионной поддержки. Машины имеют сертификаты ГОСТ Р и Таможенного Союза. Компания-производитель имеет самый широкий перечень сертификатов и лицензий для работы в различных сегментах экономики РФ и стран ТС: TUV ISO 9001-2008, ФСТЭК, Ростехнадзора, ФСБ, Минпромторга и др.

Идеология машин основана на правильных R&D-рецептах, делающих BLOK одной из основ успешной программы импортозамещения ЗАО «РТСофт»:

– опора на **собственные ресурсы с огромным опытом** (22+ лет) партнёрства с ведущими российскими и зарубежными инженерными компаниями;
– **производство на территории России** на базе собственного комплекта КД. BLOK – не «отвёрточная» сборка, а полноценный проект НИОКР;
– максимальная **независимость и защищённость** от действий поставщиков и производителей компонентов: все критически важные части BLOK имеют альтернативных поставщиков и производителей. Эмбарго и BLOK несовместимы;
– поддержка **актуальных мировых концепций** в embedded-дизайне: SWaP, IoT, MiniTCO (необслуживаемость), 24x7, кондуктивное охлаждение;
– опора на **открытые международные стандарты**: COM Express (PICMG COM.0), PCISIG MiniPCI Express и проверенные референсные дизайны;
– **Ориентированный на будущее выбор** стандартных цифровых технологий: сети, мультимедийность, процессоры, диски, архитектура расширений;
– построение **изменяемой архитектуры**, гарантирующей заказ оптимальной конфигурации в части CPU, SDRAM, SSD/HDD, miniPCI Express I/O;
– построение архитектуры BLOK, гарантирующей максимальную **plug&play-совместимость** с широким спектром готового системного ПО класса Linux, Windows, QNX, VxWorks, LynxOS и их отечественными клонами;
– использование **промышленных embedded-компонентов**, имеющих длительный жизненный цикл и исполнение E2 (–40…+85° C);
– **универсальные возможности** для встраивания и охлаждения: 19-дюймовая стойка, стол, «холодная поверхность», стена, потолок;
– возможность **модернизации машин в будущем**: переход на новые поколения микропроцессоров и операционных систем.

Важное преимущество изделий BLOK – широкие возможности индивидуализации в соответствии с пожеланиями заказчика: изменение входных характеристик питания, расширение температурного диапазона, усиление механических и IP-свойств, портация ОС, интеграция с промышленным монитором GT777, отвечающим требованиям IV группы исполнения ТС АС-ЯРО, превращающая BLOK в готовый сетевой человеко-машинный интерфейс.

Следуя современным требованиям рынка, производитель оснастил компьютеры BLOK четырьмя портами GEthernet, шестью портами USB 3.0/2.0 и двумя COM-портами, а также звуковой подсистемой Intel HD. Для расширения доступны два слота Mini PCI Express: обеспечена подготовка для работы в средах Wi-Fi и GSM, а также с модулями доверенной загрузки, российских производителей. В базовой конфигурации используется двухъядерный ЦП Intel Core i5 Haswell с тактовой частотой 1,6 ГГц (может быть заменён на другие ЦП серий Intel Core i7, Intel Atom и микропроцессоры отечественного производства), до 16 Гбайт памяти DDR3L-1600 и два накопителя формата 2,5”, которые могут быть объединены в RAID-массив.

Важное свойство платформы BLOK – поддержка вывода на три дисплея в разрешениях до 4K через три интерфейса DisplayPort. Малое тепловыделение ЦП позволяет системе быть безвентиляторной, что повышает надёжность и обеспечивает **нулевой** уровень шума. Производитель предоставляет на BLOK гарантию до 4 лет, при этом средняя наработка на отказ составляет 70000 часов. Базовая конфигурация в корпусе высоты 1U весит 4,4 кг, рассчитана на работу при температурах от –10 до +55° C и монтируется в 19-дюймовую стойку, на стену, на рейку DIN либо устанавливается на стол.

Машины доступны для бесплатного «тест-драйва» со склада «РТСофт». Учитывая нужды пользователей, производитель оказывает профессиональную поддержку комплексной совместимости в системах заказчика. Выбирая BLOK, пользователи получают современную цифровую функциональность, совместимость с перспективным оборудованием, низкую стоимость владения, чрезвычайную простоту обслуживания, техническую поддержку ведущих экспертов отрасли и 100-процентную защиту от санкций и ограничений.

С подробной информацией по BLOK можно ознакомиться на сайте компании «РТСофт» по адресу: http://www.rtsoft.ru/catalog/int/platformy/detail/2648/

Начато серийное производство защищённых промышленных мониторов серии GT777

Компания «РТСофт» запустила в серию новое поколение промышленных мультимедийных мониторов серии GT777. Мониторы предназначены для создания ответственных эргономичных диспетчерских систем с длительным жизненным циклом в атомной энергетике, на транспорте, в промышленных и специальных приложениях. В настоящее время, в соответствии с ЛКЖТ.467249.001-00 ТУ, серия GT777 включает две модели: GT777-24 и GT777-27.

Линейка GT777 привлекательна наличием необходимых сертификатов/лицензий на применение – как у самих изделий (ГОСТ Р и Таможенного Союза как оборудование IV группы исполнения ТС АС-ЯРО), так и у компании-производителя: TUV ISO 9001-2008, ФСТЭК, Ростехнадзора, ФСБ, Минпромторга, для аккредитации в службах приёмки и др.

Мониторы GT777 имеют полный комплект КД российской разработки и выпускаются на производственной площадке ЗАО «РТСофт» в г. Черноголовке. Линейка GT777 разработана с целью импортозамещения мониторов зарубежных производителей на основе более чем 20-летнего опыта компании «РТСофт».

Важное преимущество GT777 – широкие возможности индивидуализации в соответствии с пожеланиями заказчика: увеличение разрешения до 2560 × 1440, установка сенсорного экрана, расширение диапазона рабочих температур, оптимизация конструкции для работы в агрессивных средах по всему корпусу, улучшение характеристик EMC и т. п.

Отвечая требованиям рынка, производитель оснастил серию GT777 перспективными мультимедийными интерфейсами DisplayPort и HDMI, что гарантирует простую и удобную интеграцию мониторов с самым широким спектром современного компьютерного оборудования. Идеальной парой для GT777 служат новые машины специального назначения серии BLOK, также серийно освоенные на производстве «РТСофт».

Мониторы обеспечивают высокое качество изображения в формате Full HD с LED-подсветкой, имеют универсальные БП переменного тока с автоматическим выбором режима и рассчитаны на работу при температурах от 0 до +50° С. Изделия линейки GT777 весьма эргономичны: толщина 27-дюймовой модели не превышает 70 мм! Мониторы гарантируют существенные показатели наработки на отказ (не менее 50000 часов), обладают лёгким весом, прочны и отлично защищены: IP67 и IP30 по передней и задней панелям соответственно. Срок гарантии на мониторы до 4 лет! Модульный дизайн позволяет при необходимости организовать ремонт обслуживающим персоналом прямо на месте эксплуатации!

Образцы мониторов GT777 оперативно доступны для бесплатного «тест-драйва» со склада «РТСофт». Учитывая нужды пользователей, производитель оказывает профессиональную поддержку для обеспечения комплексной совместимости в системах заказчика. Выбирая серию GT777, пользователи получают современную цифровую функциональность, совместимость с перспективным оборудованием, низкую стоимость владения, чрезвычайную простоту обслуживания, техническую поддержку ведущих экспертов отрасли и 100-процентную защиту от санкций и ограничений.

С подробной информацией по GT777 можно ознакомиться на сайте компании «РТСофт» по адресу: http://www.rtsoft.ru/catalog/int/platformy/detail/2649/

Новости рынка

Новости «Интернета вещей»: модуль COMe–cBL6 и плата mITX–BDU–U на процессорах Intel Core пятого поколения

Компания «РТСофт» и международный холдинг Kontron выводят на российский рынок два новых продукта, характеризующихся повышенной надёжностью и технологичностью, которые позиционируются производителем как готовые к «Интернету вещей» (IoT ready). Речь идёт о «компьютере-на-модуле» COMe-cBL6 (стандарт COM Express) и компактной материнской плате mITX-BDU-U (форм-фактор Mini-ITX). Данные изделия оснащаются высокоинтегрированными процессорами Intel Core пятого поколения либо ЦП из линейки Intel Celeron и подходят для использования в приложениях класса «Интернет вещей» (Internet of Things – IoT).

Новый «компьютер-на-модуле» и новая материнская плата могут быть полезны в самых различных ситуациях, где требуется поддержка функции мультитач и/или необходимо оптимизировать использование электроэнергии. В качестве примеров соответствующих систем можно назвать:

– человекомашинные интерфейсы для задач автоматизации и медицинских приложений;
– промышленные планшеты для логистики, розничной торговли и производства;
– системы наблюдения и безопасности;
– системы типа Digital Signage;
– POS-терминалы.

COMe-cBL6 – это изделие типа «компьютер-на-модуле» (Computer On Module) стандарта COM Express с «распиновкой» Type 6. Поддерживая различные модели процессоров от Intel Core i7 до Intel Celeron, данный продукт хорошо масштабируется и обеспечивает охват широкого спектра прикладных требований. В частности, на нём устанавливаются новейшие ЦП Intel Core пятого поколения, которые изготавливаются по технологическим нормам 14 нм и демонстрируют повышенную производительность в обычных и графических вычислениях при малом энергопотреблении. Объём энергоэффективной памяти DDR3L достигает 8 Гбайт, чего достаточно даже для самых «прожорливых» приложений, при этом для эксплуатации изделия в особо жёстких условиях память может быть напаяна непосредственно на печатную плату. Поддержка мультидисплейных конфигураций обеспечивается за счёт наличия трёх независимых графических портов: двух интерфейсов DP++ (DisplayPort, HDMI, DVI) и одного двухканального интерфейса LVDS. Стандартная функциональность ввода-вывода включает также 4 порта SATA (6 Гбит/с), канал Gigabit Ethernet, 2 порта USB 3.0 и 6 портов USB 2.0. Для подключения реализуемых на базовой плате пользовательских расширений доступен быстрый интерфейс PCI Express x4. Возможность использования низковольтного питания (от 8,5 до 20 В) и интеллектуальных батарей (MARS) упрощает применение нового COM-модуля в мобильных системах и/или в системах с аккумуляторным питанием. «Компьютер-на-модуле» COMe-cHL6 стандарта COM Express может работать под управлением операционных систем Microsoft Windows 8.1, Windows 7, Windows Embedded 8.1 Industry, Windows Embedded Standard 7 и Linux, а также ОС реального времени VxWorks.

Изделие mITX-BDU-U представляет собой полноценную встраиваемую материнскую плату, которая отличается малыми размерами и пониженным энергопотреблением. На неё могут устанавливаться различные 14-нанометровые ЦП Intel Core пятого поколения, относящиеся к линейкам i7, i5 и i3. Благодаря использованию процессоров с энергопотреблением до 15 Вт и высотой 23 мм вместе с радиатором, данное решение является экономичным и низкопрофильным. Его можно питать от «ноутбучного» адаптера 12 В или от внутреннего 12-вольтового разъёма. Материнская плата mITX-BDU-U может работать одновременно с тремя дисплеями, для чего в ней предусмотрено 2 интерфейса DisplayPort и 1 интерфейс LVDS. Другие внешние устройства можно подключать через порты USB 3.0 и USB 2.0 (4 и 3 штуки соответственно). Также в наличии 2 интерфейса Gigabit Ethernet и 3 порта SATA III с поддержкой массивов RAID 0 и 1. Суммарный объём памяти DDR3L, устанавливающейся в 2 разъёма SO-DIMM, может достигать 16 Гбайт. Поддерживаются операционные системы Windows 7, Windows 8.1 и Linux. Как и у всех материнских плат марки Kontron, жизненный цикл изделия mITX-BDU-U достигает 7 лет и более.

Продукты COMe-cBL6 и mITX-BDU-U запущены в серийное производство.

Дополнительную информацию о COMe-cBL6 и mITX-BDU-U можно получить на страницах сайта Kontron, посвящённых данному продукту, а также в офисах компании «РТСофт», стратегического партнёра холдинга Kontron в России и странах СНГ.

Сис Линкс (Cees Links), Greenpeak technologies

«Интернет вещей» и стандарты беспроводной связи

Как показывает история, если случается война стандартов, то она одинаково невыгодна и победителям, и проигравшим. Война стандартов дорого обходится ещё и потому, что она тормозит развитие рынков, поскольку и клиенты, и компании бездействуют и ждут, когда же «всё устаканится». Это справедливо и для «Интернета вещей». «Интернет вещей» – великолепная возможность, уже создаются разнообразные приложения, но для их массового внедрения велика роль унифицированной стандартизации.

На пути развития инициатив, связанных со стандартизацией технологий, возникают, как показывает опыт, волны войн и волны плодотворного сотрудничества. Классический пример – так называемая «война» между VHS и Betamax (в районе 1980 г.), которая существенно задержала развитие рынка домашнего видео. Другой пример войны стандартов гораздо ближе к нашему времени (где-то в 2007 г.). Это война оптических DVD-дисков между Blue-ray и HD-DVD.

Итоги этих двух технологических баталий с очевидностью показали, что ничего хорошего в подобных войнах нет и что даже победители страдают от застоя в своём развитии и задержки их рыночного признания. Взлёт экономической активности, связанный с унификацией стандартов, всегда резко контрастирует с рыночным застоем, порождённым конкуренцией между стандартами или, якобы проприетарными, «псевдостандартами».

Заканчиваются войны стандартов обычно тогда, когда большая компания или доминирующая на рынке группа компаний делает выбор и создаёт критическую массу соответствующих продуктов. В 1999 году компания Apple решила использовать в своих лаптопах Wi-Fi, и через несколько месяцев после этого решения компания HomeRF практически исчезла с рынка. Нечто подобное случилось с Betamax и HD-DVD, когда Голливуд поддержал всей своей массой VHS и Blue-ray.

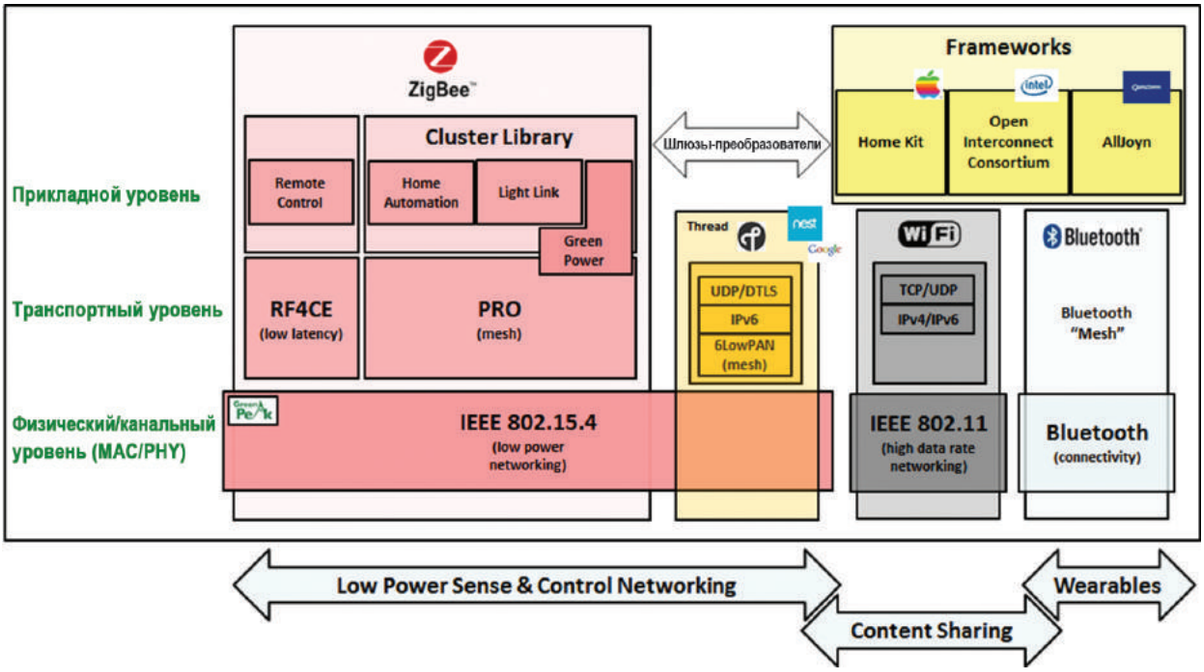


Рис. 1. Обзор различных стандартов беспроводной связи для «Интернета вещей» в контексте многоуровневой модели ISO

Однако нокауты такого типа со стороны той или иной компании обычно происходят после многолетних дорогостоящих акций по поливанию своих конкурентов грязью и затяжного застоя на рынке.

За что бьются в области «Интернета вещей» и кто ведущие Игроки?

После серьёзных войн между стандартами практически всегда наступает период сотрудничества. Стандарт DVD (1995 г.) в его исходном виде был принят без особой борьбы, возможно, потому, что большие компании ещё не забыли о войне VHS/Betamax и порождённых ею экономических потерях. Поэтому рынок принял стандарт DVD удивительно быстро и видеокассеты исчезли практически за одну ночь. Обзор основных соперников в сфере стандартов беспроводной связи для «Интернета вещей» представлен на рис. 1.

Для простоты я опустил стандарты сотовой связи, несмотря на то, что их роль в «Интернете вещей» (и в так называемом бизнесе M2M) всё же важна. Однако всякого рода конкуренция среди этих стандартов – тема отдельного разговора. Я также опустил технологию RFID, тоже весьма полезную для «Интернета вещей» с точки зрения безопасности, но менее дискуссионную, поскольку она выступает скорее в роли электронного шрих-кода, чем в роли реальной (дуплексной) связи. Также для простоты я опустил проприетарные псевдостандарты типа ANT+, Z-Wave и EnOcean. Причина проста: я полагаю, что, как и другие «нестандартные» проприетарные стандарты, они через несколько лет не выдержат конкуренции с международным стандартами, которые будут широко приняты данной отраслью.

Таким образом, поле битвы связных стандартов для «Интернета вещей» можно разделить на три горизонтальных уровня (или комбинации уровней): 1) *физический/канальный уровень* («коннектор»), 2) *сетевой/транспортный уровень* («беспроводной кабель») и 3) *прикладной уровень* («кто-то делает что-то для кого-то»).

Физический/канальный уровень

За *физический/канальный уровень* (рис. 2) в нашей отрасли ведётся несколько критически важных боёв. Так, в 1990-х годах Ethernet (IEEE 802.3) сражался с Token Ring (IBM) и ARCnet (Datapoint). А 1999 году Bluetooth (Bluetooth SIG) воевал с Wi-FI (IEEE 802.11). Это закончилось, когда оба последние стандарта нашли свои собственные устойчивые прикладные ниши и смогли окопаться ввиду возможной перспективы следующего раунда (Wi-FI Direct в атаке на Bluetooth). Далее война перекинулась в область сетей с малым энергопотреблением (low power networking). Уже не стоит удивляться, что против IEEE 802.15.4, который доминирует на этом рынке, острят мечи Wi-FI (с «low power Wi-FI») и Bluetooth (с «Bluetooth Low Energy»), стремясь тоже поучаствовать в борьбе за маломощные сети.

Всё же следует отметить, что на этом уровне доминируют всемирно принятые открытые стандарты – в основном на базе IEEE – и в реальности война практически закончилась, поскольку большинство разногласий разрешены в рамках органов по стандартизации.

Все три основных IEEE-стандарта всё ещё конкурируют за захват как можно большей части рынка приложений. Однако все они – IEEE 802.11/Wi-FI для совместного использования и распространения кон-

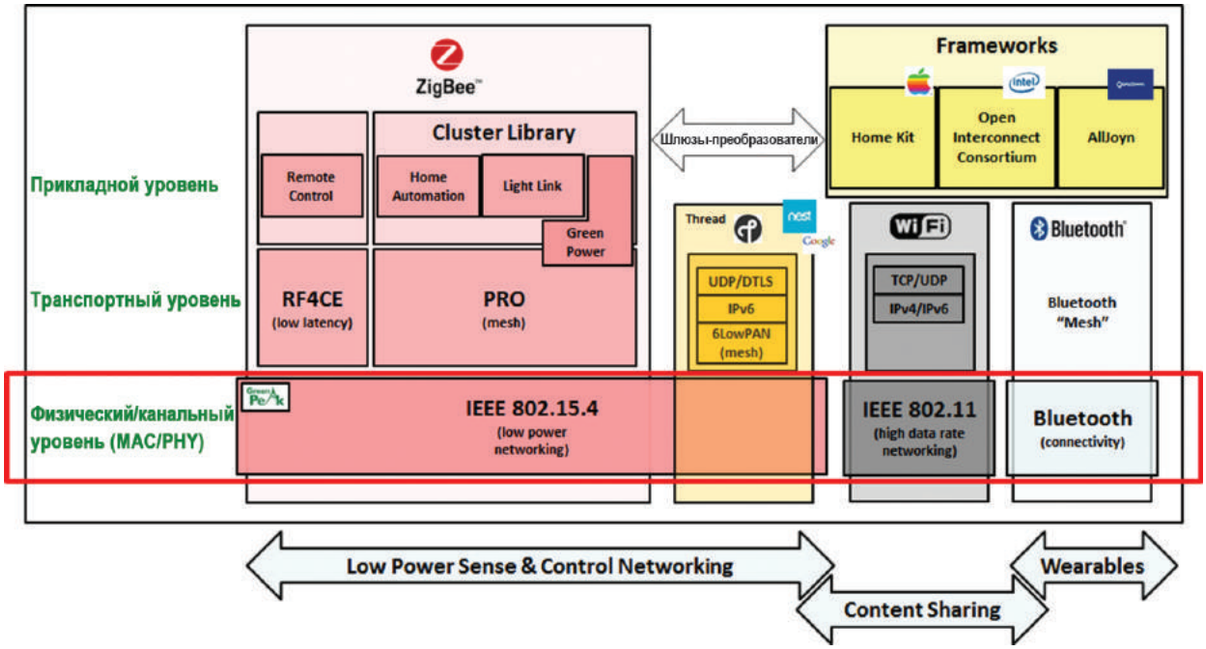


Рис. 2. Системы с большой нагрузкой на физический/канальный уровень и ограниченным энергопотреблением

тента (Content Sharing), 802.15.4/ZigBee для передачи датчиковой и управляющей информации по маломощным сетям (Low Power Sense & Control Networking) и Bluetooth для замены кабелей в носимых устройствах (Wearables) – кажется, нашли свои основные прикладные ниши и будут с нами ещё длительное время.

Сетевой/транспортный уровень

В прошлом были серьёзные битвы и за *сетевой/транспортный уровень*. Это довольно тёмная область, где когда-то доминировали такие продукты и компании, как LAN Manager (IBM, Microsoft), Netware (Novell), и некоторые другие. Однако её «демократизировало» сообщество Internet Engineering Task Force (IETF) со своим протоколом TCP/IP, который хорошо известен как распространённый сейчас IPv4 и появившийся позднее IPv6 – вклад сообщества IETF в «Интернет вещей». Также IETF создал стандарт 6LoWPAN (IPv6 over Wireless Personal Area Networks – IPv6 поверх беспроводных персональных сетей), который позволяет передавать трафик IPv6 по маломощным беспроводным ячеистым сетям (mesh) (рис. 3).

Недавно компания Google/Nest адаптировала 6LoWPAN как часть протокола Thread, благодаря чему Thread сразу получил кредит доверия и вступил в прямую конкуренцию с ZigBee PRO, ещё одним претендентом на эту нишу. Протоколы ZigBee PRO и Thread (на базе одного и того же физического/канального уровня IEEE 82.15.4) обладают относительно друг друга определёнными преимуществами. Поддерживая IPv6, протокол Thread хорошо интегрирован в мир IP. Что же касается ZigBee, то он уже широко принят, интегрирован с по-настоящему большой и тщательно протестированной прикладной библиотекой (см. ниже), доказал свою защищённость и удобство применения, и при этом тоже может взаимодействовать с IPv6.

В данный момент консорциум Google/Nest Thread Alliance пытается объединить вокруг себя как можно больше участников, чтобы подтолкнуть продвижение протокола Thread, но процесс идёт относительно медленно: пока менее 100 членов, в то время как в консорциуме ZigBee более 400 участников. Интересно, что многие члены альянса Thread входят также и в консорциум ZigBee! До тех пор, пока стандарт Thread не будет опубликован, эта ситуация останется неопределённой и, как отмечено ранее, приведёт к выжидательному поведению на рынке «Интернета вещей», что, к сожалению, замедлит его развитие.

Чтобы ещё больше усложнить ситуацию, в этой сфере есть и другая группа, которая «мутит воду» на *сетевом/транспортном уровне*. В консорциуме Bluetooth (Bluetooth SIG) серьёзно пытаются развить у протокола Bluetooth «способности к организации сети». Другими словами, консорциум Bluetooth пытается добиться того, чтобы сетевой уровень протокола Bluetooth мог поддерживать набор «носимых компьютеров» (гаджетов) не только вокруг одного устройства, но и расширить его до более широкого набора независимых устройств, работающих вместе в составе ячеистой сети (mesh). Несмотря на то, что завершение работ ожидается не ранее 2017 года, для «Интернета вещей» и разработчиков устройств «Умного дома», ситуация ещё более туманная.

Здесь, однако, важен ответ на принципиальный вопрос: а есть ли техническая возможность для создания Bluetooth Mesh (ячеистая сеть Bluetooth)? Протокол Bluetooth, как и Wi-Fi, «ориентирован на соединения»,

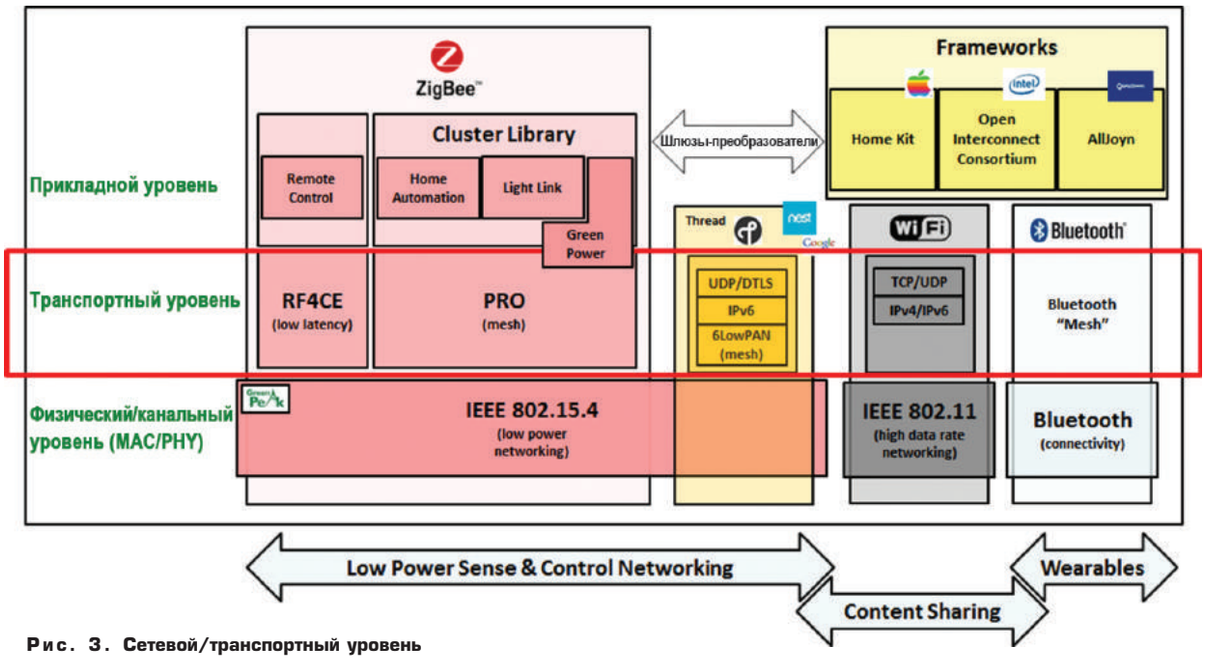


Рис. 3. Сетевой/транспортный уровень

в то время как стандарт IEEE 802.15 для ZigBee и Thread ориентирован на коммутацию пакетов, что очень подходит для протоколов ячеистых сетей. Попытка в 2001 году создать ячеистую самоорганизующуюся сеть на базе Wi-FI (стандарт IEEE 802.11s) печально провалилась, поскольку для протоколов, ориентированных на соединения, победить «задержки» оказалось неподъёмно трудной задачей. В данный момент складывается такое впечатление, что ячеистая сеть Bluetooth отличается от ячеистой сети Wi-Fi d в основном логотипом.

Для многих специалистов эта новая инициатива вокруг Bluetooth звучит как повторение более ранней попытки (где-то в 1997–2000 гг.) вытеснить Wi-FI, добавив сетевые возможности. «Bluetooth сотрёт Wi-Fi с лица земли» – вот слоган того времени. Как все мы знаем, тот проект по вытеснению Wi-Fi печально провалился. В настоящий момент Bluetooth Mesh больше похож на попытку инженеров «заняться чем-нибудь интересненьким», а не на попытку удовлетворить насущные потребности рынка. Возможно, эта новая инициатива вскоре иссякнет, как раньше создатели Bluetooth остановили попытки соперничать с Wi-Fi.

Прикладной уровень

Чтобы по-настоящему понять интригу баталий на *прикладном уровне* (рис. 4), хорошо бы посмотреть на картинку снова, но не по горизонтали, а по вертикали.

Прикладной уровень – это совокупность команд и ожидаемых результатов взаимодействия устройств («вещей») друг с другом. Это самый сложный уровень, поскольку он охватывает так много разных устройств в таком огромном количестве приложений в таком широком спектре интересов пользователей, что в данный момент трудно представить реально законченную картину предъявляемых к нему требований.

«Умные» системы для дома абсолютно не похожи на «умные» системы для зданий и сооружений или для «умных» городов (управление уличным освещением или свободными местами на автопарковках), в то время как промышленные датчики – это свой отдельный класс устройств. Неудивительно, что прикладной уровень обширен и разветвлён. Есть и непрерывное накопление связанных с этим уровнем знаний и опыта, включая облачные интерфейсы, методы анализа, взаимодействие с социальными сетями, приложениями для смартфонов и т. п.

Первый и самый зрелый боец на этом пространстве – так называемая «Cluster Library» («библиотека кластеров»), которая является частью стандарта ZigBee (ZCL). В версии 3.0 стандарта ZigBee эта библиотека полностью интегрированная, включая так называемые профили приложений домашней автоматизации (Home Automation) и освещения (Lighting), плюс приложения для поддержки сверхнизкого энергопитания (например, безбатарейного) Green Power и ZRC для приложений со сверхнизким временем ожидания (low latency), которые необходимы для удалённого управления (Remote Control). Эта ZigBee Cluster Library доведена до совершенства, обладает хорошо продуманной защищённостью и легко устанавливается. В настоящее время в ней установлена самая большая база вендоров.

Второй соперник – программный пакет Apple Home Kit. Это действительно соперник, но не в такой степени стандарт, поскольку Apple Home Kit – собственность компании Apple. Тем не менее, поскольку компания Apple – сильный рыночный игрок и «кумир»

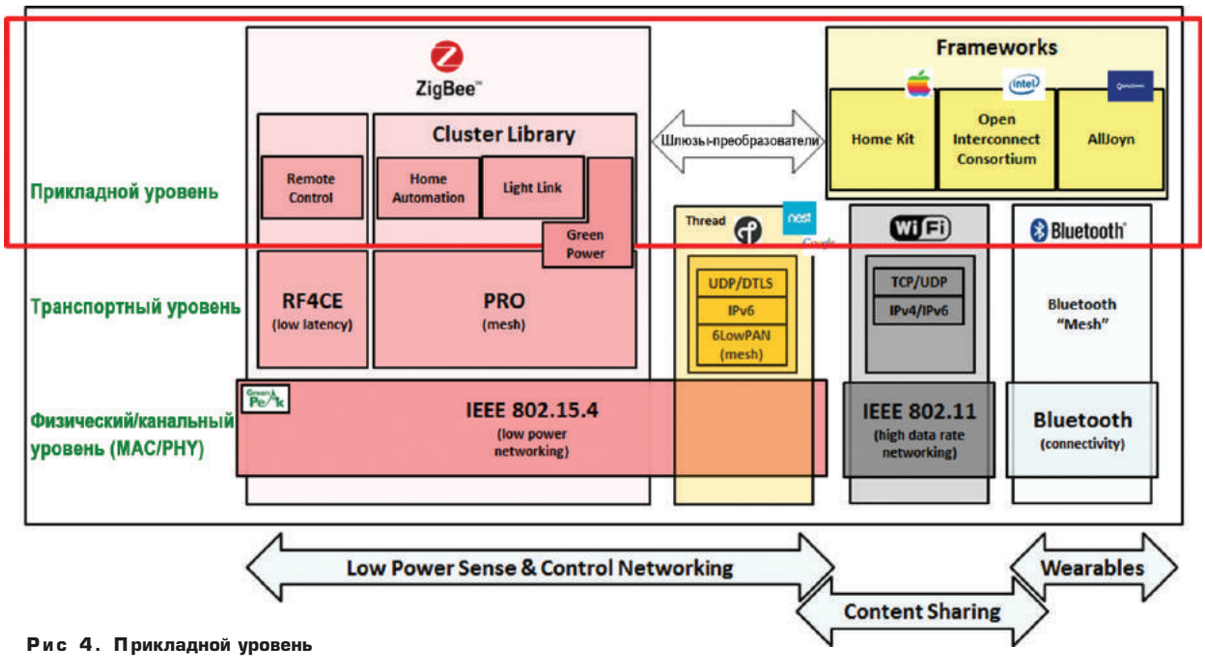


Рис 4. Прикладной уровень

для многих поклонников, Apple Home Kit расширяет своё присутствие на рынке благодаря прикладным надстройкам над Wi-Fi и Bluetooth для сетевой поддержки малопотребляющих носимых компьютеров и гаджетов. В настоящее время Home Kit со стандартом IEEE 802.15 не интегрирован, но возможности для интеграции с ZigBee и ZigBee Cluster Library у него всё же есть.

Третий игрок в борьбе за прикладной уровень – консорциум Open Interconnect, приводимый в движение компаний Intel и поддерживаемый другими компаниями типа Cisco и Samsung. Именно эта группа недавно включилась в работу и – подобно Apple – отдала предпочтение Wi-Fi и Bluetooth, с прицелом на ZigBee в перспективе. Консорциум Open Interconnect анонсировал IoTivity, проект открытого ПО (Open Source) под эгидой консорциума Linux Foundation, который помогает идентифицировать подключённые к сети устройства на прикладном уровне.

Последний соперник на этом поле – альянс AllSeen, которой (что достаточно любопытно) тоже действует под эгидой Linux Foundation. Всё началось с работы над проектом AllJoyn в компании Qualcomm, однако вскоре стало понятно, что рынок очень большой, сильно диверсифицирован и очень зависит от разработки законченной экосистемы, и что вытянуть всё это в одиночку неподъёмно. В результате Qualcomm профинансировал всю работу до момента создания альянса AllSeen, который Qualcomm по-прежнему возглавляет, но вся дальнейшая деятельность ведётся независимо.

Обо всех перечисленных инициативах, призванных заполнить прикладной уровень, есть что сказать отдельно.

Во-первых, все перечисленные соперники в борьбе за *прикладной уровень* в весомой доле участвуют в одних и тех же профессиональных сообществах, причём до такой степени, что это не только влияет на рынок, но некоторых из них даже путают. Например, многие из более четырёхсот членов консорциума ZigBee состоят также в OIC и AllSeen, играя роль «моста» между ними. Кроме того, результаты такой «работы по совместительству» – разные фреймворки (Frameworks) – мало чем отличаются по своему назначению и частично дополняют друг друга.

Главная задача, которую решает библиотека ZigBee Cluster Library, – описание функциональности простых устройств (лампы, термостаты и т. п.), и в качестве таковой хорошо укомплектована, поскольку наполнялась и совершенствовалась в течение многих лет.

Пакет Home Kit компании Apple фокусируется на представлении конкретных устройств конкретному пользователю (в доме, в комнате и т. д.) и, что не удивительно, строит эту структуру как расширение смартфона – использование смартфона в качестве центра экосистемы. В настоящее время всё это хорошо используется для «носимых устройств» («аксессуары» для смартфона), но как это могло бы работать в составе, например, «умного дома» (Smart Home) до сих пор никто не видел. Тем не менее, благодаря рыночному успеху смартфона Apple и тому факту, что Apple – продуктовая компания, а многие клиенты Apple соблюдают верность экосистеме продуктов Apple, Home Kit, возможно, не покинет нас ещё некоторое время.

Возможно, самая перекрёстная деятельность ведётся в рамках инициатив OIC/IoTivity и AllSeen/AllJoyn. Оба проекта фокусируются на создание специальных средств для обнаружения подключённых к сети устройств и выявления, как они взаимодействуют. Поэтому данные проекты – прямые конкуренты. В отличие от Apple Home Kit, оба запущены и поддерживаются полупроводниковыми компаниями. Учитывая, что и тот, и другой связаны с Linux Foundation, встаёт вопрос, насколько долго они будут развиваться отдельно.

Возможным развитием событий стало бы слияние этих проектов в один и объединение с библиотекой ZigBee Cluster Library, что позволило бы сохранить конкурентоспособность по отношению к «проприетарному» Home Kit компании Apple. Интеграция с высокоразвитой и надёжной библиотекой ZigBee Cluster Library имела бы смысл для любого из этих проектов, в то время как ZigBee Cluster Library может «выиграть» благодаря перспективе расширения фреймворка и возможности работы не только через ZigBee, но и через Wi-Fi и Bluetooth.

И последнее интересное наблюдение заключается в том, что в данном *прикладном уровне* полностью отсутствует Google/Nest и что (теоретически) он мог бы работать с ЛЮБЫМИ другими, уже специфицированными, прикладными уровнями. Однако результатом этого отсутствия становится то, что Thread не является полным стандартом и что в том виде, в каком он есть, он не позволяет взаимодействовать «разнокалиберным» устройствам. Если когда-нибудь стандарт Thread появится, потребуется его интеграция с каким-нибудь прикладным уровнем. И в данном случае имеет смысл интегрировать Thread с библиотекой ZigBee Cluster Library, так как только тогда он станет «полным» стандартом, то есть вообще стандартом...

Коммуникационные возможности «Интернета вещей» – «плохие новости» для разработчиков

1. В настоящее время стандарт IEEE 802.15.4 (2, 4 ГГц) принят главным образом в качестве стандарта физического/канального уровня для малопотребляющих датчиковых и управляющих сетей, в сочетании с Wi-FI для сетей распространения контента, а в сочетании с Bluetooth – для «носимых» устройств.

2. Неспокойно на *сетевом/транспортном уровне*, где Google/Nest пытается установить стандарт, бросающий открытый вызов официальному органу по стандартизации (альянсу ZigBee). После того как был заложен фундамент, деятели из Google/Nest реформировали себя в открытую организацию (альянс Thread). Однако, несмотря на крикливые обещания и политические махинации, сам стандарт Thread неполон и, чтобы приобрести значимость на данном рынке, нуждается в расширении.

3. Большая неразбериха на *прикладном уровне*, где требуется дальнейшее развитие технологий. Компании Apple, Google/Nest, Intel, Qualcomm пытаются определить стандарты и/или «встать во главе движения». Частично они конкурируют с альянсом ZigBee, а в чём-то его дополняют.

4. Единственной хорошо развитой и рыночно испытанной реализацией прикладного уровня является библиотека ZigBee Cluster Library, которую имеет смысл использовать для всех конкурирующих фреймворков *прикладного уровня*. Интеграция с этой библиотекой поможет каждому из них получить признание на рынке.

5. Появление на рынке стандартов IEEE 802.11ah (маломощный WiFi для уровня MAC/PHY) и Bluetooth Mesh запаздывает (ожидаются не ранее 2017 года), и с большой вероятностью они окажутся нерелевантными.

Итак, куда всё движется – к реальной войне или к мирному урегулированию? Будем надеяться, вместе со всеми компаниями, которым не терпится собрать урожай с «Интернета вещей», что случится последнее. Чем скорее, тем лучше.

Дополнение после апреля 2015 года

2 апреля 2015 года консорциумы ZigBee Alliance и Thread Group объявили о своём сотрудничестве в области разработки объединяемых в сеть бытовых приборов и устройств. Благодаря этому соглашению открывается перспектива работы протокола прикладного уровня ZigBee Cluster Library в сетях Thread.

При этом у альянса ZigBee появляется чёткая IP-стратегия, а у альянса Thread – перспектива создания стандарта на профили приложений.

Понятно, что для того чтобы воплотить это в жизнь, нужно многое сделать, включая соответствующие спецификации на тестирование и процедуры сертификации, однако это облегчит жизнь как поставщикам продуктов, так и поставщикам технологий и, в частности, поможет в решении следующих задач:

1. Сосуществование сетевого уровня ZigBee PRO и сетевого уровня Thread либо их миграция во что-то третье.

2. Интеграция устройств с малым потреблением (ZigBee Green Power) в среду Thread.

3. Внедрение ультраскоростных возможностей протокольного стека RF4CE ZRC2.0 в сети ZigBee/Thread.

Все ключевые компоненты для построения дееспособной среды локального «Интернета вещей», в принципе, есть. Остаётся добиться того, чтобы эта среда была одновременно защищённой, энергоэффективной, простой в использовании (самоустанавливающейся) и недорогой (рис. 5).

Источник: Wireless Communication Standards for the Internet of Things, GreenPeak White Paper

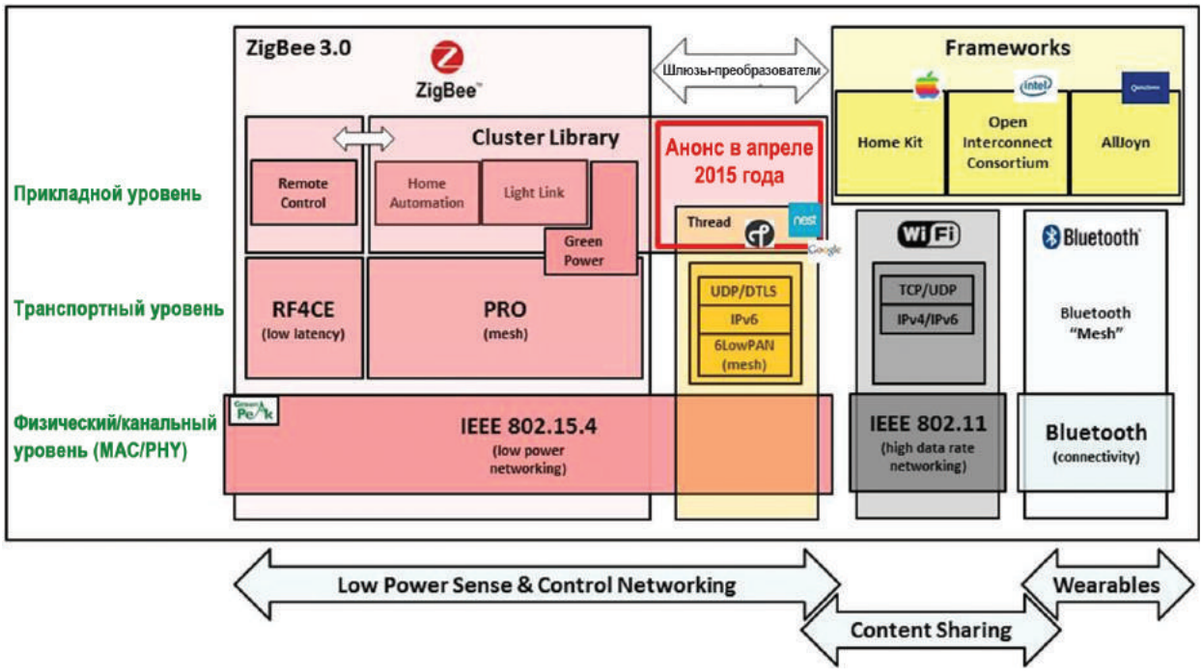


Рис. 5. Обзор ZigBee и проприетарных фреймворков после апрельского анонса 2015 года об интеграции ZigBee Cluster Library в сети Thread

Герард Хольцман (Gerard I. Holzman), NASA/JPL

За пределами границ

В любом компьютере все объекты, которые мы храним или модифицируем, с неизбежностью имеют пределы. Все ресурсы ограниченны. Стеки ограниченны, очереди ограниченны, ёмкость файловой системы ограниченна и даже числа ограниченны. Однако при написании кода об этом часто забывают.

На курсах по сертификации программного обеспечения, которые проводятся в Лаборатории реактивного движения (JPL), мы делаем акцент на том, что для создания надёжного кода необходимо тонко чувствовать границы системы. В любом компьютере для выполнения вычислений в вашем распоряжении есть лишь ограниченный кусочек памяти и конечный отрезок времени, поэтому все объекты, которые мы храним или модифицируем, с неизбежностью имеют пределы. Все ресурсы ограниченны. Стеки ограниченны, очереди ограниченны, ёмкость файловой системы ограниченна и даже числа, представьте себе, ограниченны. Поэтому мир компьютеров сильно отличается от мира математики, что при написании кода слишком многие не берут в расчёт. Дело, по-видимому, в том, что в большинстве случаев не так уж и важно, знаете вы об ограничениях вашего компьютера или нет, поскольку бóльшую часть времени всё будет работать правильно.

Есть замечательный фрагмент в серии комиксов Peanuts, где персонаж Пепперминт Пэтти настойчиво внушает своей однокласснице, что алгебра на самом деле не так уж и трудна: «x почти всегда равен одиннадцати, а y – почти всегда девять». В математике, если оба слагаемых x и y положительны, то ясно, что их сумма должна быть больше каждого из них. В компьютере не так. Если мы используем целые 32-битные числа со знаком, это свойство сохраняется лишь для сумм не выше где-то двух миллиардов. Поскольку это бóльшую часть времени так, можно с уверенностью сказать, что когда мы увеличиваем x на положительную величину, результат «почти всегда» будет больше первоначального значения.

Почти всегда

Предположим, что мы управляем 32-битным знаковым счётчиком (signed counter). Мы запускаем его с нулевого значения и инкрементируем раз в секунду. Тогда до того момента, когда он переполнится, пройдёт примерно 68 лет. Именно так хранилось количество секунд в оригинальной операционной системе Unix, где за нулевую отметку была принята дата 1 января 1970 года. Невооружённым глазом видно, что этот метод записи времени имеет ограничения. Такие 32-рязрядные часы в системе Unix могут работать бесперебойно лишь на отрезке времени порядка 136 лет: с декабря 1901 года (отрицательная шкала счёта секунд ранее января 1970 года) до января 2038 года. Если продолжать работу в Unix достаточно долго, то во вторник 19 января 2038 года произойдёт аналог проблемы 2000-го года (Y2K), когда окажется, что часы перескочили обратно на 13 декабря 1901 года.

Починить часы в Unix нетрудно. Если просто перевести счётчик времени на 64-битный формат, то для его переполнения потребуется порядка 293-х миллиардов лет. И хотя этот временной интервал небесконечен, он более чем достаточен, поскольку, по прикидкам учёных, ещё до того момента, как такой счётчик досчитает до отметки в районе пяти миллиардов лет, нашу солнечную систему ждёт огненный конец.

Но если мы начнём отсчитывать время с большей точностью, нежели посекундно, картина изменится. Если, к примеру, мы будем инкрементировать наш 32-битный счётчик каждые 100 мс, то знаковый счётчик (signed counter) переполнится примерно че-

Как точность отсчёта времени влияет на переполнение счётчика

Если инкрементировать 32-битный счётчик каждые	Знаковый счётчик переполнится через	Беззнаковый счётчик переполнится через
1 с	68, 1 лет	132,2 лет
100 мс	6,8 лет	13,6 лет
10 мс	248, 6 дней = 0,68 лет	497,1 дней = 1, 36 лет

рез 6,8 лет, а беззнаковый (unsigned counter) – через 13,6 лет. Если увеличить точность до 10 мс, то знаковый счётчик переполнится через 248,6 дней, а беззнаковый – через 497,1 дней. Запомните эти цифры (см. таблицу), мы к ним ещё вернёмся.

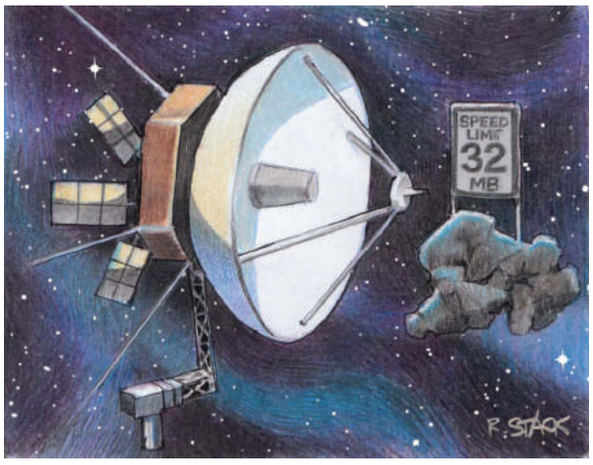
Время на борту космических аппаратов

Космический аппарат НАСА «Дип импакт» (Deep Impact) был запущен в январе 2005 года. Его встроенный контроллер вычислял время в виде числовой последовательности 100-миллисекундных интервалов, которые отсчитывались с 1 января 2000 года. Если прибавить 13,6 лет, то получим некую дату августа 2013 года, которая находится далеко за пределами запланированного срока работы миссии. Назначение этого космического аппарата – сбросить зонд-импактор на комету Темпеля 1 и исследовать состав образовавшегося пылевого облака. Миссия завершилась 4 июля 2004 года.

Часто бывает так, что космические аппараты после успешного выполнения основной задачи выполняют дополнительные задания, при условии, что у них ещё остались в достаточном количестве необходимые ресурсы. В ноябре 2010 года во время первой дополнительной миссии «Дип импакт» пролетел на близком расстоянии от кометы Хартли-2 (Hartley 2). После этого у него оставалось ещё достаточно топлива для другой дополнительной миссии – сближения с астероидом 2002 GT. Если бы всё пошло хорошо, то данный космический аппарат под новым именем EPOXI достиг бы астероид в 2020 году.

Но этому не суждено было сбыться. Бортовой хронометражный счётчик переполнился 13 августа 2013 года, что инициировало обработку исключительной ситуации. Это исключение привело к сбросу бортовой аппаратуры в исходное состояние, в результате чего она должна была перейти в режим безопасной работы. В реальности этот сброс обнулил всю память за исключением бортовых часов, что привело к зацикливанию аппарата на сбросе. Даже в этом отчаянном режиме наземные контроллеры могут «реанимировать» космическую миссию, подавая «аппаратные команды», минуя главный процессор. Однако такое вмешательство нужно делать быстро, до того, как космический аппарат «заблудится» и более не сможет получать команды с Земли. Такая помощь не поспела вовремя, и 20 сентября 2013 космический аппарат был объявлен потерянным. Его убил 32-разрядный счётчик.

Это, увы, не единственный пример числового переполнения, приводящего к проблемам даже в системах с особыми требованиями к обеспечению безопасности (safety-critical systems).



Самолёты

Пассажирский самолёт Боинг 787 (Дримлайнер) состоит из множества подсистем, где есть встроенные контроллеры. В них, как правило, предусмотрены внутренние часы и отсчёт времени. Контроллеры, встроенные в блоки управления генераторами (generator control units – GCUs), отсчитывают время каждые 10 мс. Соответствующие счётчики содержат знаковые 32-битные числа. Теперь перед тем, как продолжить чтение, гляньте ещё раз в таблицу.

9 июля 2015 года Федеральное управление гражданской авиации США выпустило директиву лётной годности (AD), предписывающую всем авиакомпаниям перезагружать блоки управления генераторами на всех Боингах 787 как минимум каждые 248 дней [1]. Директива гласит: «Цель AD – предотвратить полную потерю подачи переменного напряжения, в результате чего возможна потеря управляемости самолёта». Далее объясняется, что «Эта AD появилась после того, как было обнаружено, что самолёт модели 787, в системы которого электроэнергия подаётся непрерывно в течение 248 дней, может оказаться обесточенным из-за одновременного перехода блоков управления генераторами в отказоустойчивый режим работы. Причиной этого состояния стали программные счётчики в составе ПО генераторов..., которые каждые 248 дней непрерывной генерации электроэнергии переходят в режим переполнения».

Откуда берутся эти 248 дней, мы уже знаем, однако, по-прежнему, важно видеть, как часто программная ошибка такого типа случается на практике, причём даже в системах, которые прошли весьма жёсткий процесс сертификации. Программное обеспечение для гражданских самолётов всегда разрабатывается и тестируется с большой тщательностью. Процесс разработки должен соответствовать процедурам, оговоренным в стандарте DO-178B (и его последователе DO-178C). Нет никакого сомнения, что программное обе-

спечение для Боинга 787 не писалось в спешке. Первый Боинг 748 был показан публике 8 июля 2007 года, а первый полёт состоялся 15 декабря 2009 года. Первый коммерческий полёт был осуществлён два года спустя. Можно предположить, что к тому моменту самолёт и управляющее им ПО были под пристальным вниманием разработчиков в течение весомого количества лет. Когда в начале 2015 года была обнаружена проблема переполнения, в эксплуатации было почти 300 самолётов.

Ресурсные ограничения

Тот факт, что отказы сложных систем могут быть вызваны подобными, до безобразия простыми, причинами выглядит парадоксом. Объяснить это можно тем, что самое пристальное внимание уделяется объективно сложным задачам проекта; на периферии внимания оказываются именно простые элементы. Этим можно объяснить, почему попадание на известную границу ресурса может привести систему на грань отказа. За примерами далеко ходить не надо; здесь я приведу два из недавних новостей.

LightSail – «Солнечный парус»

20 мая 2015 года «Планетарное общество» (Planetary Society) запустило в тестовый полёт небольшой космический аппарат. Программа эксперимента, названного LightSail («Солнечный парус»), заключалась в испытаниях большого солнечного паруса. Всего через два дня испытательный полёт столкнулся с неожиданной проблемой. В новостной ленте «Mission Update» от 20 мая проблема описывалась так: «В настоящее время LightSail, вероятно, замер, наподобие того, как перестаёт реагировать настольный компьютер»[2].

Причина была относительно проста. Бортовой файл регистрации хранил записи всех телеметрических данных, передаваемых аппаратом; когда файл превысил объём 32 Мбайт, произошёл фатальный сбой системы. Почему 32 Мбайт? В пресс-релизах это не объяснялось, но эта цифра соответствует пределу старой файловой системы FAT12, которая ещё используется в старых встроенных системах. В идеологии FAT12 для хранения в файловой системе последовательности 512-байтных блоков используется 16-битная адресация, и да, $2^{16} \times 512$ байт выходит за пределы 32 Мбайт.

Curiosity – марсоход «Любопытство»

Другой пример мне гораздо ближе. Космическая программа НАСА «Марсианская научная лаборатория» (Mars Science Laboratory) была разработана и воплощена в той подразделении, где я работал. В рамках этой программы 6 августа 2012 года был успешно доставлен на поверхность Марса большой марсоход Curiosity («Кьюриосити» – «Любопытство»). С тех пор марсоход надёжно функционирует, однако за это время в его программном обеспечении случилось несколько сбоев.

Один из них произошёл примерно через полгода после начала работы на поверхности Марса, 27 февраля 2013 года. Неожиданно сбойнул банк флэш-памяти. Программное обеспечение марсохода использует флэш-память для поддержания файловой системы, где хранятся временные файлы с телеметрическими данными и фотоснимками поверхности Марса перед их передачей на Землю. Файловая система во флэш-памяти запрограммирована на режим «только для чтения», на случай, если произойдёт что-то неожиданное. Итак, когда произошёл сбой банка памяти, это и была та самая неожиданность.

Во время нормального функционирования марсохода многие задачи используют файловую систему флэш-памяти для временного хранения результатов своей работы. Поскольку работает флэш-пямять медленно, а хранить необходимо большие объёмы информации, программное обеспечение использует метод буферизации – для временного хранения данных в оперативной памяти (ОЗУ) перед тем, как перенести их в файловую систему флэш-памяти, а затем передать на Землю. Всё работало прекрасно, почти всегда.

Зная, что все ресурсы во встраиваемых системах ограниченны, можно задаться вопросом, а что произойдёт, кода ОЗУ заполнится? Если бы эта система была спроектирована правильно, это случалось бы редко и длилось бы недолго, поскольку данные, временно сохранённые в ОЗУ, перекочёвывали бы в конце концов во флэш-память. Таким образом, в этом редком случае компьютер марсохода приостанавливает работу задач, генерируюших данные, до тех пор, пока не освободится достаточное количество ОЗУ, после чего выполнение соответствующих задач продолжается.

Можно также спросить, что происходит, когда заполняется флэш-память? Это событие случалось бы ещё реже, поскольку от менеджеров миссии требуется постоянно поддерживать достаточный запас свободной флэш-памяти на протяжении всей миссии. Однако, если она всё же заполняется, то программное обеспечение пишется таким образом, чтобы стирать низкоприоритеные файлы, чтобы освободить необходимое количество флэш-памяти. Высокопроиоритетные файлы, которые хранятся во флэш-памяти, в конце концов будут переданы на Землю, и пространство, которое они занимали, вновь будет свободным.

Все эти соображения выглядели достаточно продуманными и основательными, чтобы успешно пройти все экспертизы проекта, анализ кода и тестирование блоков программы, работающих с учётом известных ресурсных лимитов. Однако один тестовый кейс (контрольный пример) не был испытан – именно тот, который случился на Марсе в феврале 2013 года. Когда флэш-память вследствие аппаратной ошибки находится в режиме «только для чтения», никаких дальнейших изменений сделать нельзя: невозможно что-то добавить или стереть. Теперь ОЗУ медленно заполняется новыми данными, ожидая, когда они перепишутся во флэш-память. В какой-то момент ОЗУ больше не может вмещать новую информацию. Соответствующие задачи одна за другой приостанавливают свою работу, и в итоге марсоход становится неактивен.

Если у этой истории есть что-то положительное, так это то, что даже в этом, казалось, безнадёжном случае, наземные контроллеры «починили» марсоход и через несколько дней восстановили его нормальную работу. А наш журнал выученных уроков пополнился ещё одной записью. Осталось надеяться только на то, что у этого журнала тоже появится граничная черта.

Следует ли вам беспокоиться? Программисты, конечно же, знают, что все ресурсы, с которыми они работают, ограниченны. Но трудно всё время помнить об этом отрезвляющем факте. Учитывая частоту, с которой эти проблемы возникают, следует их прорабатывать. Проводите тщательно спланированное тестирование системных блоков и всей системы, при котором достигаются известные системные пределы и делается попытка их превзойти. При использовании 32-битных часов, протестируйте их на перспективу за пределы 248 дней, 1,3 и 13,6 лет, и посмотрите, работает ли ваша система по-прежнему корректно. Если вы забыли об этих тестах, то у вас, конечно, много времени, чтобы об этом подумать, но спать вы будете наверняка лучше, если всё же не забудете.

Ссылки

1. «Airworthiness Directives; the Boing Company Airplanes», Federal Register, vol. 80, no. 84,2015; http://rgl.faa.gov/Regulatory_and_Guidance_Library/rgad.nsf/0/584c7ee3b270fa3086257e38004d0f3e/$FILE/2015-09-07.pdf

2. M.Wall, «LightSail Solar Sail Test Flight Stalled by Software Glitch», Space.com, 27 May 2015; www.space.com/29502-lightsail-solar-sail-software-glitch.html

Источник: IEEE Software, November/December 2015, p. 24, Out of Bounds

Новости рынка

«РТСофт» и «Лаборатория Касперского» открывают центр компетенции по защите от кибератак в области промышленности и энергетики

Российские компании «РТСофт» и «Лаборатория Касперского» объявляют об открытии «Центра Компетенции РТСофт», квалифицированного партнёра «Лаборатории Касперского» по вопросам, связанным с развитием и продвижением решений по защите предприятий и объектов промышленности и энергетики от кибератак.

Открытие центра компетенции позволит объединить в интересах заказчиков опыт и потенциал «Лаборатории Касперского», признанного мирового лидера разработки программных решений в области информационной безопасности, и «РТСофт» – одного из крупнейших системных интеграторов, работающего на рынке автоматизации в промышленности и энергетике Российской Федерации.

Основные задачи «Центра компетенции РТСофт»:

– создание приборной продукции и программно-технических комплексов, построенных с использованием защищённой операционной системы KasperskyOS;
– разработка на основе KICS (Kaspersky Industrial CyberSecurity) проектных решений, предназначенных для защиты АСУ ТП и систем автоматизации в промышленности, энергетике и на транспорте;
– демонстрация и тестирование решений по киберзащите для вертикальных рынков на специализированных стендах;
– проведение обучения специалистов заказчика, проектных и внедренческих организаций по перечисленным выше продуктам на базе «Учебного Центра РТСофт».

Результатом решения этих и смежных задач, стоящих перед Центром, будет проектирование, создание, тестирование и внедрение отечественных решений по созданию адекватной защиты от современных киберугроз; выполнение требований по информационной безопасности, предъявляемых регуляторами и внутренними стандартами организаций.

Г. С. Кузьмина, Ю. Я. Моцкин (ЗАО «РТСофт»),
М. М. Соколов, Р. Р. Хайрутдинов,
П. П. Хвостенко (НИЦ «Курчатовский институт»),

Комплекс магнитного управления плазмой информационно–управляющей системы установки «Токамак Т–15»

В статье представлены решения по построению комплекса магнитного управления плазмой, входящего в состав информационно-управляющей системы экспериментальной термоядерной установки «Токамак Т-15».

1. Постановка задачи

В настоящее время в НИЦ «Курчатовский институт» выполняются работы по модернизации экспериментальной термоядерной установки «Токамак Т-15» [1].

Цель модернизации – обеспечение дальнейшего развития исследований на установках типа токамак в России. Модернизация установки Т-15 и проведение исследований на ней – первый шаг на пути создания термоядерного источника нейтронов (ТИН), необходимого для наработки топлива для нужд атомной энергетики» [2].

Установка Т-15 представляет собой сложный комплекс взаимодействующих между собой инженерных, технологических и специализированных электрофизических систем.

Управление установкой, а также сбор и обработку экспериментальных данных обеспечивает информационно-управляющая система (ИУС Т-15) [3]. В работах по созданию ИУС Т-15 принимает участие ряд профильных организаций. Головной разработчик – ЗАО «РТСофт».

ИУС Т-15 включает набор систем управления и сбора данных.

Представленная работа посвящена вопросам создания комплекса магнитного управления плазмой, являющегося ядром ИУС Т-15.

2. Используемое оборудование и программное обеспечение

Системы, входящие в состав ИУС Т-15, по своему назначению могут быть разделены на «быстрые», обеспечивающие работу установки непосредственно во время эксперимента, и «медленные», осуществляющие подготовку к эксперименту, обслуживание во время эксперимента, останов после эксперимента.

«Медленные» инженерные и технологические системы токамака (к ним относятся, например, система мониторинга электроснабжения и система вакуумной откачки) реализуются стандартными средствами управления технологическими процессами и строятся на базе промышленных контроллеров Schneider Electric.

Комплекс магнитного управления плазмой (Комплекс) относится к «быстрым» системам, причём к его компонентам предъявляются особо жёсткие требования.

К таким требованиям относятся высокое быстродействие при значительном количестве обрабатываемой информации, точная межсистемная синхронизация и координация со смежными электрофизическими системами (в том числе с системами дополнительного нагрева плазмы), необходимость синтеза моделей и регуляторов практически для всех стадий разнообразных экспериментов, обеспечение электромагнитной совместимости.

Исходя из особенности требований и с учётом специфики решаемых задач Комплекс, как и другие «быстрые» системы ИУС Т-15, строится на основе программно-аппаратных средств и технологий компании National Instruments.

Требования к быстродействию Комплекса приведены ниже.

3. Описание решения

Магнитное управление положением, током и формой плазмы «Токамака Т-15» осуществляется по двухконтурной модели.

Схема магнитного управления приведена на рис. 1.

Комплекс состоит из двух взаимосвязанных частей:

– подсистемы управления импульсными источниками питания (СИЭП);
– подсистемы управления плазмой (СУП).

Обе подсистемы совместно обеспечивают управление в соответствии со сценарием эксперимента.

Сценарий создаётся с использованием численной модели объекта (камера с обмотками, плазменный шнур и источники питания).

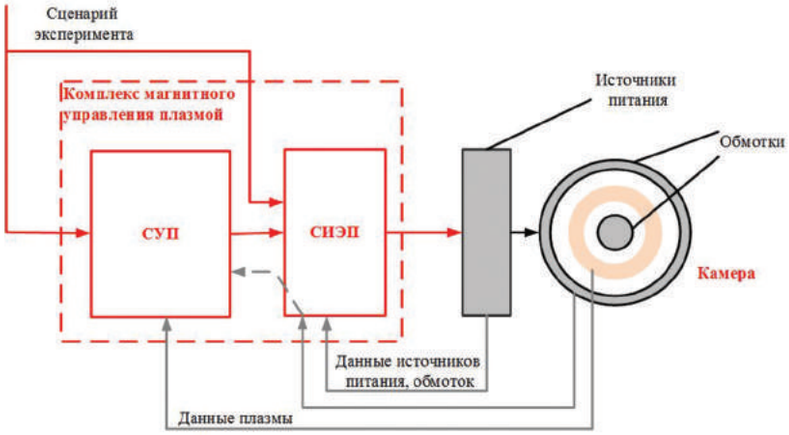


Рис. 1. Схема магнитного управления плазмой

В ИУС Т-15 используются модели, построенные на основе плазмофизического кода DINA [4, 5].

Код DINA в течение долгого времени систематически проходит тестирование по моделированию эволюции плазмы в реальных экспериментах на действующих токамаках. При этом он показывает хорошее соответствие между результатами моделирования и экспериментальными данными. В том числе код ДИНА принят в качестве основного симулятора для разработки и тестирования систем управления и для проведения проектно-исследовательских работ по выбору регуляторов в системе контроля положения, формы и величины тока плазмы международного токамака – реактора ИТЭР.

Для синтеза и тестирования регуляторов, а также для моделирования разрядов в токамаках с учётом реально используемых в эксперименте магнитных систем разработана Simulink-версия кода ДИНА в виде программно-вычислительного комплекса в рамках среды программирования MATLAB.

В установке Т-15 для поддержания плазмы в равновесном состоянии используется электромагнитная система, включающая в себя импульсные источники питания (тиристорные преобразователи), обмотки тороидального и полоидального магнитного поля:

– обмотка управления тороидальным полем;
– обмотки индуктора;
– «медленные» обмотки управления положением и формой плазмы;
– «быстрая» обмотка управления вертикальным положением плазмы.

В ИУС Т-15 применяется технология, при которой компоненты моделирования и управления разрабатываются с использованием среды программирования MATLAB-Simulink. При этом процедура включения полученных компонентов в программное обеспечение систем управления стандартизирована в соответствии с разработанными требованиями интеграции. Такой подход позволяет использовать и тестировать в Комплексе программные продукты, разработанные различными группами специалистов на основе кода MATLAB-Simulink.

В составе Комплекса подсистема СИЭП обеспечивает управление импульсными источниками питания для каждой отдельной обмотки на основе задаваемых уставок и данных, снимаемых с выходов источников питания и тороидальных и полоидальных обмоток токамака. Подсистема СУП обеспечивает управление путём выработки уставок для подсистемы СИЭП на основе замеров параметров самой плазмы.

Цикл управления для «медленных» обмоток, включающий:

– сбор данных в СУП,
– выработку управляющих значений для СИЭП,
– сбор данных в СИЭП и формирование управляющих воздействий на источники питания,

для эффективного управления не должен превышать 3 мс.

Для «быстрой» обмотки, выполняющей управление вертикальным положением плазмы, цикл управления не должен превышать 0,1 мкс.

На первом этапе пуска «Токамака Т-15» использование «быстрой» обмотки не планируется и в данной статье не рассматривается.

3.1. Структура комплекса аппаратных средств

Структура комплекса аппаратных средств управления плазмой приведена на рис. 2.

Комплекс представляет собой распределённую систему управления, компоненты которой осуществляют информационный обмен между разнесёнными шасси, используя принятый в National Instruments скоростной интерфейс MXI-Express Gen II x8 (MXIe x8) (скорость обмена – до 3,2 Гбит/с). Для обмена используются специальные медные и оптические кабели (длина оптических кабелей – до 300 м).

Информационный обмен между контроллерными компонентами Комплекса выполняется в соответствии со спецификацией PXI MultiComputing (PXImc) [6].

Ядром подсистемы СУП является стойка управления СУП, которая содержит крейт PXIe и встраиваемый контроллер NI RMC-8354.

Вычислительные ресурсы подсистемы СУП распределены между размещёнными в шасси процессором NI PXIe-8135 и сопроцессором NI PXIe-8830mc (количество сопроцессоров может быть увеличено), а также встраиваемым контроллером NI RMC-8354.

К стойке управления СУП по интерфейсу MXIe x8 (оптика) последовательно подключены шкафы диагностик (ШД), в которые установлены модули, предназначенные для сбора диагностической информации. Цикл опроса диагностик – 100 мкс.

Подсистема СИЭП включает шкаф программируемого логического контроллера (ПЛК), который содержит крейт PXIe с процессором NI PXIe-8135, коммуникационные модули, модуль синхронизации и модуль рефлективной памяти.

К шкафу ПЛК по интерфейсу MXIe x8 (оптика) последовательно подключены шкафы управления источниками питания (ШУИП), которые осуществляют непосредственное управление источниками питания (тиристорные усилители), а также сбор данных от источников питания и обмоток.

Вычислительные ресурсы подсистемы СИЭП распределены между процессором NI PXIe-8135 шкафа ПЛК и модулями программируемых логических интегральных схем (ПЛИС), установленными в шкафах ШУИП.

Информационный обмен между СУП и СИЭП осуществляется в соответствии с PXImc.

Подсистемы СУП и СИЭП имеют интерфейсы с подсистемой подготовки сценария эксперимента (АРМ ПСЭ), от которой получают необходимые компоненты сценария, с Системой координации и синхронизации скоростных систем (СКСС) и системой противоаварийных защит (ПАЗ).

Функции координации скоростных систем обеспечиваются путём обмена по сети рефлективной памяти. Время обмена по сети рефлективной памяти – десятки мкс.

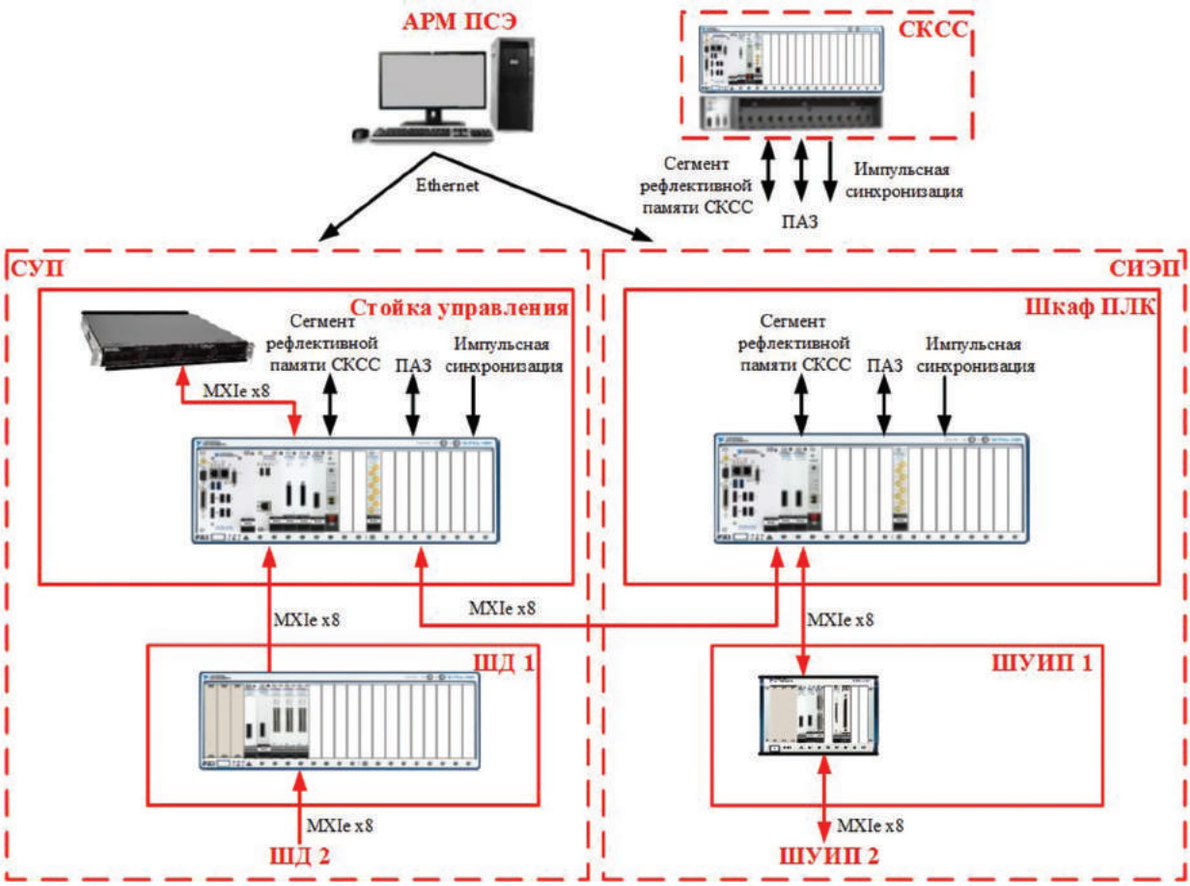


Рис. 2. Структура комплекса аппаратных средств управления плазмой

Импульсная синхронизация реализуется путём выдачи из СКСС синхронизирующих импульсов по оптическим каналам. Точность синхронизации – единицы мкс.

Реализация протокола ПАЗ обеспечивается путём импульсного обмена по оптическим каналам связи. Время цикла обмена – десятки мкс.

3.2. Программные средства Комплекса

Структура программного обеспечения Комплекса приведена на рис. 3.

Программное обеспечение Комплекса функционирует под управлением операционной системы Labview RT.

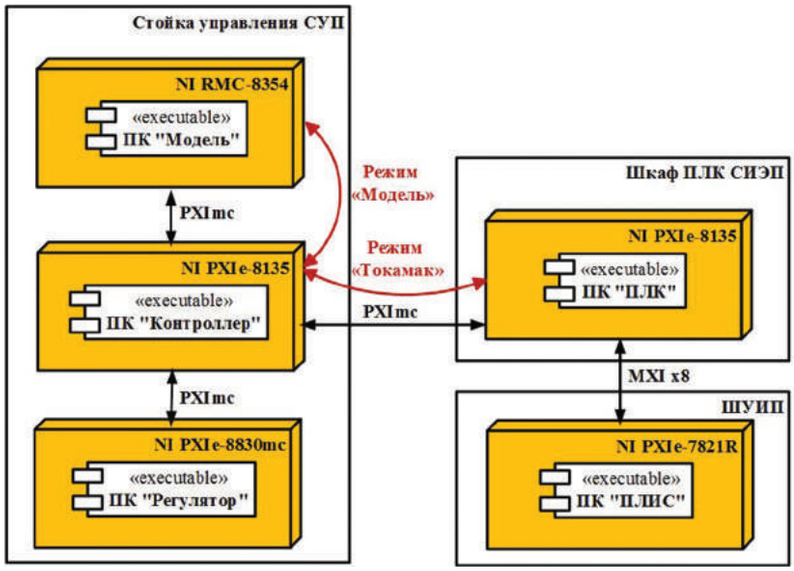


Рис. 3. Программное обеспечение Комплекса

Среда разработки программного обеспечения (ПО) – Labview 2014.

Ряд компонентов ПО (модели, регуляторы) написаны на основе кода DINA в среде Matlab – Simulink. Для включения этих компонентов в проекты Labview использована стандартная технология National Instruments по переносу программ Matlab – Simulink в Labview [7].

ПО подсистемы СУП включает 3 программных комплекса (ПК):

– ПК «Контроллер»;
– ПК «Регулятор»;
– ПК «Модель».

ПК «Контроллер» развёрнут на контроллере NI PXIe-8135 и обеспечивает:

– реализацию общей инфраструктуры СУП;
– сбор и обработку данных диагностик;
– архивирование данных;
– реализацию интерфейсов.

ПК «Регулятор» развёрнут на сопроцессоре NI PXIe-8830mc и обеспечивает реализацию регуляторов (матричные регуляторы), функционирующих на этапе создания и поддержания плазмы. В ПК «Регулятор» включены компоненты, синтезированные с использованием модели, реализованной плазмофизическим кодом DINA для условий «Токамака Т-15». Обмен между сопроцессором и контроллером производится по шине PXIe в соответствии с PXImc.

ПК «Модель» развёрнут на встраиваемом контроллере NI RMC-8354 и обеспечивает реализацию моделей источников питания, линейной модели плазмы и камеры с обмотками. В ПК «Модель» включены компоненты, созданные на основе многомерной линейной модели объекта (источников тока и плазмы в токамаке) DINA-L. Линейная модель DINA-L получена посредством линеаризации нелинейной динамической модели, численно реализованной с использованием кода плазмофизических расчётов DINA. Использование линейной модели позволяет выполнять моделирование объекта в реальном масштабе времени.

Подсистема СУП функционирует в двух режимах:

– режиме «Токамак», в котором регулятор работает на подсистему СИЭП (режим проведения эксперимента);
– режиме «Модель», в котором регулятор работает на ПК «Модель» (моделирование на основе программной петли SIL).

Режим «Модель» используется для настройки регуляторов и контроля компонентов подготовленного сценария эксперимента перед проведением эксперимента на самой установке.

ПО подсистемы СИЭП включает 2 программных комплекса (ПК):

– ПК «ПЛК»;
– ПК «ПЛИС».

ПК «ПЛК» развёрнут на процессоре NI PXIe-8135 шкафа ПЛК и обеспечивает:

– реализацию общей инфраструктуры СИЭП;
– сбор и обработку данных с источников питания и обмоток;
– формирование и выдачу на ШУИП команд, обеспечивающих сборку схем электропитания обмоток;
– исполнение заданных алгоритмов управления;
– контроль аварийных ситуаций;
– реализацию интерфейсов;
– реализацию ПИД-регуляторов для этапа ввода и вывода токов из обмоток;

– реализацию корректирующих ПИД-регуляторов для этапа поддержания плазмы;
– пересчёт управляющих напряжений в электрические углы для управления тиристорами.

Регуляторы СИЭП также синтезированы с использованием кода DINA.

ПК «ПЛИС» развёрнут на программируемой логической матрице модуля NI PXIe-7821R шкафа ШУИП и обеспечивает:
– интерфейс с ПК «ПЛК»;
– формирование и выдачу управляющих сигналов, синхронизированных с сетью, на тиристорные сборки;
– приём от шкафа ПЛК и выдачу команд на исполнительные механизмы схем электропитания обмоток.

3.3. Процедуры магнитного управления плазмой

Управление плазмой токамака осуществляется в соответствии со сценарием эксперимента. Сценарий для Комплекса определяет циклограмму событий эксперимента и программы токов обмоток. Программа токов приведена на рис. 4.

На оси абсцисс (время) определены метки времени в соответствии с циклограммой эксперимента:
– t0 – старт эксперимента;
– t3 – токи всех обмоток достигли расчётных значений;
– t_sc1 – начало разряда;
– t_sc8 – конец разряда;
– t_sc9 – конец эксперимента.

Формирование сценария эксперимента выполняется подсистемой Подготовки сценария эксперимента, входящей в состав ИУС Т-15.

Компоненты сценария загружаются в Комплекс. После этого с целью контроля заданных в сценарии параметров осуществляется процедура работы Комплекса в режиме моделирования SIL.

Если результат выполнения процедуры в режиме «Модель» не подтверждает предусмотренных сценарием параметров плазмы, то выполняется корректировка избранного сценария или регулятора.

Рис. 4. Программа токов

В противном случае, если полученные в результате исполнения модели параметры соответствуют предусмотренным в сценарии, то можно с высокой вероятностью предположить, что в результате выполнения эксперимента на установке будут получены требуемые или близкие к ним параметры плазмы.

Такой подход, очевидно, обеспечивает, во-первых, существенную экономию ресурсов, во-вторых, позволяет экономить время для подготовки и успешного проведения действительно важных экспериментов.

В режиме «Токамак» (при проведении реального эксперимента) процедура работы Комплекса в соответствии с требованиями сценария следующая:
– подсистема СИЭП обеспечивает ввод токов в обмотки до достижения значений, необходимых для выполнения разряда;
– после этого управление принимает подсистема СУП, которая осуществляет поддержание разряда с заданным сценарием. При этом в подсистеме СИЭП функционирует подключённый в каскад к регулятору СУП корректирующий регулятор;
– после завершения разряда при выводе токов из обмоток вновь управление передаётся подсистеме СИЭП.

С нашей точки зрения, такой подход позволяет наиболее эффективно использовать ресурсы Комплекса для достижения требуемых параметров управления.

4. Внедрение и его перспективы

Запуск «Токамака Т-15» предполагается осуществить в два этапа:
– первый этап – пуск в объёме, обеспечивающем получение плазмы за счёт омического разогрева (физический пуск) в 2017 г.;
– второй этап – пуск в полном объёме (с управлением формой вертикального сечения плазмы, с использованием систем дополнительного нагрева) в 2020 г.

В настоящее время в НИЦ «Курчатовский институт» работы с плазмой выполняются на установке «Токамак Т-10».

Компоненты представленного в настоящей статье решения испытаны на установке Т-10. Испытания продемонстрировали правильность выбранных решений.

Цель работ в настоящее время – обеспечить до конца 2016 г. функционирование Комплекса в объёме, необходимом для физического пуска, и в 2017 г. провести физический пуск установки, в процессе которо-

го должна быть получена плазма, с использованием омического нагрева.

В дальнейшем предполагается запустить установку в полном объёме. Будут задействованы все обмотки, в том числе и «быстрая». Будет введена в строй полномасштабная система импульсного электропитания. Будут включены системы дополнительного нагрева.

В результате установка выйдет на параметры плазмы, предусмотренные проектом.

5. Список литературы

1. В. А., Альхимович, Е. П. Велихов, М. М. Соколов, П. П. Хвостенко, и др. Инженерно-физическое обоснование реконструкции ТОКАМАКА Т-15. Вопросы атомной науки и техники. Серия Термоядерный синтез, 2008, №03.

2. Е. П. Велихов, М. В. Ковальчук, Э. А. Азизов, и др. Гибридный термоядерный реактор для производства ядерного горючего с минимальным радиоактивным загрязнением топливного цикла. Вопросы атомной науки и техники. Серия Термоядерный синтез, 2014, №04.

3. Ю. Я. Моцкин , М. М. Соколов, П. П. Хвостенко. Информационно-управляющая система экспериментальной термоядерной установки «Токамак Т-15». Мир компьютерной автоматизации: встраиваемые компьютерные системы, 2015, №03.

4. В. Э. Лукаш, В. Н. Докука, Р. Р. Хайрутдинов. Программно-вычислительный комплекс «Дина» в системе Matlab для решения задач управления плазмой токамака. Вопросы атомной науки и техники. Серия Термоядерный синтез, 2004, №01.

5. В. Н. Докука, А. А. Кавин, В. Э. Лукаш, М. М. Соколов, Р. Р. Хайрутдинов, В. А. Хайрутдинова, Численное моделирование управления плазмой в модернизированном токамаке Т-15. Вопросы атомной науки и техники. Серия Термоядерный синтез, 2014, №03.

6. PXI system Alliance. PXI MultiComputing Software Specification. Revision 1.0. September 16, 2009.

7. How to Create Simulation DLL's for LabVIEW Using The MathWorks, Inc. Simulink® Software. WWW.ni.com. Publish Date: Dec 22, 2009.

Авторы:
Г. С. Кузьмина, Ю. Я. Моцкин,
(495) 967-15-05, kuzmina_gs@rtsoft.msk.ru
М. М. Соколов, П. П. Хвостенко,
(499) 196-96-39, sokolov_mm@nrcki.ru
Р. Р. Хайрутдинов,
(495) 334-53-08, khayrutd@mail.ru

Новости рынка

В учебном центре «РТСофт» стартует новый курс «Кибербезопасность в АСУТП»

Учебный центр «РТСофт» в апреле 2016 года приглашает на новый курс «Кибербезопасность в АСУТП»

Курс ориентирован на специалистов отделов информационной безопасности, служб безопасности, экспертов по безопасности, специалистов по автоматизации технологических систем и будет полезен системным интеграторам и конечным пользователям.

Слушатели учебного курса «Кибербезопасность в АСУТП» получат базовые знания и практические навыки, относящиеся к таким сферам деятельности, как:

– информационная безопасность,
– информационные технологии и автоматизация,
– обеспечение информационной безопасности автоматизированных систем управления технологическими процессами.

Учебная программа позволит освоить методику формирования доверенной программной среды в АСУТП и унификации защищённого взаимодействия процессов обработки данных, изучить эффективные механизмы и методы обеспечения защиты автоматизированных систем. Кроме того, будет уделено повышенное внимание таким актуальным вопросам, как:

– перехват и нейтрализация угроз со стороны привилегированных категорий пользователей,
– организация защищённой области хранения данных,
– порядок регистрации и автоматической обработки инцидентов безопасности на примере защищённого комплекта программ (ЗКП) «Plato RT».

Курсы проводятся с использованием профессионального стенда для механизмов и методов обеспечения защиты АСУТП.

Более подробную информацию о курсе можно получить по телефону +7 (495) 742-96-55.

Ждём вас в нашем учебном центре!

К. Б. Здирук, В. Ю. Синенко, А. Н. Ханыгин, ЗАО «РТСофт»

Реализация задач сбора, консолидированной обработки и доступа к разнородным источникам данных

В статье рассматриваются подходы к решению задачи обеспечения вертикально- и горизонтально-ориентированных направлений информационного взаимодействия абонентов (процессов), обрабатывающих данные как открытого, так и ограниченного доступа с различным уровнем конфиденциальности. Решение указанной задачи предполагает дооснащение существующей вычислительной инфраструктуры, развёрнутой на предприятиях (объектах автоматизации), программно-аппаратным комплексом на основе Объединённого Коммуникационного Центра (ОКЦ).

Применение предлагаемых решений обеспечивает совмещение процессов сбора данных, получаемых от разнородных источников (открытых и конфиденциальных), их консолидированную обработку с гарантированной изоляцией открытого и закрытого сегментов (контуров) обработки данных на объектах применения.

Всё программное обеспечение ОКЦ является отечественным, доверенным и защищённым, в его составе отсутствуют заимствованные компоненты иностранного производства. Аппаратная часть (по требованиям Заказчика) может исполняться с применением импортной и/или отечественной электронной компонентной базы.

В интересах эффективного решения задач управления производством на предприятиях (организациях) необходимо обеспечить вертикально- и горизонтально-ориентированные направления защищённого информационного взаимодействия абонентов и процессов, обрабатывающих данные с различными уровнями конфиденциальности.

Кроме того, сопутствующей задачей, решаемой посредством внедрения ОКЦ, является сокращение производственных затрат на отработку и унификацию взаимодействия абонентов с внешними организационными структурами на всех уровнях (предприятие – холдинг – управляющая компания), а также с другими органами государственного управления.

Для реализации указанных задач предназначен ОКЦ «ПЛАТАН-РТ», разрабатываемый компанией «РТСофт».

Консолидация данных от различных источников

Процессы сбора, систематизации, хранения и совместной обработки информации открытого и ограниченного доступа выполняются средствами ОКЦ «ПЛАТАН-РТ» в автоматическом и автоматизированном режимах. Сбор технологической информации о состоянии оборудования, действиях персонала, а также управление вычислительной инфраструктурой может обеспечиваться с использованием отдельной (технологической) сети, изоляция которой от основного (информационного) тракта реализуется комплексом средств защиты (КСЗ) защищённого комплекта программ (ЗКП) «Plato-RT», разработанного в 2015 г. ЗАО «РТСофт» в рамках реализации инвестиционного проекта.

На рис. 1 представлен пример оснащения объектов заказчика средствами ОКЦ «ПЛАТАН-РТ». Каждый объект оснащается аппаратно-программным комплексом, состоящим из серверной группы и необходимого количества клиентских комплектов – автоматизированных рабочих площадок (АРП), включающих АРМ открытого и закрытого сегментов.

Масштабирование решения предполагает возможность расширения количества клиентских АРП

(до 5 000 ед. на каждом объекте). Межобъектовое масштабирование предполагает увеличение количества типовых объектов автоматизации (на рис. 1 представлены иерархией «управляющая компания–холдинг–предприятие») до 5 000 ед. с подключением к каналам связи открытых и закрытых сетей передачи данных.

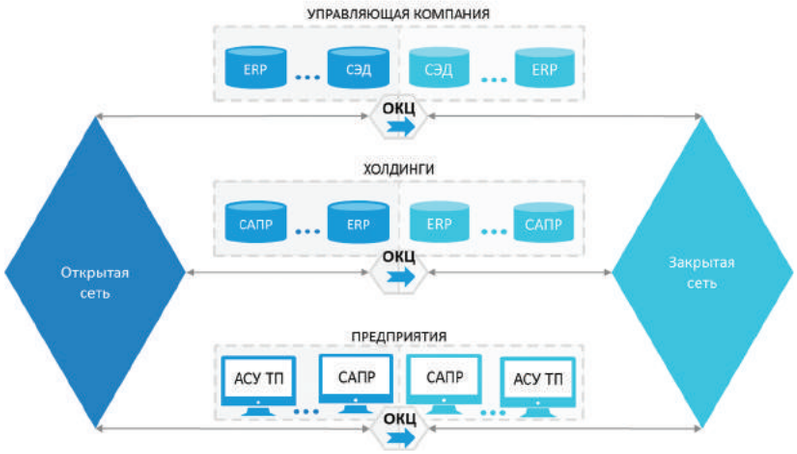


Рис. 1. Реализация взаимодействия объектов автоматизации Заказчика по открытым и закрытым сетям передачи данных с использованием унифицированных комплектов ОКЦ

Информационный обмен между открытыми и закрытыми сегментами (передача документов, формализованных сообщений, файлов) одного или различных объектов реализуется через серверные группы ОКЦ «ПЛАТАН-РТ» и входящие в их состав шлюз-фильтры однонаправленной передачи прикладного контента (на рис. 1 показаны фигурными стрелками внутри ОКЦ). На каждом уровне иерархии в составе объектов автоматизации заказчика сохраняются существующие («унаследованные») базы данных (БД) заказчика, которые дополняются формируемыми средствами ОКЦ «ПЛАТАН-РТ» Банками данных (БнД) первичной информации и Банками моделей (БнМ) вторичной информации для холдинговых структур, а также Интегрированным Банком данных и моделей (ИБнД и ИБнМ) для организационных структур на уровне Управляющей компании (центрального аппарата) заказчика. Сопряжение БнД и БнМ с существующими БД заказчика производится через Адаптеры Сопряжения (АдС), функционирующие в составе ОКЦ «ПЛАТАН-РТ» под управлением встроенной Интеграционной платформы (ИП).

ОКЦ «ПЛАТАН-РТ» посредством доверенных защищённых компонентов ИП, установленных на узлах ЛВС открытых и закрытых сегментов, обеспечивают «прозрачное» взаимодействие всех территориально-распределённых абонентов (процессов) Заказчика по принципу «каждый-с-каждым» (возможные ограничения задаются настройкой политики безопасности).

Функциональная архитектура унифицированного комплекта ОКЦ «ПЛАТАН-РТ» для реализации консолидированной обработки данных открытого и закрытого сегментов на объекте заказчика показана на рис. 2.

Задачи обеспечения безопасности информации (ОБИ), контроля и управления функционированием (КУФ) централизованно решаются на каждом объекте автоматизации одноименными компонентами соответствующих полукомплектов из состава серверной группы ОКЦ «ПЛАТАН-РТ-С». Подключение полукомплектов серверной группы к канальным интерфейсам открытых и закрытых сетей передачи данных производится посредством устройств унифицированных комплексов доступа (УКД), входящих в состав ОКЦ «ПЛАТАН-РТ».

Произвольные данные (формализованные сообщения, документы, файлы и др.), передаваемые от различных источников, автоматически упаковываются ОКЦ «ПЛАТАН-РТ» в специализированные программные контейнеры Интеграционной платформы (ИП) для последующей гарантированной доставки по унифицированной магистрали (ESB-шине) до адресуемого абонента (процесса) с автоматическим уведомлением отправителя о фактах успешной доставки и обработки содержимого контейнера. Встроенные в ОКЦ «ПЛАТАН-РТ» программные средства гарантированного хранения обеспечивают возможности распределённого и централизованного ведения Банков данных (БнД) первичной информации – систематизированных хранилищ с «прозрачным» доступом к их содержимому для удалённых абонентов (процессов) в соответствии с заданной политикой безопасности.

Серверная группа (рис. 2) ОКЦ «ПЛАТАН-РТ» состоит из двух полукомплектов, развёрнутых в составе открытых и закрытых сегментов вычислительной инфраструктуры заказчика. Каждый комплект ОКЦ ПЛАТАН-РТ обеспечивает возможность однонаправленной ретрансляции данных между сегментами, обрабатывающими информацию различных уровней конфиденциальности. Программные адаптеры сопряжения (АдС), установленные в каждом полукомплекте, обеспечивают одно- или двунаправленное взаимодействие с заданным заказчиком перечнем внешних систем общего и специального назначения.

Обработка и анализ данных

Все данные, накопленные в первичных хранилищах, при необходимости могут быть либо непосредственно отображены на визуальных интерактивных панелях (ВИП) должностных лиц, либо автоматически направляться для дальнейшей обработки, экспресс-анализа и формирования информационно-аналитических отчётов с помещением результатов автоматизированной обработки во вторичное хранилище – Банк моделей (БнМ). В ОКЦ «ПЛАТАН-РТ» осуществляется регистрация всех видов первичных информационных ресурсов БнД, которые были использованы для формирования вторичных данных – знаний, накапливаемых в БнМ. Пополнение и актуализация содержимого вторичного хранилища – БнМ обеспечивается также подключением необходимого набора прикладных систем заказчика (в частности – ERP) к интегрированному тракту прохождения информации с использованием адаптеров сопряжения (АдС на рис. 2).

Подключение производится посредством доработки или настройки АдС из унифицированного шаблона, встроенного в ОКЦ «ПЛАТАН-РТ». Всем абонентам, работающим в открытых и закрытых сегментах, гарантированно предоставляются доверенные сервисы электронного документооборота с поддержкой нескольких контуров одно- или двунаправленного прохождения информации – служебного (деловая переписка), организационно-распорядительного (управление инфраструктурой) и личного (неформальное информационное взаимодействие с гарантией конфиденциальности). Такой подход позволяет организовать в интересах заказчика как локальные, так и распределённые системы электронного документооборота с консолидированной обработкой данных и формированием итоговых отчётных документов различных уровней конфиденциальности и возможностью «прозрачного» взаимодействия с внешними организациями на основе сервисов систем межведомственного электронного взаимодействия (СМЭВ), систем межведомственного электронного документооборота МЭДО и других специальных протоколов.

Диспетчеризация и мониторинг вычислительной инфраструктуры и критически важных процессов обработки данных

Задачи комплексного мониторинга и управления вычислительным процессом решаются специализированными службами (КСЗ «Plato-RT») в составе ОКЦ «ПЛАТАН-РТ» на следующих двух уровнях:

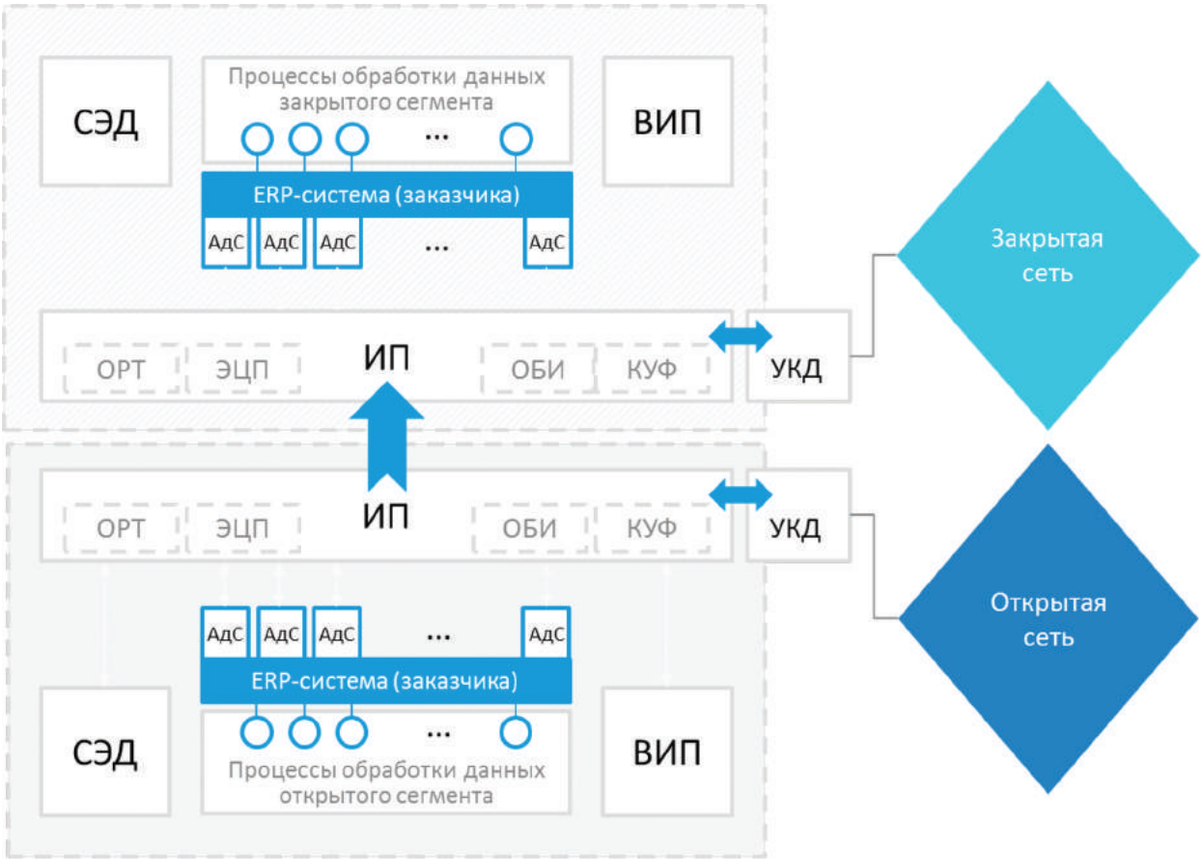


Рис. 2. Архитектура унифицированного комплекта серверной группы ОКЦ

1. Управление вычислительной инфраструктурой (нижний уровень).

Обеспечивается контроль текущего функционального состояния всех элементов распределённой гетерогенной (неоднородной) вычислительной инфраструктуры заказчика, включая:

– вычислительные установки – узлы ЛВС (серверы, рабочие станции, другое оборудование);
– линии/каналы/направления связи;
– интерфейсы всех уровней доступа (OSI) к услугам связи, передачи, хранения и прикладной обработки данных;
– общее и общесистемное программное обеспечение (ОС, СУБД, комплексы средств защиты информации, обмена данными, интеграции функциональных подсистем, ведения общесистемных классификаторов).

2. Мониторинг решения критически важных задач-процессов (верхний уровень).

Реализует событийно-ориентированный механизм контроля хода и результатов выполнения регламентных процессов решения критически важных задач с использованием всей имеющейся в распоряжении заказчика территориально-распределённой вычислительной инфраструктуры. Обеспечивается автоматический и автоматизированный запуск сценариев обработки данных при возникновении нештатных ситуаций, а также генерация отчётов о функционировании технических и программных средств, действиях персонала, состоянии и проблемах в системе операционного управления в целом.

Защищённая доверенная среда обработки и хранения данных

ОКЦ «ПЛАТАН-РТ» обеспечивает двухслойную (внешнюю и внутреннюю) изоляцию баз данных и процессов автоматизированной обработки информации посредством применения встраиваемых периметров защиты изделия «Plato-RT». На каждой вычислительной машине организуется скрытая от базовой ОС и недоступная для администратора защищённая область хранения данных. Последняя включает средства объективной регистрации и автоматической обработки (перехвата и нейтрализации) возникающих инцидентов безопасности.

Описанный механизм нейтрализует попытки сокрытия последствий несанкционированных действий пользователя любой категории, в том числе привилегированных категорий пользователей (сотрудник-инсайдер, системный администратор), а защищённые средства удалённого контроля блокируют работу вычислительной установки до устранения причин возникновения инцидента. По желанию заказчика система может поставляться в одно- или двухконтурном исполнении, с реализацией в независимом (технологическом контуре) функций удалённого контроля (управления) вычислительным процессом и защиты критически важных ресурсов на объектах заказчика.

ОКЦ «ПЛАТАН-РТ» является унифицированным средством высокой степени готовности для комплексного решения типовых задач прикладной обработки, для чего в его состав включены производительные средства защищённого экспресс-анализа данных, поступающих от независимых разнородных источников, а также необходимые инструменты интеграции для реализации двустороннего взаимодействия с внешними АСУ общего и специального назначения. Внедряемое в составе ОКЦ «ПЛАТАН-РТ» программное обеспечение является отечественным, доверенным и защищённым. Технические средства ОКЦ «ПЛАТАН-РТ» по требованию заказчика могут быть исполнены с применением изделий из перечня ЭКБ 01-22-2014.

Состав технических и программных средств, предлагаемых к внедрению на объектах автоматизации Заказчика

В состав комплекта поставки ОКЦ «ПЛАТАН-РТ» входят:

1. Серверная группа – вычислительный комплекс, состоящий из двух высокопроизводительных серверов (полукомплектов), предназначенных для работы по закрытым и открытым сетям передачи данных и шлюза однонаправленной передачи данных. Шлюз обеспечивает возможность однонаправленной ретрансляции данных между сегментами ЛВС объекта автоматизации, обрабатывающими данные различных уровней конфиденциальности. Дополнительно каждый полукомплект серверной группы ОКЦ может включать (выносные) АРМ обеспечения безопасности информации (ОБИ), контроля и управления функционированием (КУФ). Каждый полукомплект серверной группы оснащён предустановленной версией ПО Интеграционной платформы (БИГЕ.466451.099-01 Инструментальный комплект средств интеграции, далее ИКСИ), реализующей общесистемные функции ОКЦ «ПЛАТАН-РТ» в соответствии с описанием, приведённым выше.

2. Клиентский комплект – на клиентских АРМ открытого и закрытого сегментов средствами встроенной в ОКЦ «ПЛАТАН-РТ» Интеграционной платформы обеспечивается автоматизация типовых функций операционного управления корпоративными

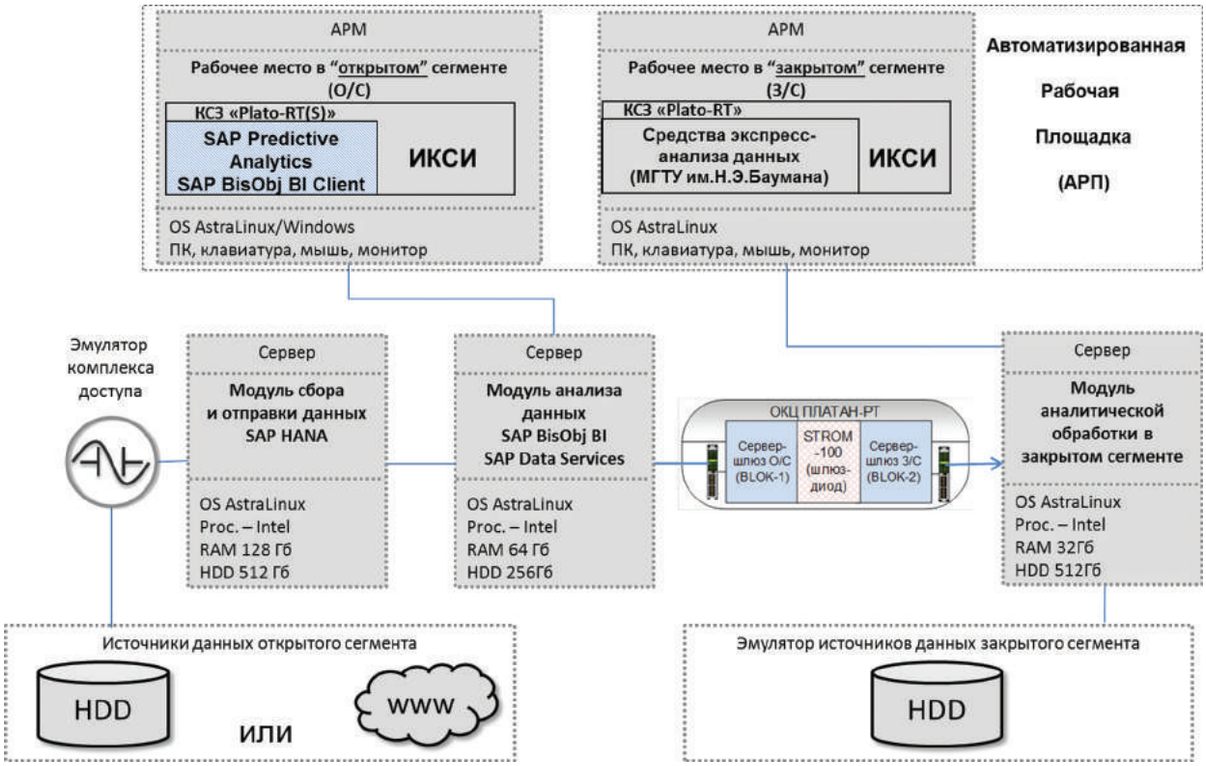


Рис. 3. Реализация консолидированной обработки данных различных уровней конфиденциальности с использованием ОКЦ «ПЛАТАН–РТ»

структурами заказчика, передачи распоряжений с использованием организационно-распорядительного тракта (ОРТ), экспресс-анализа данных с отображением результатов на визуальных интерактивных панелях (ВИП), а также реализация функций защищённого документооборота с применением средств электронной подписи (СЭД и ЭЦП).

3. Комплект разработчика (API) – предназначен для экспресс-разработки программных адаптеров сопряжения (АдС) серверной группы ОКЦ с приложениями заказчика (ERP-системы, САПР и др.).

Задачи обеспечения безопасности информации (ОБИ), контроля и управления функционированием (КУФ) централизованно решаются на каждом объекте автоматизации компонентами КСЗ «Plato-RT» полукомплектов серверной группы ОКЦ «ПЛАТАН-РТ». Подключение полукомплектов серверной группы к канальным интерфейсам открытых и закрытых сетей передачи данных производится посредством устройств унифицированных комплексов доступа (УКД), входящих в состав ОКЦ «ПЛАТАН-РТ».

Ниже (рис. 3) показан пример возможного практического применения ОКЦ «ПЛАТАН-РТ» в интересах проведения комплексного анализа данных, поступающих от открытых и закрытых источников. Автоматизированная рабочая площадка (АРП) представлена двумя АРМ, подключаемыми посредством сетевых интерфейсов к серверам сбора и накопления первичной информации (БнД) «открытого» и «закрытого» сегментов.

В качестве средств анализа накопленных данных в «открытом» сегменте используются заимствованные клиент-серверные компоненты SAP HANA (разработчик – компания SAP, Германия), функционирующие под управлением КСЗ «Plato-RT» в доверенной среде «ИКСИ». В качестве аналитических инструментов в «закрытом» сегменте применяются отечественные средства экспресс-анализа данных ALBA-ВИП (разработчик – МГТУ им. Н.Э. Баумана, Россия).

Интеграция аналитических приложений обоих сегментов, обрабатывающих данные различных уровней конфиденциальности (от канального до прикладного уровней в модели OSI/ISO), осуществляется посредством ОКЦ «ПЛАТАН-РТ» в автоматическом/автоматизированном режимах с подкачкой результатов первичной аналитической обработки данных из «открытого» в «закрытый» сегмент, их консолидации с данными от закрытых (конфиденциальных) источников. Выполнение процедур комплексного анализа на АРМ и серверах «закрытого» сегмента завершается пополнением содержимого банка данных и моделей вторичной информации (БнМ).

А. Р. Вериго, В. И. Чехов, ЗАО «РТСофт»

СИГРЭ: Информационные системы и телекоммуникации для электроэнергетики – актуальные проблемы и задачи 2014–2016 годов

В статье приведены некоторые итоги деятельности Подкомитета D2 по информационным системам и телекоммуникациям (ИСиТ) Российского Национального Комитета СИГРЭ в России и на международной арене за последние полтора года.

Представлен обзор основных направлений деятельности СИГРЭ по ИСиТ в мировой практике и приоритетов исследований в данной области на текущий момент и на ближайшую перспективу.

Российский Национальный Комитет (РНК) СИГРЭ утвердил в четвёртом квартале 2014 года ЗАО «РТСофт» в качестве базовой организации деятельности **Подкомитета D2 РНК СИГРЭ** по информационным системам и телекоммуникациям с предоставлением статуса «Ведущий научно-технический партнёр РНК СИГРЭ». Возглавила Подкомитет, а позднее и представительство России в головном Исследовательском комитете (ИК) D2 СИГРЭ, генеральный директор ЗАО «РТСофт», д.т.н. Ольга Викторовна Синенко. Организационная структура Подкомитета полностью соответствовала исследовательским рабочим группам головного CIGRE того времени и включала представителей управляющего электросетевого холдинга, ключевых российских компаний, проектных и исследовательских институтов в области управления и связи в энергетике. Появление сайта Подкомитета D2 как информационной и дискуссионной площадки позволило оперативно предоставлять технические материалы Исследовательского Комитета СИГРЭ специалистам отрасли, проводить дискуссии, готовить общие мероприятия.

В течение прошедшего года обсуждались актуальные темы на дискуссионных площадках Подкомитета в рамках деловых программ общероссийских энергетических форумов, выставок, конференций:

– «Кибербезопасность в электроэнергетике» – деловая программа ежегодного энергофорума «Electro 2016» (8 докладов);
– «Системы связи в электроэнергетике» – деловая программа ежегодной выставки «Электрические сети России–2015» (7 докладов);
– «Автоматизированные системы управления в распределительных электрических сетях России: достижения и перспективы развития с учётом международного опыта СИГРЭ» – ежегодный семинар Подкомитета D2 (14 докладов).

В истекшем году Подкомитет активно включился в подготовку «дорожных карт» Национальной технологической инициативы в части EnergyNet, предполагающей формирование новых типов рынков продажи электроэнергии с учётом роста доли распределённой генерации на стороне потребителей, включая генерацию от возобновляемых источников энергии.

Организационная структура, направления исследований рабочих и совместных групп, все новости и дискуссионные материалы размещены на сайте Подкомитета D2 – **http://d2_rus.cigre.ru/**. Наиболее важные материалы по деятельности Подкомитета сохраняются на сайте в разделах публикаций и электронной библиотеки.

Помимо пяти основных рабочих групп Подкомитета, назрела необходимость в создании двух совместных с другими подкомитетами РНК СИГРЭ рабочих групп по проблемам управления распределительными сетями с распределённой генерацией (совместно с подкомитетом C6 РНК СИГРЭ) и вопросам обеспечения информационной безопасности систем управления, защиты и связи в электроэнергетических системах (совместно с Подкомитетом B5 РНК СИГРЭ). Первая совместная проблемная рабочая группа D2/C6 **«Активно-адаптивная распределительная электрическая сеть»** под руководством к.т.н. Н. Г. Шубина начала свою деятельность в сентябре 2015 года. Установочная встреча совместной группы D2/B5 **«Кибербезопасность компонентов инфраструктуры современных объектов электроэнергетики»** под руководством к.т.н. М. В. Никандрова состоялась в начале 2016 года. Период деятельности рабочих и проблемных групп ограничен двумя годами, по завершению периода публикуются так называемые технические брошюры по направлению, выбранному совместной группой для исследований. Материалы по деятельности совместных групп размещены на сайте Подкомитета:

– **http://d2_rus.cigre.ru/press-center/materials-pwg-d2c6/**
– **http://d2_rus.cigre.ru/press-center/materials-pwg-d2b5/**

В настоящее время российские эксперты являются участниками действующих рабочих групп головного Исследовательского комитета СИГРЭ в исследованиях систем управления, систем связи и технологий обеспечения информационной безопасности энергосистем, что позволяет своевременно знакомиться с актуальными техническими решениями в энергосистемах мира, оперативно информировать профессиональное сообщество страны, а также отражать российский опыт в изданиях Исследовательского комитета.

Осенью 2015 года в Лиме состоялся Коллоквиум головного Исследовательского комитета D2 с участием наблюдательного члена от РФ, руководителя российского Подкомитета D2, д.т.н. О. В. Синенко (см. фото с Коллоквиума). Коллоквиум позволил наладить тесные рабочие связи с руководством ИК и модераторами рабочих групп, сделать сообщение об актуальных технических задачах, решаемых в России, включиться в ряд организационных структур комитета. На коллоквиум было отобрано 22 доклада, представленных экспертами 12 стран мира. Доклады были подготовлены по трём заявленным темам коллоквиума:

– **Сети телекоммуникаций в аварийных режимах энергосистемы;**
– **Сохранение устойчивости бизнеса производства и передачи электроэнергии в условиях катастроф;**

– **Лучшие практики реализации экономически эффективных систем кибербезопасности в электроэнергетике.**

В первый тематический блок вошло 10 докладов, посвящённых замене старой ATM-системы связи на IP-систему, приведён бразильский опыт построения гибких оптических сетей связи (OTN) для передачи данных в аварийных ситуациях и аргентинский доклад по оптоволоконной системе связи (OPGW) для системообразующих сетей. Докладчики из Испании представили анализ опыта эксплуатации кабеля OPPC в своей энергосистеме, а представители Уругвая поделились опытом GOOS-обмена информацией между подстанциями с использованием SDH-системы передачи. Ряд докладов был посвящён опыту подготовки к вводу в эксплуатацию систем связи и их влиянию на качество управления энергосистемами.

Второй тематический блок представлял опыт стран, переживших за последнее десятилетие крупные природные катастрофы, и акцентировал внимание специалистов на способах восстановления работы энергосистем после крупных аварий и повышения их живучести. Четыре доклада от Японии отразили опыт энергетиков этой страны в период крупного землетрясения 2011 года. Авторы из Колумбии представили результаты использования технологий мультиобъектной архитектуры системы управления ЭЭС в период аварий.

В третий тематический блок вошли доклады по опыту обеспечения кибербезопасности систем связи и управления в ЭЭС, традиционно актуальной задачи. Предлагаются различные подходы к построению системы кибербезопасности информационных систем и анализ поведения диспетчеров при сбоях в работе систем управления. В центре внимания традиционно остаётся стандарт МЭК 61850.

Результатом деятельности рабочих групп каждого ИК CIGRE является издание «Технической брошюры». В 2014–2015 годах комитетом D2 были завершены исследования по ряду направлений и подготовлены следующие публикации:

– Техническая брошюра 603, разработанная совместной рабочей группой JWGD2/B5.46 – **«Применение и управление мерами информационной безопасности для систем защиты и управления»;**
– Техническая брошюра 615 (рабочая группа WGD2.31) – **«Архитектура информационной безопасности цифровых систем и цифровых устройств объектов электроэнергетики»;**
– Техническая брошюра 618 (рабочая группа WGD2.35) – **«Масштабируемые решения коммуникаций по оптоволоконным сетям связи»;**
– Статья в журнале «ELECTRA» – **«Состояние кибербезопасности в электроэнегетики».**

Очевидно, что наиболее актуальные темы исследований последнего времени связаны с задачами обеспечения функционирования электроэнергетической системы в условиях природных и техногенных ката-

строф, крупных системных аварий, противостояния киберугрозам.

В преддверии 46-й сессии СИГРЭ 2016 года председателем Исследовательского комитета были названы темы двух «Зелёных книг» (Green book), формируемых на основе Технических брошюр комитета и излагающих перечень технологий, использованных для решения проблемы, но без раскрытия деталей этих технологий:

- **Разработки информационных технологий и телекоммуникации в электроэнергетике с обеспечением их кибербезопасности;**
- **Внедрение систем связи в электроэнергетие для критически значимых коммуникационных сервисов.**

В процессе работы коллоквиума из списка актуальных исследований, представленного экспертами разных стран, были выбраны следующие темы, требующие создания новых рабочих групп Исследовательского комитета:

- **Интернет вещей в интеллектуальном учёте электроэнергии;**
- **Информационная платформа и центр хранения данных в задачах учёта электроэнергии (агрегирование данных учета);**
- **Роль и место CRM-систем на рынке энергетики;**
- **Кибербезопасность в электроэнергетике.**

46-я сессия СИГРЭ состоится в августе 2016 года в Париже. На ней будут обсуждены и утверждены тематики новых рабочих групп комитета. В качестве актуальных направлений исследований комитета D2 на 2016 год предлагаются:

- **Новые структуры в составе систем управления электроэнергетическими системами (ЭЭС):**
  - Smart Grid для DSO и TSO;
  - Big Data;
  - объединение SCADA, EMS, DMS, OMS.
- **Кибербезопасность систем управления и связи ЭЭС:**
  - кибербезопасность цифровых систем управления и защиты;
  - нормативное обеспечение систем кибербезопасности;
  - архитектуры информационных систем ЭЭС с учётом кибербезопасности.
- **Использование систем мобильной связи в задачах управления ЭЭС:**
  - беспроводные технологии в системах управления ЭЭС;
  - обеспечение жизнеспособности ЭЭС после катастроф;
  - использование существующих структур мобильной связи для задач управления ЭЭС.

Как следует из анонсированных приоритетов, наряду с традиционными системами связи в последнее время всё более активно используются беспроводные технологии для создания каналов связи в системах управления ЭЭС. Это перекликается с темами докладов коллоквиума в Лиме и означает, что от природных и техногенных катастроф не застрахована ни одна энергосистема мира и это следует учитывать при модернизации существующих сетей связи и проектировании новых.

В рамках сессии СИГРЭ Подкомитет D2 РНК СИГРЭ планирует участие в выставке EXPO CIGRE Paris-2016 со стендом, представляющем современные решения ЗАО «РТСофт» в области управления распределённой энергетикой.

В начале 2016 г. руководство Исследовательского комитета D2 CIGRE приняло решение о проведении очередного коллоквиума в сентябре 2017 года в Москве. Это решение в первую очередь обусловлено большим профессиональным интересом к российской энергосистеме, одной из самых крупных в мире, а также к используемым при её управлении технологиям.

Согласно существующим правилам, две из трёх приоритетных тем коллоквиума заявляются страной, проводящей коллоквиум, – эта преференция позволит поднять для обсуждения вопросы по темам, особо актуальным для российской энергетики. В связи с этим Подкомитет D2 РНК СИГРЭ организовал дискуссию на своём сайте (http://d2_rus.cigre.ru/colloquium-2017/), посвящённую обсуждению тем, предлагаемых для Коллоквиума-2017 ИК D2.

Планируемое расширение активности Подкомитета D2 РНК СИГРЭ даёт уверенность в том, что плодотворное международное сотрудничество в рамках этой авторитетной организации позволит ускорить решение ряда проблем в управлении развивающейся российской энергетики и внести свой вклад в международный обмен знаниями и передовыми технологиями.

Новости рынка

Новые разработки «РТСофт» на выставке «Электрические сети России – 2015»

Компания «РТСофт» приняла активное участие в XVIII Международной специализированной выставке «Электрические сети России – 2015», представив свои инновационные продукты и новые решения для автоматизации в электроэнергетике.

Ежегодная международная выставка «Электрические сети России» проходила в Москве в период с 1 по 4 декабря. Это одна из основных выставочных площадок электроэнергетики России, где большинство ключевых компаний отрасли демонстрируют свою продукцию. «РТСофт», традиционно участвующий в этом мероприятии, представил на стенде передовые продукты, программно-технические комплексы и технические решения для электроэнергетики, среди которых было много перспективных новинок.

Повышенным вниманием посетителей пользовалась новая информационно-управляющая система AMIGO. Это программный комплекс автоматического управления микроэнергосистемами (Microgrid), который обеспечивает координированное управление распределённой генерацией, системами накопления электроэнергии, режимами и топологией Microgrid, а также локальными средствами управления нагрузкой. Важной особенностью и преимуществом AMIGO является то, что он позволяет снижать стоимость внешнего электроснабжения, уменьшать эксплуатационные расходы и повышать показатели качества электроэнергии и надёжность электроснабжения потребителей Microgrid. Оргкомитет международной специализированной выставки «Электрические сети России» высоко оценил эту инновацию «РТСофт» – AMIGO получил золотую медаль при подведении итогов работы выставки.

Для создания систем автоматизации энергообъектов «РТСофт» предложил целый ряд своих новых разработок. Это контроллеры МИК-01 и СМАРТ-ВАУ, программно-технический комплекс СМАРТ-КП2 и программная платформа SMART-SCADA.

Технические специалисты с интересом ознакомились с новыми решениями «РТСофт» для центров управления сетями и диспетчерских центров энергосистем. А также с новейшим продуктом – PF.Protection, который предлагает полный набор функций и инструментов расчёта токов короткого замыкания, выбора уставок и анализа работы РЗА энергосистем.

Посетители узнали и о новациях в уже хорошо зарекомендовавших себя продуктах компании: контроллерах АСУТП – SPRECON-E-C, SCADA АСУТП – SPRECON V460, измерительных преобразователях МИП-02. Ознакомились и с широкой линейкой приборной продукции «РТСофт».

Большой интерес у гостей стенда вызвали уникальные отечественные продукты «РТСофт», отвечающие принципам программы импортозамещения. Среди них промышленный монитор GT777, созданный на основе самых современных достижений и технологий, и бесшумный многофункциональный встраиваемый сервер BLOK для ответственных эргономичных систем с длительным жизненным циклом в формате BoxPC. Приятно отметить, что BLOK стал номинантом на получение престижной национальной премии в области импортозамещения «ПРИОРИТЕТ-2015».

В рамках деловой программы выставки состоялся круглый стол «Импортозамещение: границы энергетической безопасности», где выступили ведущие эксперты компании и подкомитета D2 РНК СИГРЭ, образованного на базе «РТСофт». Докладчиками была поднята проблема обеспечения энергетической безопасности страны на экономическом и техногенном уровне. А под эгидой подкомитета D2 РНК СИГРЭ состоялся круглый стол «Технологии и средства сетей связи и телекоммуникаций» в ходе V Международной научно-практической конференции «Автоматизация и информационные технологии в энергетике», являющейся частью деловой программы выставки «Электрические сети России».

Все дни работы выставки эксперты и технические специалисты «РТСофт» активно общались с посетителями стенда, обстоятельно и профессионально консультировали их по вопросам автоматизации подстанций и управления электрическими сетями, информационной безопасности и качества электроэнергии, а также создания Smart City. В ходе общения были установлены новые контакты, достигнуты важные договоренности и заключён ряд соглашений.

Павел Литвинов, ЗАО «РТСофт»

Имитационное моделирование вопросов информационной безопасности как инструмент оценки защищённости и оптимизации затрат

Введение

Тема кибербезопасности для энергетических компаний, в силу совершенно объективных причин, становится всё более актуальной (в тексте статьи будет сделан уклон на специфику энергетических компаний, но все методики и рекомендации практически полностью применимы к любым промышленным системам автоматизации и управления вне зависимости от отрасли). Сегодня процессы производства, передачи и распределения электроэнергии существенно зависят от информационных систем, включая и сети передачи данных. Энергокомпании централизованно осуществляют контроль и управление, что порождает качественно новые угрозы и риски, поскольку совсем недавно эти функции выполнялись локально и децентрализованно. Развитие технологий smart- и microgrids и умного учёта ведут к появлению многочисленных новых услуг и сервисов, в том числе и путём вовлечения потребителей, что кардинально меняет архитектуру систем в сторону распределённой автоматизации и меняет принципы управления, доступа и использования информационных систем. Другими словами, хакеры могут ставить под угрозу нормальное функционирование энергокомпаний уже не только путём удалённой атаки на объекты ИТ-инфраструктуры энергокомпаний, но и посредством атаки на (через) потребителей.

В ситуации, когда сокращение операционных расходов и увеличение выручки за счёт предоставления новых сервисов возможно главным образом только благодаря использованию передовых технологий, в том числе и «Интернета вещей», тенденцию к интеграции и увеличению числа связей между решениями и системами уже не остановить! Рост уязвимости подобных систем к кибератакам компенсируется использованием новых технологий и средств защиты. Как и в историческом процессе «соревнования» брони и оружия победителя не будет, 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 рисков и недопущении критических. Оговорка про критические риски является важным граничным условием. В бизнесе невозможно компенсировать все риски, такая линия поведения сделает вашу продукцию и услуги неконкурентоспособными, поэтому какие-то из них необходимо осознанно принять. Зачастую допустимо принятие даже части критических рисков. Главное – не допустить катастрофических рисков, при которых возникает угроза потери бизнеса или прямая опасность для жизни людей.

Объективные сложности оптимизации затрат

Очевидно, что целесообразность и точность определения необходимости дополнительных затрат на 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, обе части этого уравнения нам, к сожалению, неизвестны или 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 определить связь технологических сбоев с действиями хакеров,

в «продвинутых» атаках обязательным является этап сокрытия следов проникновения;

– самые потенциально 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, 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 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 подсистемах. Нарушение в энергетической инфраструктуре одной страны или региона может спровоцировать развитие каскадного эффекта в такой степени, что в результате пострадает инфраструктура других стран [1].

Предпосылки для проектирования моделей

Оптимизационная задача – сложная функция от начальных (граничных) условий, например таких, как размер организации и состав предъявляемых к ней требований регуляторов, точки зрения, с которой идёт рассмотрение, специалиста по ИБ, руководителя или собственника. Очень важно на начальных этапах не перегружать модель, в надежде, что удастся с помощью математических методов создать саморегулирующуюся и самообучающуюся программу, которая сможет оптимально отвечать на все вопросы, в том числе и не заложенные в алгоритмы изначально. Принципы проектирования модели будут также отличаться в зависимости от сценария: требуется ли оптимизация защиты существующей инфраструктуры и программно-технических средств или речь идёт о новом строительстве. При нарастающих кризисных явлениях чрезвычайно востребованным может быть моделирование сценария минимальной достаточности. Очевидно, что автоматическое урезание бюджета на мероприятия по обеспечению информационной безопасности, например на 30 %, выглядит, на первый взгляд, разумным, на фоне идущего процесса экономии и сокращения других бюджетов. Реальность такова, что без моделирования и оценки последствий легко можно оказаться в ситуации, когда из-за 30-процентной экономии получится, что оставшиеся 70 % мы потратим напрасно. Безопасность – комплексное и многофакторное понятие, способов атаки и потенциальных уязвимостей множество, и злоумышленники будут использовать любое слабое место. Метафора для этого тезиса очень простая – нет необходимости тратить деньги на решётки и сигнализацию на «окна», если мы не запираем «двери». Одним из лучших способов достижения пропорциональности и сбалансированности инвестиций для решения сложных 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.

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Рис. 1. Структура мероприятий для достижения конкретных результатов в области кибербезопасности

В рекомендациях National Institute of Standards and Technology «Framework for Improving Critical Infrastructure Cybersecurity» [2] содержится детальное описание процесса дробления функций на категории и подкатегории. Обратим внимание на верхний уровень функций (рис. 1), содержащий в причинно-следственной связи базовые функции, которые должны быть пропорционально обеспечены организационными и техническими средствами.

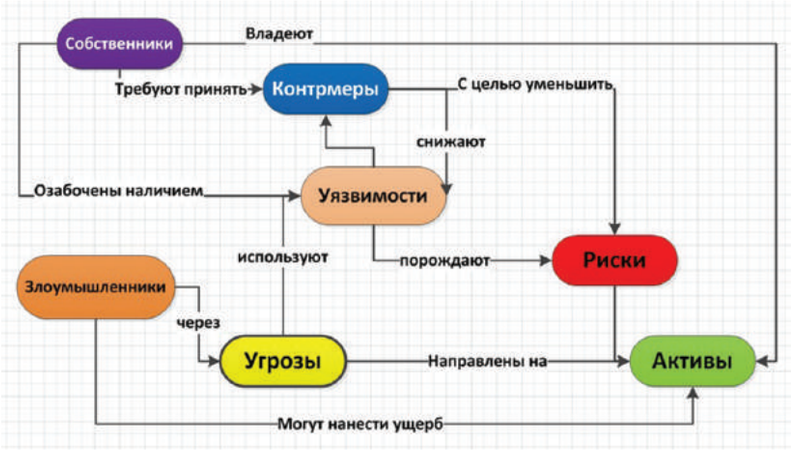


Рис. 2. Концептуальная модель понятий безопасности и связей между ними

Обоснованный способ определения необходимых для моделирования агентов можно заимствовать из стандарта ISO/IEC 27032:2012 «Guidelines for cybersecurity» [3]. На рис. 2 приведён перечень видов агентов и отражены существенные связи между ними.

Совершенно аналогичную схему 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, он представляет вероятность как суперпозицию «угроз» и «уязвимостей» (рис. 3).

В предельных случаях это уточнение совершенно понятно: как бы ни были велики угрозы, если отсутствуют уязвимости, то вероятность реализации риска равна нулю.

В предметной области менеджмента рисков существует по крайней мере 31 метод, рекомендуемый для поддержки процесса оценки риска [4]. Все они имеют различную применимость и эффективность на разных стадиях: 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, окружающей среды эффективно использовать методологии исследования опасности и работоспособности (HAZOP – Hazard and Operability Study). Сравнительная оценка риска может быть получена моделированием методом Монте-Карло. Это хороший способ оценки влияния неопределённости оценки 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. Следует только помнить, что метод Монте-Карло не может адекватно моделировать события с очень высокой или очень низкой вероятностью появления. Практические рекомендации по использованию этих и других методов можно найти в [5].

Текущее состояние вопроса

Тема потенциала использования агентного моделирования энергетических систем в контексте кибербезопасности давно обсуждается в научном сообществе. Можно рекомендовать работы зарубежных [6] и российских [7] авторов, каждая из статей содержит обширный список литературы для знакомства с историей и текущим состоянием вопроса.

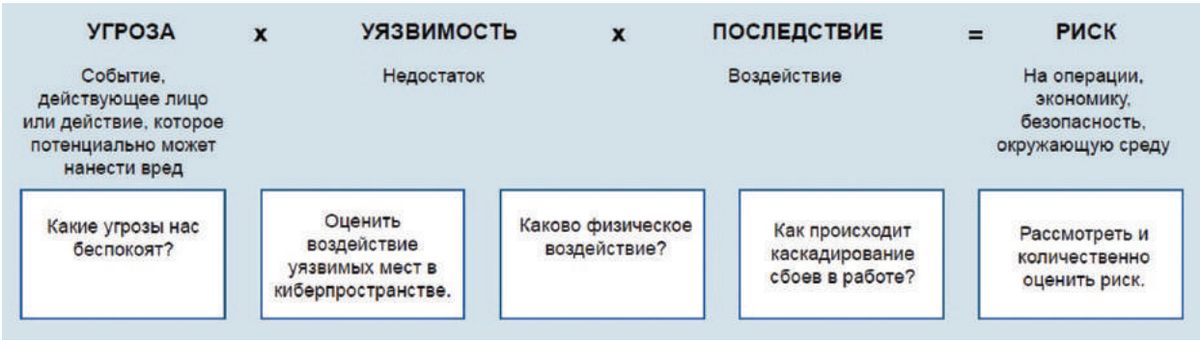


Рис. 3. Общая модель риска согласно ISO/IEC 27032:2012

Несмотря на многолетний опыт исследований, отдельные положительные результаты и очевидную полезность, методы имитационного моделирования вопросов информационной безопасности не получили широкого практического применения. Для глубокого анализа причин можно построить отдельную модель, но чтобы не попасть в бесконечную рекурсию, ограничимся логическими построениями ☺.

В первую очередь предположим, что и низкая востребованность предварительных результатов, и отказ от продолжения финансирования, связаны с отраслевой спецификой. Научная школа в энергетике чрезвычайно сильна и развита во всём, что касается планирования режимов, статики и динамики электрических процессов, оценки состояния и многого другого. В работе используется значительное количество симуляторов энергосистемы и режимных тренажёров диспетчера, построенных на их основе. Попытка, на этих же принципах и с той же высокой шкалой оценок и требований, подойти к обсуждаемой задаче, обречена на провал. В наших моделях не действуют физические законы Ома и Кирхгофа или дифференциальные уравнения, определяющие поведение электрических машин, все они, пусть и сложные для решения при большом количестве узлов, обеспечивают необходимую определённость и точность результата. Для преодоления этого конфликта ожиданий и восприятия результата необходимо взаимное движение навстречу команды аналитиков и персонала заказчика.

Другая очевидная трудность моделирования – необходимость работать на стыке совершенно разных предметных областей. Трудно ожидать, что глубокие познания в энергетике пересекутся с широкими представлениями в области информационной безопасности и умножатся на опыт в области применения статистики и методов математического моделирования в одном человеке. Даже если предположить, что мы найдём такого специалиста, то в силу масштабов задачи на решение ему потребуется слишком много времени. Мы с неизбежностью приходим к необходимости командной работы в таком проекте, распределения ролей, выработки и согласования терминологии и т. д. В крупной организации и холдинге это должна быть не разовая акция, а постоянный бизнес-процесс.

Старту работ чаще всего мешает отсутствие сформулированной постановки задач, требующих оптимизации путём моделирования. Наиболее частым состоянием вопросов информационной безопасности на предприятии является отсутствие собственных актуальных моделей угроз и нарушителя или даже заимствованных, но должным образом адаптированных к операционной деятельности энергокомпании. Ещё чаще отсутствуют какие либо метрики текущего состояния защищённости и понимание целевого состояния, что не позволяет эффективно и комплексно планировать мероприятия и объективно контролировать прогресс.

В последнюю очередь по списку, но не по значению поставим вопросы секретности. Любая информация о состоянии защищённости объектов КСИИ (Ключевая Система Информационной Инфраструктуры), пусть и полученная путём моделирования, является закрытой. Соблюдение режима конфиденциальности серьёзным образом осложняет выполнение работ по моделированию. Например, заказчик не имеет права (или опасается) раскрывать определённые данные и передаются только небольшие выборки или даже намеренно искажённые значения. При отладке модели это приводит, соответственно, к ошибочному определению вида распределения исходных данных и серьёзным ошибкам в масштабных коэффициентах, в результате чего оптимизационная кривая имеет «правильную форму и поведение», но начальная достоверность предсказанных численных значений становится низкой.

Метрики информационной безопасности

Вышеперечисленное наводит на мысль, что перед нами типичная «слоновая» задача, которая поддаётся решению только путём разбиения на части. Начнём процесс декомпозиции.

В первую очередь, для каждого объекта надо определиться с его «размерностью» и потенциальными «слабостями». Уязвимость – это неотъемлемое свойство практически любого элемента инфраструктуры информационных технологий: компьютера, телекоммуникационного оборудования, ПО, сервера, контроллера и т. п. Очевидно, что чем больше таких позиций, тем больше потенциальная «поверхность для атаки» в этом же перечне. (В скобках хотелось бы отметить, что при проведении моделирования наглядным образом можно продемонстрировать, что для каждой «размерности» объекта существует некий оптимум состава и средств защиты. В самом деле, оборудование и специализированное программное обеспечение, предназначенное для защиты от атак, также может содержать уязвимости и его наличие увеличивает «поверхность» для атаки. Особенно часто мишенью для хакеров становятся средства защиты, действующие в автоматическом режиме. Не будем также забывать, что взломщик обычно не является специалистом в энергетике, а в противодействии системам защиты разбирается лучше, поскольку одно

и то же программное обеспечение используется в разных отраслях).

Отдельным вектором необходимо учесть и обслуживающий персонал. Каждому из видов устройств есть возможность экспертным путём или, основываясь на данных статистики, установить индивидуальный весовой коэффициент «уязвимости». Очевидно, что устройства, не имеющие доступа по IP, менее уязвимы, а по данным статистики ОС Linux, реже подвергается вирусным атакам. Эти сравнительно несложные оценки, после нанесения на радарную диаграмму, дадут нам наглядную картину распределения потенциальных уязвимостей для обоснованного планирования мероприятий, а использовав формулу длины n-мерного вектора a = {a1 ; a2; ... ; an},

$$|a| = \sqrt[2]{\sum_{i=1}^{n} a_i^2} \quad (1)$$

получим требуемую метрику.

Полученное значение можно привести таким образом, чтобы максимальное значение было равно единице, и получить синтетическую метрику «уязвимости» конкретного объекта. Принципиально важным является процесс запуска процедуры пересчёта при каждом изменении таких параметров как:

– изменение количества, вида и состояния оборудования (отключённое и выведенное в ремонт оборудование не может использоваться для атаки);
– численного состава персонала, его квалификации, ролей и обязанностей;
– изменение конфигурации сети, разделения и объединения её сегментов;
– при появлении новых сведений в базах данных уязвимостей (ФСТЭК России совместно с заинтересованными федеральными органами исполнительной власти и организациями сформировал банк данных угроз безопасности информации).

После нанесения значений на линию времени мы получим динамику изменений уязвимости как функцию времени, пока без учёта эффективности наших контрмер. При любом количестве объектов разных видов, применяя те же действия, мы можем получать различные радарные диаграммы в зависимости от решений, которые нам необходимо принять. И всегда иметь интегральный показатель, важный не сам по себе, а именно в динамике. Руководство компании будет иметь оценку, в какую сторону меняется ситуация со временем и какова динамика этих изменений.

Следуя описанной технологии, можно получить нужное количество как независимых метрик, так и производных от них KPI, ориентированных на принятие управленческих решений. В качестве отправной точки можно порекомендовать схему (рис. 4) приведённую в [8].

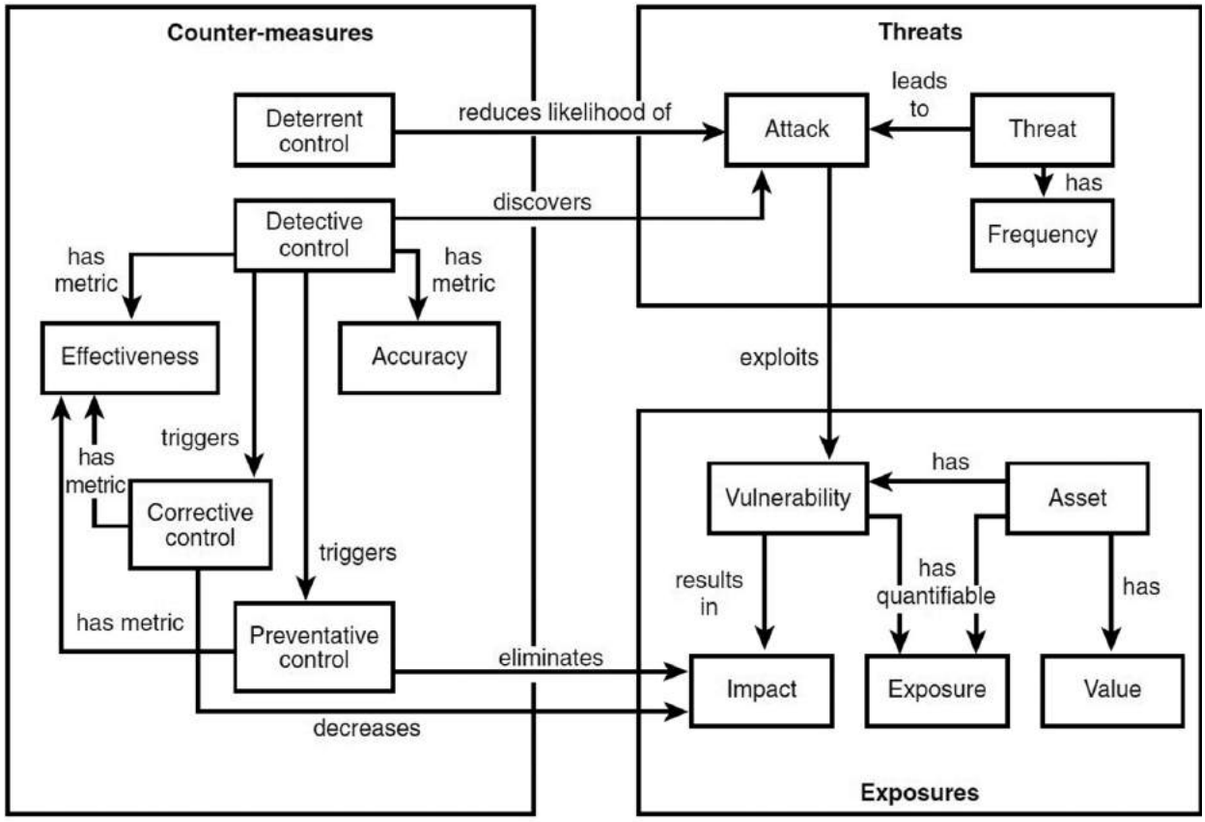


Рис. 4. Логическая структура контроля мероприятий по обеспечению информационной безопасности

И ещё несколько слов о пользе, которая может быть получена от регулярного расчёта метрик и измерений характеристик процессов, связанных с информационной безопасностью. Общеизвестно, что решения надо принимать, основываясь на объективных данных. В большинстве случаев даже 15 значений это уже неплохо, а 30 – позволяет делать достаточно обоснованные предположения. В том числе появляется возможность сделать важное заключение: является ли измеряемый процесс регулярным в бизнес-понимании этого термина. Невозможно улучшать нерегулярные бизнес-процессы, их сначала надо «поставить»! Основным статистическим критерием и доказательством регулярности бизнес-процесса является тот факт, что отклонения его метрики или KPI хорошо описываются нормальным распределением (эти положения являются одним из краеугольных камней Лин Шесть Сигм).

Направления и методы оптимизации

Один из базовых способов ускорения вычислений в имитационных моделях, упрощения их создания и отладки – снижение размерности модели при одновременном уменьшении количества связей между агентами. Применим эту технику к получению портрета злоумышленника. Для классификации нарушителей определим набор признаков, влияющих на успех проведения атаки (рис. 5).

Разные наборы значения по разным осям дают нам возможность построить «спектр нарушителей», для практических целей количество групп надо свести к уровню минимальной достаточности. В качестве первого приближения рекомендуем ограничиться следующей типизацией:

– «Хакер-любитель» – частное лицо, пытающееся найти возможности и способы взлома технологических и SCADA-систем, имеющих интерфейсы в Интернет с помощью известных уязвимостей, найденных с использованием поисковой системы «Shodan»;
– «Инсайдер» (в том числе «без злого умысла») – недовольный сотрудник или обслуживающий персонал собственной или сторонних организаций (поставщики, партнёры, наладчики), имеющий права доступа и знающий тонкости эксплуатации систем и способы хранения конфиденциальных данных;
– «Враг» – преступные группировки и иностранные правительства (Cyber Espionage, Cyber Crime, Cyber Activism, Cyber Terrorism, Cyber War и т. п.).

Такое деление эквивалентно в математическом смысле переходу от матриц большей размерности к матрицам меньшей размерности или даже векторам.

На практике поведение «хакеров-любителей» успешно описывается языком вероятностей, поскольку по частоте и способам таких атак есть значительное количество статистических данных. Достаточно эффективной защитой являются специализированные программные и технические средства, даже простые и бюджетные. Мероприятия от этой категории нарушителей должны планироваться и выполняться в первую очередь. (Следует помнить, что в этом случае «не обязательно быть целью, чтобы стать жертвой». Например, вирус, предназначенный для кражи паролей в онлайновых играх, вполне может повредить АСУ ТП. Разумеется, авторы не тестировали его на совместимость с технологическими системами).

«Инсайдер» – самый сложный в моделировании и противодействии тип нарушителя. Риски, связанные с ними, часто недооцениваются. Компенсационные меры обязательно должны включать в себя комплекс организационно-технических мероприятий. Для их обоснованной разработки должны рассматриваться различные типизированные образы внутреннего нарушителя, такие как «халатный», «манипулируемый», «обиженный», «нелояльный», «подрабатывающий», «внедрённый». Полезную методологию и рекомендации можно также найти в [9]. Статистические данные, иллюстрирующие мотивацию внутренних нарушителей (рис. 6), опубликованные в [10], можно использовать в качестве начального приближения для выполнения оценок и как руководство к планированию мероприятий по противодействию.

Что касается последнего типа нарушителя, то мы имеем сразу и наиболее сложные, и дорогие мероприятия по защите, а для объектов КСИИ ещё и высокие риски. Выходом из этой тупиковой, на первый взгляд, ситуации является понимание того факта, что вы не можете (и не должны!) самостоятельно и в одиночку противостоять таким угрозам. Наглядную аналогию можно найти в смежной области физической защиты и безопасности. Предположим, вокруг

[УСПЕХ ВЗЛОМА] ~ [МОТИВАЦИИ] × [РЕСУРСУ] × [ОПЫТУ] × [ИНФОРМИРОВАННОСТИ] × [ВРЕМЕНИ]

Рис. 5. Набор признаков, влияющих на успех проведения атаки

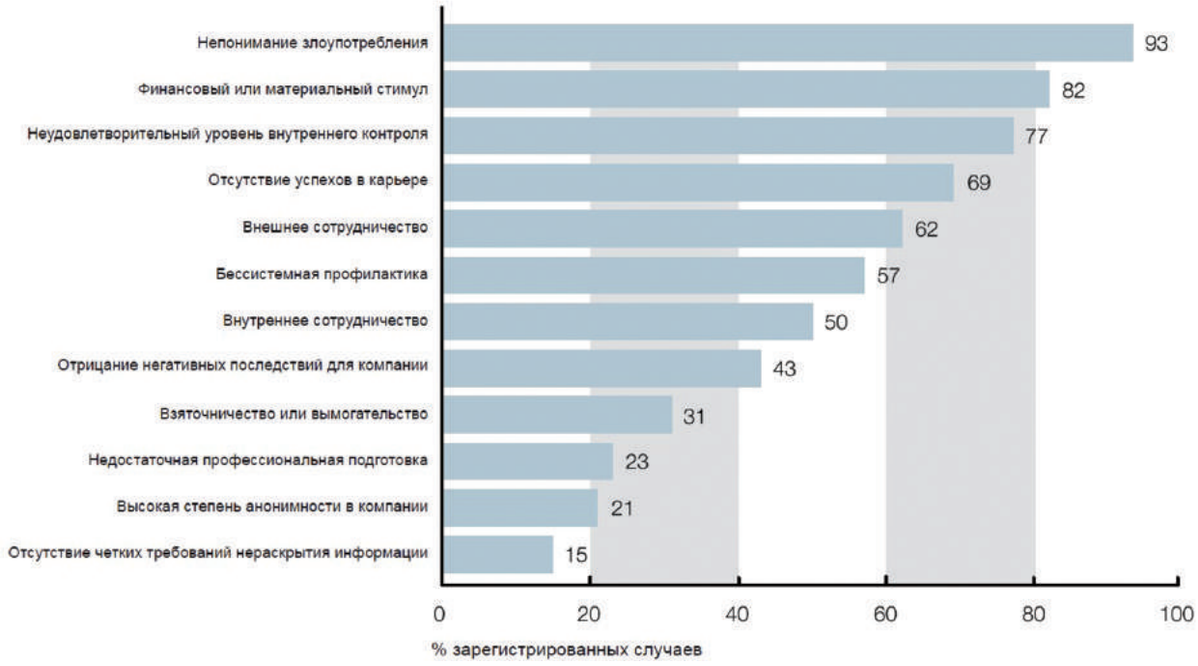


Рис. 6. Мотивация внутренних нарушителей

объекта установлен забор и ведётся видеонаблюдение, это совершенно адекватный способ защиты от диких животных, нетрезвых граждан, «охотников» за цветными металлами, но если объект атакует вооружённое бандформирование, надо вызывать ОМОН, спецназ или даже обращаться к военным. В нашем случае в специализированные подразделения МВД и ФСБ России. Целиком делегировать риск не получится. Обращение за помощью должно быть своевременным и обоснованным, а для последующего розыска и наказания виновных предоставлена доказательная база. С этой целью техническими и организационными средствами должно быть обеспечено обнаружение атак, мониторинг состояния и надёжное ведение журналов событий. В части мониторинга перспективным представляется сотрудничество с центром круглосуточного мониторинга киберугроз, недавно открытого на базе дочерней компании «Ростеха» — «РТ-Информ». Новое подразделение в круглосуточном режиме собирает данные о киберугрозах и инцидентах, связанных с информационной безопасностью всех входящих в состав госкорпорации предприятий, проводит мероприятия по нейтрализации угроз, а также будет расследовать инциденты.

Вероятная структура угроз

Точное понимание видов угроз имеет решающее значение для планирования мероприятий по защите. В качестве отправной точки можно использовать рекомендации [1], представленные в таблице.

Не всегда можно полностью полагаться на готовые рекомендации в выборе пар {[угрозы] × [меры защиты]}. Во-первых, для части узкоспециальных систем их может просто не быть, во-вторых, ландшафт угроз постоянно меняется, и наконец авторы могли что-то пропустить или забыть учесть. Обеспечить полноту перебора всех возможных вариантов не прибегая к помощи вспомогательных средств достаточно сложно. В качестве примера (рис. 7) приведён один из интерфейсов информационно-аналитической системы, одна из подсистем которой помогает декомпозировать нормативно-справочную документацию предметной области и хранить её в виде иерархии тезисов.

Работа по декомпозиции – это совместный труд аналитика и технолога, программное обеспечение позволяет формализовать этот процесс, поддержать процедурно и организовать коллективный ввод и редактирование информации, в том числе с использованием веб-интерфейса. На следующем этапе появляется возможность устанавливать связи между различными сущностями. Связи могут быть логические, семантические, причинно-следственные и т. п. На экране для примера взяты два документа – ГОСТ Р 51275-2006 «Перечень объективных и субъективных факторов, воздействующих на безопасность защищаемой информации объекта информатизации» и Приказ ФСТЭК №31 «Состав мер защиты информации и их базовые наборы для соответствующего класса защищённости автоматизированной системы управления». Каждому фактору мы можем поставить

Десять основных угроз для промышленных систем автоматизации и управления

№	Угроза	Примечание
1	Несанкционированное использование точек доступа дистанционного технического обслуживания	Точки доступа для технического обслуживания – специально созданные внешние входы в сеть ICS*, которые часто бывают недостаточно безопасными.
2	Сетевые атаки через корпоративную сеть	В большинстве случаев также существуют сетевые связи между офисами и сетью ICS, которые нарушители также могут использовать для получения доступа к сети.
3	Атаки на стандартные компоненты, используемые в сети ICS	Стандартные компоненты ИТ (готовые коммерческие продукты), такие как системное программное обеспечение, сервер приложений или баз данных, часто содержат недостатки и уязвимости, которыми могут воспользоваться нарушители. Если эти стандартные компоненты также используются в сети ICS, то риск успешной атаки на сеть ICS повышается.
4	(D)DoS-атаки	(Распределённая) атака типа «отказ в обслуживании» может негативно сказаться на работе сетевых соединений и важнейших ресурсов, а также вызвать сбой систем, например для того, чтобы прервать работу ICS.
5	Человеческая ошибка и саботаж	Преднамеренные действия – как со стороны внутренних, так и внешних нарушителей – представляют собой массовую угрозу для всех защищаемых объектов. Большую угрозу также представляют халатность и человеческая ошибка, особенно в отношении защиты конфиденциальности и доступности объектов.
6	Проникновение вируса через съёмный носитель и внешние устройства	Использование съёмных носителей и мобильных ИТ-компонентов персоналом всегда связано с высоким риском заражения вирусом.
7	Чтение и запись данных в сети ICS	Большинство компонентов контроля в настоящее время использует протоколы без использования шифрования, таким образом, коммуникации остаются незащищёнными. Это упрощает чтение и ввод команд управления.
8	Несанкционированный доступ к ресурсам	Внутренним нарушителям и нападающим, чьи атаки следуют за первоначальным внешним проникновением, особенно просто добиться успеха, если сервисы и компоненты в сетевой схеме процесса не используют методы аутентификации и авторизации или если эти методы ненадёжны.
9	Атаки на компоненты сети	Нападающие могут манипулировать компонентами сети, чтобы провести атаку с применением технологии «незаконный посредник» или, например, упростить анализ трафика.
10	Технические сбои или форс-мажор	Сбои в результате экстремальных погодных условий или технических неполадок могут произойти в любое время – в таких случаях можно только минимизировать риск и потенциальный ущерб.

** Промышленные системы автоматизации и управления. Также часто используется аббревиатура IACS – Industrial Automation & Control Systems*

в соответствие одну или несколько мер защиты. Количество сущностей может быть и больше, «держать в голове» и ничего не пропустить без использования вспомогательных средств, в случае множественных связей, нереально даже в случае большого опыта и знаний в предметной области. Также средствами информационно-аналитической системы решается задача организации работы и консолидации оценок экспертов из разных предметных областей. Каждый эксперт отвечает за нахождение существенных связей между наборами сущностей в своей области знаний. Следующим шагом за установлением связей является «привязка узлов» к другим сущностям. Например, привязка к задачам и событиям даёт нам план мероприятий, к описаниям – связный структурированный документ и т. п.

Другой интересный опыт с целью упростить моделирование – это попытка создать специализированный язык – Cyber Security Modeling Language (CySeMoL) – предпринятая в «KTH Royal Institute of Technology» в Швеции [11]. Язык позволяет формально описать 59 видов атак, 58 типов защиты для 23-х разновидностей активов и установить отношения между этими сущностями. По замыслу авторов, CySeMoL позволяет пользователю, не обладающему специальными знаниями в области кибербезопасности, моделировать информационные системы масштаба предприятия и анализировать их уязвимость.

Мероприятия по обеспечению кибербезопасности

Мы рассмотрели темы рисков, уязвимостей, злоумышленников и угроз. Перейдём к обсуждению способов планирования, осуществления и контроля контрмер, направленных на защиту. Применим тот же самый приём – декомпозируем задачу на составляющие. Это позволит нам перейти от глобальной

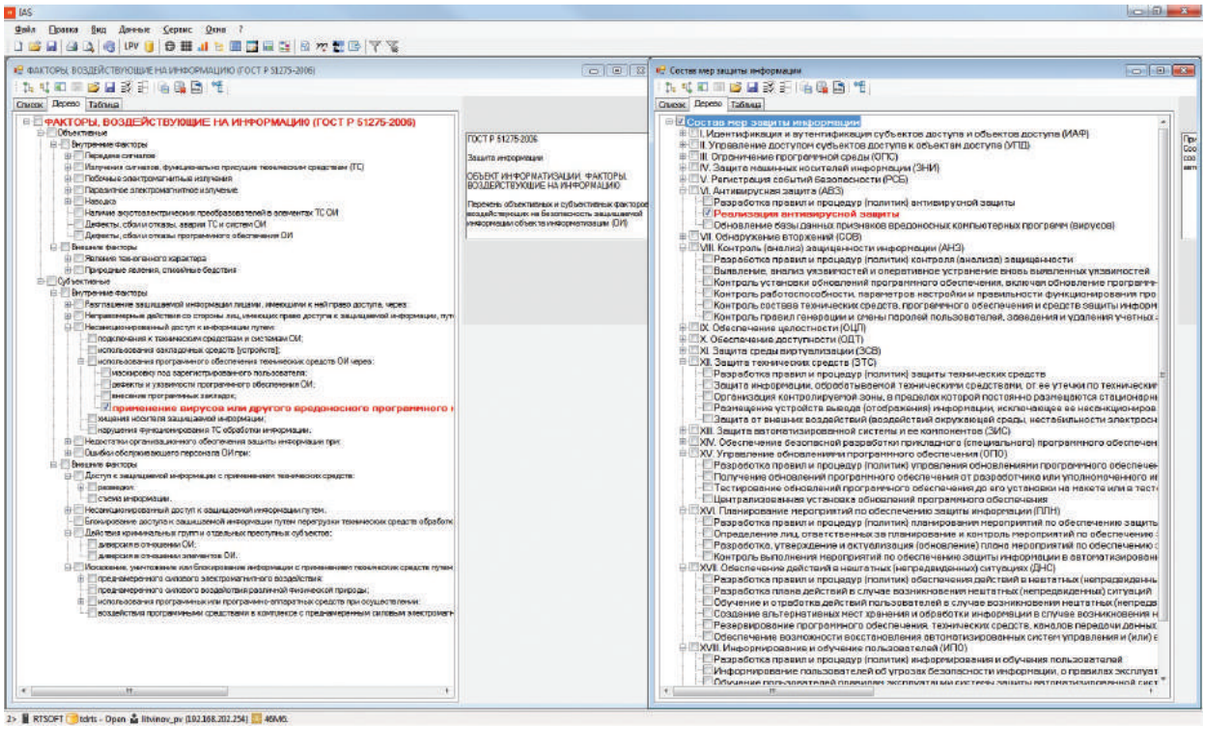


Рис. 7. Интерфейс информационно–аналитической системы разработки «РТСофт»

модели к суперпозиции локальных моделей. На первых шагах можно пренебречь связями, затем учесть только самые существенные из них и так постепенно увеличивать сложность. Такое приближение и последовательность действий вполне допустимы при выборе «ортотональных» друг другу доменов, что минимизирует взаимовлияние. Хороший вариант можно найти в [12]:

– системное администрирование (SA);
– сетевая безопасность (NS);
– безопасность приложений (AS);
– безопасность рабочих станций, серверов и устройств (ESDS);
– идентификация, аутентификация и управление доступом (IAAM);
– защита данных и криптография (DPC);
– мониторинг, управление исправлениями (MVPM);
– аварийное восстановление и физическая защита (HADRPP);
– реагирование на инциденты (IR);
– управление активами и управление цепочками поставок (AMSC);
– политики безопасности, аудит и обучение персонала (PAET).

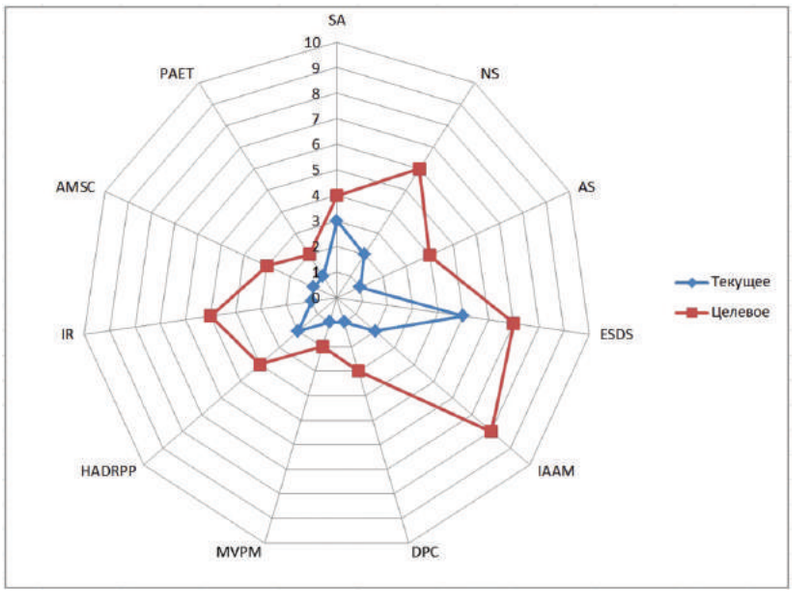


Рис. 8. Пример представления текущего и целевого состояния мер по обеспечению киберзащиты

Как уже рассматривалось в разделе «Метрики информационной безопасности», радарная диаграмма является наглядным способом визуализации (рис. 8). Для примера возьмём экспертные оценки в баллах, нанесём значения на соответствующие оси, применим формулу (1) и получим соответственно метрики 7,2 и 15,7 (после приведения к единице – 0,22 и 0,47).

Вы можете использовать собственное разделение или адаптировать из существующих стандартов, как правило, содержащих такое де-

ление. В зависимости от выбранного стандарта количество доменов может колебаться от десяти (Department of Homeland Security Cyber Resilience Review – DHS CRR) до тридцати пяти (Australian Defense Signals Directorate (DSD) Strategies)!

Если бы автору разрешили дать только один совет, на тему, как оптимизировать построение моделей, ответ был бы: «Меньше изобретайте сами, больше полагайтесь на стандарты!». Для каждого случая можно найти рекомендации, выбрать из них наиболее подходящие и на их основе начинать моделирование. В качестве примера рассмотрим подробнее порядок действий, выбрав раздел, где находится «управление исправлениями». Подходящим стандартом будет IEC TR 62443-2-3 «Patch management in the IACS environment» [13]. В нём содержится блок-схема алгоритма применения «заплаток безопасности», выпущенных производителями (рис. 9). Изучив схему, можно однозначно выбрать оптимальную методологию – дискретно-событийное моделирование. Также становятся очевидными направления прогнозирования и оптими-

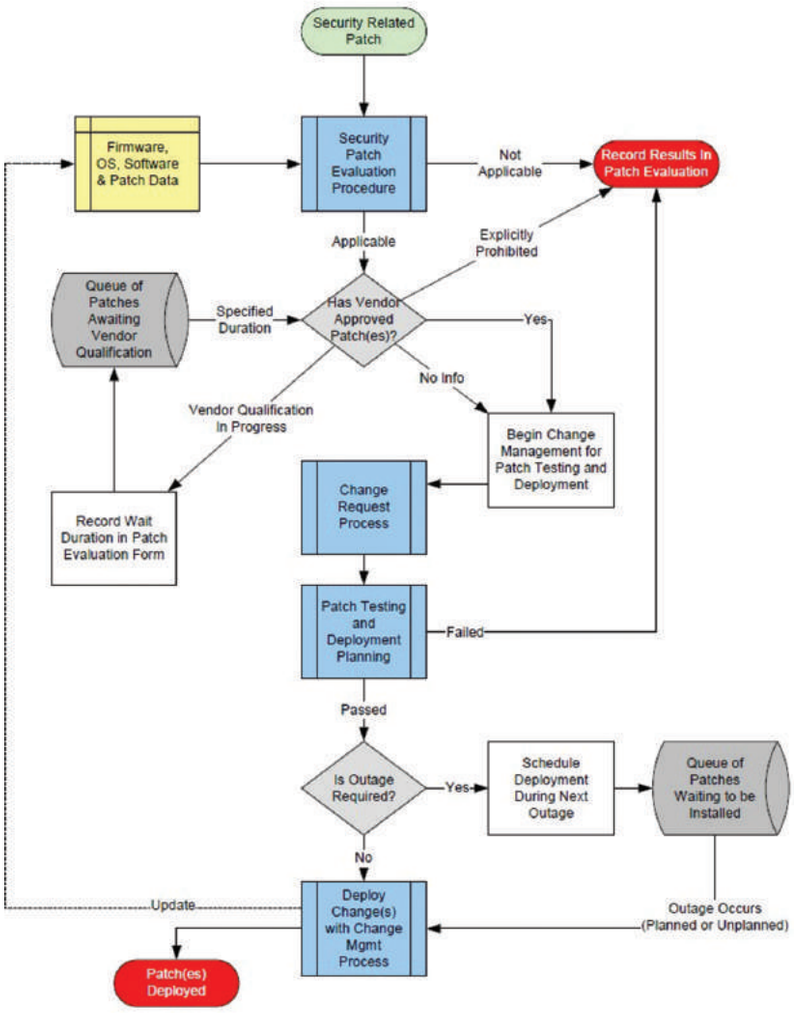


Рис. 9. Patch management (Блок–схема в упомянутой версии стандарта может немного отличаться, автор использовал Draft 1 Edit 4, опубликованный в 2012 г.)

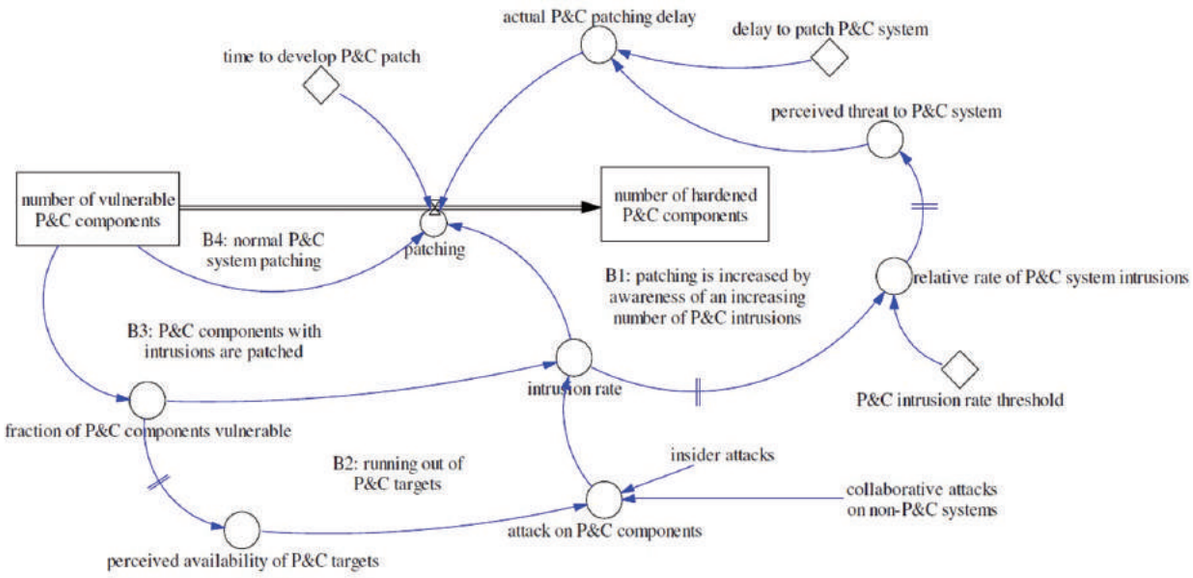


Рис. 10. Модель системной динамики для применения исправлений

зации – предполагаемое время ожидания, в течение которого система будет оставаться уязвимой, и порядок и момент наложения исправлений в случае необходимости остановки технологического процесса (нижняя часть схемы). Потенциально оптимизация времени наложения исправлений безопасности может дать значительный экономический эффект при обоснованном выборе альтернатив:

– ждать до следующего планового отключения для вывода в ремонт или технического обслуживания;
– инициировать немедленное обновление и мириться с потерями;
– изменить график ТОиР, если потери от простоя значительные, но нельзя откладывать обновление из-за высоких рисков.

В случае большого парка оборудования и потока работ по обновлению ПО и прошивок контроллеров, если нас интересует моделирование на большой промежуток времени с целью принятия стратегических решений, лучше использовать моделирование методом системной динамики. За отправную точку при составлении системы дифференциальных уравнений можно взять схему, опубликованную в материалах CIGRE [14] (рис. 10).

Заключение

На частый вопрос заказчиков, в какой мере можно доверять результатам моделирования, можно ответить так. Сам процесс моделирования уже полезен, поскольку он подталкивает мыслить широко и объёмно и помогает нам формализовать знания и опыт инженеров и экспертов. В пользу моделирования свидетельствует также и такой простой факт, что при принятии решения мы доверяем своей интуиции и опыту. В теме кибербезопасности опыта у всех ещё мало, что касается «интуиции», это не более чем простые модели, которые строит наш мозг. Из психологии известно, что человеческому мозгу сложно построить интерполяции-экстраполяции и регрессии, отличные от линейных, и отслеживать взаимовлияние более чем пяти факторов. При этом процессы, зависимые от времени, обычно описываются системами дифференциальных уравнений, и форма и поведение результирующей оптимизационной кривой могут быть совершенно неожиданными.

У каждой методологии есть свои ограничения и область наиболее эффективного применения. Построить модель, которая «сама» предложит способы оптимизации, практически невозможно. Другое дело, когда есть конкретная задача и идеи по её решению. Тогда, с помощью моделирования, реально выполнить оценку последствий, сроков, стоимости, вероятности успешной реализации для каждого сценария, выбрать лучший вариант и оптимизировать план его реализации. Обсуждение и примеры моделирования различных сценариев оптимизации – это тема отдельной статьи.

Список литературы

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

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

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

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

5. 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

6. 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., Т. Vol:7, No:8

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

8. Jaquith, Andrew. Security metrics : replacing fear, uncertainty, and doubt. б.м. : Pearson Education, Inc., 2007. ISBN 0-32-134998-9

9. Федюнина, А. П. Выявление характерологических признаков и составление психологического портрета возможного нарушителя и лояльного сотрудника в сфере информационной безопасности. Вестник АГТУ. 2006 г., Т. 4, 39

10. SiFo-Studie 2009/10. Know-how-Schutz in Baden-Württemberg. Steinbeis-Edition Stuttgart, 2010 г.

11. 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

12. Scott Donaldson, Stan Siegel, Chris Williams, Abdul Aslam. Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats. б.м. : Apress, 2015

13. IEC TR 62443-2-3. Security for industrial automation and control systems – Part 2-3: Patch management in the IACS environment. Edition 1.0 2015-06

14. Application and Management of Cybersecurity Measures for Protection and Control Systems. CIGRE, Joint Working Group B5/D2.46. 2014

Павел Литвинов, Сергей Нестеров, ЗАО «РТСофт»

«РТСофт» на конференции PTC LiveWorx Europe 2015

С 17 по 18 ноября в выставочном центре ICS Messe г. Штутгарт, Германия, прошла выставка и конференция PTC LiveWorx Europe 2015. Своими впечатлениями об этом мероприятии, информацией о трендах развития систем автоматизированного проектирования и управления производством, новых возможностях Индустриального интернета вещей с Редакцией журнала «МКА» поделились начальник аналитического отдела компании «РТСофт» Павел Васильевич Литвинов и руководитель проектного офиса Сергей Андреевич Нестеров.

Редакция: *Чем вызван интерес к не профильной для нашей компании выставке?*

Павел Литвинов: Ещё несколько лет назад такое утверждение было бы справедливым. Работа конференции была разделена на 8 сессий, которые логически можно объединить в три группы: системы автоматизации проектных работ и управления жизненными циклами (CAD, PLM, ALM, SLM); «Интернет вещей» (IoT, IIoT) и развитие бизнеса. Все эти темы сегодня имеют непосредственное отношение к инновационным технологиям «РТСофт»: развитию направления IoT и Industry 4.0 и Инженерного центра разработки электронной аппаратуры.

Р.: *Сегодня, кажется, нет недостатка информации в сети Интернет и литературе.*

П.Л.: Вы совершенно правы, информации много, её даже слишком много! Увы, количество не переходит в качество. Особенностью информации в сети является её, как бы это мягко сформулировать, «разное качество и время подготовки». Концепция «Интернета вещей» развивается настолько стремительно, что многие представления начала 2015 года уже перестали быть актуальными. Что касается книг, которых издаётся достаточно, по вполне понятным причинам они тоже отстают, даже если не дожидаться переводных изданий. Международная конференция – это шанс получить всё самое свежее из первых рук. Вы можете быть совершенно уверены, что находитесь на переднем крае, а в обсуждениях и дискуссиях появляется возможность не только заглянуть в будущее, но и проектировать и строить его вместе с коллегами.

Р.: *Действительно так масштабно?*

П.Л.: Более 2500 участников конференции, 55 компаний из ключевых отраслей и 104 доклада прозвучало за два дня работы.

Р.: *Как можно было успеть всё посетить и прослушать?*

С.Н.: Доклады, за исключением пленарных заседаний, проходили по тематическим секциям до десяти одновременно. «Центром тяжести» наших интересов была тема IoT и развитие связанных бизнесов. От «РТСофт» было три участника. Разделяясь по сессиям,

затем обмениваясь впечатлениями, нам удалось обеспечить полный охват темы.

Р.: *Почему именно «Интернет вещей», спрашивать даже не буду. Какие же новые тренды мы могли бы представить нашим читателям?*

С.Н.: Достаточно широко, в том числе и в нашем журнале, освещалось то, что развитие «Интернета вещей» поддерживается стеком новых технологий: большие данные, искусственный интеллект, облачные сервисы. Теперь к ним мы можем смело добавить ещё одну – дополненная реальность (Augmented reality, *AR)*. Её ещё иногда называют расширенной реальностью. Современные технологии позволяют в реальном времени совместить трёхмерное изображение или модель физических объектов и виртуальных.

Р.: *Все видели рекламу программ, которые помогают подбирать мебель, виртуально расставляя её по комнате. Но какое это отношение имеет к IoT и индустриальному производству?*

С.Н.: Действительно, первые применения дополненной реальности были в индустрии игр и развлечений, затем в ритейле. Представим себе другую ситуацию. Мастер подходит к оборудованию, требующему диагностики и, возможно, ремонта, наводит на него камеру своего телефона или планшета и на изображение узла накладываются выноски, содержащие информацию о его текущих параметрах, в реальном времени получаемых с сенсоров. Тут же из облака можно запросить историю измерений, например как менялась вибрация или его температура в течение последней смены или месяца. В зависимости от полученных данных, аналитическое приложение даёт рекомендацию, например, по замене фильтра. На экране появляются инструкции по последовательности вывода агрегата из работы, в облако тут же передаётся и доставляется всем заинтересованным сторонам информация о начале выполнения регламентных работ, необходимости добавить в заказ на следующий месяц детали, которые будут установлены, и т. д.

Р.: *Фантастика! Но это требует колоссальной подготовительной работы, окупится ли это?*

П.Л.: Вот здесь мы подошли к пониманию концепции компании PTC, которая поставляет весь спектр продукции по проектированию и управлению производством, и теперь добавила в свой портфель платформу для реализации решений IoT. Да, окупится и принесёт максимальную выгоду только в том случае, если весь цикл от проектирования до постановки на производство будет целостным и непрерывным. Вернёмся к нашему примеру. Перед заменой любого узла на планшете обслуживающего персонала появляется его трёхмерная модель с указанием порядка выполнения операций по разборке и сборке. Создание этой модели и поддержание её в актуальном состоянии действительно большой труд. Но если проектирование выполнялось с использованием САПР, то уже на этом этапе была создана модель, датчики для измерения необходимых параметров были заранее предусмотрены, а аналитика по обработке информации с сенсоров была предварительно настроена на этапе компьютерного моделирования расчётов прочности, надёжности и т. п.

Р.: *А производство?*

П.Л.: Мы уже говорили, что полный жизненный цикл изделия – от возникновения потребности до утилизации – станет интегрированным. Информационный обмен между стадиями будет быстрым и двунаправленным, обратные связи будут возникать на каждом этапе, позволяя быстро исправлять ошибки, добиваясь технического и потребительского совершенства изделия. Простой пример: уже сейчас на этапе проектирования методы имитационного моделирования позволяют с высокой вероятностью рассчитать и оптимизировать детали и узлы. Эти расчёты, по сути, проверяются один раз во время испытаний, и перед запуском в серию вносятся коррективы и исправления. Но никакие испытания не способны полностью достоверно воспроизвести результаты эксплуатации тысяч изделий в различных условиях. Опираясь на технологии IoT, мы получаем возможность непрерывно собирать информацию с реальных устройств, агрегатов, станков или машин и вносить необходимые коррективы уже в следующий (а то и текущий!) производствен-

ный цикл. При этом обновлённая эксплуатационная документация будет повсеместно доступна уже при следующем цикле обслуживания. Такие устройства и системы принято называть киберфизическими (CPS). Для нас подобное непрерывное совершенствование уже стало привычным, когда речь идёт о разработке программного обеспечения.

Р.: *Подобные технологии производства и обслуживания уже используются, есть примеры?*

С.Н.: В обслуживании одним из самых масштабных внедрений можно считать технологии компании Schindler, которые перемещают на лифтах и эскалаторах собственного производства до 1 млрд человек в день по всему миру. В производстве – конечно, компания General Electric, начавшая реализацию концепций Brilliant Manufacturing и Smart Manufacturing.

Р.: *Как изменится промышленность с внедрением таких технологий?*

П.Л.: В двух словах очень трудно изложить, как изменится технология производства, насколько масштабные и интересные будут последствия новой индустриальной революции. Перспективы проще и нагляднее раскрывать со стороны потребителя и бизнеса. Новые бизнес-модели появляются как результат развития технологий и открывают широкий спектр получения прямых и косвенных доходов для предпринимателей. Например, массовая кастомизация. В ближайшем будущем появится возможность создавать индивидуальные продукты для каждого клиента, исходя из его требований и даже предпочтений. Слишком дорогое для традиционного товарного производства решение становится возможным и рентабельным. Автоматизированный распределённый и самонастраиваемый цикл позволит свести к нулю необходимость иметь товарные складские запасы: многие товары будут запускаться в производство только после того, как вы сделаете заказ в интернет-магазине, в точном соответствии с параметрами этого заказа. При этом количество опций для каждого изделия начнёт стремиться к бесконечности.

Р.: *Можно ли назвать Индустрию 4.0 революцией без потерь? Не приведёт ли исключение человека из участия во многих процессах к росту безработицы или рискам, если, например, хакеры взломают фабрику?*

С.Н.: Точнее было бы говорить не о революции, а об эволюции технологий: облачных (cloud), искусственного интеллекта (IA, RTI), больших данных (Big Data), «Интернета вещей» (IoT) и прогрессе в развитии микропроцессоров в части снижения размеров, стоимости и энергопотребления и т. д., которые в своём развитии сделали технически возможным и экономически целесообразным создать «Умное предприятие».

П.Л.: Хорошо известно, что у каждой медали есть оборотная сторона, но процесс запущен и его уже не остановить. Можем ли мы себе представить отказ от использования мобильных телефонов или сети Интернет? Тот вред, который они могут нанести, компенсируется развитием новых технологий и решений по защите. Очевидно, что в промышленности использование беспроводных технологий увеличивает уязвимость. Конечно, различные производители уже готовы предложить решения по обеспечению кибербезопасности, но их эффективность сильно зависит от ресурса атакующего и его мотивации. В случае значительного ресурса и высокой мотивации – гарантированной защиты пока не существует, какие-то риски мы можем компенсировать, некоторые, увы, надо принять. Что касается роста безработицы, эти опасения возникают при каждой промышленной революции (вспомним луддитов). И каждый раз в долгосрочной перспективе оказываются беспочвенными – меняется структура занятости, список престижных и востребованных профессий и т. п.

Р.: *Сколько времени займёт процесс перевода производства на новые рельсы в мире и России?*

П.Л.: В Германии этот процесс стартовал два года назад и уже есть первые успешные примеры и результаты. Все промышленно развитые страны будут вынуждены включиться в эту гонку, поскольку «новое» производство будет выигрывать в конкурентной борьбе у «старого». Раз мы поднимаем и обсуждаем эту тему сегодня, а не два года назад, то можно предположить, что Россия сейчас имеет небольшое отставание, но ничто не мешает его сократить.

Р.: *Были ли деловые результаты поездки, помимо лучшей информированности?*

П.Л.: Разумеется, но это, как говорится, тема для отдельной статьи и интервью. Раскрою только в самых общих чертах – лаборатория IoT компании «РТСофт» в следующем году перейдёт на новый этап своего развития, это действительно будет качественно новый уровень возможностей и темпа перехода от идей и бизнес-кейсов к работающим прототипам, готовым для демонстрации потенциальным заказчикам.

Р.: *Спасибо! Интересно!*

Анна Шихина, ЗАО «РТСофт»

Основные тенденции развития Smart City

В настоящее время всё большую известность приобретает концепция «Умных городов» (Smart City), которая направлена на решение проблем, связанных с перенаселённостью городов, изменением климата, необходимостью рационального использования ресурсов, предоставления и потребления жизненно необходимых услуг. В данной статье даётся обзор существующих сегодня основных программ создания Smart City и краткое описание основных используемых технологий.

Введение

Ожидается, что к 2050 году в городах будет проживать как минимум 75 % всего населения, хотя в настоящее время эта доля составляет около половины населения Земли, а в 1910 г. в городах проживало только 10% от всего населения планеты [1]. Такое изменение, по мнению ведущих мировых исследовательских институтов [2], может привести к глобальным проблемам перенаселённости городов, изменению климата, природным бедствиям и т. д. Населённость городов становится плотнее, а соответственно встаёт вопрос о более эффективном (рациональном) использовании природных ресурсов (воды, газа, тепловой и электрической энергии), предоставления и потребления жизненно неоходимых услуг. Другая задача, которую необходимо решать, – это обеспечение устойчивого развития инфраструктуры городов [3], адекватной происходящим изменениям. Третья задача – это создание городов, способных легко адаптироваться к изменяющимся условиям. В этом смысле широко известная концепция «Умных городов» (Smart City) – это ответ на перечисленные выше вызовы и в общем случае включает три составляющие: эффективность (Efficiency), устойчивость (Sustainable Cities) и адаптивность (Resilient Cities). Оптимальные решения по повышению эффективности, устойчивости и адаптивности городов, основанные на новых экономических моделях и новых технологиях, могут закладываться на этапе строительства новых городов или районов, а также применяться в уже существующих городах. В настоящей статье приведён обзор основных текущих программ создания «Smart City» и краткое описание основных используемых технологий.

Обзор текущих проектов «Smart City»

Чтобы определить модель идеально «города будущего», в настоящее время по всему миру реализуется огромное количество экспериментальных проектов по созданию Smart City. В основе каждого из них лежат различные концепции, которые сильно зависят от страны, окружающей среды и проблем, стоящих перед каждым конкретным городом, например проблем нехватки энергетических ресурсов или тяжелой ситуации с дорожным движением. Главная задача при выборе, какую концепцию, в каком городе реализовывать, – это изучение образа жизни горожан, которые в итоге и будут определять модель «Smart City».

«Smart City» в Европе

Для борьбы с пробками, загрязнением воздуха, высокими ценами на энергоресурсы, для улучшения мобильности, заботы об окружающей среде и повышения энергетической эффективности европейских городов в 2011 г. было специально создано Европейское инновационное партнёрство «Smart Cities & Communities» [4]. Основная задача данного партнёрства – объединить усилия городских администраций, промышленности и жителей для улучшения городской жизни за счёт применения инновационных решений, более точного планирования, более комплексного подхода, применения интеллектуальных информационно-коммуникационных технологий (ИКТ), в первую очередь в секторах «энергетика» и «транспорт». Основные области, в которых работает партнёрство «Smart Cities & Communities» приведены на рис. 1 в виде следую-

щих компонентов: городская мобильность (Urban Mobility), технологии развития концепции «открытых данных» (Open Data), бизнес-модели (Business Models), финансы и закупки (Finance & Procurement), законодательное регулирование (Policy & Regulation), расчёт и анализ показателей производительности, интеграция электрических (Integrated Energy Networks), транспортных и коммуникационных сетей, повышение энергетической эффективности (Energy Efficiency), удельное снижение потребления углеводородов (Low Carbon Solutions). В настоящее время партнёрство «Smart Cities & Communities» курирует 26 проектов. Города сгруппированы в проекты, исходя из общих характеристик, полученных при анализе характера потребления и производства энергии, установленных целевых показателей сокращения выбросов углеродов и снижения потребления ресурсов. Краткая информация о некоторых реализуемых в настоящее время проектах «Smart City» приведена в таблице [5].

Еще одна европейская программа – «Sustainable Cities» [6] также направлена на создание «Smart City» и охватывает следующие направления:

- «Мониторинг и оценка» – проект разработки стратегий устойчивого развития городов, оказания реального влияния на законодательство и распределение бюджетных средств для достижения плановых показателей, а также внедрения инструментов мониторинга ключевых показателей, отражающих устойчивость развития городов и степени достижения поставленных целей;
- «Климат и энергетика» – проект сокращения выбросов парниковых газов, экономии энергии и увеличения доли использования возобновляемых источников энергии;
- «Управление и участие» – проект развития взаимодействия муниципальных органов власти с научно-исследовательскими центрами и населением;
- «Адаптация и устойчивость» – проект адаптации городской жизни к изменениям климата;
- «Интегрированное управление» – проект интеграции всех данных, мнений, опыта, стратегий развития всех секторов экономики и промышленности в единую систему управления;
- «Биоразнообразие и экосистемные услуги»;
- «Городское планирование» – проект, объединяющий мобильность, землепользование, энергетику и др. с целью планирования устойчивого развития городской инфраструктуры;
- «Транспорт и мобильность» – проект развития мобильности, широкого распространения безмоторных транспортных средств, улучшения работы общественного транспорта, изучения возможности использования нетрадиционных видов личного транспорта;
- «Бесперебойное снабжение» – проект развития рационального и эффективного использования ресурсов и внедрения системы поощрения бесперебойного потребления и производства;
- «Экологически-ориентированная экономика»;
- «Здоровье»;
- «Социальная интеграция» – проект преодоления социальной и экономической изоляции, характерной для отдельных районов многих европейских городов.

Рис. 1. Партнёрство «Smart Cities & Communities»

Краткая информация о реализованных проектах «Smart City»

Наименование проекта	Краткое описание проекта	Города (страны)
«STEEP» – системное мышление для комплексного планирования	Задачи проекта: 1) модернизация систем водоснабжения; 2) снижение потребления воды; 3) управление отходами; 4) развитие тригенерации и распределённой генерации; 5) управление генерацией, распределением и сбытом энергии внутри городов; 6) создание районов с потреблением энергии, близким к нулю; 7) развитие системных услуг; 8) электрификация транспорта; 9) создание интеллектуальной транспортной инфраструктуры.	Доностия-Сан-Себастьян (Испания), Бристоль (Великобритания), Флоренция (Италия)
«SOLUTION» – проект создания в Европе энергетически самодостаточных территорий	Данный проект направлен на удовлетворение потребностей повышения энергоэффективности с помощью применения новых технических и технологических решений в области энергетики и интегрированных между собой в пределах одной территории с помощью интеллектуального моделирования. Задачи проекта: 1) анализ последних результатов исследований по использованию накопителей электроэнергии, характера энергопотребления и интеллектуального управления возобновляемыми источниками электроэнергии; 2) тестирование различных решений в области энергетики в целях достижения самодостаточности района; 3) создание бизнес-среды, комфортной для внедрения подобных решений; 4) разработка типового решения и его распространение.	Австрия, Хорватия, Финляндия, Швейцария, Словения
«READY» – комплексный проект создания «Умных городов» на базе «Умных домов»	Цель проекта: выработка сбалансированного и целостного подхода к переоборудованию домов и офисов. Задачи проекта: 1) разработка инновационных систем низкотемпературного теплоснабжения; 2) разработка сбалансированной системы использования накопителей электроэнергии и возобновляемых источников электроэнергии, в т.ч. для обогрева, охлаждения зданий и для заряда электромобилей; 3) повышение эффективности использования воды, использования тепловой энергии сточных вод; 4) урегулирование спроса и предложения на ресурсы с помощью точного прогнозирования потребления.	Векшё, Орхус (Швеция)
«PITAGORAS» – проект планирования устойчивого развития городов с использованием возобновляемых источников энергии	Задачи проекта: 1) добиться высокой производительности, низкой стоимости и высокой энергоэффективности использования возобновляемых источников энергии; 2) добиться устойчивого развитие городских районов со слабой степенью теплоснабжения; 3) использовать избыточную для территорий технопарков энергию для снабжения жилых районов.	Грац (Австрия), Брешия (Италия)
«PIME'S» – проект оптимального теплоснабжения и электроснабжения зданий и районов	Задачи проекта: 1) широкое распространение распределённой генерации (в т.ч. возобновляемых источников энергии), накопителей энергии; 2) внедрение интеллектуальной системы управления распределённой генерацией; 3) внедрение бизнес-модели реализации проектов через энергосервисные контракты и бизнес-модели повышения ответственности жителей за достижение показателей энергоэффективности.	Витория (Испания), Стендре (Венгрия), Саннес (Норвегия)

«Smart City» в Японии

В Японии «Smart City» рассматривается прежде всего как новый стиль жизни города, его устойчивого развития, поощрение производства, не причиняющего вред окружающей среде [7]. За основной показатель эффективности «Smart City» при этом принято значение показателя QoL (Quality of Life) – «качество жизни». Ключевым событием, толкнувшим Японию на создание «Smart City», послужила трагедия – Великое Восточно-Японское Землетрясение, случившееся 11 марта 2011 г., и последующая за ним авария на АЭС.

Урбанизация Японии – огромная проблема для всей страны на данный момент. Сельскохозяйственные земли передаются под городскую застройку также быстро, как быстро развивается сама нация. Создание социальной инфраструктуры, обеспечение ресурсами (вода, тепловая и электрическая энергия),

строительство зданий, создание транспортной инфраструктуры, коммуникаций, доступных административных сервисов – необходимые факторы существования жителей и развития бизнеса. Всё это должно создаваться в очень короткие сроки, использоваться в течение длительного периода и иметь задел для дальнейшего развития.

В тоже время имеющаяся инфраструктура в таких быстроразвивающихся странах, как Япония, стареет слишком быстро, перестаёт отвечать требованиям современного образа жизни и становится непригодной для использования, требует полной замены.

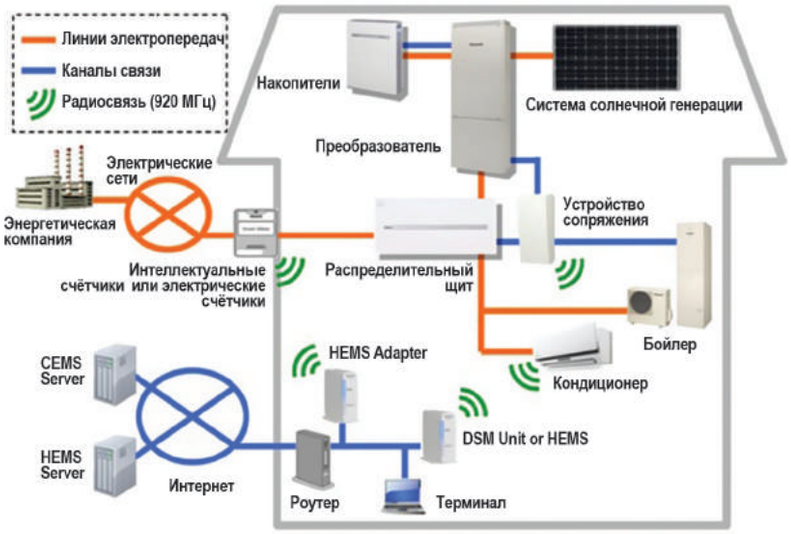


Рис. 2. Интеграция систем CEMS и HEMS на примере решений Panasonic

Ещё одно важное условие, влияющее на значение показателя QoL, – сокращение выбросов CO2, и одна из основных причин создания «Smart City» именно в этом – в стремлении максимально перевести генерацию энергии на возобновляемые источники (солнечная и ветровая генерация). Однако при использовании возобновляемых источников энергии передача и распределение электроэнергии может значительно эффективнее осуществляться по интеллектуальным сетям («Smart Grid»). Именно интеллектуальные сети могут обеспечить стабильное, гибкое и надёжное электроснабжение.

Для того чтобы добиться более эффективного использования энергии, не стоит фокусироваться только на энергетических системах, а требуется комплексный подход, включая пересмотр функционирования большинства общегородских систем, например процессов использования тепловой энергии, системы организации транспорта и др.

Комплексность подхода к созданию «Smart City» требует также внедрения инновационных информационно-технологических систем, способных работать с огромными массивами данных.

Создание «Smart City» – это не только изменение облика городских территорий, это стремление внедрить инновации в образ жизни самих горожан. Многие из этих инноваций были немыслимы ещё 10 лет назад. Например, широкое использование электромобилей с возможностью их повсеместной зарядки, а в случае чрезвычайных ситуаций использование заряда аккумулятора электромобилей для обеспечения временного электроснабжения. Этот пример также наглядно демонстрирует тот факт, что создание интеллектуальных сетей «Smart Grid» и проблему создания «Smart City» следует рассматривать как взаимосвязанные задачи.

Поэтому не случайно Министерство экономического развития Японии совместно с Министерством торговли и промышленности выбрали четыре города для разработки и тестирования систем и технологий «Smart Grid» и «Smart City»:

- Йокогама (the City of Yokohama) – «The Yokohama Smart City Project»;
- Тойота-сити (Toyota City) – «Toyota City Low-carbon Society Verification Project (Smart Melit»);
- наукоград Кайхана в Префектуре Киото (Keihanna Science City) – «Keihanna Eco City the Next-Generation Energy and Social Systems»;
- Китакюсю (the City of Kitakyushu) – «Kitakyushu Smart Community Project».

Поставленная задача – предложить оптимальную модель развития интеллектуальных сетей («Smart Grid») и «умных городов» («Smart City»), в том числе разработать бизнес-модели и определить механизмы стимулирования внедрения инновационных технологий. В связи с тем, что Япония – один из лидеров на рынке интеллектуальных решений для энергетики и энергосберегающих технологий, среди задач данных проектов есть и разработка международных стандартов «Smart City», в том числе стандартов передачи информации.

Для начала работ по проектам в первую очередь требовалось добиться визуализации точного потребления энергоресурсов, вплоть до контроля потребления каждым домашним устройством. Далее необходимо было отрегулировать взаимосвязанные процессы потребления и процессы поставки энергоресурсов. Следующий этап состоял в монтаже домовых зарядных устройств для электромобилей и про-

ектировании оптимальных систем аккумулирования энергии.

Все системы и технологии были объединены на уровне общей системы энергоменеджмента (CEMS – Community Energy Management System). Внедрение этой системы способствовало широкому использованию возобновляемых источников энергии и других элементов «Smart City» без каких-то серьёзных усилий со стороны администраций. CEMS интегрирована с домашними системами энергоменеджмента (HEMS – Home Energy Management System). Пример интеграции систем CEMS и HEMS приведён на рис. 2.

HEMS может включать два варианта реализации подсистем управления спросом: DSM или ADR. Подсистема управления спросом DSM (Demand-side Management), которая позволяет достичь оптимального использования фотоэлектроэнергии (PV– Photovoltaic Power) и уменьшения объёмов покупаемой электроэнергии. Подсистема DSM управляет накопителями электроэнергии и системами солнечной генерации в автоматизированном режиме и позволяет контролировать потребление электроэнергии всеми системами и приборами (рис. 3).

Рис. 3. Пользовательский интерфейс системы HEMS (Panasonic)

Подсистема автоматического управления спросом ADR (Automatic Control Demand Response) автоматически управляет домашним электроснабжением. ADR осуществляет автоматическое управление накопителями электроэнергии на основании прогнозных объёмов выработки электроэнергии, которые, в свою очередь, строятся на основании прогноза погоды и прогноза потребления (построенных на исторических данных за заданный период). Также имеются решения для управления комбинированным использованием дизельных генераторов и накопителей электроэнергии, заряжаемых от возобновляемых источников энергии.

Достигаемый эффект от «умного» управления системами солнечной генерации и накопителями электроэнергии приведён на рис. 4. На рисунке приведены график потребления электроэнергии (синяя линия) и график генерации электроэнергии солнечными фотоэлементами (красная линия). Слева показан случай обычного использования солнечной генерации и накопителей электроэнергии, позволяющий снизить приобретаемую из внешней сети электроэнергию в дневные часы (за счёт генерируемой электроэнергии) и в вечерние часы (за счёт используемой накопленной электроэнергии). Справа показан случай, когда избыток выработанной солнечной электроэнергии отдаётся в сеть. При этом видно, что и отдача в сеть, и потребление накопленной электроэнергии происходит в пиковые часы.

Ещё одна система, с которой интегрируется CEMS, это система «Автомобиль к дому» (V2H – Vehicle to Home). Система V2H разработана таким образом, чтобы заряжать аккумулятор электромобилей от домашних систем солнечной генерации, а при необходимости включать электроснабжение дома от аккумулятора электромобиля. V2H имеет встроенную систему управления зарядной

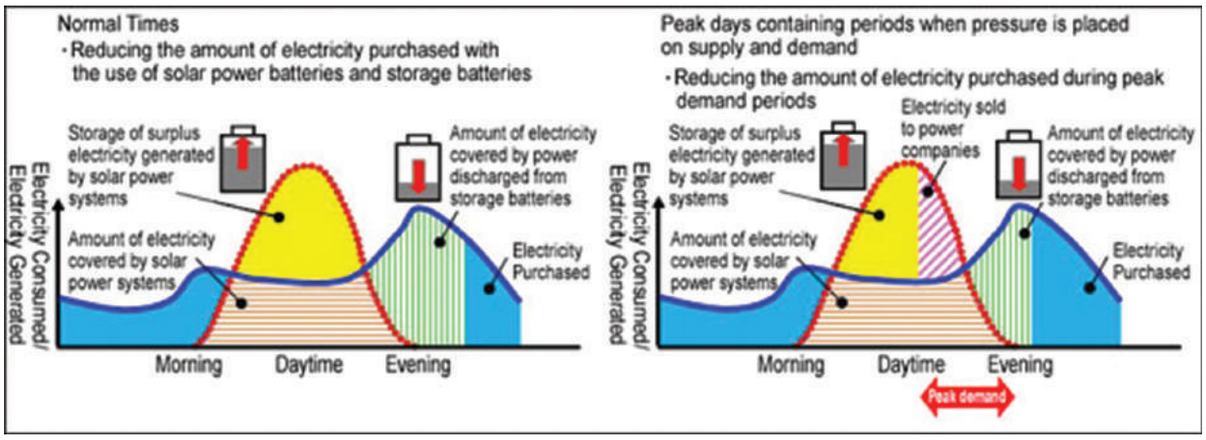


Рис. 4. Эффект от разумного управления системами солнечной генерации и накопителями электроэнергии (Panasonic)

станцией (EV-EMS – Electric Vehicles Energy Management System), интегрированную с системами управления спросом (DR – Demand Response) и CEMS. Система V2H разработана для комбинированного использования: в качестве зарядной станции для электромобиля и использования аккумулятора электромобиля в качестве накопителя электроэнергии. Система V2H – это совместная разработка Nissan Motor, Hitachi, Orix и др. Архитектура системы приведена на рис. 5.

Экологический эффект внедрения системы V2H в г. Йокогама состоял в сокращении выбросов CO2 на 25–30 %.

В рамках указанного проекта была также разработана SCADA-система для управления зарядом/разрядом аккумуляторов электромобилей, посредством которой все электромобили рассматриваются как один виртуальный накопитель электроэнергии. Архитектура системы приведена на рис. 6.

В том же проекте для управления офисными зданиями и коммерческими центрами была создана отдельная система энергоменеджмента зданий (BEMS – Building Energy Management System). Система BEMS, установленная в Музее природоведения и истории человечества (г. Китакюсю), позволила музею добиться экономии в 10–15 % за счёт оптимального комбинированного использования собственной электроэнергии (дизель-генераторов и солнечной энергии) и внешнего электроснабжения, сохраняя при этом жёсткие требования к поддержанию заданной температуры и степени освещённости. Архитектура системы приведена на рис. 7. Музей природоведения и истории человечества в г. Китакюсю по праву считается реализованным в жизни проектом «Умный музей» (Smart Museum).

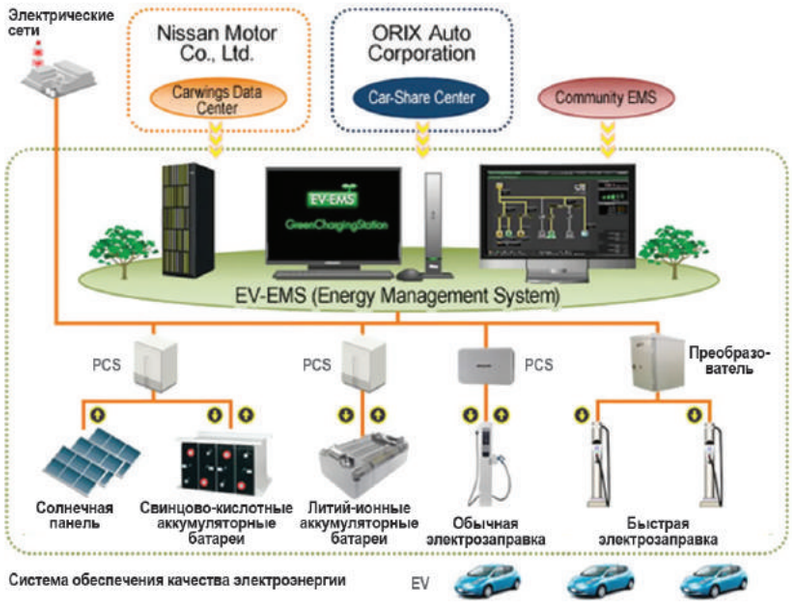


Рис. 5. Пример архитектуры улучшенной системы управления зарядом электромобилей (Hitachi)

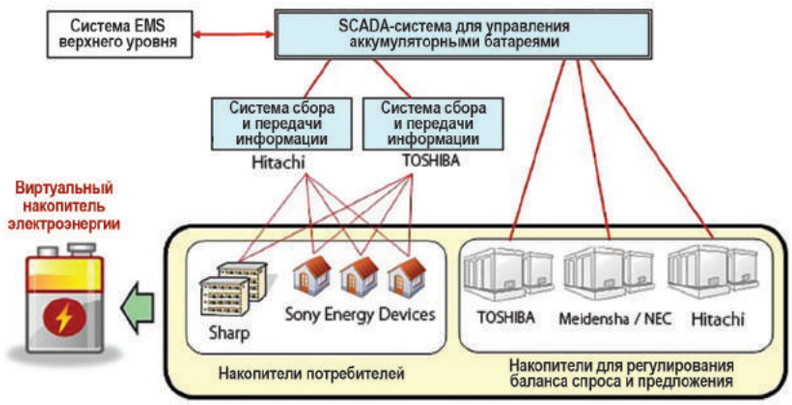


Рис. 6. Пример использования SCADA-системы для управления зарядом / разрядом аккумуляторных батарей

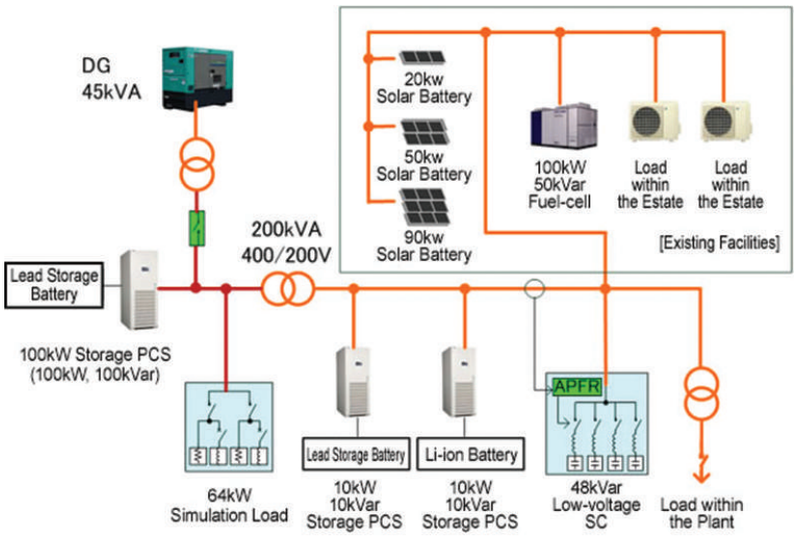


Рис. 7. Архитектура системы BEMS Fuji Electric

Для промышленных предприятий был создан отдельный продукт – система энергоменеджмента предприятии (FEMS – Factory Energy Management Systems), также интегрированная с CEMS. Система FEMS позволяет управлять энергопотреблением вплоть до моделирования оптимальных производственных планов в зависимости от прогнозных значений потребления и выработки электроэнергии в масштабе всего города. В отличие от систем CEMS, HEMS и BEMS, система FEMS имеет встроенный модуль управления освещением. На заводе «Тойота» в г. Китакюси совокупный экономический эффект использования светодиодной системы освещения и интеллектуальной системы управления освещением достигает 60 %.

Это далеко не все решения, которые были созданы и внедрены в рамках четырёх пилотных проектов «Smart City» в Японии. Заметим, что отдельно для каждого потребителя и каждого района разрабатывались собственные решения с учётом климатических, географических, политических и демографических особенностей.

Считается, что создание «Smart City» на пилотных площадках в Японии оправдало ожидания. Только в г. Кайхана уровень потребления электроэнергии снизился на 64 % (рис. 8), а выбросы CO2 – на 58 % (рис. 9). Разработанные в рамках четырёх пилотных проектов решения таких компаний, как Accenture, ORIX, Sharp, Sony, Toshiba, Nissan, NEC, Panasonic, Hitachi, Mitsubishi и др., являются готовыми решения для создания «Smart City» и активно поставляются далеко за пределы Японии.

«Smart City» в Великобритании

В Великобритании вопрос создания «Smart City» находится в ведении Департамента бизнес-инноваций и опыта (Department of Business Innovation & Skills) [8].

Существует пять ключевых аспектов для создания «Smart City» в Великобритании:

- необходимость создания современной цифровой инфраструктуры, позволяющей всем жителям получать быстрый, полный и безопасный доступ ко всей информации, которая им необходима;
- необходимость создания ориентированной на жителей системы предоставления услуг;
- необходимость внедрения интеллектуальных систем и технологий «Internet of Things» для возможности оперативного использования информации, предоставления/получения услуг, а также для анализа данных (например, анализа, как транспортная система справляется с потоком в часы пик) и выработки стратегий развития всей городской инфраструктуры на основании результатов анализа;
- необходимость перенимать опыт и экспериментировать, применяя новые подходы и бизнес-модели;
- необходимость предоставить жителям возможность сравнивать достижения различных учреждений, населённых пунктов.

Авторы проекта представили своё видение принципиальных отличий «Smart City» от обычного города, как приведено на рис. 10. и рис. 11. По их мнению, создание «Smart City» улучшает взаимодействие всех участников (государственный сектор, частный сектор, поставщики услуг, жители и органы власти), поскольку делает процесс взаимодействия двусторонним.

В Великобритании программа создания «Smart City» включает пять проектов:

- проект «Интеллектуальная транспортная система» – мониторинг и управление дорожным движением, управление перегрузками, устранение аварийных ситуаций, система информирования

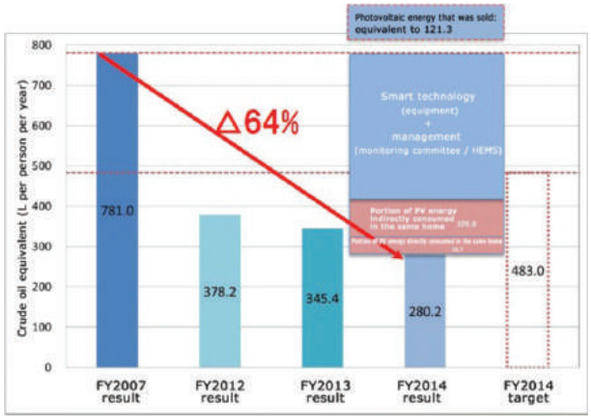


Рис. 8. Статистические показатели снижения потребления электроэнергии г. Кайхана (Киото) – данные Omron

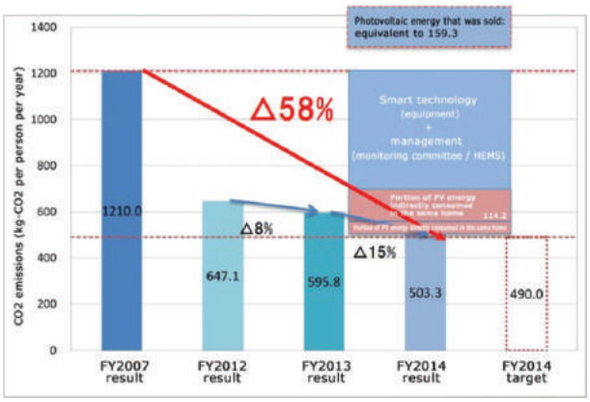


Рис. 9. Статистические показателя снижения выбросов CO2 г. Кайхана (Кеото) – данные Omron

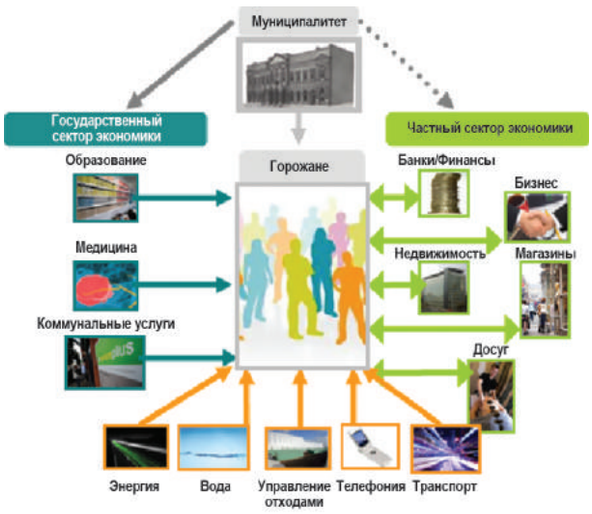


Рис. 10. Традиционная модель

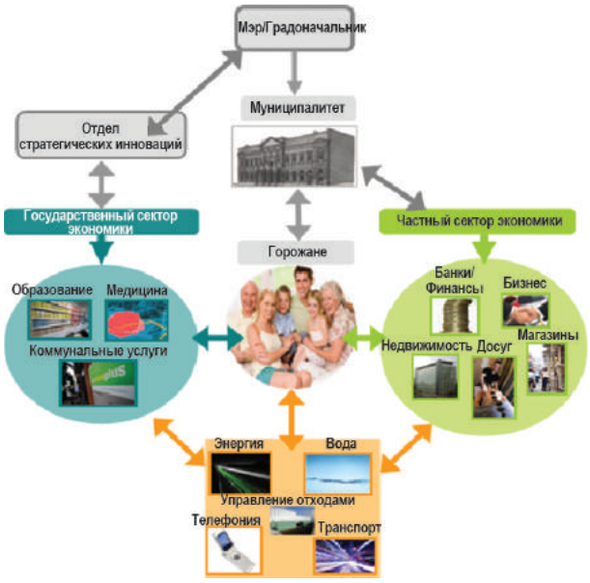


Рис. 11. Модель «Smart City»

горожан, «умные парковки», система управления светофорами;

– проект «Независимая (частично или полностью) система жизнеобеспечения» – телемедицина (оказание медицинских услуг по телефону), продукты и системы для удалённой диагностики, цифровые услуги;
– проект «Управление водой» – модернизация систем водоснабжения, мониторинг потребления, очистка сточных вод, системы защиты окружающей среды, управление половодьем;
– проект «Интеллектуальные сети» – управление электропотреблением, электротранспорт, программа обеспечения энергоэффективности, подключение возобновляемых источников электроэнергии;
– проект «Утилизация отходов» – моделирование утилизации отходов для генерации энергии.

Выводы

Анализ существующих в настоящее время проектов создания «Smart City» показывает, что практически в каждой стране, в каждом городе подходы к внедрению концепции «Smart City» хотя в чем-то универсальны, но имеют весьма существенные различия. Выбор конкретной версии концепции «Smart City» во многом зависит от тех проблем, которые необходимо срочно решать именно в данном регионе и при сложившихся приоритетах, будь то повышение эффективности использования природных ресурсов, модернизация транспортной системы, совершенствование процедур предоставления и получения жизненно-необходимых для населения услуг и т. д.

Создание «Smart City» – это всегда глобальный проект, который требует решения широкого комплекса взаимосвязанных социально-экономических, экологических, инфраструктурных и технических задач.

Технологии «Smart City» – это технологии, основанные прежде всего на применении распределённых интеллектуальных систем. В частности эффективной интеграции отдельных интеллектуальных объектов – «умного дома», «умного завода», «умного музея» и т. д. При этом интеграция основывается в первую очередь на использовании технологии «Интернета вещей» (Internet of Things), с помощью которой все интеллектуальные составляющие «Smart City» эффективно взаимодействуют друг с другом.

Одно из ключевых направлений развития «Smart City» – направление интеллектуальной энергетики («Smart Energy») как основы для создания эффективной, устойчивой и адаптивной городской инфраструктуры.

Литература

1. http://100resilientcities.rockefellerfoundation.org/resilience
2. http://smart-cities.ieeecss.org/sites/ieeecss.org/files/technicalCommitteeProposalFinal.pdf
3. http://hbr.org/2013/07/building-sustainable-cities/
4. http://ec.europa.eu/eip/smartcities/
5. https://eu-smartcities.eu/eu-projects
6. http://www.sustainablecities.eu/
7. http://jscp.nepc.or.jp/en/
8. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246019/bis-13-1209-smart-cities-background-paper-digital.pdf