УЧЕБНЫЙ ЦЕНТР
РТСофт

20 ЛЕТ УСПЕШНОЙ РАБОТЫ В ОБЛАСТИ ПРОФЕССИОНАЛЬНОГО ИТ-ОБРАЗОВАНИЯ

УЧЕБНЫЙ ЦЕНТР «РТСофт»

3500+	40+	15+
СЛУШАТЕЛЕЙ	ПРОГРАММ КУРСОВ	ТЕМ СЕМИНАРОВ

Программы учебного центра по направлениям:

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

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

ЖДЕМ ВАС В УЧЕБНОМ ЦЕНТРЕ «РТСофт»!

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

Лицензия Департамента образования города Москвы № 037032 от 25.01.2016 г.

В НОМЕРЕ

CONTENTS

ОБЩИЙ ВЗГЛЯД

BIRD'S EYE VIEW

То, что мы делаем, делается в верном направлении
Ольга Синенко | АО «РТСофт»
4
What We Are Doing Is Going to the Right Direction,
by Olga Sinenko | RTSoft

Коллоквиум SC D2 CIGRE: успешный дебют в России
По материалам АО «РТСофт»
11
CIGRE SC D2 Colloquium 2017: Successful Début in Russia,
by RTSoft Materials

«РТСофт» на Международном военно-морском салоне – 2017
По материалам АО «РТСофт»
18
RTSoft at the International Maritime Defense Show 2017,
by RTSoft Materials

ВСТРАИВАЕМЫЕ КОМПЬЮТЕРНЫЕ ТЕХНОЛОГИИ

EMBEDDED COMPUTER TECHNOLOGIES

Беспроводные информационно-развлекательные системы
По материалам Контрон
24
Wireless InFlight Entertainment Systems,
by Kontron Materials

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

SOFTWARE

Построение программного обеспечения управляющих контроллеров на основе открытых интерфейсов IPMI, HPI, RedFish
Сергей Жуков, Игорь Починок | Auriga Inc., НИВЦ МГУ
31
Building the Software for Managing Controllers on the Base of Open Interfaces: IPMI, HPI, RedFish,
by Sergey Zhikov and Igor Pochinok | MCU RCC, Auriga Inc

ИУС ДЛЯ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ И ИНФРАСТРУКТУРНЫХ ОБЪЕКТОВ

INDUSTRIAL ENTERPRISE AND INFRUSTRUCTURE IMSs

Защищённый комплект программ «PLATO RT» – реализация базовых требований информационной безопасности АСУ КВО
Константин Здирук, Алексей Ханыгин | АО «РТСофт»
34
PLATO RT Secure Software Kit – Implementation of Information Security Base Requirements of Critical Important Object Automatic Control Systems,
by Konstantin Zdiruk and Alexey Khanygin | RTSoft

Система управления процессом технологической подготовки токамака Т-15МД к эксперименту
Галина Кузьмина, Юрий Моцкин | АО «РТСофт»
Александр Качкин, Иван Образцов, Михаил Соколов, Пётр Хвостенко, Михаил Чуканов | НИЦ «Курчатовский институт»

49 **Process Control System of T-15МД Tokamak Preparation for The Experiment,**
by Galina Kuzmina and Yuri Motskin | RTSoft
Alexander Kachkin, Ivan Obraztsov, Mikhail Sokolov, Petr Khvostenko and Mikhail Chukanov | NRC «KURCHATOV INSTITUTE»

ИУС ДЛЯ ЭЛЕКТРОЭНЕРГЕТИКИ

POWER INDUSTRY IMSs

Кто и зачем использует Микрогрид?
Элиза Вуд (Elisa Wood) | Microgrid Knowledge

39 **Who Uses Microgrids and Why?,**
by Elsa Wood, Microgrid Knowledge

НОВОСТИ

MARKET NEWS

Испытания российских машин серии BLOK на платформе Intel 7-го поколения успешно завершены

21 **Testing of Russian BLOK Machine Series Based on the 7th Generation Intel Platform Was Successfully Finished**

Модули COM Express от Kontron на базе Intel Core 7-го поколения стали серийными

23 **Kontron COM Express Modules Based on the 7th Generation Intel Core Processors Become Off-The-Shelf Ones**

РТСофт» получил сертификаты СТ-1 ТПП для компьютеров BLOK

64 **RTSoft Got СТ-1 ТПП Certificates for BLOK Computers**

РЕДАКЦИОННЫЙ СОВЕТ:

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

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

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

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

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

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

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

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

РЕДАКЦИЯ:

Главный редактор – **Зеленова Т. И.**

ЭКСПЕРТЫ ПО НАПРАВЛЕНИЯМ:

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

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

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

ИУС для энергетики – **Небера А. А.**

Ответственный за вёрстку – **Белов И. В.**

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

Тираж 900 экз., цена свободная.
«Мир компьютерной автоматизации. Век XXI»
Computer Automation World
№3 (112) 2017

Издаётся с 1995 года.
Выходит 4 раза в год.

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

mka@rtsoft.ru
www.mka.ru

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

То, что мы делаем, делается в верном направлении

Ольга Синенко | АО «РТСофт»

Интервью генерального директора АО «РТСофт», доктора технических наук, действительного члена АИН РФ им. Прохорова, председателя подкомитета D2 РНК СИГРЭ Ольги Викторовны Синенко главному редактору журнала «Автоматизация и IT в энергетике» Егорову Александру Александровичу.

Вопрос: Девиз Вашей компании – «От лучших отечественных инженерных решений к конкурентоспособной стране». Как понимает этот девиз компания, которая успешно функционирует в современных условиях, включая кризисы и санкции?

Ответ: Действительно, этот девиз отражает глубинную сущность нашей компании, которая всегда, независимо ни от каких кризисов, санкций и других явлений, которые

были, есть и будут, базировалась на том, что мы научно-техническая, инновационная, инженерная и производственная компания. Мы не занимаемся переизобретением велосипедов, а тщательно анализируем мировые тенденции в области автоматизации и встраиваемых систем управления и на базе всего лучшего, что есть в мире, в партнёрстве с передовыми зарубежными компаниями, создаём российские продукты, решения, системы и внедряем их на отечественных предприятиях. С другой стороны, создаваемые нами решения и продукты должны быть конкурентоспособны и за рубежом. Поэтому мы не подвержены каким-то временным, случайным решениям, которые приходят и уходят, а на этой базе оставались и будем оставаться. На сегодняшний день, да и всегда, создание современных и перспективных конкурентоспособных инженерных решений не может происходить в отрыве от международных трендов, от международного сотрудничества, в том числе технологического. Хотелось бы здесь подчеркнуть, что инженерное решение – это не только аппаратура или программное обеспечение, во многом это прежде всего люди. В этом плане нам, наверное, повезло. «Несмотря ни на что и вопреки всему» наша страна продолжает рождать умных, талантливых людей, очень способных к инженерному труду. И задача таких компаний, как наша, – помогать людям, начиная со школьной, студенческой скамьи, увидеть и полюбить именно инженерную

профессию, сделать из них профессионалов, а в стране в целом превратить инженерный потенциал, научно-технический потенциал в реальный актив. С моей точки зрения, конкурентоспособность нашей страны в будущем состоит именно в этом – в креативном и профессиональном научно-техническом потенциале.

Вопрос: ***Многие аналитики считают последние годы годами кризисов. Как Ваша компания проходит через них? Как изменились обороты компании? Какие меры были приняты для преодоления этих последствий? Поддерживаете ли Вы тезис «Кризис – это время работать!»?***

Ответ: Экономический кризис объективно существует, длится определённое время и не только в нашей стране, но и повсеместно – мы это с вами хорошо знаем. Бизнес на то и есть бизнес, чтобы уметь правильно адаптироваться к таким временам. Кризисы были и будут. Задача лидеров компаний – к ним приспосабливаться, но не только за счёт того, чтобы сокращать затраты, обрезать что-то лишнее, но и, что очень важно, уметь увидеть будущее. Что будет делать компания в послекризисное время? Где будет её место? Какие там должны быть люди? И несмотря ни на что использовать это кризисное время – да, тяжёлое, да, неблагодарное – на то, чтобы ни при каких условиях не отдавать поле с новым, перспективным делом на растерзание сиюминутным задачам, которые приходится ежеминутно решать в форс-мажорной обстановке. Поэтому очень важно определиться с теми направлениями, которые нужно взрастить за это время, подготовиться, вложить энергию, ресурсы, в том числе финансы, чтобы потом на этом поле в послекризисное время быть первыми.

По поводу Вашего тезиса «Кризис – это время работать!» – он мне очень понравился. Но я хотела бы ответить любимой цитатой из «Алисы в Стране чудес»: «Нужно бежать со всех ног, чтобы только оставаться на месте, а чтобы куда-то попасть, надо бежать как минимум вдвое быстрее!» Поэтому наша задача, если хочешь выйти в нужную точку в новой, конкурентоспособной форме, – энергии и креатива применять существенно больше и эффективнее. Как мы сейчас видим по многим компаниям, и не только по нашей, темп жизни, потоков информации и их обработки, участия в каких-то мероприятиях увеличился как минимум вдвое, а то и больше.

Вопрос: ***Какие трудности Вы видите в своей работе по созданию конкурентоспособных отечественных решений, в том числе для энергетики?***

Ответ: Трудности общие у всех аналогичных компаний, здесь я не скажу ничего нового. Обратная сторона кризисов – в это время, как правило, пышно расцветает бюрократия, различные ограничительные, запретительные меры, удлиняются и усложняются аттестации, сертификации, учащаются и ужесточаются всякого рода проверки. Это всем хорошо известный процесс. К сожалению, он оттягивает непропорционально много времени и ресурсов. Это, собственно, основное, что мешает сегодня гибко, эффективно и оптимально использовать и финансовые, и экономические, и человеческие ресурсы.

Вопрос: ***Как Вы относитесь к такому модному сегодня вопросу, как интеллектуальные распределительные сети, Smart Grid? И как эти идеи отражаются на Ваших новых разработках?***

Ответ: По поводу Smart Grid. Термин был введён около 10 лет назад. Он действительно подразумевал «умные» распределительные сети. Сегодня этот термин стал гораздо шире, и его уже трактуют, например,

как «интеллектуальная распределённая энергетика». Одно из направлений – платформа EnergyNet, над которой мы с Вами вместе активно работаем в настоящее время. Сюда уже входят такие понятия, как Microgrid, Nanogrid, «виртуальная электростанция». Действительно, вокруг этого начального и узкого понимания Smart Grid наросло много новейших применений, что делает жизнь в области «умной» энергетики гораздо интереснее. Сюда, конечно, нужно добавить и возобновляемые источники энергии, которые, несмотря на период нерешительности, всё-таки стартовали в нашей стране. Мы не могли не отреагировать на такую перспективу и два года назад создали отдельное бизнес-направление – Центр Smart Grid. Здесь мы сконцентрировали основную научно-техническую, аналитическую, экспертную составляющую в области технологий интеллектуальной распределённой энергетики. Здесь мы готовим, ставим и решаем задачи – конечно, с помощью наших партнёров, основных потребителей этих будущих продуктов и решений. Например, задачи по новым видам мониторинга контроля состояния энергообъектов, по оптимальному, эффективному управлению новыми типами энергосистем (Microgrid, Nanogrid), гибридными системами, распределённой генерацией. Также в рамках этого направления мы сейчас занимаемся вопросами снижения энергозатрат для промышленных предприятий, что в условиях кризиса становится очень актуальным. В основе этих работ лежат такие интересные инженерные или научные профессии, как, например, математик-алгоритмист. На сегодняшний день мы уже собрали группу талантливых специалистов, занимающихся именно процессами и алгоритмами оптимизации, контактируем с лучшими мировыми университетами для обмена информацией по данным вопросам. У нас есть целый ряд совместных работ с университетами и научно-исследовательскими институтами. В практическом применении это выливается в то, что в создаваемых нами новых изделиях и программном обеспечении для «умных» сетей оптимизационная составляющая является конкурентоспособным моментом, делая наши разработки привлекательными, в том числе и на зарубежных рынках.

Вопрос: ***Всем известна проблема киберзащиты в электроэнергетике. Участвует ли компания «РТСофт» в решении этой проблемы?***

Ответ: Хорошо, что Вы этот вопрос поднимаете. Несмотря на усиленное продвижение в последнее время кибербезопасности технологических систем управления и АСУ ТП, в отличие от защиты банковских, информационных и офисных систем различного вида, эта тема ещё далека до глубин проработки, а последствия от нерешения данного вопроса могут быть катастрофическими. Мы тоже включены в эту работу, тесно сотрудничаем с «Лабораторией Касперского» и участвуем в совместных разработках и внедрениях ряда новых продуктов, а также завершили аттестацию и сертификацию нашего собственного ПО – «Плато-РТ», с помощью которого можно защищать крупные информационные системы от несанкционированных вторжений. Однако темпы внедрения систем информационной безопасности именно в электроэнергетике, с моей точки зрения, остаются неудовлетворительными, что вызывает серьёзную тревогу и у меня, и у моих коллег – специалистов как по АСУ ТП, так и по системам управления. Конечно, на эту тему нужно обращать более пристальное внимание.

Вопрос: ***Четвёртая промышленная революция (Индустрия 4.0) – прогнозируемое событие, связанное с массовым внедрением киберфизических систем в производство, а также обслуживанием человеческих потребностей, включая быт, труд и досуг. По оценкам экспертов, изменения охватят самые***

разные стороны жизни людей: рынок труда, жизненную среду, политические системы, технологический уклад и т. п. Как компания «РТСофт» откликается на эту революцию?

Ответ: Как Вы правильно задали мне вопрос, что это не только технические решения, которые в нашей компании тоже поддерживаются, но и серьёзные изменения, которые возникнут в жизни людей вплоть до бытового уровня. Помимо аппаратуры, программных средств и систем управления и мониторинга, построенных на базе «Интернета вещей», мы уделяем большое внимание тому, как смогут программисты, системщики, архитекторы будущего быстро и надёжно создавать конкретные системы с помощью частей, созданных различными производителями. Для этого необходимо иметь и системное мышление программистов, и прекрасный инструментарий, и средства тестирования. Это не те «тяжёлые» проекты, которыми характеризуются классические АСУ ТП типа нефтяных, нефтеперерабатывающих производств, металлургических, машиностроительных заводов. Это системы, которые будут работать повсеместно – в супермаркетах, складских, офисных помещениях и т. д., но создавать и эксплуатировать их надо будет грамотным людям. Для этого мы ведём обучающие курсы, организуем лаборатории в университетах. В частности, в прошлом году была открыта лаборатория «Интернета вещей» в МГТУ им. Баумана с нашим участием. Мы проводим летние школы для молодых специалистов, где учим создавать системы по принципу «Интернета вещей», готовим их к тому, чтобы они могли овладеть основными элементами, которыми характеризуется Индустрия 4.0. Это очень важно, потому что одним из ключевых компонентов 4-й промышленной революции будет человек. Но не тот человек, которого эта революция высвобождает от труда, а те люди, которые будут заниматься подготовкой технической базы, обслуживанием её развития. Для примера скажу, что уже к 2020 году прогнозируется 10-кратный рост конечных устройств, которые будут связаны в сети в повседневной жизни людей. Безусловно, ими нужно управлять, с ними нужно работать и, поскольку их будет больше, чем население Земли, с ними нужно обращаться очень аккуратно и правильно.

Вопрос: ***Компания «РТСофт» организовала подкомитет D2 РНК СИГРЭ «Информационные системы и телекоммуникации». Каких успехов достиг подкомитет? Какие наиболее важные задачи стоят перед ним?***

Ответ: Участие в международных органах по сертификации, по продвижению новых технологий, в лучших международных профессиональных ассоциациях по нашей тематике – это всегда было принципом нашей работы, потому что невозможно развивать инженерный потенциал и ориентировать команду на будущее, если нет понимания мировых тенденций, опыта других стран, наиболее продвинутых передовых проектов и т. д. Поэтому после того как компания начала активно работать в области электроэнергетики, следующим шагом была активизация нашей работы с СИГРЭ как с самой крупной в мире ассоциацией по большим электрическим сетям.

Четыре года назад я получила предложение от руководства Российского национального комитета СИГРЭ на базе «РТСофт» создать подразделение Исследовательского комитета – D2 (ИК D2) как симметричного исследовательского комитета большому СИГРЭ. На сегодняшний день так и организована работа РНК, то есть в России на основе базовых компаний, которых выбирает технический совет, административный совет РНК организует работу по соответствующему исследовательскому направлению, одному из шестнадцати. Поэтому направление «Информационные системы и телекоммуникации» ведёт компания «РТСофт» как базовая, но участие в работе ИК D2 уже

сейчас принимают десятки российских организаций: и государственных компаний, и промышленных предприятий – соответственно, и сами производители, и системные интеграторы. И это очень здорово. Сегодня ИК D2 РНК СИГРЭ добился проведения международного коллоквиума D2, который проходит раз в два года между Парижскими сессиями СИГРЭ, – в России. Это впервые! Он будет проходить 20–22 сентября. Очень серьёзно к этому подошли наши коллеги из «большого» СИГРЭ и руководство РНК. В результате мы имеем беспрецедентный набор докладов и докладчиков – более 50 выступающих из 23 стран! Это действительно уникальная ситуация. Темы, которые заявлены как основные, думаю, будут очень интересны тем, кто придёт на конференцию даже в качестве слушателя. Эти темы как раз связаны и с информационной безопасностью, и с организацией «умных» сетей на базе возобновляемых источников энергии, и с системным управлением распределёнными ресурсами, и с новыми телекоммуникационными средствами и подходами в области электроэнергетики. Кроме того, у нас есть специально приглашённый докладчик Джованна Дондоссола из Италии – эксперт мирового уровня по международным стандартам в области безопасности технологических систем управления. Её доклад мы вынесли отдельно. Думаю, будет очень интересно узнать о международном опыте стандартизации. Среди докладчиков, которые прошли серьёзный отбор, много молодёжи. Это возможность в 2018 году поучаствовать в качестве докладчиков на Парижской сессии СИГРЭ.

Вопрос: ***Книги издательства «РТСофт» всегда можно увидеть на стендах ежегодных международных книжных ярмарок в Москве. Издательство принимает активное участие в различных мероприятиях: конференциях, семинарах, выставках, проходящих в течение года в России и СНГ. Эта деятельность компании является удачным бизнес-процессом или носит в основном благотворительный характер?***

Ответ: Я бы хотела сказать: это не совсем бизнес-проект, но он несёт вполне определённую цель – продвижение и освещение уникальных достижений российских инженеров, учёных, испытателей в наиболее критических, важных для нас областях и возможность доступа людей, прежде всего нашей молодежи, к этим знаниям. Это космос, авиация, морской флот. Мы не можем охватить всё, но стараемся концентрироваться именно на этом, потому что хотим продолжать традиции отечественной инженерной школы. Не зная прошлого, не зная, как это происходило и развивалось, кто внёс свой вклад, не будет будущего. Нам приятно, что наши книги читают те, кто сам был непосредственным участником этих событий – создания новой техники, освоения морских глубин, космоса, а также новое поколение, у которого все достижения впереди. Знаете, иногда бывает так, что, читая наши книги, люди видят там своих родных, близких знакомых. Они бесконечно счастливы, потому что понимают: вот она, живая история. Практически все книги нашего издательства поддержаны государственными грантами. Это хороший знак того, что это действительно нужно стране.

Одна из наших уникальных идей, которую мы реализовали, и я этим очень горжусь, это календарь-энциклопедия. Мы их выпускаем каждый год. Они посвящены людям, технике, событиям в какой-то серьёзной области. На двенадцати разворотах мы должны собрать самые главные вехи, касающиеся, например, морского флота, подводного флота, авиации, космонавтики, вычислительной техники. Работа над таким календарем идёт как минимум в течение полугода, с привлечением экспертов. Мы сотрудничаем с научно-исследовательскими институтами, например с Институтом истории естествознания и техники, который уходит корнями в почти 300-летнюю историю. Несколько

«РТСофт» отметил 25-летний юбилей

14 июля 2017 года компания «РТСофт» отметила круглую дату – 25 лет со дня основания! За плечами компании сложная дорога побед и разочарований, достойная история и колоссальный опыт работы в сфере промышленной автоматизации, программных разработок и встраиваемых компьютерных технологий в России и за рубежом.

В свой юбилей компания больше чем когда-либо стремится сохранить свои базовые ценности, которые являются основой успешного бизнеса. Это продвижение инноваций в области высоких технологий. Это профессионализм команды и следование лучшим традициям отечественной инженерной школы. Это эффективное многолетнее партнёрство, уважение и защита интересов заказчика и безусловное выполнение взятых на себя обязательств.

Опираясь на мощный проектный опыт в энергетике, нефтегазовой, атомной, металлургической, машиностроительной, транспортной и других отраслях, «РТСофт», сохраняя лидерство, активно развивается, строит амбициозные планы и уверенно смотрит вперёд.

Через свои филиалы, представительства и инженерно-производственные центры «РТСофт» работает в различных регионах нашей страны и на международном рынке. Дальний Восток, Сибирь, Юг России, Поволжье, Урал, Центральный регион, страны ближнего и дальнего зарубежья – мы всегда рядом с вами!

За 25 лет группа компаний «РТСофт» успешно реализовала свыше 9 000 проектов. Благодаря компетенции и глубоким экспертным знаниям наших специалистов заказчик получает полный цикл услуг и сервисов под ключ. Мы осуществляем профессиональный консалтинг, разработку и внедрение программного обеспечения, поставку оборудования и ПТК, в том числе собственного производства, техподдержку и обслуживание, а также обучение пользователей. Это наше важное конкурентное преимущество!

Поддержка государственной программы импортозамещения, работа в рамках инициативы EnergyNet, выход на отечественные и международные рынки с инновационными продуктами для «умной» энергетики, энергоэффективности и кибербезопасности, участие в крупнейших мировых инженерно-технологических выставках и международных коллоквиумах под эгидой РНК СИГРЭ – сфера профессиональной деятельности «РТСофт» постоянно расширяется. А это значит, у компании большой потенциал и хороший задел на будущее.

Команда «РТСофт» благодарит своих друзей, партнёров и заказчиков за доверие, – для нас это очень ценно! Благодарим всех сотрудников за вклад в общее дело и надёжную репутацию компании!

наших исторических календарей-энциклопедий мы выпустили вместе с ними. Это большая, серьёзная, интересная работа. Мы считаем это чрезвычайно патриотическим проектом.

Хотела бы открыть небольшой секрет: в честь юбилея компании и в знак уважения к давнему другу нашего издательства лётчику-космонавту Алексею Архиповичу Леонову мы выпускаем уникальный альбом. Это и биография, и репродукции его картин, и целая серия фотографий о жизни и творчестве Алексея Архиповича.

Кроме того, у нас есть книги с рассекреченными документами о создании космических аппаратов, начиная с конца 50-х годов. Огромная работа была проделана Ю. М. Батуриным и коллективом его института. Люди,

которые сегодня работают в космической промышленности, могут понять, какого серьёзного труда и высокого профессионализма требовало создание конкурентоспособных решений. Какого уровня были специалисты и те, кто руководил отраслью. Какую ответственность они брали на себя, чем и как они за это отвечали. Это, конечно, удивительно, и об этом говорят документы, на которых стоят резолюции, подписи руководства страны того времени.

Самое главное, мы хотели бы, чтобы читатели, приобретая наши издания, обязательно давали прочитать такую книгу детям. Когда есть чем гордиться в прошлом, люди больше настроены на будущее.

Также в честь 25-летия компании мы решили создать Музей истории управляющей вычислительной техники. Нам удалось собрать все физические образцы, описания ПО, воспоминания тех, кто создавал управляющую вычислительную технику в Советском Союзе, кто занимался автоматизацией научных исследований с начала 70-х годов. Ну а книгу по истории электронно-управляющих машин мы уже опубликовали два года назад. Конечно, мы не можем показать всё, но тем, кому интересно знать, как выглядело то, что сегодня занимает квадратные сантиметры, в 70-е годы, с чего начинались системы АСУ ТП, ОСРВ, мы показать можем. На мой взгляд, это должно быть очень интересно.

Ещё мы работаем над созданием лаборатории инновационных решений, где в интерактивном виде посетители лаборатории (даже школьники или студенты) смогут сами смоделировать систему умных сетей распределённой энергетики Microgrid, «пощупать» её, соединить с диспетчерским центром. Можно будет самому поучаствовать в проектировании моделей, например энергоснабжения острова, удалённого поселка или курортной зоны, технопарка, завода. И это здорово, потому что в какой-то степени перекликается с вопросом 4-й промышленной революции. Нами уже созданы две лаборатории: одна в Сколтехе, вторая в Сочи (школа «Сириус» для талантливых детей), в которых как раз школьники и студенты могут управлять различными возобновляемыми источниками энергии.

Вопрос: ***Вы создали компанию и 25 лет являетесь её бессменным лидером. У Вас накопился бесценный опыт. Сегодня многие женщины стремятся стать успешными бизнес-леди. Какими, на Ваш взгляд, чертами и какими характеристиками они должны обладать?***

Ответ: Женщина должна обладать двойным запасом энергии, чтобы совмещать семейную жизнь и работу. Никто никогда ещё не освобождал женщину от счастья в личной жизни в обмен на карьеру в бизнесе. Если женщина хочет идти вперед в этом направлении, которое подразумевает постоянную гонку за новыми технологиями, и быть всегда в курсе происходящего, она должна быть собранной, готовой к тому, что на двух фронтах ей придётся трудиться гораздо больше. Мы должны успевать всё. Если мы будем делать бизнес в ущерб семье, то это не нужно ни семье, ни бизнесу, ни себе самой – никому вообще.

Будущее, хоть оно и непредсказуемо, обещает быть очень интересным. Мы будем его активнейшими участниками. Наша самая главная задача – подготовить тех, кто будет в нём работать и это будущее развивать. Они будут совсем другими – не такими, как мы, а гораздо более продвинутыми, умными, стремительными. Поэтому хочется завершить наш разговор словами Алисы про будущее: «Не грусти... Рано или поздно всё станет понятно, всё станет на свои места и выстроится в единую красивую схему, как кружева. Станет понятно, зачем всё было нужно, потому что всё будет правильно». Иными словами, то, что мы делаем, делается в верном направлении.

Редакция журнала «Автоматизация и IT в энергетике» благодарит Вас за содержательные ответы.

Коллоквиум **SC D2 CIGRE: успешный** дебют в России

По материалам АО «РТСофт»

С 18 по 22 сентября в Москве состоялось значимое событие в сфере информационных технологий для электроэнергетики – Международный коллоквиум Исследовательского комитета (ИК) D2 международной неправительственной некоммерческой организация в области электроэнергетики CIGRE, которая объединяет усилия стран-участниц со всего мира для формирования стратегии развития отрасли. Россия, как одна из ведущих стран-участниц CIGRE, играет активную роль в этой деятельности и впервые в истории отечественной энергетики принимала гостей у себя.

Международные коллоквиумы исследовательских комитетов Международного совета по большим энергетическим системам высокого напряжения (Conseil International des Grands Réseaux Électriques – CIGRE) проводятся один раз в два года в разных странах мира. Это один из основных форматов научно-практической деятельности организации. Коллоквиум-2017 по тематике D2 («Информационные системы и телекоммуникации») впервые в новейшей истории России состоялся в нашей стране.

Организатором проведения Международного коллоквиума ИК D2 CIGRE была выбрана компания «РТСофт» – ведущий научно-технический партнёр Российского национального комитета (РНК СИГРЭ) по направлению D2 «Информационные системы и телекоммуникации» в электроэнергетике и базовая организация подкомитета D2 РНК СИГРЭ. Генеральный директор «РТСофт» Ольга Викторовна Синенко является его руководителем, а также регулярным членом Исследовательского комитета D2 CIGRE от Российской Федерации. Решение о проведении коллоквиума в нашей стране было принято по её инициативе.

Генеральными партнёрами коллоквиума выступили ПАО «ФСК ЕЭС» и ПАО «Россети», среди партнёров – РНК СИГРЭ, АО «СО ЕЭС», АО «НТЦ ФСК ЕЭС».

Событие вызвало большой интерес у зарубежных специалистов, приславших рекордное количество заявок к участию. Количество присланных докладов почти вдвое превысило показатели двух прошлых коллоквиумов D2. Всего в мероприятии приняли участие более 150 экспертов из 26 стран, это представители крупнейших мировых электроэнергетических компаний (рис. 1) и ведущих производителей оборудования. Более 50 процентов участников – иностранные гости. Самая большая иностранная делегация прибыла из Японии.

Коллоквиум проводился с целью обмена информацией и опытом между энергокомпаниями, производителями оборудования, научно-техническими и проектными организациями отрасли из разных стран. Главная ценность мероприятия – уникальная возможность для его участников ознакомиться с результатами внедрений конкретных практических разработок.

Насыщенная программа коллоквиума вобрала в себя широкий спектр мероприятий – от деловых до культурно-развлекательных. В первые два дня, 18 и 19 сентября, проводились заседания рабочих групп и консультации в закрытом формате. 20 и 21 сентября были представлены 40 докладов по трём тематическим направлениям:

– программные платформы управления распределёнными энергоресурсами,
– устойчивость к киберугрозам информационных и телекоммуникационных систем в электроэнергетике,

Рис. 1. В коллоквиуме приняли участие более 150 экспертов из 26 стран

– высоконадёжная инфраструктура связи для традиционных и новых приложений в энергетике.

Торжественная церемония открытия коллоквиума состоялась 20 сентября. На церемонии открытия с приветственным словом к участникам обратились генеральный секретарь Международного совета по большим электрическим системам высокого напряжения (CIGRE) Филипп Адам; председатель РНК СИГРЭ, председатель правления ПАО «ФСК ЕЭС» Андрей Муров; председатель Исследовательского комитета D2 CIGRE Филипп Куэнадон; представитель от РФ и регулярный член SC D2 CIGRE, председатель Подкомитета D2 РНК СИГРЭ,

Рис. 2. Генеральный секретарь CIGRE Филипп Адам

Рис. 3. Председатель РНК СИГРЭ, председатель правления ПАО «ФСК ЕЭС» Андрей Евгеньевич Муров

генеральный директор АО «РТСофт» Ольга Синенко.

В приветственной речи Филипп Адам (рис. 2) поблагодарил организаторов за тёплый приём и подчеркнул важность обмена информацией в отрасли, способствовать которому призван Коллоквиум. Он также отметил, что по итогам 2016 года Российская Федерация поднялась на первое место в Европе, опередив Францию и Германию, и на пятое место в мире в рейтинге членства, уступая только Китаю, Бразилии, США и Японии.

Андрей Муров (рис. 3) поблагодарил руководство SC CIGRE за оказанное доверие и решение провести Коллоквиум в Москве и отметил, что темы развития цифровых технологий и кибербезопасности – в списке актуальных и важнейших тем мировой экономики. В России придаётся большое значение новейшим разработкам и техническому прогрессу во всех областях отечественной электроэнергетики. В частности, отметил Андрей Муров, в ФСК ЕЭС существенно растёт число научно-исследовательских и опытно-конструкторских разработок, связанных с цифровизацией производственных и управленческих процессов.

Филипп Куэнадон (рис. 4) в свою очередь также коснулся важности обмена информацией в отрасли и заметил, что сегодня «ландшафт» электроэнергетики меняется очень быстро, либерализация рынков инициирует новые процессы. Для построения надёжных и безопасных сетей нужно заложить конкретные идеи, и этому, безусловно, будет способствовать Коллоквиум. Он призвал российских представителей к более активному участию в работе комитета и сообщил, что по итогам Коллоквиума будут выбраны 3–5 наиболее значимых докладов, которые будут предложены к публикации в изданиях СИГРЭ.

Ольга Синенко (рис. 5) поприветствовала участников, пожелала им плодотворной работы и выразила надежду, что это мероприятие послужит отправным моментом для проведения в России больших конференций СИГРЭ.

По завершении церемонии открытия стартовала деловая часть программы. В этот день звучали доклады на тему «Высоконадёжная инфраструктура связи для тради-

Рис. 4. Председатель Исследовательского комитета D2 CIGRE Филипп Куэнадон

Рис. 5. Руководитель Подкомитета D2 РНК СИГРЭ Ольга Синенко

Рис. 6. Люсьен Лассани (Нидерланды) – модератор секции «Высоконадёжная инфраструктура связи для традиционных и новых приложений в энергетике»

ционных и новых приложений в энергетике», модератор Люсьен Лассани (рис. 6), глава службы кибербезопасности STEDIN, Нидерланды. Перед аудиторией выступили эксперты из Австралии, Бразилии, Ирландии, России, Сербии, Уругвая, Финляндии, Южно-Африканской Республики и Японии (рис. 7).

В рамках программы коллоквиума состоялась постер-сессия, подготовленная Молодёжной секцией РНК СИГРЭ (рис. 8). На ней было представлено 11 работ молодых учёных и студентов-энергетиков. Важно, что им была предоставлена возможность принять участие в этом значимом отраслевом событии. С представителями молодёжной секции встретился Филипп Адам (рис. 8, вверху справа). Он ответил на многочисленные вопросы аудитории, с интересом выслушал предложения по созданию новых форм общения молодёжных секций CIGRE и по организации международных молодёжных инженерных чемпионатов и пообещал оказать содействие в налаживании контактов молодёжи РНК СИГРЭ с подобными секциями других стран.

21 сентября участники коллоквиума обсудили темы: «Программные платформы управления распределёнными энергоресурсами» и «Устойчивость к киберугрозам информационных и телекоммуникационных систем в электроэнергетике».

Модератором первой темы выступил Алексей Небера (рис. 9), технический директор по направлению электроэнергетики, директор центра Smart Grid АО «РТСофт». Эксперты из Германии, России, Словении и Хорватии представили свои доклады и ответили на вопросы аудитории. Среди докладов в общей программе было два полноформатных выступления представителей молодёжной секции РНК СИГРЭ, выбранных из числа 11-ти постерных презентаций.

Тему «Устойчивость к киберугрозам информационных и телекоммуникационных систем в электроэнергетике» вёл Дэннис Холстейн, главный эксперт OPUS Consulting Group, США

Рис. 7. Выступления и вопросы

Рис. 8. Молодёжная секция РНК СИГРЭ: встреча с Филиппом Адамом и постер-сессия

(рис. 10). Свои доклады презентовали специалисты из Италии, Китая, Нидерландов, России, США, Франции, ЮАР и Японии.

Следует отметить, что формат коллоквиума предусматривает выступления с мест (рис. 11) не только с вопросами к докладчикам, но и с ответами на вопросы, заранее сформулированные модераторами и предусматривающие вклад выступающих в решение злободневных проблем или постановку задач по соответствующей тематике.

Насыщенная программа 22 сентября включила в себя выступления иностранных специалистов, работу круглого стола, технический

Рис. 9. Алексей Небера, технический директор по направлению электроэнергетики, директор центра Smart Grid АО «РТСофт»

Рис. 10. Дэннис Холстейн, главный эксперт OPUS Consulting Group, США

Рис. 11. Работа коллоквиума в диалоговом формате: ответы на вопросы от модераторов, обмен опытом, внесение предложений

визит участников в АО «СО ЕЭС» и экскурсионный тур по Москве.

Иностранные специалисты, из числа участвующих в Коллоквиуме экспертов, представили специальные доклады на круглом столе. Джованна Дондоссола, Италия (рис. 12), выступила на тему «Применение стандартов мониторинга для повышения безопасности энергосистем». А Нарендра Сингх Содха из Индии (рис. 13.) представил доклад «Инновационный мониторинг Smart Grid (умной сети) транспорта ЭЭ с использованием систем векторных измерений, систем защиты и управления».

Рис. 12. Джованна Дондоссола, Италия

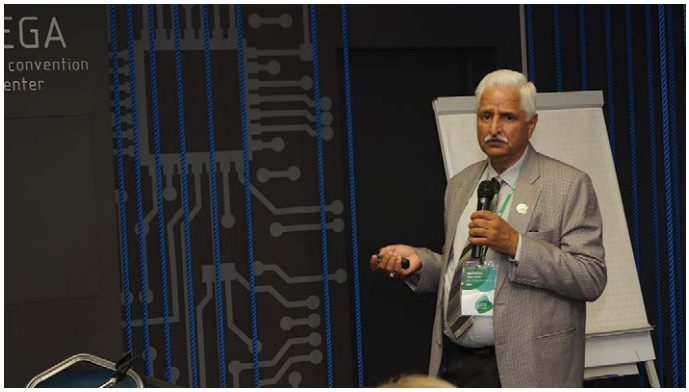


Рис. 13. Нарендра Сингх Содха, Индия

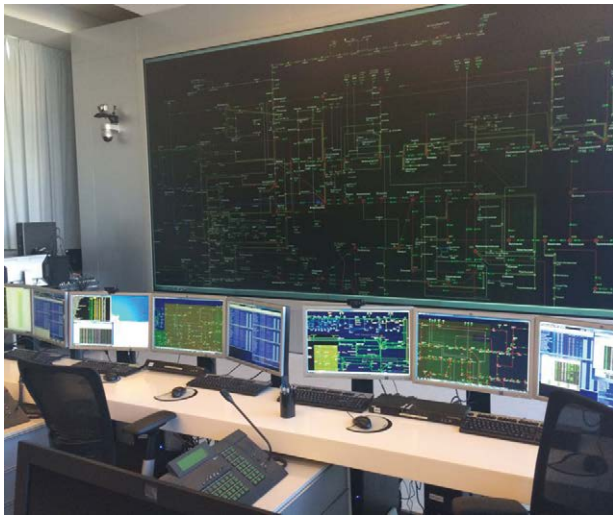
Деловую программу коллоквиума в формате круглого стола продолжило обсуждение таких актуальных тем, как «Интернет вещей» и «Кибербезопасность в энергетике». Важно отметить, что круглый стол по кибербезопасности систем технологического управления посетили представители ключевых отраслевых предприятий нашей страны – от Минэнерго до специальных институтов из ведомства силовых структур.

Общение проходило активно, в живой обстановке (рис. 14). Участники обсудили пути решения задач сертификации продукции на соответствие требованиям информационной безопасности. Спикерами были предложены варианты решения этих задач методами шифрования и рассмотрены основные аспекты этого вопроса. Представитель Министерства энергетики РФ Ирина Васильева в своём докладе «Цифровизация электроэнергетики» продемонстрировала аудитории картину нового «цифрового энергомира» и озвучила планы Минэнерго по созданию основы «цифровой энергетики».

Вице-президент Национальной ассоциации промышленного интернета Сергей Попов рассказал о целях создания ассоциации, выполняемых ею задачах и текущих приоритетах, а также об особенностях реализации Технологии промышленного интернета 4.0 в России.

Эксперт отдела внедрения и развития систем информационной безопасности Центра кибербезопасности и защиты «Ростелекома» Николай Ковтун поделился опытом разработки и внедрения облачных сервисов на основе решений компании.

Рис. 14. Дискуссия в рамках «круглого стола»



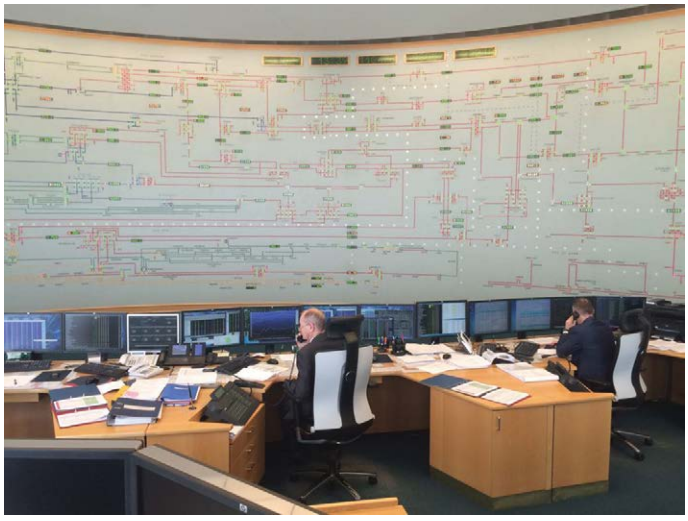


Рис. 15. В главном диспетчерском центре управления АО «СО ЕЭС»

Максим Никандров, директор ООО «Интеллектуальные сети» и руководитель проблемной рабочей группы (ПРГ) № 2 «Кибербезопасность РЗА и систем управления современных объектов электроэнергетики», рассказал об опыте и о результатах деятельности этой смешанной рабочей группы подкомитетов РНК СИГРЭ D2 и B5.

В финале мероприятия выступил руководитель рабочей группы № 4 «Обеспечение информационной безопасности для систем связи и управления в электроэнергетике» Подкомитета D2 РНК СИГРЭ Владимир Карантаев. Он доложил об особенностях правового регулирования в области информбезопасности на территории Российской Федерации и подвёл итоги дискуссии, предложив формулировки, которые будут представлены в виде официального документа в Минэнерго.

По окончании круглых столов участники Коллоквиума побывали в главном диспетчерском центре управления АО «СО ЕЭС» – «рулевой рубке» Единой энергосистемы Российской Федерации. В ходе технического визита члены Исследовательского комитета D2 CIGRE посетили главный диспетчерский щит и центр тренажёрной подготовки персонала (рис. 15). Гости ознакомились с историей Системного оператора, его ролью в формировании современной национальной энергетики, перспективами развития, а также с особенностями оперативно-диспетчерского управления в Российской Федерации. Участникам Коллоквиума представили уникальную систему подготовки персонала АО «СО ЕЭС», позволяющую поддерживать высокую квалификацию диспетчеров и специалистов технологического блока компании.

Программу финального дня Коллоквиума завершила пешеходная экскурсия по центру Москвы, организованная в рамках культурной программы мероприятия.

«РТСофт» на Международном военно-морском салоне – 2017

По материалам АО «РТСофт»

Компания «РТСофт» приняла участие в Международном военно-морском салоне (МВМС-2017), который проходил с 28 июня по 2 июля в Санкт-Петербурге. Компания представила отечественные сверхнадёжные бортовые системы, решения по кибербезопасности и энергоэффективности и специализированное ПО для судостроения и спецприменений.

Международный военно-морской салон – масштабный форум в сфере судостроения, морской техники и спецприменений, проводимый раз в два года в Санкт-Петербурге. Это площадка для обсуждения вопросов развития производственного и научно-технического сотрудничества, продвижения продукции отечественных производителей и формирования новых, перспективных заказов. Компания «РТСофт» традиционно участвует в этом ключевом событии, демонстрируя широкий спектр продуктов, решений и инженерно-конструкторских сервисов (рис. 1).

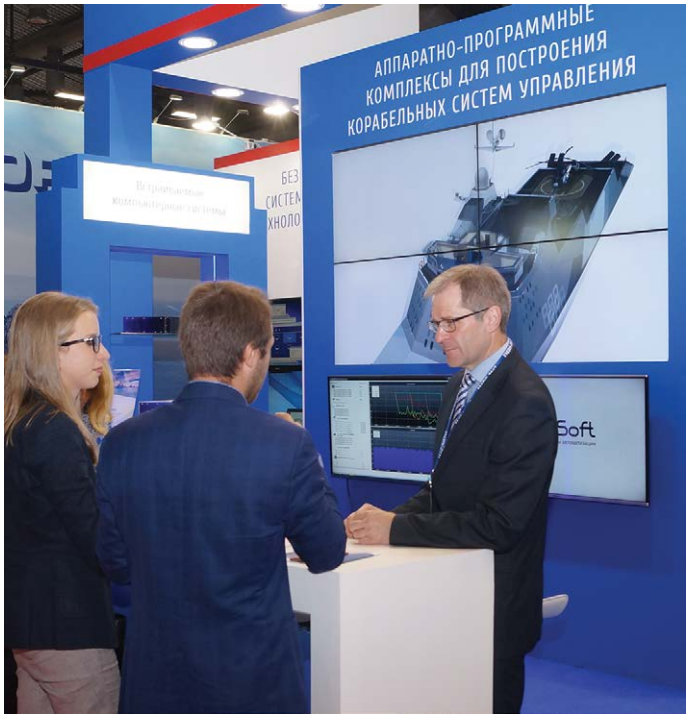


Рис. 1. Стенд «РТСофт»

В частности, высокий интерес у посетителей стенда «РТСофт» вызвал целый ряд модификаций **аппаратно-программных комплексов универсальной вычислительной платформы (УВП) «Интегро»** (рис. 2), предназначенной для построения интегрированных мостиковых систем, автоматизированных систем управления и обработки информации надводного, подводного размещения, прибрежной инфраструктуры и предприятий судостроения. Это универсальное решение **отвечает повышенным требованиям к надёжности, максимальной производительности в полевых условиях при жёстких условиях эксплуатации**, адаптивности функционала, вычислительной мощности и кибербезопасности. УВП «Интегро» построена на основе открытого технологического стандарта и имеет модульную структуру. Вычислительные и коммуникационные характеристики позво-

ляют применять её в качестве отдельного управляющего компьютера, строить системы с резервированием информации, формировать структуры центров обработки данных, а также создавать высокопроизводительные автоматизированные рабочие места операторов или серверы для обработки больших объёмов графической информации.

Повышенным вниманием специалистов пользовались российские безвентиляторные промышленные компьютеры высокой надёжности серии BLOK для ответственных систем с длительным жизненным циклом. Разработанный в рамках программы импортозамещения, BLOK базируется на ультрасовременных достижениях в области микропроцессорной техники, сетевых решений, мультимедийных интерфейсов, систем электропитания и производства точной 3D-механики. Встроенный модуль в стандарте COM Express на базе мобильных процессоров Intel Core и Xeon даёт гарантию совместимости, высоких показателей производительности и энергоэффективности. Его архитектура имеет всё необходимое для локального и удалённого мониторинга состояния, а безвентиляторный кондукционный дизайн обеспечивает абсолютно бесшумную работу.

Особое место в линейке передовых разработок «РТСофт» занимают **решения по кибербезопасности**. Предприятия судостроения, кораблестроения, сферы специальных и ответственных применений сегодня особо заинтересованы в устойчивом, стабильном функционировании объектов информационной и технологической инфраструктуры и предотвращении рисков от деструктивных информационных воздействий на них. Эти задачи призван решать программно-технический комплекс предотвращения угроз кибербезопасности, разработанный «РТСофт». Его функционал был продемонстрирован посетителям нашего стенда.

Ещё одно актуальное решение «РТСофт» для организации защищённой обработки конфиденциальных данных на объектах критически важных информационно-управляющих систем – сертифицированный программный комплекс средств защиты «Плато-РТ» – было представлено в экспозиции компании. Важно отметить, что «РТСофт» как разработчик решения по кибербезопасности имеет ряд преимуществ перед конкурентами – компания, разрабатывая промышленное решение для конечного заказчика, в течение ряда лет опирается на деятельность кафедры защиты информации МГТУ им. Баумана. Это сотрудничество позволило создать передовое и на сегодняшний день уникальное решение с двухконтурной системой защиты. Внутренний контур встроен в операционную систему, а внешний работает на уровне гипервизора безопасности. Это позволяет взять под контроль все категории пользователей и гарантированно нейтрализовать внутреннего нарушителя, в том числе привилегированного пользователя, например администратора. Это имеет большое значение, особенно для объектов, где возможная утечка информации нанесёт существенный ущерб.

Отдельно стоит отметить **инновационное решение «РТСофт» в области энергоэф-**

Рис. 2. Универсальная вычислительная платформа «Интегро» на стенде «РТСофт»

Рис. 3. ИУС AMIGO для управления микросетью (microgrid) судостроительного предприятия

Рис. 4. Модульная программная платформа дополненной реальности RtsReality

Рис. 5. Стенд издательства «Космоскоп»

фективных технологий и микросетей Smart Grid семейства AMIGO, предназначенное для судостроительных предприятий. Посетители смогли увидеть модель такого предприятия, в которой были представлены все возможные варианты энергоснабжения (внешняя сеть, микротурбина, накопитель и даже солнечные панели), а также регулируемые и нерегулируемые типы нагрузки (рис. 3). Все элементы объединены в единую систему и за счёт правильного выбора оптимальных режимов позволяют **существенно повысить энергоэффективность предприятия и сэкономить средства при оплате электроэнергии**. Такой эффект достигается с помощью возможности прогнозирования стоимости электроэнергии, учёта стоимости топлива для турбины, использования прогноза погоды и других параметров. Интеллектуальная информационно-управляющая система AMIGO на основе всей поступающей информации делает оптимальный прогноз по использованию имеющегося оборудования и управляет его работой в автоматическом, полуавтоматическом или ручном режимах.

Внимание посетителей выставки привлекала **демонстрация информационной системы нового поколения RtsReality для транспорта с поддержкой дополненной реальности** (рис. 4)**.** Эта модульная программная платформа позволяет использовать преимущества дополненной реальности на мобильных устройствах: с помощью бортовой камеры создаётся обширное информационное пространство, предоставляющее пользователям новые широкие возможности взаимодействия с объектами реального мира. Так, у пользователя системы, например пассажира, появляется доступ к навигационным данным, информации о близлежащих зданиях и другой полезной информации, которая накладывается на изображения объектов в видео, транслируемом в реальном времени. Таким образом, **технология дополненной реальности открывает новые перспективы для развития бизнеса в самых разных отраслях.**

Также на стенде компании расположились **площадки учебного центра «РТСофт»**

с предложением учебных программ, отражающих новейшие тенденции и передовые разработки компании в области промышленной автоматизации и встраиваемых компьютерных технологий, и **издательства «Космоскоп», выпускающего уникальные исторические, научные и научно-популярные издания**. Среди них – «Мировая пилотируемая космонавтика» под редакцией лётчика-космонавта Ю. М. Батурина, четырёхтомник «Ракеты и люди» академика Б. Е. Чертока, трилогия «Ракетчики подводных глубин» П. И. Качура и другие бестселлеры издательства.

За пять дней работы салона на стенде «РТСофт» побывали сотни посетителей, которые проявили высокий интерес к представленным на салоне решениям компании. Профессионалы в области судостроения, моряки, специалисты в области спецприменений, судоходства, средств связи и информационных технологий смогли обсудить все интересующие вопросы с экспертами «РТСофт» и заложить фундамент для развития дальнейшего сотрудничества.

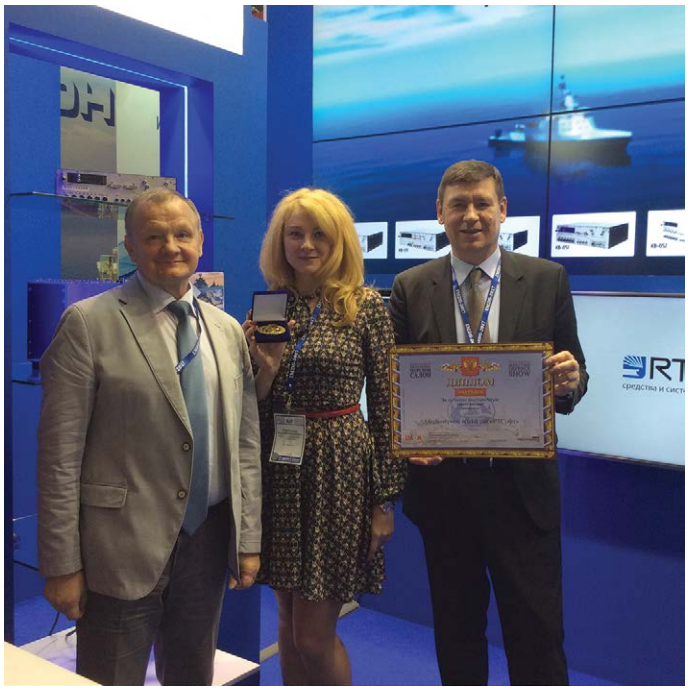


Рис. 6. Стенд АО «РТСофт» удостоился высокой награды – медали и диплома лауреата «За лучшую выставочную экспозицию»

И в заключение приятно отметить, что стенд АО «РТСофт» удостоился высокой награды – **медали и диплома лауреата «За лучшую выставочную экспозицию».**

НОВОСТИ

Испытания российских машин серии BLOK на платформе Intel 7-го поколения успешно завершены

Специалисты «РТСофт» успешно завершили процесс валидации новейших мобильных встраиваемых компьютерных платформ компании Intel 7-го поколения с кодовым наименованием Kaby Lake для собственной программы выпуска безвентиляторных промышленных компьютеров BLOK Industrial (ЛКЖТ.466259.012ТУ О1) и BLOK Rugged (ЛКЖТ.466259.023ТУ О1).

Успех валидации позволяет команде «РТСофт» и её партнёрам вывести на рынок ультрасовременное инженерное решение с опережением или в полном соответствии с темпами развития мировой компьютерной индустрии в примерно аналогичных классах промышленного и специального компьютерного оборудования для энергетики, транспорта, промышленности и специальных приложений.

В качестве целевых платформ валидации использовались топовые версии Core i7-7820EQ с чипсетом QM175 и Xeon E3 1505M v6 с графикой P630 и чипсетом CM238.

Машины BLOK успешно прошли все стадии функционального и краш-тестирования в рамках операционных систем Windows и Linux, подтвердив полное соответствие требованиям конструкторской документации.

По словам директора по развитию бизнеса «РТСофт» Александра Ковалёва, «валидация мобильных платформ Kaby Lake для лине-

НОВОСТИ

ек BLOK – это необходимый и естественный процесс поддержки конкурентоспособности собственных продуктов в контексте роста производительности, ценовой и энергоэффективности, функциональности и длительности жизненного цикла, а также уверенности наших клиентов в разумности инвестиций в классные отечественные платформы серий BLOK».

Седьмое поколение мобильных Intel Core и Xeon позволяет сохранить и частично улучшить все основные конкурентные преимущества машин серии BLOK, в том числе для задач кибербезопасности.

Архитектура машин серии BLOK построена на модульной модернизируемой платформе COM Express Type 6 (PICMG COM.0) на базе встраиваемых (embedded) микропроцессоров Intel Core и Xeon 4–7-го поколений. Она позволяет гарантировать актуальность свойств и использовать все лучшие мировые инструментальные средства разработки для реализации важнейших инженерных и бизнес-концепций в IT-индустрии для различных рынков: IoT, IIoT, Fog Computing, Cloud Computing, Industrial Revolution 4.0 и др.

Критично повышает конкурентоспособность машин возможность использовать наиболее актуальные технологии в разработке продвинутых гетерогенных и графических приложений: OpenCL 2.1, MS C++ AMP, DirectX 12, OpenGL 5.0 и других.

Благодаря открытой и стандартной архитектуре гарантируется великолепная совместимость с самым современным системным ПО класса Linux, Windows, ОСРВ и гипервизорами. Компьютеры серии BLOK способны функционировать в стандартном (-10...+50 °C) и расширенном (-40...+70 °C) температурных диапазонах.

Машины обеспечены высоким уровнем сертификационной и лицензионной поддержки. Имеют сертификаты ГОСТ Р и Таможенного союза, СТ-1 ТПП вместе с сертификатами и лицензиями АО «РТСофт»: TÜV ISO 9001-2008, ФСТЭК, Ростехнадзора, Минпромторга на разработку ВВТ и др.

По требованию партнёров изделия обеспечиваются большим числом удобных поддерживающих сервисов: инженерной кастомизации аппаратного и программного обеспечения, СИиСП, а также отраслевыми аккредитациями и сертификациями. Предметом сервисов могут быть UEFI/BIOS, подсистемы ввода-вывода, готовые BSP в целевые операционные системы, протокольные стеки, системы встроенного тестирования и т. п.

Машины BLOK на базе 7-го поколения процессоров Intel доступны для заказа и бесплатного тест-драйва с длительной фирменной гарантией 3, 4 или 5 лет.

Дополнительную информацию о компьютерах серии BLOK можно получить на обновлённом сайте http://blok.rtsoft.ru/ или в офисах компании «РТСофт».

НОВОСТИ

Модули COM Express от Kontron на базе Intel Core 7-го поколения стали серийными

АО «РТСофт» и международный холдинг Kontron AG объявляют о старте продаж новых «компьютеров-на-модуле» в формате COM Express: COMe-bKL6 (COM Express basic) и COMe-cKL6 (COM Express compact). Оба модуля обеспечивают более высокие показатели производительности, энергоэффективности и безопасности благодаря новейшим процессорам Intel Core и Intel Xeon 7-го поколения (кодовое название – Kaby Lake).

Новинки включены в актуальную программу Kontron Security Line, которая предоставляет разработчикам целевых систем комплексный набор средств обеспечения кибербезопасности. Программа поддержана развитым пакетом возможностей, основанных как на аппаратных, так и на программных решениях.

В новых модулях используется существенно более мощная графика Intel HD P630/630, поддерживающая до трёх независимых дисплеев с разрешением до 4K. Широкий диапазон доступных процессоров, от бюджетного Celeron до высокопроизводительных процессоров Intel Core i7 и Xeon E3, предоставляет пользователям максимальную гибкость при выборе оптимального решения.

Оба модуля поддерживают новейшую технологию Intel Optane – энергонезависимое решение на основе технологии памяти 3D X-Point. Память этого типа работает существенно быстрее, чем флеш-память NAND, увеличивает количество циклов перезаписи и способна обеспечить практически мгновенный запуск приложений. Это чрезвычайно важные преимущества для высокопроизводительных вычислений или обработки изображений практически для любых рынков встраиваемых компьютеров.

Модули поддерживают до 32 Гбайт памяти DDR4-2400 с режимом ECC в старших версиях. Обеспечена работа как в стандартном для промышленных приложений диапазоне температур (от 0 до 60 °C), так и в расширенном (от –40 до 85 °C)

Использование новых модулей гарантирует разработчикам максимум свободы и удобства в выборе и операционных систем, и инструментальных средств разработки.

Модули доступны для заказа. Планируемый срок коммерческой доступности – 7 лет, что делает их великолепной платформой для разработки любых критичных к надёжности приложений, требующих длительного жизненного цикла.

Модули COMe-bKL6 на базе Intel Core i7/i5 и Xeon E3 v6 уже валидированы для отечественных промышленных платформ BLOK Industrial и BLOK Rugged: http://blok.rtsoft.ru/.

С дополнительной информацией о COMe-bKL6 и COMe-cKL6 можно ознакомиться на сайте www.kontron.com и в офисах компании «РТСофт», стратегического партнёра холдинга Kontron в России и странах СНГ.

Беспроводные информационно-развлекательные **системы**

По материалам Контрон

В статье даётся описание технологий построения информационно-развлекательных систем, устанавливаемых на борту пассажирских самолётов (IFE – InFlight Enteraiment Systems). Это безопасные недорогие и простые в установке платформы, открывающие новые возможности для получения дохода авиакомпаний и расширения спектра предлагаемых пассажирам услуг. Беспроводные технологии существенно расширяют «традиционный» функционал IFE-систем, позволяя обеспечить выход в Интернет как на земле (через 3G/4G LTE), так и в полёте (воздух–земля или воздух–спутник).

Оснащение воздушного судна оборудованием для доступа в Интернет – это не просто дополнительный сервис для пассажиров, но и дополнительные технические возможности для получения данных о полёте в режиме реального времени, что, в конечном счёте, делает пребывание на борту более комфортным. С развитием технологии «Интернета вещей» (IoT – Internet of Things) появляется возможность отслеживать критические данные при помощи новых программных решений. В результате такого нововведения авиаперевозчики смогут повысить качество обслуживания, сократить расходы за счёт экономии времени и оптимизировать процесс принятия решений при анализе больших

объёмов данных. Для пассажиров же появляются новые услуги на борту – начиная от Интернет-магазинов и систем онлайн-бронирования, заканчивая информацией о пункте назначения, информацией о полёте в режиме реального времени и удобной возможностью вести переписку с другими пассажирами в салоне. Всё это даёт авиакомпаниям новые способы получения дохода и расширяет спектр предлагаемых пассажирам услуг. Внедрение беспроводных технологий ведёт к снижению эксплуатационных расходов – в кабине отсутствуют лишние провода, в результате значительно снижается масса воздушного судна и упрощается развёртывание и техобслуживание IFE-системы.

Возможности систем развлечений и связи: сочетание удобного сервиса и широких возможностей монетизации

Доступ в Интернет на борту позволяет авиакомпании повысить качество обслуживания клиентов. С реализацией этой идеи на борту самолёта появляется беспроводная сеть связи, доступная для каждого пассажира и члена экипажа: можно подключаться к бортовому серверу с помощью своих ноутбуков, смартфонов или планшетных ПК. Беспроводные платформы для воздушного транспорта становятся всё лучше, и уже сейчас существуют экономически эффективные и простые решения, которые дают возможность обеспечить подключение к Wi-Fi в салоне самолёта. Авиакомпании получают новые источники дохода, дифференцируют свои услуги по цене и расширяют линейку продуктов для развлечения пассажиров в полёте.

Ключевое значение для эволюции IFE имеет простота организации сети Wi-Fi. Для снижения затрат и стоимости услуг, а также удовлетворения растущих ожиданий пассажиров (так как они ожидают качества услуг не хуже чем «на земле») потребуются новые решения. Это довольно сложный процесс. Полный цикл внедрения IFE может занять до двух лет – сюда входит время, затрачиваемое на оценку технологий, утверждение со стороны соответствующих властных и контролирующих органов (FAA/EASA/CAAC), STC, лётные испытания и непосредственно внедрение на борт самолёта. Исходные данные постоянно меняются, но применение стандартных решений и предварительно сертифицированных систем значительно ускоряет развёртывание системы. Совместив работу стандартных беспроводных точек доступа и бортовых серверов, авиакомпании могут быстро и экономически выгодно создать современную и высокоэффективную структуру беспроводного IFE.

Поддержка нескольких клиентов

Основная задача состоит в предоставлении возможности всем пассажирам смотреть видео онлайн. Однако точки доступа стандартов 802.11a/b/g пока не в состоянии поддерживать высокую пропускную способность для большого количества пользователей. Теоретические скорости передачи для разных стандартов приведены в таблице. При этом следует помнить, что фактические скорости передачи данных значительно меньше теоретических стандартов (см. данные о производительности).

Теоретическая скорость передачи данных для различных стендартов

СТАНДАРТ 802.11	ТЕОРЕТИЧЕСКАЯ СКОРОСТЬ ПЕРЕДАЧИ ДАННЫХ
802.11 a/b/g	54 Мбит/с
802.11n	600 Мбит/с
802.11ac	1300 Мбит/с

Рис. 1. Гибкая система CWAP CAB-N-CONNECT™ A100 может передавать данные по локальной сети (CWLU) или работать как терминал беспроводной локальной сети (TWLU). Встроенные антенны устраняют необходимость использования внешних антенн, а также позволяют упростить процесс установки удалённых внешних антенн

Встроенные в кабину беспроводные точки доступа (CWAP – Cabin Wireless Access Points) (рис. 1) созданы по последним стандартам и позволяют организовать высокопроизводительную беспроводную сеть на борту воздушного судна. Основанные на семействе изделий Cab-n-Connect производства Kontron, эти точки доступа уже доказали свою эффективность в полёте и прошли сертификацию DO-160. Используя Cab-n-Connect, авиакомпании получат выгоду, положительные отзывы и довольных пассажиров.

Поскольку в системе используется последний стандарт IEEE 802.11, точка доступа Cab-n-Connect A100 802.11ac от Kontron имеет значительно более высокую пропускную способность, в отличие от более ранних решений стандарта 802.11n. Kontron CWAP поддерживает также технологию Multiple-Input Multiple-Output (MIMO), базирующуюся на двух отдельных передатчиках Wi-Fi (частотой 2,4 и 5 ГГц), которая поддерживает три пространственных потока одновременной передачи данных на устройство и модуляцию 256 QAM. Это приводит к существенному повышению эффективности в использовании имеющегося канала. Ещё одно преимущество – встроенные внутренние антенны. Такое решение упрощает установку точки на борт самолёта и повышает общую надёжность. Если же в конкретном месте установки требуется наличие внешних антенн, система может быть дооснащена внешними антеннами для работы на каждой частоте (2,4 и 5 ГГц).

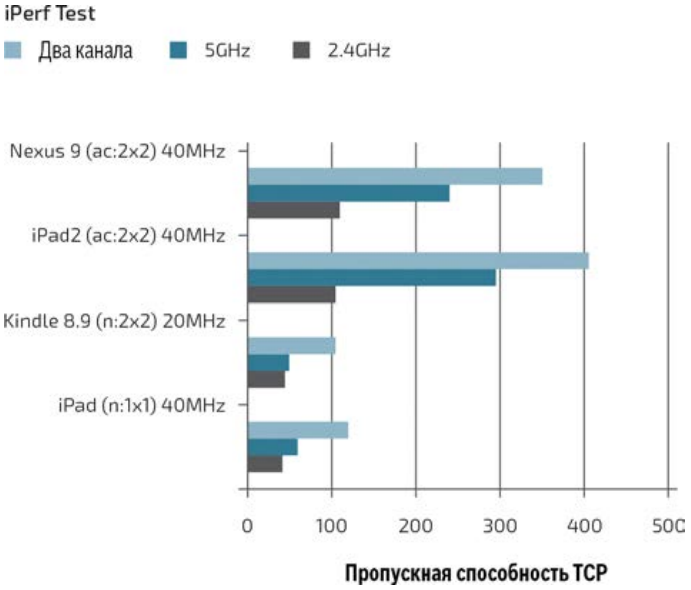


Рис. 2. Результаты тестирования пропускной способности гаджетов с использованием 802.11ac CWAP

Проверка пропускной способности

Для получения достоверных результатов тестирования компания Kontron создала лабораторию System Integration Lab (SIL), предназначенную для моделирования среды на борту воздушного судна. Эта лаборатория позволяет создавать контролируемую среду для получения воспроизводимых результатов, и с её помощью можно отслеживать улучшения продукта после каждого обновления. Лаборатория также прекрасно подходит для клиентов, позволяя им тестировать свои программные приложения и настройки системы перед её установкой на борт воздушного судна. Kontron регулярно тестирует новые гаджеты, планшетные ПК, смартфоны, обновления их ПО. Это придаёт уверенность клиентам Kontron в современном качестве IFE-систем, столь востребованное в динамично меняющемся мире авионики.

Результаты тестирования пропускной способности с использованием 802.11ac CWAP представлены на рис. 2.

Данный тест выполнялся с помощью программы iPerf, используемой для определения пропускной способности по протоколу TCP. Kontron протестировал несколько планшетов 802.11n и 802.11ac. Результаты показывают, что CWAP 802.11ac обеспечивают в 4–5 раз более высокую пропускную способность на частоте 5 ГГц при использовании планшета 802.11ac по сравнению с 802.11n. Результаты приведены для 20 МГц и 40 МГц; лучшие результаты могут быть достигнуты на частоте 80 МГц при работе с клиентским устройством 3x3 (ноутбуком), однако есть ограничения на количество устанавливаемых точек доступа на борт воздушного судна.

Проверка видеотрансляции с клиентами 802.11n

Kontron провёл тест с устройством 802.11n, используя Cab-n-Connect A100 для трансляции

видео в формате HD на скорости 1 Мбит/с (рис. 3).

Этот тест помог определить максимальное количество трансляций видео, которое может поддерживаться одной точкой доступа Cab-n-Connect A100. Следует отметить, что фактическая скорость передачи данных каждого потока равна 1,2 Мбит/с, так как в передачу входят файлы H.264.

Результаты показывают, что система может поддерживать более 75 клиентских устройств стандарта 802.11n. Однако результаты тестов сильно зависят от производительности клиентского устройства. Более производительные устройства позволяют достичь лучших результатов (например, устройства 802.11n или ноутбуки 3x3). Чтобы результаты были максимально приближены к реальности, Kontron отобрал наиболее часто используемые планшетные ПК.

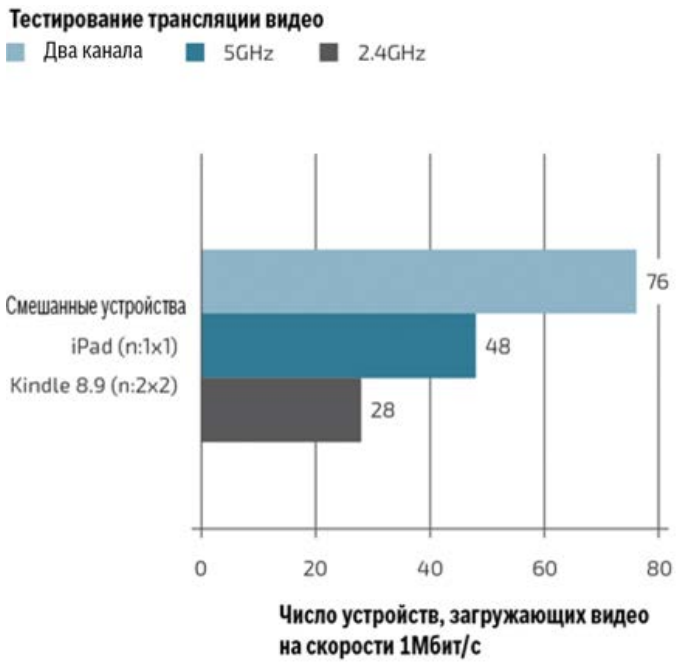


Рис. 3. Тестирование трансляции видео на смесь клиентских устройств стандарта 802.11n

Проверка видеотрансляции с клиентами 802.11ac

Тест устройств 802.11ac проводился в лаборатории SIL с использованием Cab-n-Connect A100 и трансляцией видео в формате HD со скоростью 1 Мбит/с. Как и в тесте устройств 802.11n, целью было определить максимальное количество трансляций видео, которое может поддерживаться одной точкой доступа Cab-n-Connect A100. Следует отметить, что фактическая скорость передачи данных каждого потока равна 1,2 Мбит/с, так как в передачу входят также файлы H.264.

Результаты данного теста (рис. 4) показывают, что Cab-n-Connect A100 поддерживает более 100 устройств стандарта 802.11ac. Однако результаты тестов сильно зависят от производительности клиентского устройства. Более производительные устройства позволяют достичь лучших результатов.

Повышение качества услуг с помощью совместимости и адаптивности

Следует отметить, что Cab-n-Connect A100 имеет обратную совместимость с более ранними стандартами 802.11 за счёт использования двух радиоканалов. Точка доступа Cab-n-Connect A100 поддерживает частоты 2,4 и 5,0 ГГц и совместима со стандартами 802.11 a/b/g/n, тем самым позволяя авиакомпаниям модернизировать уже существующие решения IFE. Версия 802.11ac обеспечивает гибкость, необходимую для работы: может работать как блок беспроводной локальной сети в кабине воздушного судна (CWLU) или как терминальный блок беспроводной локальной сети (TWLU).

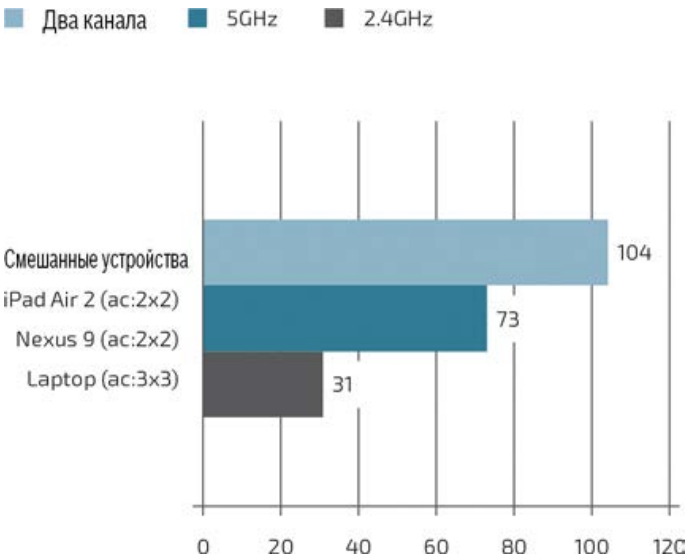


Рис. 4. Тестирование трансляции видео на смесь клиентских устройств стандарта 802.11ac

Сетевая безопасность самолёта

Для систем «Интернета вещей» безопасность – одна из важнейших проблем, и особенно это касается сети на борту воздушного судна. Есть два основных аспекта безопасности, требующих внимания: безопасность на борту воздушного судна и безопасность самой системы IFE.

Безопасность на борту воздушного судна

Разворачиваемая на борту воздушного судна система IFE обычно получает сертификат безопасности (Design Assurance Level – DAL) уровня E или D по руководствам FAA DO-254 (аппаратное обеспечение) и DO-178 (программное обеспечение). Уровень E присваивается, когда неисправности не влияют на безопасность воздушного судна, а уровень D присваивается при наличии незначительного влияния на безопасность. Таким образом, система IFE устанавливается и сертифицируется так, что не контактирует с остальными подсистемами воздушного судна. Это исключает любую возможность ущерба оборудованию воздушного судна, к которому подключена система IFE. Например, физическое подключение к шине данных ARINC 429 может быть настроено в режим «только чтение» для приёмника, подключённого к серверу IFE. Это позволяет получать данные о высоте и местоположении воздушного судна и составлять карту полёта в режиме реального времени. В этом случае система IFE может только считывать данные и не может передавать команды или заменять данные в подсистеме.

Безопасность беспроводной точки доступа IFE

Другой аспект безопасности касается самой системы IFE, так как любая беспроводная сеть может подвергаться сетевым атакам. Чтобы защититься от этого, Cab-n-Connect A100 CWAP имеет новейшие средства безопасности корпоративного уровня и построена на базе операционной системы WiNG 5. Эта операционная система имеет надёжную распределённую архитектуру, которая позволяет улучшить качество услуг, безопасность работы точек доступа на воздушном судне. Система работает надёжнее, и маршрутизация выполняется эффективнее.

Система имеет интеллектуальный виртуальный контроллер, который оптимизирует работу сети для сохранения качества потокового видео, одновременно обеспечивая безопасность беспроводной сети самолёта и защищая её от несанкционированного доступа. Брандмауэр второго уровня на точках доступа представляет собой дополнительный уровень защиты данных при их передаче. Точка доступа Cab-n-Connect A100 автоматически обнаруживает любые угрозы сети, начиная от попыток взлома и заканчивая уязвимостями сети.

Например, встроенное средство AirDefense Wireless Intrusion Detection and Protection (Обнаружение и защита от сетевых проникновений) (WIPS) защищает сеть от атак. WIPS определяет MAC-адрес спуфинга, когда взломщик во время атаки притворяется авторизованным устройством. AirDefense WIPS выявляет повторные атаки и реагирует, если количество проникновений превышает заданный порог в пределах некоторого диапазона времени. Система также может генерировать сигналы тревоги или отправлять SNMP-ловушки, предупреждая системы управления о нарушении безопасности.

Кроме того, система может быть настроена таким образом, чтобы атакующее устройство заносилось в чёрный список, и все поступающие от него данные будут отфильтровываться, пока устройство не будет удалено из списка. Также Cab-n-Connect A100 имеет функцию IP-фильтрации, преобразования сетевых адресов (NAT), управление доступом по порту, IPSec (шифрование пакетов точка-точка по Ethernet), протокол безопасности AAA (RADIUS).

Больше интеллекта

Kontron наделил Cab-n-Connect A100 невероятными интеллектуальными возможностями. Каждая точка доступа имеет распределённую архитектуру и за счёт этого автоматически выбирает оптимальный маршрут для всего трафика. Функция SMART-RF интегрирована в ОС WiNG 5 и позволяет точке

доступа автоматически оптимально адаптироваться к изменениям в радиочастотной среде, поддерживая производительность и устраняя пробелы в сетевом покрытии. Она чувствует потенциальные помехи от Wi-Fi и не-Wi-Fi источников (например, неисправные антенны или неполадки соседних точек доступа) и по мере необходимости автоматически регулирует каналы и их мощности. Кроме того, ОС WiNG 5 смещает плоскость управления к краям. Это решение уменьшает помехи точек, регулирует каналы и их мощности в зависимости от текущих условий и выбирает оптимальные маршруты. В результате передача видео и данных работает без сбоев, покрытие стабильно, а помехи гасятся. CWAP равномерно распределяет клиентов по точкам доступа и полосам частот для достижения максимальной общей производительности сети для всех пользователей.

Такой подход позволяет уйти от привязки клиента к точкам доступа и повышает общую производительность сети. Функция Roaming Assistance обеспечивает бесшовное соединение клиентов и улучшает общую производительность сети. Функция 802.11 Fast Roaming позволяет быстрее переключать клиентов между точками доступа. Помимо этих усовершенствований, для оптимизации канала используются модифицированные способы формирования диаграммы направленности передачи данных между точкой доступа и клиентским устройством, что повышает скорость передачи данных. Клиентские устройства работают быстрее и экономят заряд батареи, что, несомненно, повышает качество обслуживания. Все перечисленные особенности позволяют увеличить полноту использования полосы пропускания, транслировать видео в формате HD и передавать другие данные пассажирам воздушного судна.

LTE как средство модернизации сети

Подключение по LTE – ещё один вариант модификации сети, который авиакомпании могут использовать, чтобы порадовать пассажиров и повысить качество услуг. Устройство ACE Flight 4600 семейства Kontron ACE Flight Server оптимизировано для работы с медиаданными и имеет 4G/LTE-модем для подключения к сети, когда воздушное судно находится на земле. Кроме того, в линейке ACE Flight Server есть сверхкомпактные системы для работы в качестве многофункционального загрузчика данных через 4G/LTE, включая средства управления хранимым контентом и контроллер IFE. Такая система, опционально оборудованная Wi-Fi, может обеспечить максимальное количество сценариев загрузки данных. В результате авиакомпании получают широкий выбор безопасных вариантов загрузки таких данных, как фильмы, музыка, электронные книги, игры и многое другое. Экипаж и обслуживающий персонал на земле может получать данные о полёте. Система поддерживает до четырёх наземных модемов 4G/LTE, которые могут быть объединены для обеспечения высокой пропускной способности. В этой конфигурации становится возможным быстро совершать обновления, когда воздушное судно находится в ангаре. В среднем (плюс-минус отклонения, связанные с загрузкой сети и подключением), менее чем за 30 минут можно загрузить около 10 Гбайт данных, если на все 4 модема будет установлена скорость 40 Мбит/с. После подключения к сети система автоматически координирует загрузку данных на бортовой сервер через GbE. Эта гибкая система имеет опциональную возможность работы через

Рис. 5. Сервер Kontron ACE Flight 4600 имеет двухъярусный процессор Intel Core 17 1,5 ГГц, 16 Байт DDR3 и до 1,8 Тбайт SSD. Система отвечает современным требованиям к производительности, программному обеспечению и доступу к данным. Создана специально для работы в самолёте, формфактор ARINC 600 4MCU, 6 RX-каналов ARINC 429 и встроенный модем. Система энергоэффективная, лёгкая, герметичная и имеет естественное охлаждение

Wi-Fi для загрузки данных в качестве терминала (TDL) или беспроводного подключения к другим устройствам.

Обеспечение стабильной и надёжной работы

Разработка оптимальной беспроводной системы IFE – задача непростая, требующая всестороннего понимания работы беспроводных сетей, радиопередачи, конструкции оборудования и работы воздушных судов. Семейство устройств ACE Flight – это готовые решения для организации высокоскоростных сетей за счёт интеграции технологий и функциональности, обеспечивающих надёжную производительность. Благодаря герметичной конструкции с естественным охлаждением система сертифицирована по стандарту DO-160G и выполнена в формфакторе ARINC 600 для авиационного радиоэлектронного оборудования (рис. 5).

Сервер ACE Flight 4600 также усовершенствован благодаря хранению данных на SSD-носителе объёмом несколько терабайт, новейшим процессорам Intel, а также средствам для разработки программного обеспечения (SDK – Software Development Kits), которые отвечают современным растущим требованиям и помогают ускорить процесс разработки. Платформа может управлять веб-серверами для экипажа и пассажиров, работать с приложениями для авионики, такими как приложения для лётного техобслуживания, серверы соединений, серверы беспроводного контента и IFE-серверы.

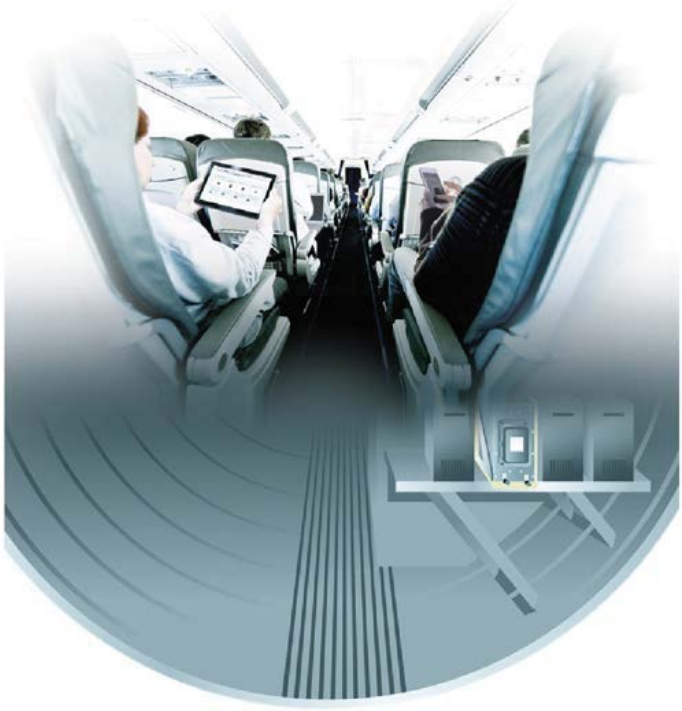


Рис. 6. Высокий уровень интеграции от Kontron (управляемый коммутатор и расширяемое хранилище) позволяет разрабатывать мощные системы IFE, ориентированные на сервисы. Беспроводные решения Kontron для гражданской авиации – это экономически выгодный инструмент, позволяющий авиакомпаниям расширить спектр предлагаемых услуг и получать дополнительные доходы

Будь то IFE-системы в новых или в модернизируемых самолётах, сервер ACE Flight 4600 фирмы Kontron прекрасно иллюстрирует, как авиационные серверы общего назначения превратились в один из основных компонентов современных систем IFE. ACE Flight Server встраивается в системы безопасной связи для организации сетей Ethernet с высокой скоростью передачи данных для загрузки видео или других типов потоковых данных. Масштабируемая открытая архитектура системы обеспечивает превосходную гибкость и оптимизацию предоставляемых услуг. Сервер имеет встроенный управляемый коммутатор Ethernet Gigabit L2/L3, а в сочетании с беспроводной точкой доступа разработчики системы IFE могут создать сеть корпоративного класса, проверенную и одобренную FAA (PMA).

Стандартизированные системы Kontron уже доказали свою эффективность в создании надёжных беспроводных сетей и лучшую в своем классе производительность при работе с мультимедийным контентом. Эти системы позволяют снизить затраты и упростить процедуру развёртывания, отвечают жёстким требованиям данной отрасли по габаритам, весу и энергопотреблению. Как ведущий разработчик инновационных технологий для аэрокосмической промышленности Kontron использует свой опыт для вывода экономически эффективных систем развлечения и связи на качественно новый уровень с целью их применения в коммерческой и бизнес-авиации для решения задач по управлению безопасностью полётов и обеспечению комфорта экипажа и пассажиров (рис. 6).

Построение программного обеспечения **управляющих контроллеров** на основе открытых интерфейсов **IPMI, HPI, RedFish**

Сергей Жуков, Игорь Починок | Auriga Inc., НИВЦ МГУ

В статье описывается построение архитектуры программного обеспечения для управляющего контроллера на основе интерфейса SAF HPI. На нижнем уровне управляющий контроллер взаимодействует с интеллектуальными контроллерами по интерфейсу IPMI и с неинтеллектуальными устройствами. На верхнем уровне управляющий контроллер поддерживает интерфейс Redfish и протокол MQTT, которые реализованы поверх интерфейса HPI; эти реализации логически отделены от внутренней архитектуры системы.

Интерфейс IPMI

Интерфейс IPMI (Intelligent Platform Management Interface) – стандарт низкоуровневого интерфейса управляющего контроллера и набор сопутствующих стандартов (протокол IPMB, формат FRU-информации и т. д.), введённый компанией Intel в 1997 году. Версия 2 опубликована в 2004 году и актуальна до сих пор. Представляет из себя набор низкоуровневых команд типа запрос-ответ.

Благодаря поддержке Intel стандарт стал очень популярен и до сих пор многие из существующих контроллеров реализуют IPMI. В частности, стандарт PICMG ATCA (Advanced Telecommunications Architecture), популярный в телекоммуникационной отрасли, основан на IPMI.

В модели IPMI каждый управляющий контроллер несёт на себе набор сенсоров, каждый из которых имеет номер и специальное описание (SDR – Sensor Data Record), значение сенсора может быть прочитано специальной командой. Изменение состояния сенсора может порождать события.

Сенсоры могут быть числовые (нести значение) и дискретные (находиться в одном или нескольких состояниях). Для числовых сенсоров задаются пороги, при выходе за пороги происходят события. Для дискретных сенсоров события происходят при изменении состояния сенсора. События сохраняются в логе (SEL – System Event Log), возможно задавать действия в ответ на события (PEF – Platform Event Filtering).

Интерфейс IPMI в настоящее время устарел и в связи с этим имеет существенные недостатки:

- интерфейс очень низкоуровневый: формат каждой команды детально расписан по байтам и битам;
- длина команды ограничена – максимум 32 байта;
- ограничено количество сенсоров на одном контроллере – максимум 1024 (но, например, для контроллеров ATCA ограничение ещё строже – максимум 768);
- отсутствует единый механизм для управляющих воздействий: изменения состояния сигналов, установки значений управляющих регистров (создаются специальные команды для каждого случая);
- размер значения в команде для числовых сенсоров – 8 бит, вычисление реального значения сенсора производится клиентом с использованием коэффициентов из описания сенсора SDR; в результате реальное значение может иметь большую погрешность.

Интерфейс RedFish

Этот интерфейс разработан организацией DMTF в 2015 году, позиционируется как замена IPMI.

Интерфейс высокоуровневый, использует HTTP и RESTful Web Services для передачи

данных, XML для описания структур данных, JSON как формат данных в процессе передачи.

Используется объектная сетецентричная модель данных. Объекты содержат ссылки на другие объекты, существуют объекты – коллекции объектов. Модель данных описана схемой, которая является неотъемлемой частью стандарта. Схема поставляется в двух форматах: XML и JSON.

Для доступа к данным используются стандартные HTTP-операции (GET, PUT, POST, DELETE), таким образом, клиентский доступ возможен из любого Web-браузера.

Если результатом запроса является массив объектов, возможно чтение этого массива по частям, начиная с любого места.

В то же время схема Redfish ориентирована более на управление серверами и дата-центрами, чем на управление системами в общем случае (например, в телекоммуникационной отрасли). Так, в схеме нет общей модели сенсоров и элементов управления (контролов). Предусмотрен ряд особых случаев: сенсоры температуры, напряжения и скорости вращения вентиляторов (тахометры). Дискретные сенсоры не поддерживаются. В связи с этим построение на основе модели данных Redfish архитектуры программного обеспечения для управляющего контроллера в достаточно общем случае может быть затруднительно.

Интерфейс HPI

HPI (Hardware Platform Interface) – интерфейс доступа к аппаратным платформам, разработанный организацией SAF (Systems Availability Forum). Интерфейс основан на механизме удалённого вызова процедур (RPC).

Интерфейс описывается в терминах типов данных и прототипов функций языка Си, но также существуют привязки к языкам Java и Python.

Модель данных HPI основана на IPMI, но основные недостатки её устранены:

- числовые сенсоры имеют размер 64 бита, тип целый (знаковый или беззнаковый) или плавающий;
- трансляция значений на стороне клиента не требуется, реализация HPI сразу возвращает реальное значение;
- определены элементы управления (controls) различных типов: бинарные (вкл/выкл), дискретные, аналоговые;
- система (домен HPI) строится как набор ресурсов, каждый ресурс содержит набор сенсоров и элементов управления и может поддерживать горячую замену;
- система может содержать до 2^{32} ресурсов;
- каждый ресурс может содержать до 2^{32} сенсоров и до 2^{32} элементов управления.

Интерфейс HPI можно рассматривать как хороший компромиссный вариант между IPMI и Redfish.

Пример построения архитектуры системы управления на основе HPI

При работе над одним из проектов, заказчиком была поставлена задача построения программного обеспечения управляющего контроллера для управления электропитанием, охлаждением, мониторинга окружающей среды в центрах обработки данных.

Управляемые объекты включают в себя:

- неинтеллектуальные сенсоры и устройства, подключённые по протоколу 1-wire, I^2C (сенсоры температуры, напряжения, тока, мощности, влажности, давления и т. д.);
- неинтеллектуальные дискретные сенсоры на основе сигналов GPIO (General Purpose Input/Output – сигналов ввода-вывода общего назначения);
- дискретные элементы управления на основе сигналов GPIO (включение/выключение соответствующего сигнала);
- интеллектуальные устройства охлаждения с интерфейсом Modbus;
- интеллектуальные вспомогательные управляющие контроллеры с интерфейсом IPMI.
- дочерние управляющие контроллеры того же типа, подключённые к материнскому контроллеру по выделенному сетевому соединению и не имеющие внешнего интерфейса (таким образом, управляющие контроллеры образуют иерархию).

Для интерфейса с внешним миром должны были использоваться интерфейсы SNMP, Redfish и графический Web-интерфейс, а также протокол MQTT для встраивания контрол-

лера в инфраструктуру IoT (Internet of Things – интернет вещей).

При разработке, в качестве основы для архитектуры управляющего контроллера выбрана модель данных HPI. Также HPI используется в качестве интерфейса между ядром программного обеспечения и управляемыми объектами. Каждый из интерфейсов нижнего уровня экспортирует набор ресурсов HPI, по своим правилам. Все ресурсы объединяются ядром в единый набор ресурсов, и функции ядра работают со всеми ресурсами одинаковым образом.

Архитектура программного обеспечения показана на схеме.

Для разных интерфейсов нижнего уровня отображение на модель данных HPI выглядит следующим образом:

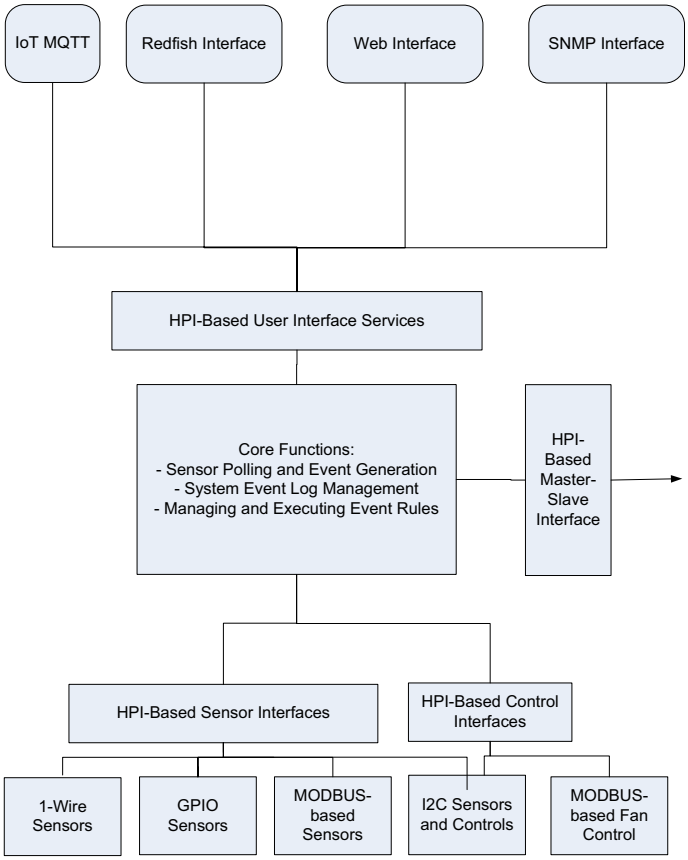
- каждое устройство 1-wire отображается на отдельный ресурс, поддерживающий горячую замену (устройства 1-wire могут динамически добавляться на шину и удаляться с неё);
- один HPI-ресурс создаётся для всех GPIO-сигналов, все дискретные сенсоры и элементы управления принадлежат этому ресурсу;
- для устройств, подключённых по I^2C, каждый набор логически связанных между собой устройств отображается как отдельный HPI-ресурс;
- каждый интеллектуальный контроллер охлаждения, подключённый по Modbus, представляет собой отдельный ресурс, его регистры отображаются на сенсоры и управляющие элементы HPI;
- каждый интеллектуальный IPMI-контроллер представляет собой отдельный ресурс, в соответствии со стандартом отображения между IPMI и HPI;
- каждый дочерний контроллер экспортирует набор HPI-ресурсов, эти ресурсы встраиваются в набор ресурсов материнского контроллера как есть, лишь с изменением номера во избежание конфликта по номерам ресурсов.

Для отображения устройств 1-wire, I^2C, Modbus на HPI в составе программного обеспечения разработаны специальные модули. Для отображения интерфейса IPMI используется открытое программное обеспечение.

Реализация интерфейса Redfish сделана в отдельном модуле, который взаимодействует только с верхним HPI-интерфейсом управляющего контроллера. Этот модуль ничего не знает о функциональности ядра и может предоставлять интерфейс Redfish для любой программной системы, экспортирующей интерфейс HPI.

Аналогично сделана реализация протокола MQTT, для включения управляющего модуля в состав инфраструктуры интернета вещей (IoT). Модуль интерфейса с MQTT использует верхний интерфейс HPI, топики MQTT используют номера или имена ресурсов, сенсоров и элементов управления (например, часть строки топика, соответствующая значению сенсора 20 на ресурсе 2 может выглядеть как "/sensors/value/2/20").

Таким образом, построение архитектуры программного обеспечения управляющего контроллера на основе интерфейса и модели данных HPI позволило интегрировать в единую модель данных разнородные управляемые объекты и предоставить для доступа к этой модели данных различные интерфейсы верхнего уровня, реализация которых логически отделена от внутренней архитектуры системы.



Архитектура программного обеспечения управляющего контроллера

Защищённый комплект программ **«PLATO RT» –** реализация **базовых требований** информационной безопасности **АСУ КВО**

Константин Здирук, Алексей Ханыгин | АО «РТСофт»

В статье описывается разработанный АО «РТСофт» «Защищённый комплект программ «PLATO RT» (СЗИ ЗКП «PLATO RT»), реализованной с применением оригинальных отечественных технологий организации доверенного информационного взаимодействия процессов и групп пользователей автоматизированных систем управления критически важных объектов (АСУ КВО). В основе реализованного АО «РТСофт» подхода лежит гарантированная на уровне вычислительной архитектуры изоляция критически важных данных и процессов их обработки от деструктивного воздействия со стороны недоверенного программного обеспечения отечественного и зарубежного производства, а также потенциально вредоносных субъектов – информационных террористов, привилегированных пользователей и т. п. Предлагаемое программно-аппаратное решение может встраиваться в существующую на предприятии вычислительную инфраструктуру или функционировать в отдельном (скрытом) сегменте сети.

1. Актуальность

Как показывают результаты анализа ряда известных инцидентов, строить системы защиты для вычислительных сетей объектов критической информационной инфраструктуры на базе стандартных (типовых/шаблонных) решений на сегодняшний день недостаточно эффективно.

В этой связи 27 января 2017 года Госдума РФ приняла в первом чтении пакет правительственных законопроектов, которые касаются защиты критической информационной инфраструктуры РФ. По определению законодателей, объекты критической информационной инфраструктуры (КИИ) являются особым защищаемым классом, включающим информационные системы, информационно-телекоммуникационные сети государственных органов, а также информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления технологическими процессами, функционирующие в оборонной промышленности, области здравоохранения, транспорта, связи, кредитно-финансовой сфере, энергетике, топливной промышленности, атомной промышленности, ракетно-космической промышленности и химической промышленности.

В свою очередь, в действующих руководящих документах ФСТЭК РФ рассматриваются так называемые «ключевые системы информационной инфраструктуры» (КСИИ), под которыми понимаются:

- системы органов государственной власти и органов местного самоуправления;
- системы финансово-кредитной и банковской деятельности;
- системы предупреждения и ликвидации кризисных и чрезвычайных ситуаций;
- географические и навигационные системы;

– программно-технические комплексы центров управления взаимоувязанной сети связи России;
– сети связи общего пользования на участках, не имеющих резервных или альтернативных видов связи;
– системы специального назначения;
– спутниковые системы, используемые для обеспечения органов управления и в специальных целях;
– системы управления добычей и транспортировкой нефти, нефтепродуктов и газа;
– системы управления водоснабжением;
– системы управления энергоснабжением.

Как видим, области определения понятий КИИ и КСИИ в значительной степени совпадают, что позволяет применить к объектам КИИ (в части АСУ технологическими процессами) положения, содержащиеся в Приказе № 31 от 14 марта 2014 г. ФСТЭК РФ «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» (далее по тексту – Приказ № 31 ФСТЭК РФ) и в Информационном сообщении от 25 июля 2014 г. № 240/22/2748 «По вопросам обеспечения безопасности информации в ключевых системах информационной инфраструктуры...».

В рамках дальнейшего рассмотрения, автоматизированные системы управления всеми вышеперечисленными объектами будем обозначать аббревиатурой АСУ КВО (АСУ критически важных объектов), рассматривая положения Приказа 31 ФСТЭК РФ в качестве единого набора требований по их защите от угроз информационной безопасности.

2. Основные сведения

АО «РТСофт» является разработчиком и правообладателем сертифицируемой системы защиты изделия ЛКЖТ.ПП.50 1410-01 «Защищённый комплект программ «PLATO RT» (СЗИ ЗКП PLATO RT), реализованной с применением оригинальных отечественных технологий организации доверенного информационного взаимодействия процессов и групп пользователей АСУ КВО. В основе реализованного АО «РТСофт» подхода лежит гарантированная на уровне вычислительной архитектуры изоляция критически важных данных и процессов их обработки от деструктивного воздействия со стороны недоверенного программного обеспечения отечественного и зарубежного производства, а также потенциально вредоносных субъектов – внутренних нарушителей особых категорий: информационных террористов, привилегированных пользователей (системные администраторы, администраторы обеспечения безопасности информации, VIP-сотрудники), в отношении которых общепринятый набор организационно-технических мероприятий по вскрытию и нейтрализации, как правило, недостаточен.

Предлагаемое АО «РТСофт» программно-аппаратное решение может встраиваться в существующую на предприятии заказчика вычислительную инфраструктуру или функционировать в отдельном (скрытом) сегменте сети.

Всё используемое программное обеспечение является отечественным, доверенным и защищённым, в его составе отсутствуют неавторизованные заимствованные фрагменты программного кода отечественных или зарубежных разработчиков.

Дополнительным свойством продукта является возможность реализации на объектах заказчика консолидированной обработки сведений как открытого, так и ограниченного доступа с организацией взаимодействия изолированных информационных контуров (сегментов ЛВС), предназначенных для хранения и обработки данных различных уровней конфиденциальности, посредством включения СЗИ ЗКП «PLATO RT» в состав изделия ОКЦ «ПЛАТАН-РТ» [1].

В целом продукт применяется для построения высоконадёжных, гарантированно защищённых сегментов критически важных систем, оснащаемых нижеперечисленными (встраиваемыми) компонентами СЗИ:
– программным комплексом обеспечения безопасности информации (ПК ОБИ);

– программным комплексом функционального контроля (ПК ФК);
– программными интерфейсами (API) взаимодействия с подсистемами СЗИ ЗКП «PLATO RT» (управление доступом, регистрация и учёт, обеспечение целостности, технологическое преобразование информации);
– подсистемой хранения данных;
– общесистемным программным обеспечением (ОСПО) – доверенной программной средой функционирования СЗИ, организуемой с использованием Инструментального комплекта средств интеграции БИГЕ.466451.099-01 (далее ИКСИ) и встроенного защищённого гипервизора безопасности HyperON БИГЕ.99001-01.

Сертифицируемая в настоящее время (по состоянию на 15.05.2017г.) версия СЗИ для обработки сведений уровня не выше «конфиденциально» функционирует под управлением нижеперечисленных операционных систем:
– Microsoft Windows Server 2008 R2 x64, Microsoft Windows Server 2012 x64 – для серверов;
– Microsoft Windows 7x32, Microsoft Windows 7x64, Microsoft Windows 8x32, Microsoft Windows 8x64 – для клиентских рабочих мест.

Рекомендуемые характеристики аппаратных средств, при которых будет обеспечена комфортная работа пользователей и приемлемое время реакции системы на запросы, составляют:

1. Для ПВЭМ клиентских рабочих мест пользователей:
– процессор: Intel core i5(i7) с поддержкой VT и VMX;
– ОЗУ: не менее 4 Гбайт;
– 2 сетевых карты, одна из которых технологический тракт – карта с чипсетами Rtl 8169 (для карт PCI могут использоваться модели TP Link TG3269, D-Link DGE-530T или их аналоги), Rtl 8168E (для карт PCI-Express могут использоваться модели TP Link TG3468, D-Link DGE-560T или их аналоги). При установке и настройке платы, в качестве поставщика драйвера должен выступать её производитель;
– 2 HD-диска, один из которых технологический тракт с интерфейсом SATA 2 (не менее 500 Мбит);
– базовая ОС (64 бит) MS Windows 7/8.

2. Для Серверов:
– процессор: двухъядерный Intel/AMD с тактовой частотой не менее 2,6 ГГц, кэш не менее 4 Мбайт, с поддержкой VT и VMX;
– оперативная память: не менее 8 Гбайт PC-6400;
– 2 сетевых карты, одна из которых – технологический тракт, с требованиями, аналогичными предъявляемым к клиентским рабочим местам (см. п. 1 выше).

3. Ключевые преимущества

3.1. Как указывалось выше, СЗИ ЗКП «PLATO RT» построена только из авторизованных компонентов отечественной разработки, для обеспечения гарантий его последующего беспрепятственного применения в составе АСУ ТП КВО, обрабатывающих информацию ограниченного доступа.

3.2. СЗИ ЗКП «PLATO RT» обеспечивает двухслойную (внешнюю и внутреннюю) изоляцию защищаемых баз данных и процессов автоматизированной обработки посредством применения уникальной технологии «встраиваемых периметров защиты».

3.3. СЗИ ЗКП «PLATO RT» обеспечивает гарантируемый (на уровне архитектуры) перехват и нейтрализацию угроз со стороны всех, в том числе привилегированных, категорий пользователей (VIP-сотрудник, системный администратор, администратор ОБИ).

3.4. СЗИ ЗКП «PLATO RT» предусматривает организацию на каждой вычислительной установке скрытой от базовой ОС и недоступной для администратора защищённой области хранения данных, дополненной средствами объективной регистрации и автоматической обработки возникающих инцидентов безопасности. Данный механизм исключает сокрытие последствий несанкционированных действий пользователя любой категории, при этом защищённые средства удалённого контроля блокируют работу вычислительной установки до устранения причин возникновения инцидента.

3.5. СЗИ ЗКП «PLATO RT» использует двухконтурную схему мониторинга и управления состоянием узлов ЛВС объекта, с реализацией в независимом контуре (так называемом «технологическом тракте») функций контроля целостности и доступности объектов защиты нижеперечисленных классов:

– сегментов вычислительной инфраструктуры (нижний уровень);
– технологических и бизнес-процессов (верхний уровень).

Для передачи управляющих воздействий при этом могут использоваться оба контура (информационный и технологический тракты).

3.6. На нижнем уровне управления изделие обеспечивает отображение и контроль текущего функционального состояния всех элементов распределённой гетерогенной (неоднородной) вычислительной инфраструктуры заказчика, включающей доступность:

– вычислительных установок – узлов ЛВС объекта применения;
– линий/каналов/направлений связи;
– интерфейсов доступа к услугам передачи, хранения и прикладной обработки данных;
– прикладных и общесистемных (доверенных) процессов обработки данных.

3.7. На верхнем уровне управления распределённой вычислительной инфраструктурой изделие реализует событийно-ориентированный механизм контроля хода и результатов выполнения регламентных процессов решения критически важных задач с использованием автоматических/автоматизированных режимов запуска сценариев обработки (так называемых «реакторов») при возникновении нештатных ситуаций.

3.8. Для хранения эталонных конфигураций и текущего состояния контролируемых узлов, а также сценариев обработки используется встроенная подсистема хранения данных ИКСИ, реализующая функции специализированной файловой системы на основе API-интерфейсов многомерной темпоральной СУБД. Эксклюзивность решения достигается включением возможностей экстренного уничтожения и технологического закрытия (преобразования) критически важных («чувствительных») данных пользователей-клиентов в online-режиме.

3.9. На уровне архитектуры изделия реализовано требование Приказа № 31 ФСТЭК РФ о разделении функций по управлению функционированием (администрированию) автоматизированной системы и управлению (администрированию) системой защиты.

Соответствие функциональных возможностей СЗИ ЗКП «PLATO RT» базовым наборам мероприятий по защите информации АСУ КВО приведено в табл. 1.

Как видно из табл. 1, всего в составе продукта программно-техническими сред-

Табл. 1. Соответствие функциональных возможностей СЗИ ЗКП «PLATO RT» базовым наборам мероприятий по защите информации АСУ КВО (Приказ №31 2014г. ФСТЭК РФ)

Наименование мероприятий по защите информации	Оргтех-мероприя-тия	СЗИ ЗКП «PLATO RT» (компоненты)	Примечание
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)			
Разработка правил и процедур (политик) идентификации и аутентификации субъектов доступа и объектов доступа		ИКСИ (СЭД-компонент «Ъ») ПК ОБИ	
Идентификация и аутентификация пользователей, являющихся работниками оператора		ПК ОБИ	
Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных		ИКСИ ПК ОБИ	
Управление идентификаторами, в том числе создание, присвоение, изменение, уничтожение идентификаторов		ИКСИ ПК ОБИ	
Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	Да	Нет	

Исключение отображения для пользователя действительного значения аутентификационной информации и (или) количества вводимых символов (защита обратной связи при вводе аутентификационной информации)	Да	Нет	
Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)		ИКСИ (компонент «CAPI»)	
Идентификация и аутентификация объектов файловой системы, запускаемых и исполняемых модулей, объектов систем управления базами данных, объектов, создаваемых прикладным и специальным программным обеспечением, иных объектов доступа		ПК ОБИ ПК ФК	Требование не входит в базовый набор мероприятий по ЗИ
II. Управление доступом субъектов доступа к объектам доступа (УПД)			
Разработка правил и процедур (политик) управления доступом субъектов доступа к объектам доступа		ИКСИ (СЭД-компонент «Ъ») ПК ОБИ	
Управление (заведение, активация, блокирование и уничтожение) учётными записями пользователей, в том числе внешних		ПК ОБИ	
Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа		ПК ОБИ	
Управление (экранирование, фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами автоматизированной системы управления, а также между автоматизированными системами управления		ИКСИ (компонент «CAPI»)	
Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование автоматизированной системы управления		ПК ОБИ	
Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование автоматизированной системы управления		ПК ОБИ ПК ФК	
Ограничение неуспешных попыток входа в автоматизированную систему управления (доступа к системе)		ПК ОБИ	
Предупреждение пользователя при его входе в автоматизированную систему управления о том, что в ней реализованы меры защиты информации, и о необходимости соблюдения им установленных оператором правил обработки информации	Нет	Нет	Требование не входит в базовый набор мероприятий по ЗИ
Оповещение пользователя после успешного входа в автоматизированную систему управления о его предыдущем входе в автоматизированную систему управления	Нет	Нет	Требование не входит в базовый набор мероприятий по ЗИ
Ограничение числа параллельных сеансов доступа для каждой учётной записи пользователя автоматизированной системы управления		ИКСИ	Требование не входит в базовый набор мероприятий по ЗИ
Блокирование сеанса доступа в автоматизированную систему управления после установленного времени бездействия (неактивности) пользователя или по его запросу		HyperON	Требование не входит в базовый набор мероприятий по ЗИ
Разрешение (запрет) действий пользователей, разрешённых до идентификации и аутентификации		ПК ОБИ	
Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе её хранения и обработки		ПК «Подсистема хранения данных»	Требование не входит в базовый набор мероприятий по ЗИ
Реализация защищённого удалённого доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети		ИКСИ	
Регламентация и контроль использования в автоматизированной системе управления технологий беспроводного доступа	Да	Нет	
Регламентация и контроль использования в автоматизированной системе управления мобильных технических средств	Да	Нет	

Управление взаимодействием с автоматизированными (информационными) системами сторонних организаций (внешние системы)		ИКСИ	
Обеспечение доверенной загрузки средств вычислительной техники		HyperON	Требование не входит в базовый набор мероприятий по ЗИ
III. Ограничение программной среды (ОПС)			
Разработка правил и процедур (политик) ограничения программной среды		ИКСИ / ПК ОБИ / ПК ФК	
Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения		ИКСИ HyperON	Требование относится только к АСУ ПТП КВО 1 кл.
Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения		ИКСИ ПК ФК	Реализуется посредством сценариев ЗКП «PLATO RT»
Установка (инсталляция) только разрешённого к использованию программного обеспечения и (или) его компонентов		ИКСИ HyperON	
Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов		ИКСИ	Требование не входит в базовый набор мероприятий по ЗИ
IV. Защита машинных носителей информации (ЗНИ)			
Разработка правил и процедур (политик) защиты машинных носителей		ИКСИ (СЭД-компонент «Ъ»)	
Учёт машинных носителей информации	Да	Нет	
Управление доступом к машинным носителям информации	Да	Нет	
Контроль перемещения машинных носителей информации за пределы контролируемой зоны	Да	Нет	Требование не входит в базовый набор мероприятий по ЗИ
Исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях, и (или) использования носителей информации в иных автоматизированных системах управления	Да	Нет	Требование не входит в базовый набор мероприятий по ЗИ
Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации		ИКСИ / HyperON	
Контроль ввода (вывода) информации на машинные носители информации		Нет	Требование относится только к АСУ ПТП КВО 1кл.
Контроль подключения машинных носителей информации		ИКСИ / HyperON	
Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)	Нет	Нет	Требование не входит в базовый набор мероприятий по ЗИ
V. Регистрация событий безопасности (РСБ)			
Разработка правил и процедур (политик) регистрации событий безопасности		ИКСИ (СЭД-компонент «Ъ») ПК ОБИ / ПК ФК	
Определение событий безопасности, подлежащих регистрации, и сроков их хранения		ПК ОБИ / ПК ФК	
Определение состава и содержания информации о событиях безопасности, подлежащих регистрации		ПК ОБИ / ПК ФК	
Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения		ИКСИ / HyperON / ПК «Подсистема хранения данных»	
Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объёма (ёмкости) памяти		ИКСИ / ПК ФК	Реализуется посредством сценариев ЗКП «PLATO RT»

Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них		ПК ОБИ / ПК ФК	
Генерирование временных меток и (или) синхронизация системного времени в автоматизированной системе управления	Нет	Нет	
Защита информации о событиях безопасности		ПК «Подсистема хранения данных»	
Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей		ПК ОБИ ПК ФК	Требование не входит в базовый набор мероприятий по ЗИ
VI. Антивирусная защита (АВЗ)			
Разработка правил и процедур (политик) антивирусной защиты	Да	Нет	
Реализация антивирусной защиты	Нет	Нет	Требуются внешние сертификационные средства
Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	Да	Нет	
VII. Обнаружение вторжений (СОВ)			
Разработка правил и процедур (политик) обнаружения вторжений	Да	Нет	Требование относится только к АСУ ПТП КВО 1кл.
Обнаружение вторжений		Нет	Требуются внешние сертификационные средства Требование относится только к АСУ ПТП КВО 1кл.
Обновление базы решающих правил	Да	Нет	Требование относится только к АСУ ПТП КВО 1кл.
VIII. Контроль (анализ) защищённости информации (АНЗ)			
Разработка правил и процедур (политик) контроля (анализа) защищённости		ИКСИ (СЭД-компонент «Ъ») ПК ОБИ / ПК ФК	
Выявление, анализ уязвимостей и оперативное устранение вновь выявленных уязвимостей		Нет	
Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации		ПК ФК	
Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации		ИКСИ HyperON ПК ФК	
Контроль состава технических средств, программного обеспечения и средств защиты информации		ИКСИ / HyperON / ПК ФК	
Контроль правил генерации и смены паролей пользователей, заведения и удаления учётных записей пользователей, реализации правил разграничения доступа, полномочий пользователей		ПК ОБИ	
IX. Обеспечение целостности (ОЦЛ)			
Разработка правил и процедур (политик) обеспечения целостности		HyperON / ПК ФК / ПК ОБИ	
Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации		HyperON / ПК ФК	
Контроль целостности информации, содержащейся в базах данных	Да	Нет	Требование не входит в базовый набор мероприятий по ЗИ
Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций		ПК ОБИ / ПК ФК	
Обнаружение и реагирование на поступление в автоматизированную систему управления незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к её функционированию (защита от спама)	Нет	Нет	Требуются внешние сертификационные средства Требование не входит в базовый набор мероприятий по ЗИ

Контроль содержания информации, передаваемой из автоматизированной системы управления (контейнерный, основанный на свойствах объекта доступа, и контентный, основанный на поиске запрещённой к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации		ИКСИ	Контейнеры ИКСИ содержат описание свойств вложенных объектов, сигнатурный анализ вложений – не реализован (ограничения безопасности)
Ограничение прав пользователей по вводу информации в автоматизированную систему управления		ИКСИ	Требование относится только к АСУ ПТП КВО 1кл.
Контроль точности, полноты и правильности данных, вводимых в автоматизированную систему управления	Да	Нет	
Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях	Да	Нет	
X. Обеспечение доступности (ОДТ)			
Разработка правил и процедур (политик) обеспечения доступности		ПК ФК	
Использование отказоустойчивых технических средств	Да	Нет	
Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования системы	Нет	Нет	Требуются внешние сертификационные средства
Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование	Да	Нет	
Периодическое резервное копирование информации на резервные машинные носители информации		ИКСИ / ПК ФК	
Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала		ИКСИ / ПК ФК	
Кластеризация автоматизированной системы управления и (или) её сегментов		ИКСИ / ПК ФК / ПК ОБИ	
Контроль состояния и качества предоставления поставщиком телекоммуникационных услуг вычислительных ресурсов (мощностей), в том числе по передаче информации		Нет	
XI. Защита среды виртуализации (ЗСВ)			
Разработка правил и процедур (политик) защиты среды виртуализации		HyperON	
Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации		HyperON / ПК ОБИ	
Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин		HyperON / ПК ОБИ	
Регистрация событий безопасности в виртуальной инфраструктуре		HyperON / ПК ФК	
Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры		ИКСИ / ПК ОБИ / ПК ФК	
Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией		HyperON	
Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных	Да	Нет	
Контроль целостности виртуальной инфраструктуры и её конфигураций		HyperON / ПК ФК / ПК «Подсистема хранения данных»	

Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры	Да	Нет	Требование относится только к АСУ ПТП КВО 1кл.
Реализация и управление антивирусной защитой в виртуальной инфраструктуре	Да	Нет	Требуются внешние сертификационные средства
Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей	Да	Нет	
XII. Защита технических средств (ЗТС)			
Разработка правил и процедур (политик) защиты технических средств		ПК ОБИ / ПК ФК	
Защита информации, обрабатываемой техническими средствами, от её утечки по техническим каналам	Нет	Нет	Требуются внешние сертификационные средства Требование не входит в базовый набор мероприятий по ЗИ
Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, исполнительные устройства и средства защиты информации, а также средства обеспечения функционирования	Да	Нет	
Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ	Да	Нет	Требуются внешние сертификационные средства
Размещение устройств вывода (отображения) информации, исключающее её несанкционированный просмотр	Да	Нет	Требование не входит в базовый набор мероприятий по ЗИ
Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов)	Да	Нет	
XIII. Защита автоматизированной системы и её компонентов (ЗИС)			
Разработка правил и процедур (политик) защиты автоматизированной системы и её компонентов		ПК ОБИ / ПК ФК	
Разделение функций по управлению (администрированию) автоматизированной системой управления, управлению (администрированию) системой защиты, функций по обработке информации и иных функций автоматизированной системы управления		ПК ОБИ / ПК ФК / HyperON	
Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом	Нет	Нет	Требование не входит в базовый набор мероприятий по ЗИ
Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при её передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи		ИКСИ	Реализовано, за исключением защиты информации при передаче по беспроводным каналам связи
Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации)		ИКСИ / HyperON	Требование не входит в базовый набор мероприятий по ЗИ
Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода	Нет	Нет	Термин «технология мобильного кода» требует дополнительного уточнения
Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи	Да	Нет	Требование не входит в базовый набор мероприятий по ЗИ

Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации	Да	Нет	Требование не входит в базовый набор мероприятий по ЗИ
Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам		ИКСИ	Требование не входит в базовый набор мероприятий по ЗИ
Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов		ИКСИ HyperON	
Исключение возможности отрицания пользователем факта отправки информации другому пользователю		ИКСИ HyperON	Требование не входит в базовый набор мероприятий по ЗИ
Исключение возможности отрицания пользователем факта получения информации от другого пользователя		ИКСИ HyperON	Требование не входит в базовый набор мероприятий по ЗИ
Использование устройств терминального доступа для обработки информации		ИКСИ	Требование не входит в базовый набор мероприятий по ЗИ
Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации		HyperON ПК «Подсистема хранения данных»	
Выявление, анализ и блокирование скрытых каналов передачи информации в обход реализованных мер защиты информации или внутри разрешённых сетевых протоколов		Нет	Требование не входит в базовый набор мероприятий по ЗИ
Разбиение автоматизированной системы управления на сегменты (сегментирование) и обеспечение защиты периметров сегментов		ИКСИПК ОБИ	
Обеспечение загрузки и исполнения программного обеспечения с машинных носителей информации, доступных только для чтения, и контроль целостности данного программного обеспечения		HyperON ПК ФК	Требование не входит в базовый набор мероприятий по ЗИ
Изоляция процессов (выполнение программ) в выделенной области памяти		ИКСИ HyperON	Реализовано только для процессов в составе КСЗ Требование не входит в базовый набор мероприятий по ЗИ
Защита беспроводных соединений, применяемых в автоматизированной системе управления	Нет	Нет	Требуются внешние сертификационные средства
Исключение доступа пользователя к информации, возникшей в результате действий предыдущего пользователя через реестры, оперативную память, внешние запоминающие устройства и иные общие для пользователей ресурсы		ИКСИ / ПК ОБИ	Требование не входит в базовый набор мероприятий по ЗИ
Защита автоматизированной системы управления от угроз безопасности информации, направленных на отказ в обслуживании	Да	Нет	
Защита периметра (физических и (или) логических границ) автоматизированной системы управления при её взаимодействии с иными автоматизированными (информационными) системами и информационно-телекоммуникационными сетями		ИКСИ ПК ОБИ	
Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения	Нет	Нет	Требуются внешние сертификационные средства Требование не входит в базовый набор мероприятий по ЗИ
Использование в автоматизированной системе управления различных типов общесистемного, прикладного и специального программного обеспечения (создание гетерогенной среды)		ИКСИ HyperON	Требование не входит в базовый набор мероприятий по ЗИ
Использование прикладного (специального) программного обеспечения, имеющего возможность функционирования в средах различных операционных систем		ИКСИ HyperON	Требование не входит в базовый набор мероприятий по ЗИ

Создание (эмуляция) ложных компонентов автоматизированной системы управления, предназначенных для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз безопасности информации	Нет	Нет	Требование не входит в базовый набор мероприятий по ЗИ
Воспроизведение ложных и (или) скрытие истинных отдельных технологий и (или) структурно-функциональных характеристик автоматизированной системы управления или её сегментов, обеспечивающее навязывание нарушителю ложного представления об истинных технологиях и (или) структурно-функциональных характеристиках	Нет	Нет	Требование не входит в базовый набор мероприятий по ЗИ
Перевод автоматизированной системы или её устройств (компонентов) в заранее определённую конфигурацию, обеспечивающую защиту информации, в случае возникновении отказов (сбоев)		ИКСИ HyperON	Требование не входит в базовый набор мероприятий по ЗИ
Защита мобильных технических средств, применяемых в автоматизированной системе управления	Да	Нет	Требуются внешние сертификационные средства
XIV. Обеспечение безопасной разработки программного обеспечения (ОБР)			
Разработка правил и процедур (политик) обеспечения безопасной разработки программного обеспечения		ИКСИ (СЭД-компонент «Ъ») ПК ОБИ	
Анализ уязвимостей и угроз безопасности информации в ходе разработки программного обеспечения	Нет	Нет	Требуются внешние сертификационные средства
Статический анализ кода программного обеспечения в ходе разработки программного обеспечения	Нет	Нет	Требуются внешние сертификационные средства
Ручной анализ кода программного обеспечения в ходе разработки программного обеспечения	Нет	Нет	Требование не входит в базовый набор мероприятий по ЗИ
Тестирование на проникновение в ходе разработки программного обеспечения	Нет	Нет	Требуются внешние сертификационные средства
Динамический анализ кода программного обеспечения в ходе разработки программного обеспечения	Нет	Нет	Требуются внешние сертификационные средства
Документирование процедур обеспечения безопасной разработки программного обеспечения разработчиком и представление их заказчику (оператору)		ИКСИ (СЭД-компонент «Ъ»)	
XV. Управление обновлениями программного обеспечения (ОПО)			
Разработка правил и процедур (политик) управления обновлениями программного обеспечения (включая получение, проверку и установку обновлений)		ИКСИ (СЭД-компонент «Ъ») ПК ФК	
Получение обновлений программного обеспечения от разработчика или уполномоченного им лица	Да	Нет	
Тестирование обновлений программного обеспечения до его установки на макете или в тестовой зоне	Да	Нет	
Централизованная установка обновлений программного обеспечения		ПК ФК	Реализуется посредством сценариев ЗКП «PLATO RT» Требование не входит в базовый набор мероприятий по ЗИ
XVI. Планирование мероприятий по обеспечению защиты информации (ПЛН)			
Разработка правил и процедур (политик) планирования мероприятий по обеспечению защиты информации		ИКСИ (СЭД-компонент «Ъ»)	
Определение лиц, ответственных за планирование, реализацию и контроль мероприятий по обеспечению защиты информации в автоматизированной системе управления		ИКСИ (СЭД-компонент «Ъ»)	
Разработка, утверждение и актуализация плана мероприятий по обеспечению защиты информации в автоматизированных системах управления		ИКСИ (СЭД-компонент «Ъ»)	
Контроль выполнения мероприятий по обеспечению защиты информации в автоматизированных системах управления, предусмотренных утверждённым планом		ИКСИ(СЭД-компонент «Ъ»)	

XVII. Обеспечение действий в нештатных (непредвиденных) ситуациях (ДНС)			
Разработка правил и процедур (политик) обеспечения действий в нештатных (непредвиденных) ситуациях		ИКСИ (СЭД-компонент «Ъ») ПК ФК	
Разработка плана действий на случай возникновения нештатных (непредвиденных) ситуаций		ИКСИ (СЭД-компонент «Ъ»)	
Обучение и отработка действий персонала в случае возникновения нештатных (непредвиденных) ситуаций	Да	Нет	
Создание альтернативных мест хранения и обработки информации на случай возникновения нештатных (непредвиденных) ситуаций	Да	Нет	
Резервирование программного обеспечения, технических средств, каналов передачи данных автоматизированных систем управления на случай возникновения нештатных (непредвиденных) ситуаций		ПК ФК	Реализуется посредством сценариев ЗКП «PLATO RT» (только в части ПО и ИО)
Обеспечение возможности восстановления автоматизированной системы управления и (или) её компонентов в случае возникновения нештатных (непредвиденных) ситуаций		ПК ФК	Реализуется посредством сценариев ЗКП «PLATO RT» (только в части ПО и ИО)
XVIII. Информирование и обучение персонала (ИПО)			
Разработка правил и процедур (политик) информирования и обучения персонала		ИКСИ (СЭД-компонент «Ъ») ПК ОБИ / ПК ФК	Реализуется с использованием стендовой базы УЦ ЗАО «РТСофт»
Информирование персонала об угрозах безопасности информации, о правилах эксплуатации системы защиты автоматизированной системы управления и отдельных средств защиты информации		ИКСИ (СЭД-компонент «Ъ») ПК ОБИ / ПК ФК	Реализуется с использованием стендовой базы УЦ ЗАО «РТСофт»
Обучение персонала правилам эксплуатации системы защиты автоматизированной системы управления и отдельных средств защиты информации		ИКСИ (СЭД-компонент «Ъ») ПК ОБИ / ПК ФК	Реализуется с использованием стендовой базы УЦ ЗАО «РТСофт»
Проведение практических занятий с персоналом по правилам эксплуатации системы защиты автоматизированной системы управления и отдельных средств защиты информации		ИКСИ (СЭД-компонент «Ъ») ПК ОБИ / ПК ФК	Реализуется с использованием стендовой базы УЦ ЗАО «РТСофт»
XIX. Анализ угроз безопасности информации и рисков от их реализации (УБИ)			
Разработка правил и процедур (политик) анализа угроз безопасности информации и рисков от их реализации		ИКСИ (СЭД-компонент «Ъ», экспресс-анализатор ALBA)	
Периодический анализ изменения угроз безопасности информации, возникающих в ходе эксплуатации автоматизированной системы управления		ИКСИ (СЭД-компонент «Ъ», экспресс-анализатор ALBA)	
Периодическая переоценка последствий от реализации угроз безопасности информации (анализ риска)		ИКСИ (СЭД-компонент «Ъ», экспресс-анализатор ALBA)	
XX. Выявление инцидентов и реагирование на них (ИНЦ)			
Разработка правил и процедур (политик) выявления инцидентов и реагирования на них		ИКСИ (СЭД-компонент «Ъ») ПК ОБИ / ПК ФК	
Определение лиц, ответственных за выявление инцидентов и реагирование на них		Нет	
Обнаружение, идентификация и регистрация инцидентов		ПК ОБИ / ПК ФК	
Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов		ИКСИ (СЭД-компонент «Ъ»)	
Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий		ИКСИ (СЭД-компонент «Ъ», экспресс-анализатор ALBA)	

Принятие мер по устранению последствий инцидентов		ИКСИ (СЭД-компонент «Ъ»)	
Планирование и принятие мер по предотвращению повторного возникновения инцидентов		ИКСИ (СЭД-компонент «Ъ»)	
XXI. Управление конфигурацией автоматизированной системы управления и её системы защиты (УКФ)			
Разработка правил и процедур (политик) управления конфигурацией автоматизированной системы управления и её системы защиты		ИКСИ (СЭД-компонент «Ъ») ПК ФК	
Определение лиц, которым разрешены действия по внесению изменений в конфигурацию автоматизированной системы управления и её системы защиты		Нет	
Управление изменениями конфигурации автоматизированной системы управления и её системы защиты		ИКСИ (СЭД-компонент «Ъ») ПК ФК	Реализуется посредством сценариев ЗКП «PLATO RT» (только в части ПО и ИО)
Анализ потенциального воздействия планируемых изменений в конфигурации автоматизированной системы управления и системы защиты на обеспечение защиты информации и согласование изменений в конфигурации автоматизированной системы управления с должностным лицом (работником), ответственным за обеспечение безопасности автоматизированной системы управления		ИКСИ (СЭД-компонент «Ъ», экспресс-анализатор ALBA)	
Документирование информации (данных) об изменениях в конфигурации автоматизированной системы управления и её системы защиты		ИКСИ (СЭД-компонент «Ъ») ПК ФК / ПК «Подсистема хранения данных»	
Регламентация и контроль технического обслуживания, в том числе дистанционного (удалённого), технических средств и программного обеспечения автоматизированной системы управления		ИКСИ / ПК ФК	Реализуется посредством сценариев ЗКП «PLATO RT» (только в части ПО и ИО)
ВСЕГО требований (мероприятий): 167		Реализовано в СЗИ ЗКП «PLATO RT» – 106 (63%)	

ствами реализовано 106 требований (63%) из 167, содержащихся в базовом наборе мероприятий, определённых Приказом №31 2014 г. ФСТЭК РФ. Предполагается, что оставшаяся часть требований подлежит реализации посредством разработки и применения комплекса организационно-технических мероприятий, а также (при необходимости) привлечения дополнительных сертифицированных средств защиты.

4. Что даёт применение продукта различным категориям пользователей

Для **категории I (руководство предприятия/организации):**

– бескомпроматность хранения и передачи критической информации АСУ ТП, реализацию организационно-распорядительных функций, доверенный (защищённый) обмен документами, вскрытие вредоносной активности и гарантированную (на уровне архитектуры) объективную регистрацию инцидентов безопасности;

– организацию дополнительного (встроенного) информационного контура, гарантированно защищённого как от внешних угроз (в лице любознательных искателей брешей в программном обеспечении и нечистых на руку взломщиков), так и от внутренних – в лице инсайдеров, к которым можно отнести привилегированных сотрудников, системных администраторов, администратора ОБИ.

Для **категории II (диспетчерская служба объекта автоматизации):**

– минимизацию количества ручных операций по авторизации в распределённой системе сбора и обработки данных, запуску/завершению технологических (регламентных) процессов, подготовке и рассылке итоговых отчётных данных (документов) о работе системы, реализации организационно-распорядительных функций.

Для **категории III (специалисты подразделений автоматизации):**

– оптимизацию ресурсов (прежде всего временны**х**) на реализацию полнофункционального объективного контроля текущего состояния и сопровождение территориально-распределённого вычислительного процесса в АСУ ТП КВО (контроль целостности технических и программных средств, смена версий, оперативность локализации сбоев/отказов и их устранения).

Для **категория IV (специалисты по ИБ / администраторы ОБИ**):

– обеспечение службы ИБ сертифицированными (РД ФСТЭК) средствами,
– исключение каналов утечки критической информации,
– разделение трактов управления функциональной и информационной безопасностью,
– гарантированное обнаружение и проактивную нейтрализацию угроз, регламентированных моделью нарушителя (в том числе – инсайдерских угроз).

В табл. 2 содержится перечень 30-ти основных функциональных возможностей СЗИ ЗКП «PLATO RT», ориентированных на соответствующие категории пользователей (отмечены знаком +).

Табл. 2. Привязка функциональных возможностей СЗИ изделия ЗКП ««PLATO RT» к различным категориям пользователей АСУ ТП КВО

Наименование функциональной возможности	Категории пользователей			
	(I) Руководство организации	(II) Диспетчерская служба	(III) Специалисты подразделений автоматизации	(IV) Специалисты по ИБ (Адм. ОБИ)
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)				
Управление идентификаторами, в том числе создание, присвоение, изменение, уничтожение идентификаторов			+	+
II. Управление доступом субъектов доступа к объектам доступа (УПД)				
Управление (заведение, активация, блокирование и уничтожение) учётными записями пользователей, в том числе внешних пользователей	+		+	+
Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	+	+	+	+
Управление (экранирование, фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами автоматизированной системы управления, а также между автоматизированными системами управления	+	+	+	
Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование автоматизированной системы управления	+		+	
Ограничение неуспешных попыток входа в автоматизированную систему управления (доступа к системе)	+	+	+	
Блокирование сеанса доступа в автоматизированную систему управления	+	+	+	
Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе её хранения и обработки			+	
Реализация защищённого удалённого доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	+		+	
Обеспечение доверенной загрузки средств вычислительной техники			+	+
III. Ограничение программной среды (ОПС)				
Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения		+	+	

V. Регистрация событий безопасности (РСБ)				
Определение состава и содержания информации о событиях безопасности, подлежащих регистрации			+	+
Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения			+	+
Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них		+	+	+
Защита информации о событиях безопасности			+	+
Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей	+		+	+
VIII. Контроль (анализ) защищённости информации (АНЗ)				
Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации		+	+	+
Контроль состава технических средств, программного обеспечения и средств защиты информации		+	+	+
Контроль правил генерации и смены паролей пользователей, заведения и удаления учётных записей пользователей, реализации правил разграничения доступа, полномочий пользователей			+	+
IX. Обеспечение целостности (ОЦЛ)				
Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации		+	+	+
X. Обеспечение доступности (ОДТ)				
Кластеризация автоматизированной системы управления и (или) её сегментов	+		+	
XI. Защита среды виртуализации (ЗСВ)				
Регистрация событий безопасности в виртуальной инфраструктуре	+		+	+
Контроль целостности виртуальной инфраструктуры и её конфигураций	+		+	+
XIII. Защита автоматизированной системы и её компонентов (ЗИС)				
Разделение функций по управлению (администрированию) автоматизированной системой управления, управлению (администрированию) системой защиты, функций по обработке информации и иных функций автоматизированной системы управления	+		+	+
Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов			+	+
Защита периметра (физических и (или) логических границ) автоматизированной системы управления при её взаимодействии с иными автоматизированными (информационными) системами и информационно-телекоммуникационными сетями			+	+
Использование в автоматизированной системе управления различных типов общесистемного, прикладного и специального программного обеспечения (создание гетерогенной среды)			+	+
Перевод автоматизированной системы или её устройств (компонентов) в заранее определённую конфигурацию, обеспечивающую защиту информации, в случае возникновении отказов (сбоев)	+		+	+
XIX. Анализ угроз безопасности информации и рисков от их реализации (УБИ)				
Периодический анализ изменения угроз безопасности информации, возникающих в ходе эксплуатации автоматизированной системы управления	+		+	
XXI. Управление конфигурацией автоматизированной системы управления и её системы защиты (УКФ)				
Управление изменениями конфигурации автоматизированной системы управления и её системы защиты			+	+
Документирование информации (данных) об изменениях в конфигурации автоматизированной системы управления и её системы защиты	+		+	+

Система управления процессом технологической подготовки **токамака Т-15МД** к эксперименту

Галина Кузьмина, Юрий Моцкин | АО «РТСофт»
Александр Качкин, Иван Образцов, Михаил Соколов, Пётр Хвостенко, Михаил Чуканов | НИЦ «Курчатовский институт»

В статье представлены технические решения по реализации задачи автоматизированной технологической подготовки установки «Токамак Т-15МД» к проведению эксперимента. Дано описание технологических систем, автоматизированных систем управления ими, технологии реализации поставленной задачи.

1. Введение

В настоящее время в Национальном исследовательском центре «Курчатовский институт» проводится сооружение крупнейшей отечественной экспериментальной термоядерной установки «Токамак Т-15МД», предназначенной для создания высокотемпературной плазмы с диверторной конфигурацией. Работа выполняется в рамках ФЦП «Ядерные энерготехнологии нового поколения на период 2010–2015 годов и на перспективу до 2020 года» [1].

Установка Т-15МД будет иметь вытянутую конфигурацию плазменного шнура с аспектным отношением 2.2, током плазмы 2 МА в тороидальном магнитном поле 2 Т с квазистационарной системой дополнительного нагрева суммарной мощностью до 20 МВт. Установка рассчитана на длительность импульса до 30 с [2]. На токамаке Т-15МД будут проводиться исследования в поддержку развития технологий управляемого термоядерного синтеза и проекта ИТЭР, а также для создания термоядерного источника нейтронов (ТИН), необходимого для гибридной энергетики [3].

Токамак Т-15МД представляет собой сложный комплекс взаимодействующих между собой инженерных, технологических, электрофизических и информационно-измерительных систем, распределённых по территории нескольких зданий НИЦ «Курчатовский институт».

Задачи подготовки установки к проведению эксперимента и поддержания в процессе эксперимента технологических параметров, необходимых для создания плазмы в камере токамака, решают следующие технологические системы (ТС):

– система вакуумной откачки (СВО),
– система обезгаживающего прогрева вакуумной камеры (СОП),
– система чистки камеры токамака тлеющим разрядом (СЧРК),
– система технологического газонапуска (ГНСУ),
– система водяного охлаждения (СОВ).

2. Технологическое оборудование Т-15МД

2.1. Система вакуумной откачки

СВО предназначена для получения и поддержания рабочих вакуумных давлений в следующих объектах установки Т-15МД:

– в разрядной камере,
– в инжекторах,
– в источниках инжекторов.

Получение вакуумных рабочих давлений в объектах установки Т-15МД производится в два этапа:

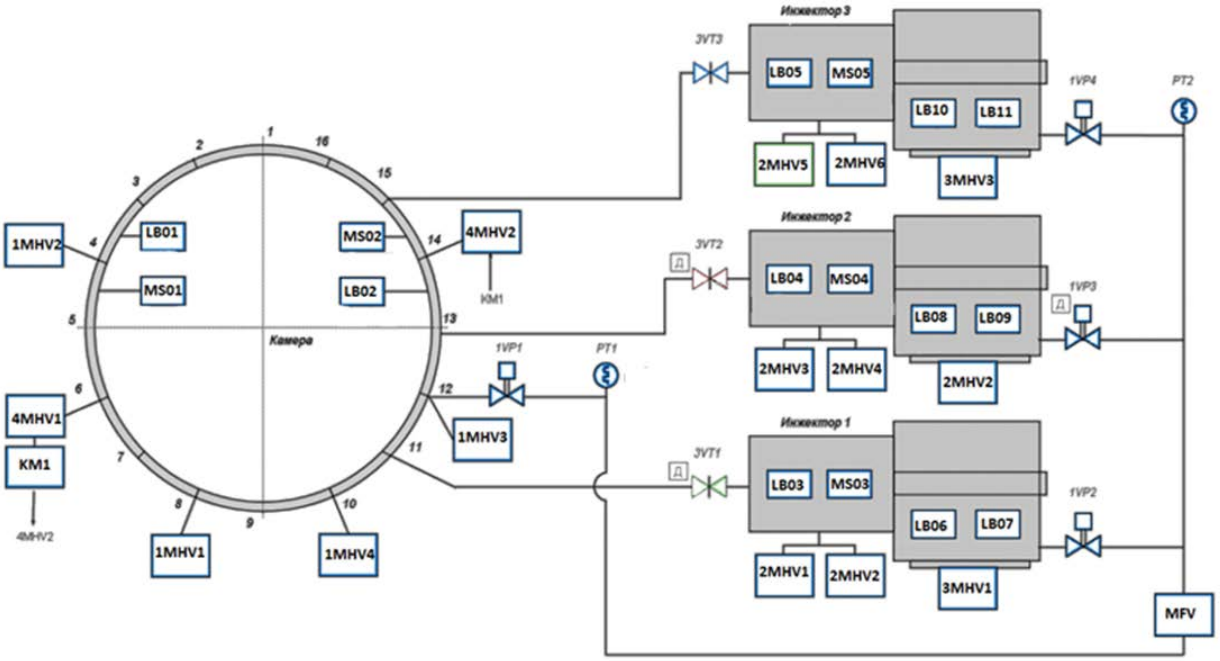


Рис. 1. Технологическое оборудование СВО Т-15МД

– предварительная откачка разрядной камеры и инжекторов до давления ~1 Па и переход на высоковакуумную откачку;
– высоковакуумная (турбомолекулярная и криогенная) откачка разрядной камеры и инжекторов до давления $<5\cdot10^{-6}$ Па с целью получения предельного остаточного давления.

Технологическое оборудование СВО распределено по вакуумным ячейкам четырёх типов. Количество ячеек – 16. Каждая из ячеек выполняет конкретные этапы вакуумной откачки из определённого объёма.

Состав технологического оборудования СВО представлен на рис. 1.

2.2. Система обезгаживающего прогрева

Прогрев вакуумной камеры (ВК) токамака необходим для выведения из внутренних стенок растворённых в металле газов, которые ухудшают характеристики вакуума во время разряда. На базе имеющего опыта прогрева ВК токамаков разработана СОП установки Т-15МД, которая должна обеспечивать поддержание температуры на поверхности ВК 220 ± 20 °С в режимах подготовки к эксперименту.

В качестве электронагревателя в СОП используется нагревостойкий кабель КНМСНХ 1×1,131 ТУ16-505.564-75 общей длиной около 700 м, поделённый на секции и закреплённый на поверхности камеры с помощью керамических изоляторов. Мощность прогрева регулируется однофазными тиристорными регуляторами мощности ТРМ-1М-125. Сигналом обратной связи для регулятора служит температура поверхности камеры, которая регистрируется с помощью термопар ТП.ХК(L)-К5.Н.05-4×30,0×L-2 в количестве 102 шт., равномерно распределённых по поверхности. Для преобразования сигнала 0–30 мВ с термоэлектродов хромель-копель в унифицированный сигнал 4–20 мА и в целях гальванической развязки используются нормирующие преобразователи НПСИ-ТП-0-220-М0.

Структурная схема АСУ СОП представлена на рис. 2.

Операция прогрева проводится при непрерывной вакуумной откачке, а длительность прогрева определяется давлением и спектром остаточных газов в ВК Т-15МД с помощью масс-спектрометрического прибора СВО Т-15МД.

Требования к продолжительности и порядку работы нагревателей будут сформулированы в ходе испытаний, запланированных на 2018 год в Курчатовском институте (системный интегратор – АО «РТСофт»), во время которых необходимо определить инерционность и неравномерность нагрева, настроить программный регулятор и отладить специальное программное обеспечение.

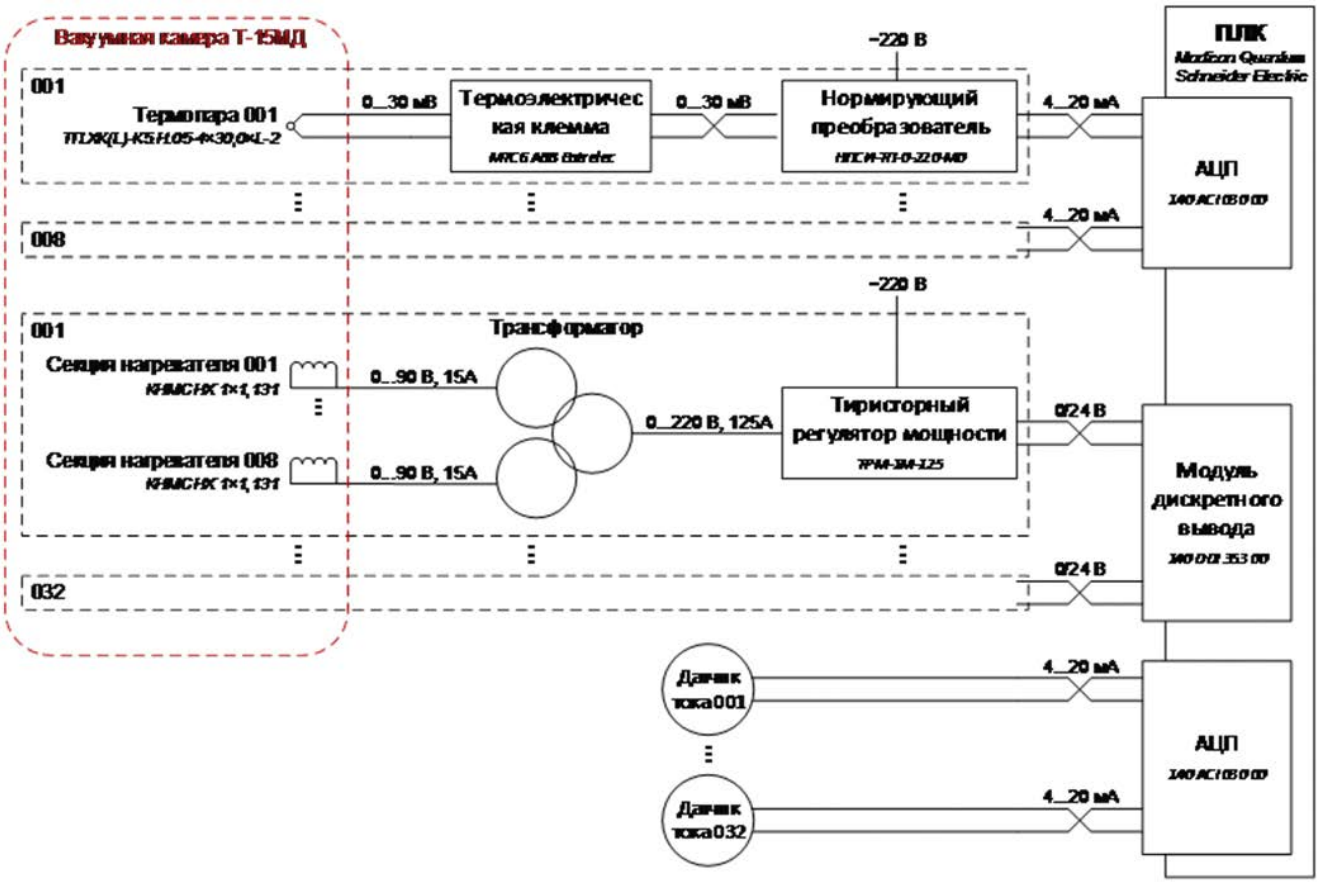


Рис. 2. Структурная схема АСУ СОП

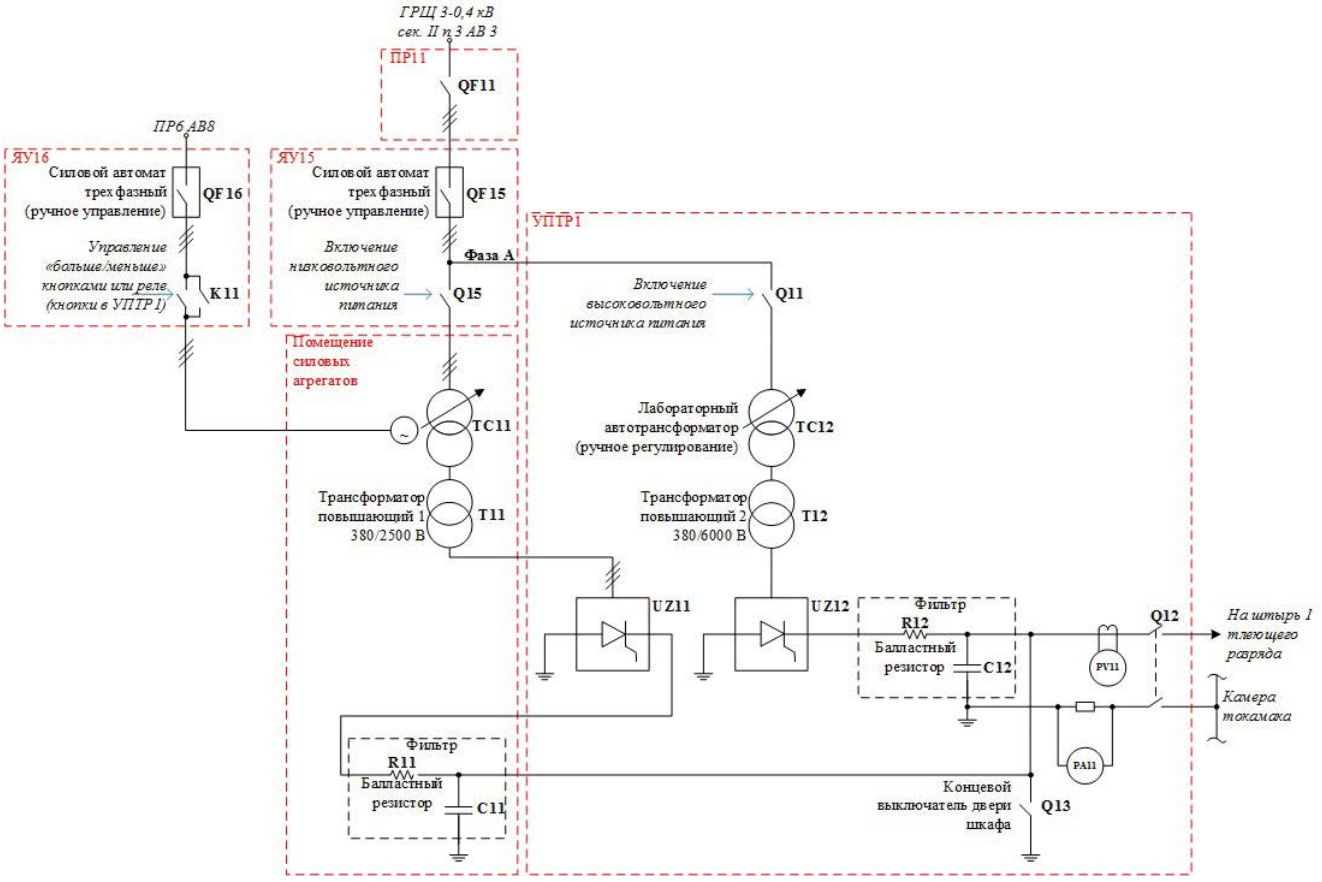


Рис. 3. Структурная схема электропитания электродов тлеющего разряда

2.3. Система чистки камеры тлеющим разрядом

СЧРК предназначена для очистки и обезгаживания стенок разрядной камеры. При таком разряде происходит десорбция со стенок камеры примесей, образовавшихся в процессе эксперимента.

СЧРК включает четыре электрода тлеющего разряда. Каждый из электродов состоит из штыря, двух контакторов и индукционного регулятора. Структурная схема электропитания электродов приведена на рис. 3.

В процедуре чистки камеры тлеющим разрядом участвуют следующие ТС:

– СЧРК,
– ГНСУ, обеспечивающая напуск в камеру инертного газа (аргона или гелия),
– СВО, обеспечивающая требуемое давление газа.

2.4. Система водяного охлаждения

СОВ предназначена для отвода выделяющегося тепла от следующих компонентов оборудования установки Т-15МД:

– обмотки электромагнитной системы,
– элементов конструкции разрядной камеры (дивертор),
– оборудования плазменных диагностик (диагностический инжектор, болометры),
– оборудования СВО,
– оборудования систем дополнительного нагрева плазмы.

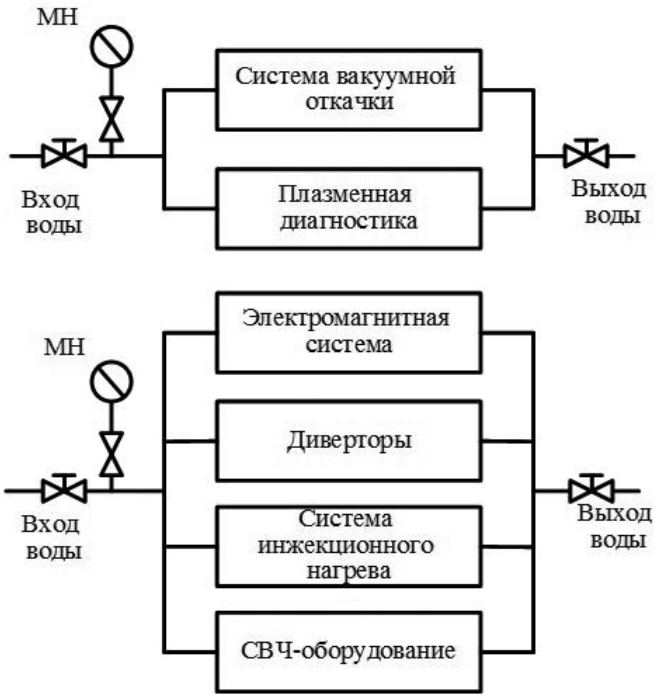


Рис. 4. Структурная схема СОВ токамака Т-15МД

СОВ работает по замкнутой схеме. В цикле охлаждения используется дистиллированная вода. Хладагентом для охлаждения дистиллированной воды служит речная вода.

Структурная схема СОВ приведена на рис. 4.

Оборудование, подключённое к системе водяного охлаждения разбито на две ветки в зависимости от давления охлаждающей воды (5 и 10 атмосфер). Каждая ветка запитывается собственным насосом.

3. Автоматизированные системы управления установки «Токамак Т-15МД»

Автоматизация всех стадий подготовки и проведения экспериментальных и исследовательских работ на установке осуществляется распределённой информационно-управляющей системой Т-15МД (ИУС Т-15) [4], в состав которой входят следующие компоненты:

– АСУ инженерных систем (АСУ ИС);
– АСУ технологических систем подготовки токамака к плазменному эксперименту (АСУ ТС);
– АСУ системы импульсного электропитания магнитных обмоток токамака (АСУ СИЭП);
– АСУ систем дополнительного нагрева и поддержания тока плазмы (АСУ СДН);
– система управления плазмой (СУП);
– система сбора и обработки экспериментальных данных (ССОД);
– система координации и синхронизации скоростных систем (СКСС);
– центральная система управления (ЦСУ), локальная вычислительная сеть (ЛВС) и центр обработки данных (ЦОД).

Автоматизация и противоаварийная защита медленных процессов (характерная длительность цикла управления 100 мс), происходящих в инженерных и технологических системах токамака Т-15МД во время подготовки к эксперименту, реализована на основе платформы Schneider Electric. Инструментальная среда программирования контрол-

леров Unity Pro XL версии 7.0. – прикладное программное обеспечение на базе SCADA-системы InTouch (Wonderware). Это надёжное индустриальное решение, соответствующее задачам АСУ ТП токамака.

3.1. АСУ системы вакуумной откачки

АСУ системы вакуумной откачки (АСУ СВО) предназначена для автоматизированного управления системой вакуумной откачки установки Т-15МД.

Структурная схема АСУ СВО приведена на рис. 5.

АСУ СВО строится на основе программных и аппаратных средств фирмы Schneider Electric.

В качестве активного контроллерного оборудования используется оборудование семейства Quantum [5].

Прикладное программное обеспечение реализуется в виде программ, написанных на языках программирования в соответствии со стандартом МЭК 61131 в среде разработки Schneider Electric Unity Pro. Основной используемый язык – ST.

Комплекс аппаратных средств АСУ СВО включает:

- шкаф контроллерный, который построен на основе двух контроллеров Quantum 140CPU67160 (горячее резервирование);
- шкафы распределённого ввода-вывода, построенные по архитектуре RIO-Ethernet Schneider Electric. Шкафы оснащены требуемой номенклатурой модулей ввода-вывода.

В состав АСУ СВО также входят автоматизированные рабочие места (АРМ), описание которых приведено в разделе 3.4.

3.2. Общесистемная АСУТП

Функциональность АСУ ТС (обезгаживающий прогрев, чистка камеры тлеющим разрядом, водяное охлаждение) реализована на едином программно-аппаратном комплексе – общесистемной автоматизированной системе управления технологическим процессами (ОС АСУТП).

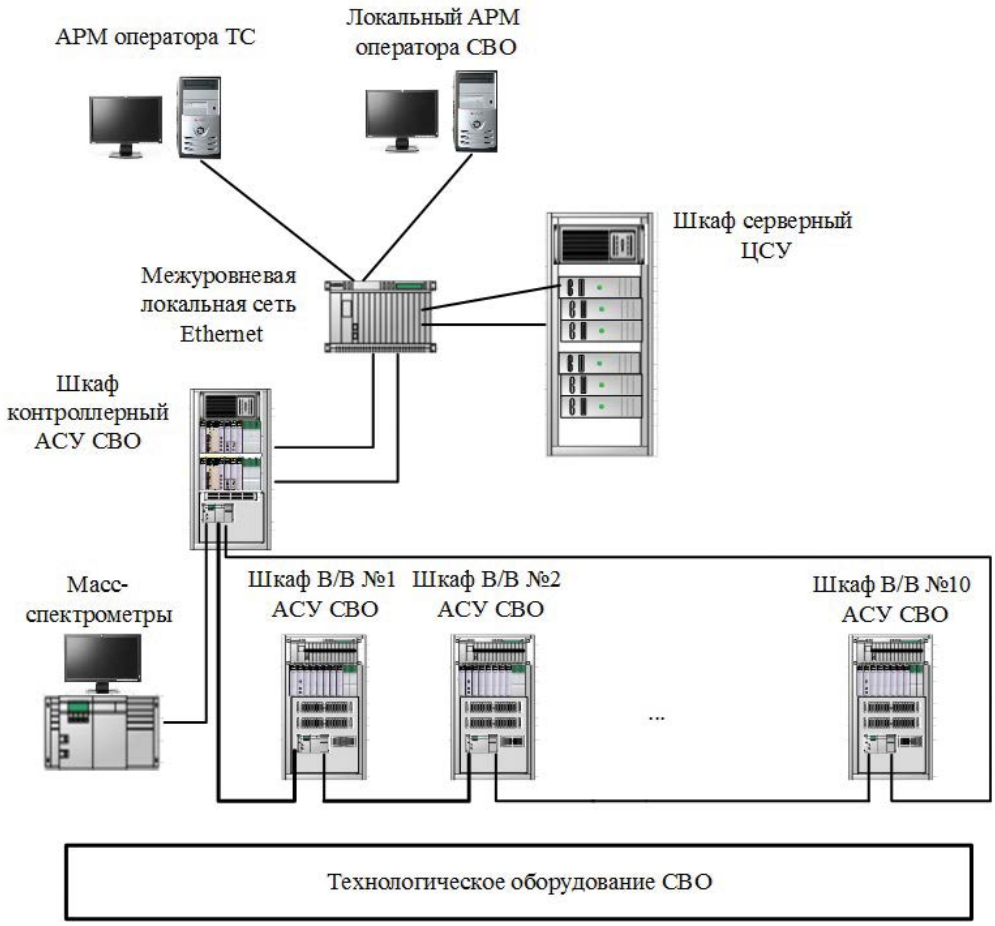


Рис. 5. Структурная схема АСУ СВО

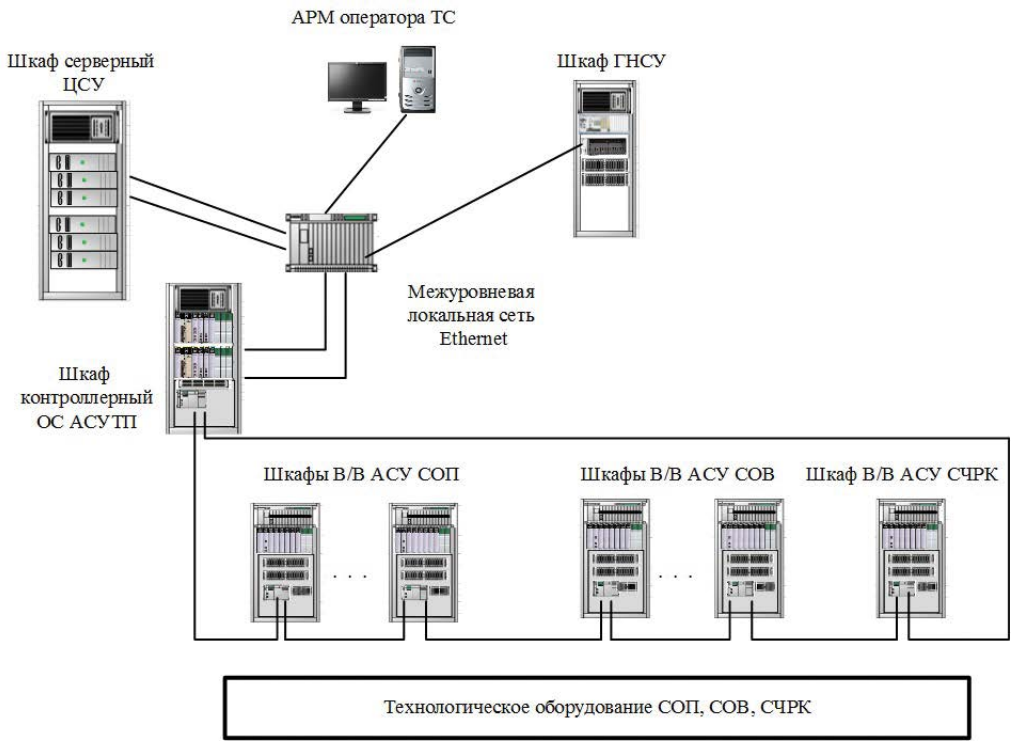


Рис. 6. Структурная схема ОС АСУТП

Структурная схема ОС АСУ ТП приведена на рис. 6.

Так же, как и АСУ СВО, ОС АСУ ТП строится на основе программных и аппаратных средств фирмы Schneider Electric (контроллерное оборудование Quantum, инструментальное программное обеспечение Unity Pro).

Шкафы ввода-вывода комплекса распределены между АСУ подсистем и оснащены соответствующей номенклатурой модулей ввода-вывода.

3.3. Система общесистемных блокировок и противоаварийных защит

Система общесистемных блокировок и противоаварийных защит (ОС АЗ), входящая в состав ИУС Т-15, обеспечивает реализацию функций межсистемной координации, межсистемных блокировок и противоаварийных защит для технологических подсистем ИУС Т-15, а также смежных с ними подсистем:

– АСУ ГНСУ,
– АСУ системы СВЧ-нагрева;
– АСУ криогенного обеспечения;
– АСУ энергоснабжения.

ОС АЗ взаимодействует также с ЦСУ ИУС Т-15. Взаимодействие осуществляется по ЛВС ИУС Т-15.

Физический интерфейс ОС АЗ с подключёнными подсистемами осуществляется с использованием межуровневой кольцевой оптоволоконной сети Ethernet.

Помимо этого ОС АЗ имеет собственную распределённую систему ввода-вывода, обеспечивающую сбор данных и выдачу команд на технологическое оборудование подключённых подсистем.

Структурная схема ОС АЗ приведена на рис. 7.

ОС АЗ строится на основе программных и аппаратных средств фирмы Schneider Electric. В качестве активного контроллерного оборудования используется оборудование семейства Quantum.

С учётом особых требований к данной системе в ней используются аппаратные и программные средства, сертифицированные на соответствие уровню безопасности SIL3.

Прикладное программное обеспечение реализуется в виде программ, написанных на языках программирования в соответствии со стандартом МЭК 61131 и допустимых в среде разработки Schneider Electric Unity Pro XLS (FBD, LD).

Комплекс аппаратных средств ОС АЗ включает:

– шкаф контроллерный ОС АЗ, который построен на основе двух контроллеров Quantum 140CPU67160S (соответствие STL3, горячее резервирование);
– шкафы распределённого ввода-вывода, построенные по архитектуре RIO-Schneider Electric. Шкафы оснащены требуемой номенклатурой модулей ввода-вывода, в том числе соответствующие уровню безопасности SIL3.

3.4. Автоматизированные рабочие места технологических систем

В состав АРМ ТС ИУС Т-15 входят:
– АРМ оператора технологических систем (АРМ ТС),
– АРМ системы вакуумной откачки (АРМ СВО).

АРМ ТС обеспечивает управление технологическими процессами подготовки установки к работе и контроль состояния установки во время эксперимента с возможностью детализации (укрупнённого вывода данных) по каждой подсистеме и изменения технологических процессов в них, ручным пуском и остановкой (блокировкой).

Основное назначение АРМ СВО:
– отображение состояния объектов системы вакуумной откачки в реальном времени;
– информирование оператора о нарушениях хода технологического процесса;
– ведение журнала аварийных сообщений;
– управление механизмами системы вакуумной откачки;
– архивирование технологических параметров и просмотр их за заданный промежуток времени.

АРМ ТС и АРМ СВО входят в состав ЦСУ ИУС Т-15, реализующей функции автоматизированной системы оперативного диспетчерского управления установкой Т-15МД.

ЦСУ разрабатывается и функционирует под управлением системной платформы Wonderware System Platform (Platinum-RT) [6].

Необходимое для функционирования АРМ ТС и АРМ СВО программное обеспечение, установленное на компьютеры, включает в себя:
– операционную систему Microsoft Windows 7 Professional x64;
– InTouch for System Platform 2014, Bootstrap.

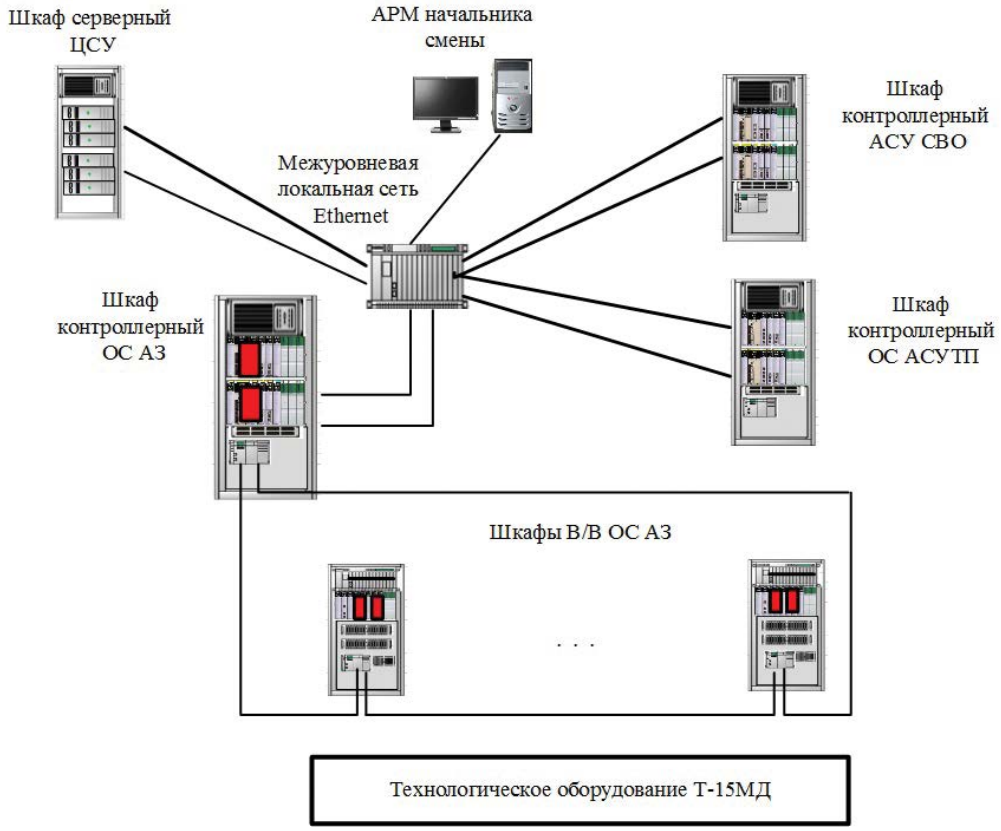


Рис. 7. Структурная схема ОС АЗ

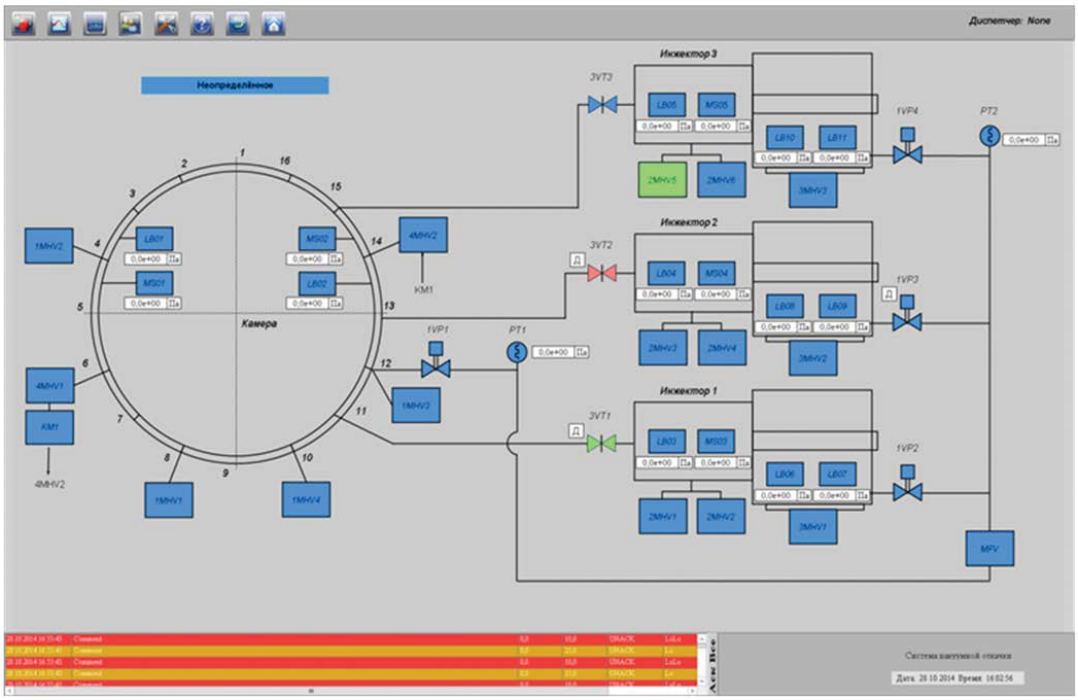


Рис. 8. Главное окно АРМ СВО

Примеры экранных форм АРМ приведены на рис. 8 и 9.

4. Функционирование АСУ ТС в процессе подготовки к эксперименту

В процессе подготовки эксперимента выполняется ряд следующих процедур с участием технологических подсистем:

– прогрев ВК,
– водяное охлаждение,
– вакуумная откачка,
– чистка камеры тлеющим разрядом (с участием технологического газонапуска).

4.1. Прогрев ВК

Прогрев ВК заключается в прогреве стенок камеры до температуры 200°С и поддержании данной температуры в течение длительного времени для проведения дегазации.

При этом во время прогрева разрядной камеры температурная неравномерность по оболочке не должна превышать 50–70°С. Равномерность прогрева и поддержания температуры на поверхности камеры обеспечивается включением и выключением (или плавным регулированием тока) источников питания нагревостойких кабелей на соответствующих зонах прогрева.

4.2. Водяное охлаждение

Используется для охлаждения элементов конструкций токамака и технологического оборудования. Охлаждение оборудования ряда ТС установки Т-15МД (система вакуумной откачки, системы дополнительного нагрева плазмы) осуществляется во время подготовки, проведения и завершения эксперимента.

4.3. Вакуумная откачка

Получение вакуумных рабочих давлений в объектах установки Т-15МД производится в два этапа:

– предварительной откачки до давления ~1 Па;
– высоковакуумной откачки до давления $<5\cdot10^{-6}$ Па.

Предварительная откачка состоит из следующих процедур:

– предварительной откачки разрядной камеры;
– предварительной откачки инжекторов.

Высоковакуумная откачка состоит из следующих процедур:

– турбомолекулярной откачки разрядной камеры;
– криогенной откачки разрядной камеры;
– турбомолекулярной откачка инжекторов;

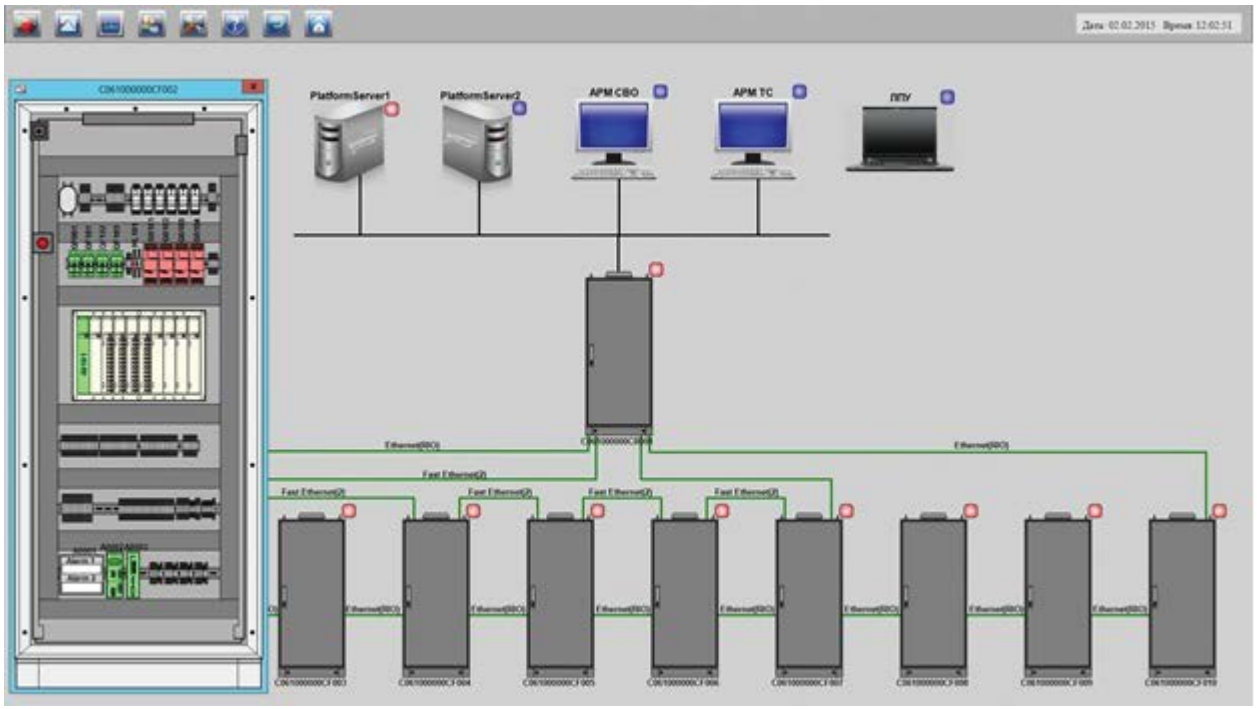


Рис. 9. Окно диагностики АСУ СВО

– турбомолекулярной откачки источников инжекторов.

Предварительная откачка разрядной камеры предназначена для получения низкого вакуума для возможности проведения дальнейшей высоковакуумной откачки.

Турбомолекулярная откачка разрядной камеры предназначена для получения высокого вакуума для возможности проведения рабочего импульса в разрядной камере.

Криогенная откачка разрядной камеры предназначена для получения в камере предельного остаточного вакуума.

Предварительная откачка инжекторов предназначена для получения низкого вакуума для возможности проведения дальнейшей высоковакуумной откачки.

Турбомолекулярная откачка инжекторов предназначена для получения высокого вакуума в объёмах инжекторов.

Турбомолекулярная откачка источников инжекторов предназначена для получения высокого вакуума в объёмах источников инжекторов.

4.3.1. Предварительная откачка

Периодичность выполнения предварительной откачки разрядной камеры – по команде оператора. Продолжительность выполнения предварительной откачки разрядной камеры 2–3 часа.

Предварительная откачка разрядной камеры завершается при достижении величины вакуума 1 Па в разрядной камере.

4.3.2. Высоковакуумная откачка

Высоковакуумная откачка состоит из турбомолекулярной и криогенной откачек.

4.3.2.1. Турбомолекулярная откачка

Продолжительность выполнения турбомолекулярной откачки разрядной камеры – от нескольких часов до нескольких дней.

Турбомолекулярная откачка разрядной камеры завершается при достижении величины вакуума $5 \cdot 10^{-4}$ Па в разрядной камере.

4.3.2.2. Криогенная откачка

Периодичность выполнения криогенной откачки разрядной камеры – каждые сутки. Продолжительность выполнения криогенной откачки разрядной камеры – около 10 часов.

Криогенная откачка разрядной камеры завершается при достижении величины вакуума $5 \cdot 10^{-6}$ Па в разрядной камере.

4.4. Чистка камеры тлеющим разрядом

Процедура тлеющего разряда состоит из следующих шагов:

– установка электродов (выдвижные штыри тлеющего разряда, 4 шт.) в рабочее положение, по команде начальника смены;

– задание уставок тока и напряжения;
– запуск процедуры «Согласование запуска с АСУ СВО и АСУ ГНСУ»;
– при достижении давления в рабочей камере (для Ar: $(3–5)\cdot10^{-3}$ торр; для He: $(4{,}8–5)\cdot10^{-3}$ торр) пробой от первого источника при напряжении 2,5 кВ и токе 10 мА за время 0,1 мкс;
– включение 2-го источника тока и поддержание тлеющего разряда с параметрами тока 15 А и напряжения 700–800 В. (Ar – 8 А, 750–800 В, уменьшение напряжения разряда на 50 В от начального является признаком очистки камеры от CO; He – 4,5 А, 380–400 В);
– отслеживание давления и состава остаточного газа в рабочей камере АСУ СВО (вакуумметрия и масс-спектрометрия). При этом контролируется заданное давление в камере и уменьшение отношений парциальных давлений остаточного газа. Отслеживание тока и напряжения источника питания;
– при достижении требуемых значений отключение источника питания;
– вывод электродов в нерабочее положение.

Ориентировочная длительность процедуры около 3 часов для аргона, 12–20 часов для гелия.

В процессе подготовки к эксперименту выполняется высоковакуумная откачка от атмосферного давления и дегазация вакуумной камеры токамака с периодическим обезгаживающим прогревом стенок камеры и очисткой стенок камеры токамака тлеющим разрядом.

4.5. Поддержание технологических параметров в процессе эксперимента

В процессе эксперимента выполняется высоковакуумная откачка разрядной камеры с одновременным напуском рабочего газа с целью поддержания расчётного значения давления (плотности электронов) в камере. Одновременно выполняется охлаждение элементов конструкции и оборудования токамака, подготовка к новому эксперименту.

Расчёты показали, что нет необходимости охлаждать первую стенку токамака Т-15МД водой. Но предусмотрено охлаждение водой диверторных пластин, которые планируется установить в токамаке после физического пуска. Также осуществляется охлаждение водой катушек электромагнитной системы.

Заключение

В настоящее время работы по модернизации установки токамак Т-15МД переходят в фазу подготовки к физическому пуску. Подготовка и проведение физического пуска предполагает полномасштабное использование подсистем управления технологическим оборудованием.

В том числе стоит задача проведения индивидуальных испытаний технологического оборудования и конструкций установки.

На 2018 г. запланировано проведение автономных и комплексных испытаний отдельных технологических подсистем ИУС Т-15 с развёрнутым к настоящему времени технологическим оборудованием.

Уже проведённые автономные испытания частей подсистем ИУС Т-15 показали правильность заложенных в системы управления решений. В ходе реализации АСУ ТС установки Т-15МД будут получены решения, которые можно будет использовать и при создании перспективных установок УТС, например экспериментального энергетического термоядерного реактора ДЕМО [7].

Ссылки

1. Федеральная целевая программа «Ядерные энерготехнологии нового поколения на период 2010–2015 годов и на перспективу до 2020 года». Постановление Правительства Российской Федерации от 3 февраля 2010 г. №50.

2. P. P. Khvostenko, I. O. Anashkin, V. A. Belyakov and others. // Status of Tokamak T-15MD. 26th IAEA Fusion Energy Conference (CN-234), FIP/P7–40.

3. Кутеев Б. В., Гончаров П. Р., Сергеев В. Ю., Хрипунов В. И. Мощные нейтронные источники на основе реакций ядерного синтеза // Физика плазмы, 2010, т. 36, С. 307–346.

4. 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.

5. Программируемые логические контроллеры Modicon Quantum. Брошюра. Schneider Electric. Май 2011.

6. А. Н. Ханыгин, С. В. Кирюхин (ЗАО «РТСофт»). // Отечественная инструментальная платформа для разработки информационно-управляющих систем «PLATINUM-RT». Автоматизация & IT в энергетике. 2015, №01.

7. Колбасов Б. Н., Борисов А. А., Васильев Н. Н. и др. Концепция демонстрационного термоядерного реактора ДЕМО–С // Вопросы атомной науки и техники. Сер. Термоядерный синтез, 2007, вып. 4, С. 3–13.

Кто и зачем использует Микрогрид?

Элиза Вуд (Elisa Wood) | Microgrid Knowledge

Сегодня многие предприятия и учреждения используют микросети (microgrid – микросеть, микрогрид) с целью повысить надёжность энергоресурсов, сделать электроснабжение более экологичным, снизить затраты, повысить эффективность и улучшить обслуживание потребителей или местного сообщества.
По мере активного развития технологии микрогрид становятся очевидны преимущества её применения в широких масштабах. Расскажем подробнее о том, какие предприятия и учреждения используют микрогрид и зачем.

Микросети в больницах

По данным Бюро переписи США, пожилых людей в США станет вдвое больше. Это приведёт к необходимости увеличения числа больниц, сетей здравоохранения, домов престарелых, центров дневного ухода за престарелыми людьми и домов-интернатов для престарелых инвалидов.

При этом больницы потребляют в 2,5 раза больше электроэнергии, чем коммерческие здания такого же размера.

Неудивительно, что руководители учреждений здравоохранения так озабочены проблемой энергопотребления, особенно ввиду ожидаемого роста цен на электричество в ближайшие годы.

Установленные в больницах микросети позволяют эффективно и грамотно планировать объёмы энергопотребления. Контроллер микросети улучшенного действия способен обеспечить оптимальную и синхронную работу различных компонентов энергооборудования. С его помощью ресурсы микросети используются в круглосуточном режиме, удовлетворяя потребности руководства больницы в электроэнергии в любое время.

Микросети в учреждениях здравоохранения – не просто красивые генераторы. Они органично объединяют источник электроснабжения больницы с электростанцией, резервными генераторами и внутренними источниками питания, используя динамичную программную логику. Такая микросеть призвана обеспечить потребности больниц в энергоснабжении и снизить на него затраты. А руководство больницы обязано при этом обеспечить работу отделения интенсивной терапии и реанимации для помощи тяжелобольным.

Микросети для университетов и исследовательских учреждений

Первыми использовать технологию микросетей начали колледжи и университеты США. Это объяснялось необходимостью круглосуточно обеспечивать студенческие городки стабильной и доступной электроэнергией. Для этого микросеть должна постоянно находиться в рабочем состоянии, чтобы обслуживать студенческий городок и более широкое сообщество, а в случае отключения электроэнергии – стать её резервным источником.

Микросети особенно важны для исследовательских лабораторий при университетах, поскольку в таких лабораториях часто хранятся образцы, чувствительные к изменениям температуры. И в случае аварийного отключения будут потеряны годы работы и миллионы долларов.

Микросети часто устанавливают в колледжах и университетах для решения вопросов изменений климата. Кроме того, микросети могут использоваться в программах-тренажёрах для студентов энергетических факультетов.

Студенческие городки потребляют большое количество тепла, пара и горячей воды, поэтому зачастую они становятся подходящим местом для установки микросетей, обеспечивающих комбинированное производство электроэнергии и тепла. Установки для комбинированной выработки тепла и электроэнергии используют тепло как побочный продукт выработки электрической энергии. Благодаря этому комбинированная выработка тепла и электроэнергии представляет собой эффективный энергоресурс.

В США усовершенствованные микросети установлены в университетах, среди которых – Принстонский университет, Техасский университет в Остине и Калифорнийский университет в Сан-Диего.

В Алгонкин-колледже (Онтарио) микрогрид наглядно демонстрирует, как можно получить максимальный доход от инвестиций. Мощность микросети вдвое превышает мощность установки для комбинированной выработки тепла и электроэнергии – от 2 до 4 мегаватт, что позволило обеспечить источник электропитания колледжа непосредственно на его территории. Микрогрид объединяет такие экологически чистые технологии, как использование солнечной энергии и наличие аккумуляторов для хранения энергии, а также удовлетворяет потребность в энергии и обеспечивает регенерацию тепла для колледжа. Установленная в Алгонкин-колледже микросеть может работать независимо от центральной сети. Правда, только в случае аварийного отключения или при условии экономической выгоды от изолированного электроснабжения. В остальных случаях микрогрид будет обеспечивать энергоснабжение параллельно с местной электростанцией.

Умные города и сообщества

Многие сообщества начали использовать микросети после череды ураганов на северо-востоке США в течение последних десяти лет. Коннектикут, Массачусетс, Нью-Джерси и Нью-Йорк запускают программу государственного финансирования в помощь сообществам.

Во время аварийных отключений общественные микросети (также называемые «публичные микросети»), как правило, обеспечивают электроэнергией службы жизнеобеспечения, такие как полиция, пожарная служба, телекоммуникационные башни и станции очистки сточных вод. Помещения многих микросетей служат также убежищем во время урагана.

Микросети часто выступают частью концепции умных городов. Умные города позволяют наиболее эффективно осваивать бюджетные средства, благодаря использованию технологий, позволяющих анализировать, улучшать и предоставлять услуги жителям и гостям города. С помощью технологически сложных контроллеров микросети помогают удовлетворить потребности в электроснабжении целого умного города.

Так, микросети используются в концепции умного города Питтсбурга. В городе планируется построить системы энергоснабжения, которые будут связаны с интеллектуальными системами электропитания, транспорта и коммуникаций. В самом городе и в пригородах планируется установить микросети, которые будут работать вместе и объединять существующие в районах энергосистемы.

Локальная сеть микрогридов в Питтсбурге спроектирована с учётом потребностей больниц, университетов, информационно-аналитических центров и объектов жизнеобеспечения населения. Власти города надеются усилить безопасность сетей, сократить избыточность и разработать систему бесперебойной подачи электроэнергии на предприятия и компании за счёт «взаимодействия» городских энергосистем.

Городу нужны микросети, способные обеспечить более эффективное энергоснабжение в будущем.

«Концепция электростанции, расположенной в 100 милях от твоего дома и генерирующей электроэнергию для приготовления твоего тоста, осталась в XIX веке», – сказал мэр Питтсбурга Вильям Педуто.

Микросети для правительственных зданий

Правительство штата Нью-Йорк не только учит, как делать, но и делает, как учит. Непонятно? На самом деле всё просто. Штат, который

уже давно поощряет и финансирует установку микросетей силами местных сообществ, и сам построит собственную микросеть в г. Олбани, где работает правительство штата.

В столице штата Нью-Йорк микрогрид мощностью 16 мегаватт будет обеспечивать электроэнергией комплекс административных и общественных зданий площадью 98 акров Эмпайр-Стейт-Плаза (Empire State Plaza) губернатора Нельсона А. Рокфеллера, (рис. 1). Это один из примеров того, как само правительство способно обеспечить более эффективную и отказоустойчивую систему энергоснабжения своих зданий с помощью микросетей.

90% поставляемой микрогридом в г. Олбани электроэнергии будет составлять комбинированная выработка тепла и электроэнергии, а также теплоснабжение и охлаждение 10 зданий, в которых работают 11 000 государственных служащих. Ожидается, что после перевода микросети в онлайновый режим в конце 2019 г. ежегодные расходы штата на электроэнергию сократятся на 2,7 миллиона долларов.

Руководство штата разместит микрогрид в Олбани, чтобы исключить аварийное отключение электропитания в кризисной ситуации и обеспечить оказание государственных услуг населению. Проект также призван помочь штату в снижении парниковых выбросов на 40 % к 2030 году (по сравнению с уровнем 1990 года). По подсчётам властей штата, микрогрид позволит сократить их объём на 25 600 тонн в год.

Микросети для коммунальных нужд

Коммунальные службы и их клиенты заинтересованы в более низких ценах, надёжных услугах и экологически чистой электроэнергии – всё это может обеспечить микрогрид.

В последнее время коммунальные службы всё чаще рассматривают микросети не как соперника, а как решение. Только в 2016 году коммунальные компании инвестировали минимум 1,2 миллиарда долларов, чтобы получить возможность использовать микросети и распределённую энергию. Среди инвесторов – крупные поставщики коммунальных услуг, такие как Duke Energy, Exelon, National Grid, Sempra и Southern Company (рис. 2).

Рис. 1. Комплекс Эмпайр-Стейт-Плаза в Олбани, штат Нью-Йорк

Для коммунальных служб микросети – это более дешёвый вариант покрыть потребности в электроэнергии во время пиковых нагрузок и решить ряд других проблем, связанных с цепочкой поставок. Локальные энергетические микросети называются также беспроводной альтернативой централизованной инфраструктуре – электростанциям, подстанциям, системам передачи и распределения электроэнергии.

Одни коммунальные компании в США разрабатывают микросети для потребителей в своей зоне обслуживания; у других есть конкурентоспособные филиалы, которые устанавливают микросети по всей стране. Например, компания Duke Energy работает в обоих направлениях.

Однако создание микросетей для коммунальных нужд не обходится без конфликтов и «палок в колёса». Коммунальные службы в неко-

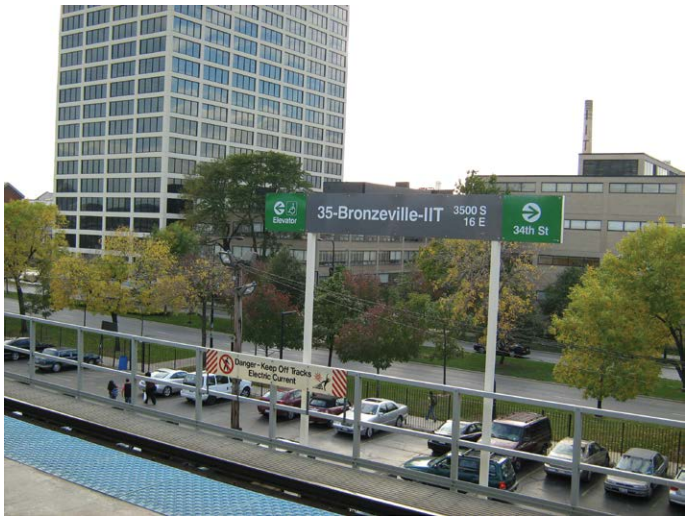


Рис. 2. Энергетическая компания Commonwealth Edison планирует построить микрогрид в чикагском районе Бронзвилл

торых штатах пытаются убедить власти штата разрешить им оплачивать микросети за счёт налогоплательщиков. Оппоненты заявляют, что микросети выгодны только ограниченному числу потребителей, поэтому за них не должны платить все. Коммунальщики возражают: налогоплательщики могут не беспокоиться о том, на что будут потрачены их деньги, ведь микросети различными способами дополняют более широкую сеть. Например, коммунальная служба использует микрогрид в качестве источника энергоснабжения и для обслуживания всей сети в периоды повышенного спроса на электроэнергию. Или как «островок энергобезопасности» для населения во время сильной непогоды.

Также существуют разногласия по поводу того, стоит ли разрешать владение микросетями и использование их штатам, подвергшимся реорганизации. В таких штатах независимые компании имеют право конкурировать с энергетическими предприятиями за право поставлять энергоресурсы потребителям. Чтобы обеспечить равные конкурентные условия, власти этих штатов запрещают энергетическим компаниям владеть электростанциями. Поэтому возникает вопрос, можно ли считать микрогрид электростанцией.

Военные микросети

Пэррис-Айленд известен как тренировочная база морской пехоты США, на которой готовят одних из лучших солдат мира.

Но скоро Пэррис-Айленд станет и домом для самой «стойкой» микросети в мире.

Микросеть, которая предназначается для Рекрутского депо морской пехоты (MCRD) на Пэррис-Айленд, штат Южная Каролина, будет включать новую газифицированную установку для комбинированной выработки тепла и электроэнергии мощностью 3,5 мегаватт, фотоэлектрические солнечные панели мощностью 6,7 мегаватт (постоянный ток), а также аккумуляторные батареи мощностью 8 мегаватт/час.

Благодаря чему эта микросеть так устойчива?

Её современный высокотехнологичный контроллер отслеживает и координирует передачу энергии, а также работу аварийных дизельных генераторов. Он постоянно проверяет качество подключения к энергосетям и в случае аварийного отключения питания изолирует микрогрид. Электроэнергия будет поступать на военную базу от установленных на месте источников электропитания. Контроллер также облегчит работу системы быстрого сброса нагрузки.

Микрогрид Пэррис-Айленда – лишь один из нескольких аналогичных проектов по всей стране, цель которых – обеспечить военные базы автономными источниками питания. Кроме того, в настоящее время микросети устанавливаются на военных объектах с целью сделать электроэнергию экологически чистой и повысить уровень кибербезопасности.

Микросети находят применение и непосредственно в зоне боевых действий – передвижные модули можно установить в сжатые сроки. В мобильных микросетях часто используются возобновляемые источники энергии или батареи, поэтому устраняется необходимость доставки топлива на отдалённые посты. Случай в Афганистане наглядно показал, как экономия топлива спасает жизни. По данным армейского исследования, в этой стране было совершено нападение на один из 24 топливных конвоев США, что привело к человеческим жертвам.

Микросети для складов и заправочных станций

Хьюстон часто подвергается атакам ураганов, ветров и наводнений. Поэтому один из главных принципов работы местной сети супермаркетов H-E-B – своевременное оказание помощи во время стихийного бедствия. «Двери наших магазинов всегда открыты для тех, кто нуждается в помощи. Таким образом мы лишь укрепляем свои позиции в служении нашим гражданам», – сказал Джордж Прессес, вице-президент топливно-энергетического комплекса сети продуктовых магазинов, которая обслуживает население вот уже 110 лет. Сеть H-E-B насчитывает более 370 магазинов в США и Мексике, а её годовой объём продаж равен 23 миллиардам долларов.

Неудивительно, что микросети были установлены в 45 магазинах сети по всему Хьюстону. За счёт использования генераторов, работающих на природном газе, микросети

обеспечат непрерывную работу холодильных установок в магазинах, а покупатели смогут приобрести продукты и такие незаменимые на случай аварийного отключения электроэнергии запасы, как уголь, свечи, батарейки и фонарики.

В Бруклине, штат Нью-Йорк, владельцы сети продуктовых магазинов Whole Foods организовали микрогрид, которая в случае аварийного отключения электроснабжения поможет жителям города зарядить телефон, связаться с членами семей и обеспечит их горячей пищей.

Кроме того, общественные микросети по всей стране предусматривают и наличие станций обслуживания в своей сети энергоснабжения. Как и продуктовые магазины, станции обслуживания находятся в частной собственности, но городские власти считают их настоящими объектами жизнеобеспечения, которые являются не только своего рода «заправочными» станциями для жителей города, но и обеспечивают работу полицейского управления, пожарной службы, спасательной службы и национальной гвардии, а также коммунальных служб. Преимуществом станций обслуживания с круглосуточными магазинами является и возможность приобрести продукты питания, необходимые запасы, зарядное устройство для мобильных телефонов и другие приборы в случае аварийного отключения электричества.

Микросети для организаций и производственных предприятий

До недавнего времени микросети использовали в основном военные, местные сообщества, учебные заведения и энергетические компании. Но сегодня ситуация меняется. По данным исследователей из Navigant Research, в настоящее время технологию микросетей планируют внедрить бизнес-компании и производственные предприятия, опережая другие отрасли.

Это обусловлено несколькими причинами. Прежде всего, аварийные отключения электроэнергии больно бьют по национальной экономике. На ликвидацию их последствий правительство США ежегодно тратит 18–33 миллиардов долларов.

Особенно дорого аварийные отключения обходятся центрам обработки и хранения данных – и ситуация только ухудшается. В Институте Понемон (Ponemon Institute) говорят, что средняя стоимость аварийного отключения электричества в дата-центре увеличилась с 505 502 долларов в 2010 году до 740 357 долларов в 2016, то есть рост составил 38 %.

Для промышленного предприятия даже кратковременное отключение электричества тоже может привести к значительным убыткам. Например, если из-за отключения питания оборудование по переработке молока останавливается всего на несколько минут, его придётся полностью выключить для очистки в соответствии с требованиями безопасности. Этот процесс может занять несколько часов.

А установка микросети на территории бизнес-парков способна привлечь многих ключевых арендаторов, для которых вопрос аварийных отключений стоит особенно остро. Также есть большая вероятность привлечения предприятий, клиенты которых поддерживают принципы защиты окружающей среды и предпочитают сотрудничать с предприятиями, разделяющими их ценности.

Более того, благодаря эффективности микросетей и их способности влиять на развитие рынков энергоносителей можно снизить затраты на энергоресурсы – ещё один большой плюс для бизнес-парков. Микросети с установкой для комбинированной выработки тепла и электроэнергии предлагают значительное финансовое преимущество для промышленного производства, требующего большого количества тепла, пара, кондиционирования воздуха или горячей воды.

Микросети для жилых домов

Микросети всё еще слишком дороги для большинства домохозяйств, но уже есть исключения. Например, микросети могут стать экономически выгодным решением для многоквартирных домов (рис. 3).

В июне 2017 года в Нью-Йорке была представлена первая микросеть, обслуживающая жилой комплекс Marcus Garvey. Она была установлена в рамках проекта рефинансирования

Рис. 3. Микросети могут стать экономически выгодным решением для многоквартирных домов

и реновации стоимостью 190 миллионов долларов для 10 кварталов Бруклина Дополнительно к новым кухням, ванным комнатам и другим удобствам жилой комплекс на 625 квартир теперь оснащён микрогридом с солнечными батареями и хранилищем энергии (solar plus storage). Солнечные панели общей мощностью 480 киловатт, соединённые с топливным элементом на 400 киловатт и литиевой батареей на 300 киловатт, установлены на 21 участке крыши жилого комплекса.

Помимо этого, микросети используются в районах, где источники питания в нескольких домах образуют виртуальную электростанцию. Коммунальная компания Green Mountain Power (GMP) в штате Вермонт недавно установила микросети типа solar plus storage в 14 модульных домах, где проживают квартиросъёмщики с низкими доходами. Используемые в системе аккумуляторные батареи обеспечивают резервное питание во время аварийных отключений электричества. Кроме того, они служат универсальным энергоресурсом, позволяющим энергетической компании снизить расходы на обслуживание микросети. Компания-владелец этих систем аккумулирует и перенаправляет энергию батареи на сеть в периоды повышенного энергопотребления. Цель компании GMP – снизить расходы на передачу электроэнергии и плату за установленную мощность в адрес организации ISO New England.

Источник:

https://microgridknowledge.com/microgrids-businesses-institutions/

НОВОСТИ

«РТСофт» получил сертификаты СТ-1 ТПП для компьютеров BLOK

28 августа 2017 года на машины серий BLOK Rugged и BLOK Industrial компания «РТСофт» получила сертификаты происхождения товара по форме СТ-1 Торгово-промышленной палаты РФ. Сертификаты получены в полном соответствии с процедурой ТПП РФ.

Цели получения сертификатов:

а) соблюдение регламентов таможенного регулирования при экспортировании товаров в страны СНГ;

б) исполнение требований законодательства РФ при закупках для обеспечения государственных и муниципальных нужд.

Сертификаты получены в том числе для упрощения бизнеса партнёров АО «РТСофт» при поставках компьютеров BLOK собственным клиентам или при использовании машин в составе целевых систем, разработка, производство и поставка которых требует использования входящих комплектующих отечественного производства, подтверждённого сертификатами происхождения товара в соответствии с законодательным полем РФ.

АО «РТСофт» видит свою миссию не только в разработке и производстве надёжной, удобной и конкурентоспособной продукции мирового класса, но и в обеспечении этой продукции адекватным набором легитимных юридических механизмов, позволяющим вести бизнес в точном соответствии с законодательством РФ. Такой подход гарантирует клиентам компании предельную минимизацию рисков, удобство и выгоды кооперации с «РТСофт» по использованию компьютеров семейства BLOK и поддерживающих сервисов компании.