WWW.SOEL.RU

Современная электроника

4
2021

YouTube

КТО ОБЕСПЕЧИТ ТЕХНОЛОГИЧЕСКУЮ НЕЗАВИСИМОСТЬ РОССИИ?

В номере:

Сделайте измерения в своей лаборатории эффективнее!

Для тестирования доступны демо-версии приборов MFLI/MFIA (синхронный усилитель/анализатор импеданса до 5МГц), а также HDAWG8 (8-канальный генератор сигналов произвольной формы до 600 МГц)

Генераторы сигналов произвольной формы

- 2.4 гигасэмплов/с, 16 бит, 750 МГц
- количество каналов - 4, 8 и более
- <50 нс время реакции на триггерные сигналы

Типичные области применения
Тестирование полупроводников, создание квантовых компьютеров, разработка и тестирование фазированных решеток, лидары спектроскопия, ЯМР

Анализаторы импеданса

- Частоты от DC до 5 МГц, сопротивления от 1 мОм до 1 ТОм
- Базовая точность 0,05%
- Встроенные в ПО советник по компенсации и индикатор ошибок

Типичные области применения
Высокодобротные диэлектрики, емкостные сенсоры, суперконденсаторы, PV-материалы, характеризация компонентов

Синхронные усилители

- Частоты до 600 МГц
- ПО: Scope, FFT, FRA, Sweeper, Imaging tool
- Доступные опции: AWG, PID, PLL, усреднитель (Boxcar), счетчик импульсов, AM & FM модуляция

Типичные области применения
AFM, LVP, CARS, SRS, SNOM, исследования графена, оптические PLL, THz, зондовая накачка, RFID, MEMS, NEMS, NDT, MRFM

ПО LabOne®

Все инструменты оснащаются ПО LabOne — специально разработанным Zurich Instruments управляющим ПО, предоставляющим множество функций, удобный интерфейс и обеспечивающем эффективную работу. Вы можете получить доступ к прибору через любой веб-бразуер или интегрировать его в ПО LabVIEW, MAT-LAB, Python, C и .NET

Zurich Instruments

info@zhinst.com • www.zhinst.com

ПОСТАВКА КРИОГЕННОГО, ИЗМЕРИТЕЛЬНОГО, ОПТИЧЕСКОГО И АНАЛИТИЧЕСКОГО ОБОРУДОВАНИЯ ДЛЯ ИССЛЕДОВАНИЙ

CRYOTRADE engineering
...WE MAKE IDEAS WORK

sales@cryotrade.ru • www.cryotrade.ru • +7 (495) 374-6952

ТЕСТПРИБОР

ИСПЫТАТЕЛЬНАЯ ЛАБОРАТОРИЯ ЭЛЕКТРОННОЙ КОМПОНЕНТНОЙ БАЗЫ

АО «ТЕСТПРИБОР» ПРОВОДИТ СЕРТИФИКАЦИОННЫЕ ИСПЫТАНИЯ ЭКБ

Преимущества:

- ☑ Безупречное качество всех выполняемых работ
- ☑ Конфиденциальность
- ☑ Независимая оценка
- ☑ Современное оборудование
- ☑ Квалифицированный инженерно-технический персонал

ВИДЫ РАБОТ

- Анализ применяемой ЭКБ, сбор и разработка технической документации
- 100% входной контроль и идентификация продукции
- 100% отбраковочные испытания
- 100% диагностический неразрушающий контроль
- Разработка программного обеспечения и методик сертификационных испытаний
- Климатические испытания
- Механические испытания
- Разработка и изготовление технологической оснастки

+7 (495) 657-87-37
tp@test-expert.ru
www.test-expert.ru
125480, г. Москва,
ул. Планерная, д. 7А

Планка запросов к вычислительной мощности, объёмам памяти, скорости передачи данных между устройствами, их энергопотреблению, непрерывно поднимается. Между тем, казалось, незыблемые законы Мура и Деннарда о ежегодном удвоении плотности упаковки транзисторов в чипах и соответствующем повышении их вычислительной мощности, дают сбои. В области традиционной кремниевой электроники темпы роста явно замедляются: битва за микроминиатюризацию привела к столь малым размерам элементов чипов, что начинают сказываться физические ограничения, приводящие к недостатку проводимости и появлению недопустимых токов утечки. Тем не менее экономически эффективной альтернативы кремнию пока не придумали.

Многие специалисты видят перспективы не в экстенсивном наращивании плотности транзисторов на квадратный миллиметр поверхности кристалла, а в создании сложных полупроводниковых структур нового поколения на основе нитрида галлия. Такие структуры могут обладать на несколько порядков высшими быстродействием и энергоэффективностью, поэтому как нельзя лучше подойдут для реализации вычислителей в составе носимых гаджетов эпохи 5 и 6G. В качестве замены кремнию при производстве наноэлектронных устройств рассматриваются графен и углеродные нанотрубки, удивляющие своими необычными свойствами. Экспериментальный углеродный нанотранзистор уже создан. Хотя идея использовать наноуглерод витает в воздухе чуть ли не 20 лет, до промышленных технологий всё ещё далековато.

IBM, Google, Intel и другие высокотехнологичные компании работают над созданием компьютеров на основе сверхпроводящих структур, функционирующих по законам квантовой механики. В частности, проводятся эксперименты с квантовыми ячейками-битами (quantum bit), но физикам и компьютерным архитекторам предстоит сделать очень многое, прежде чем потенциал квантовых вычислений будет реализован. И хотя экспериментально уже достигнуты впечатляющие результаты быстродействия, основную проблему – работоспособность устройств лишь при близких к абсолютному нулю температурах – пока преодолеть не удалось.

Не теряют времени и системные архитекторы: лауреаты премии Тьюринга Джон Хеннесси и Дэвид Паттерсон выдвинули плодотворную идею доменноспецифичных архитектур. Аппаратные архитектуры вычислителей, «заточенные» под предметную область, вкупе с применением предметноориентированных языков программирования, существенно повысят эффективность вычислительных платформ.

Каким путём пойдёт прогресс? Не забывайте: самые яркие страницы истории написаны энтузиастами, кажущимися большинству фантазёрами и мечтателями. «Современная электроника» представляет на ваш суд множество уникальных публикаций о перспективных технологиях. Читайте наш журнал и смотрите наш YouTube¬канал! Оставаясь с нами, вы всегда будете в центре событий!

Всего вам доброго!

Юрий Широков, главный редактор

Журнал «Современная электроника»
Издаётся с 2004 года

Главный редактор Ю. В. Широков
Заместитель главного редактора
Д. А. Трофимов
Редакционная коллегия А. Е. Балакирев, В. К. Жданкин, С. А. Сорокин, Р. Х. Хакимов
Вёрстка А. М. Бабийчук
Обложка Д. В. Юсим
Распространение А. Б. Хамидова (info@soel.ru)
Реклама И. Е. Савина (advert@soel.ru)

Учредитель и издатель ООО «СТА-ПРЕСС»
Генеральный директор К. В. Седов
Адрес учредителя и издателя:
117279, г. Москва, ул. Профсоюзная, д. 108, пом/ком/эт I/67/тех
Почтовый адрес: 119313, Москва, а/я 26
Тел.: (495) 232-0087 • **Факс**: (495) 232-1653
info@soel.ru • www.soel.ru

Производственно-практический журнал
Выходит 9 раз в год. Тираж 10 000 экз.
Цена свободная

Журнал зарегистрирован в Федеральной службе по надзору за соблюдением законодательства в сфере массовых коммуникаций и охране культурного наследия (свидетельство ПИ № ФС77-18792 от 28 октября 2004 г.)

Отпечатано: ООО «МЕДИАКОЛОР».
Адрес: Москва, Сигнальный проезд, 19, бизнес-центр Вэлдан. Тел./факс: (499) 903-6952

СОДЕРЖАНИЕ 4/2021

РЕКЛАМОДАТЕЛИ

Читайте в «СТА» № 2/2021:

От Li-Fi до 5G: коммуникации на любой вкус и кошелёк

Успехи биометрической аутентификации: обойдёмся без паспортов?

Вездесущий ИИ: как меняются технологии в промышленности, экологии, медицине

Острота зрения: интеллектуальные платформы машинного зрения в промышленности

Битумный терминал: производство и хранение битума для дорожного строительства

Оформляйте подписку на журнал «СТА» и читайте печатную версию или электронную версию на www.cta.ru

РЫНОК

СОВРЕМЕННЫЕ ТЕХНОЛОГИИ

ЭЛЕМЕНТЫ И КОМПОНЕНТЫ

ИНЖЕНЕРНЫЕ РЕШЕНИЯ

ПРОЕКТИРОВАНИЕ И МОДЕЛИРОВАНИЕ

ВОПРОСЫ ТЕОРИИ

КОМПЕТЕНТНОЕ МНЕНИЕ

Новости российского рынка

СОВРЕМЕННЫЕ ТЕХНОЛОГИИ

Индикатор на лобовом стекле автомобилей Hyundai KIA разработан в среде DiSTI GL Studio

Компания DiSTI, производитель среды разработки графического пользовательского интерфейса GL Studio, объявила о том, что компания Hyundai Mobis выбрала GL Studio для разработки новой версии индикатора на лобовом стекле (Head-Up Display), который является частью системы ADAS (Advanced Driver Assistance System) автомобилей Hyundai KIA. Одним из главных критериев выбора явилось то, что исполнительные библиотеки GL Studio сертифицированы по стандарту функциональной безопасности ISO 26262 для автомобильной электроники на наивысший уровень критичности для безопасности ASIL D.

Недавно DiSTI провела вебинар «Augmented Reality HUDs - Using Safety-Critical Neural Networks in Automotive Applications» (Индикаторы на лобовом стекле с дополненной реальностью – применение критических для безопасности нейронных сетей в автомобильных приложениях).

Вебинар был проведен совместно с компанией CoreAVI, производителем сертифицируемой библиотеки стандарта OpenVX для критически важных систем компьютерного зрения и искусственного интеллекта. Запись вебинара доступна по ссылке https://youtu.be/4_DCW5Kacw4.

Среда разработки графического пользовательского интерфейса DiSTI GL Studio доступна для тест-драйва. Представитель DiSTI и CoreAVI в России – компания АВД Системы, поставщик средств разработки программного обеспечения критически важных для безопасности сертифицируемых встраиваемых компьютерных систем. «Миром управляет ПО».

+7 (916) 194-42-71
glstudio.disti.com

СОБЫТИЯ

ЭРЕМЕКС приглашает разработчиков радиоэлектронной аппаратуры на семинар «День Радио ЭРЕМЕКС» в Санкт-Петербурге

Компания ЭРЕМЕКС – ведущий российский разработчик ПО для автоматизации проектирования радиоэлектронной аппаратуры, возобновляет очные семинары «День радио ЭРЕМЕКС», посвящённые проблемам проектирования электроники и российской САПР РЭА Delta Design. Первый в этом году «День радио ЭРЕМЕКС» пройдёт 19 мая в Санкт-Петербурге.

На семинаре будет рассказано о тенденциях развития российского рынка САПР, представлены примеры интеграции отечественных продуктов от ведущих разработчиков. Запланировано участие представителей компаний-партнёров ЭРЕМЕКС – разработчика и интегратора инженерного ПО компании АСКОН и производителя электрорадиоизделий промышленного и специального назначения АО «НПО «ЭРКОН».

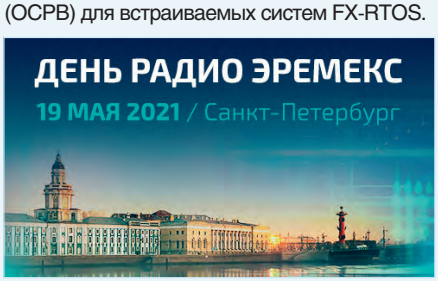
Также будут рассмотрены прикладные вопросы, связанные с особенностями работы в новой версии САПР Delta Design 3.0. В частности, будут анонсированы возможности Delta Design для цифрового моделирования с использованием программируемой логики (ПЛИС), а также новый компонент DeltaCAM, предназначенный для верификации и редактирования производственных файлов.

«День радио ЭРЕМЕКС» традиционно представляет возможность ознакомиться с САПР РЭА Delta Design на демонстрационных терминалах, увидеть, как в ней решаются актуальные задачи отрасли. Участники семинара смогут получить консультации и рекомендации по внедрению системы на своём предприятии.

Семинар «День радио ЭРЕМЕКС» проводится 19 мая 2021 г., в г. Санкт-Петербург, в отеле «Холлидэй-Инн». Специалистам для участия в этом бесплатном семинаре необходимо зарегистрироваться.

О компании ЭРЕМЕКС:

ЭРЕМЕКС – российская компания, ведущий разработчик программного обеспечения. Основные продукты ЭРЕМЕКС: система автоматизированного проектирования (САПР) радиоэлектронной аппаратуры Delta Design, семейство операционных систем реального времени (ОСРВ) для встраиваемых систем FX-RTOS.



Компания регулярно обновляет и совершенствует свои продукты, созданные с целью оптимизации сроков разработки продукции и снижения производственных издержек заказчика. На любой стадии проекта команда ЭРЕМЕКС готова оказать клиентам оперативную поддержку и обеспечить индивидуальный подход к решению поставленных задач.

Ознакомиться с программой семинара и зарегистрироваться для участия в нём можно на сайте ЭРЕМЕКС https://www.eremex.ru.

«РТСофт» и Kontron запустили новый сайт, посвящённый встраиваемым компьютерным технологиям и Интернету вещей

Группа компаний «РТСофт» и холдинг Kontron объявляют об очередном этапе в развитии стратегического партнёрства – запуске русскоязычного сайта, посвящённого современным встраиваемым компьютерным технологиям (ECT), Интернету вещей (IoT/IIoT) и продуктам Kontron для различных отраслей промышленности. Сайт предназначен для специалистов в области разработки, создания изделий и систем, в которых применяется встраиваемое оборудование и программное обеспечение: от процессорных модулей, магистрально-модульных плат и 19" стоечных серверов до платформ на основе искусственного интеллекта (AI), Интернета вещей и других инновационных сквозных технологий. Наряду с описаниями технологий, продуктов и сервисов посетители сайта могут ознакомиться с технической документацией, актуальными новостями, статьями, а также информацией о совместных мероприятиях компаний.

Уже более 20 лет «РТСофт» и Kontron выводят на рынок России и стран СНГ наиболее современные и надёжные открытые международные технологии и продукты, благодаря которым у разработчиков, производителей и системных интеграторов появляются новые возможности для увеличения производительности и энергоэффективности своих решений. Это также помогает сокращать время вывода на рынок и общую стоимость владения (TCO) решений для промышленности, энергетики, транспорта, телекоммуникаций и различных применений в сложных условиях эксплуатации. Запуск нового русскоязычного сайта о технологиях и продуктах Kontron предоставит посетителям самый удобный и быстрый способ для получения актуальной новостной и технической информации, а также консультаций ведущих специалистов, что поможет разработчикам закладывать наиболее перспективные решения в свои проекты, а компаниям – своевременно осуществлять цифровую трансформацию своего бизнеса.

Среди представленных на сайте продуктовых направлений – «компьютеры-на-модуле» COM Express®, COM-HPC®, SMARC module™, SoM, Qseven, платы CompactPCI® и VPX®, материнские платы, одноплатные компьютеры (SBC), промышленные компьютеры, серверы для телекоммуникаций и облачных вычислений, платформы для авиационных систем развлечения и связи (IFEC) и автономных транспортных средств (AV) и другие. Найти нужный продукт или технологию посетителю не составит труда – на сайте реализована удобная навигация по продуктовым направлениям в каталоге, используемым технологиям, рекомендуемым отраслям, а также система поиска, фильтрации и сравнения продуктов. Поддержку и развитие сайта обеспечивает компания «РТСофт» – эксклюзивный партнёр Kontron в России и СНГ.

О компании «РТСофт»

Инжиниринговая компания «РТСофт» работает на российском рынке промышленной автоматизации, встраиваемых компьютерных технологий и разработки программного обеспечения с 1992 года. «РТСофт» активно разрабатывает и внедряет в своих проектах новейшие технологии, такие как промышленный интернет вещей, искусственный интеллект, большие данные, цифровые двойники, САЦ и другие. На их основе компания создает надежные решения в области интеллектуальных систем управления для различных отраслей промышленности и энергетики.

Сегодня «РТСофт» – это группа компаний (ГК), в которую входят инженерно-производственные центры, филиалы, представительства как на территории РФ, так и за рубежом, собственное производство и учебно-лабораторные комплексы.

ГК «РТСофт» сотрудничает с ведущими производителями и поставщиками оборудования, международными ассоциациями, в том числе с Международным сообществом экспертов по электроэнергетическим системам CIGRE, проектными институтами и вузами. Многолетний опыт в реализации успешных проектов, знание специфики различных отраслей, команда профессионалов, наличие всех необходимых лицензий и сертификатов, включая TUV NORD CERT, гарантируют высокий уровень сервисов и решений «РТСофт».

ООО «РТСофт-ВС», входящая в группу компаний «РТСофт», вобрала в себя более чем 25-летний опыт разработки, поставки, интеграции и поддержки современных аппаратных и программных продуктов для встраиваемых приложений.

Деятельность «РТСофт-ВС» ориентирована на всемерную поддержку отечественных разработчиков и серийных производителей и способствует ускорению разработки и производства конкурентоспособных встраиваемых систем высшего качества авиационного, коммуникационного, промышленного и других ответственных назначений.

О компании Kontron, входящей в группу компаний S&T

Компания Kontron – мировой лидер в области встраиваемых компьютерных технологий (ECT) и Интернета вещей (IoT). Являясь частью группы компаний S&T, Kontron разрабатывает широкий ассортимент встраиваемых прикладных платформ, специализированных технических решений, проектных и программных услуг, в том числе для приложений интернета вещей (IoT) и Industry 4.0. Благодаря стандартным серийно выпускаемым продуктам и кастомизированным решениям, основанным на высоконадежных встраиваемых технологиях, Kontron создает безопасные и инновационные устройства для различных отраслей промышленности. Продукция Kontron – выбор для тех производителей, где требуется длительный жизненный цикл изделий, высокая производительность и низкая стоимость владения для решения критических и ответственных задач.

Добро пожаловать на kontron.com.ru!

На правах рекламы

ИНЖЕНЕРНЫЕ РЕШЕНИЯ

Технологии быстрой зарядки для электромобилей от HARTING Technology Group способствуют развитию отрасли электротранспорта

HARTING Technology Group выпускает обширный портфель продуктов и позиционируется как пионер и партнёр многих перспективных проектов в области электротранспорта. Дочерняя компания HARTING Automotive специализируется на производстве решений для электромобилей и поставляет индивидуальные продукты и компоненты для многих заметных игроков рынка.

В частности, HARTING Automotive занимается разработкой и производством решений для зарядной инфраструктуры для электрических и гибридных автомобилей. В рамках пресс-конференции на выставке HANNOVER MESSE компания HARTING представила инновационный разъём для зарядки, который заряжает аккумулятор электромобиля в кратчайшие сроки. В новом разъёме применяется новейшая технология высокоточной подзарядки от HARTING, использующая напряжение постоянного тока с низкими потерями.

Управляющий директор HARTING Automotive Марко Гринблатс отметил, что в последние месяцы сфера электромобилей развивается очень динамично. Высокопроизводительная быстрая зарядка ещё больше повысит популярность электрических транспортных средств.

«Технология быстрой зарядки с разъёмом для постоянного тока CCS является предпосылкой для обеспечения того, чтобы в будущем автомобили получали достаточную мощность не в течение нескольких часов, а уже через несколько минут», – подчеркнул Марко.

HARTING Technology Group охватывает всю цепочку энергетических процессов – от возобновляемой энергии ветра до децентрализованного накопления энергии и зарядных устройств для электромобилей, что выгодно отличает компанию от конкурентов. Например, HARTING поставляет решения для зарядки модульной системы электропривода Volkswagen (MEB), а также для платформ Audi e-tron и Porsche Taycan. Прошлым летом компания HARTING Automotive получила престижную премию Volkswagen Group Award 2020 в категории E-Mobility. Этой наградой концерн Volkswagen подтвердил исключительные достижения и высокий уровень гибкости, с которыми HARTING Automotive вносит свой вклад в успех Volkswagen AG.

В рамках выставки HANNOVER MESSE были представлены основные достижения HARTING в области современной зарядной инфраструктуры для электромобилей. Одним из примеров решений для зарядки от сети переменного тока является Innogy Wall-Box, который можно использовать не только в качестве зарядной станции в общественных местах, но и в частном секторе в качестве Wall-Box.

Также HARTING Technology Group в течение многих лет успешно сотрудничает с инновационным швейцарским производителем автомобилей Rinspeed. Новаторский концептуальный автомобиль metroSNAP, выпущенный Rinspeed AG, тоже опирается на инновационные технологии HARTING – специально разработанный интерфейс, обеспечивающий транспортное средство электропитанием, данными и сигналами.

«ПРОЧИП» и «ПРОСОФТ» являются официальными дистрибьюторами фирмы HARTING.

www.prochip.ru

ЭЛЕМЕНТЫ И КОМПОНЕНТЫ

Семейство прецизионных миниатюрных кварцевых генераторов ГК197-ТС, ГК199-ТС, ГК200(М)-ТС и ГК291-ТС от АО «МОРИОН» (г. Санкт-Петербург)

АО «МОРИОН» (Санкт-Петербург) – ведущее предприятие России и один из мировых лидеров в области разработки и серийного производства пьезоэлектронных приборов стабилизации и селекции частоты – представляет семейство малогабаритных прецизионных термостатированных кварцевых генераторов ГК197-ТС, ГК199-ТС, ГК200(М)-ТС и ГК291-ТС. Данная линейка пьезоэлектронных приборов ориентирована на задачу хранения времени. При производстве этих генераторов используются резонаторы одного семейства, что позволяет достичь очень хорошей долговременной стабильности до 2×10^{-8} в год. Все генераторы имеют одинаковую высоту (12,7 мм), что важно для удобной компоновки оборудования и минимизации размеров изделий в целом. Несмотря на малую высоту, генераторы обеспечивают низкую реакцию на перепады температуры.

	Температурная стабильность при –40…+85°С	Долговременная стабильность, в год	Фазовые шумы на 1 Гц, дБ/Гц	Габаритные размеры, мм
ГК200(М)-ТС	$\pm0{,}2\times10^{-9}$	$\pm2\times10^{-8}$	–108	51×51
ГК197-ТС	$\pm0{,}5\times10^{-9}$	$\pm2\times10^{-8}$	–100 –117	27×36
ГК291-ТС	$\pm0{,}5\times10^{-9}$	$\pm2\times10^{-8}$	–108	25×25
ГК199-ТС	$\pm3\times10^{-9}$ ($3E^{-9}$)	$\pm2\times10^{-8}$	–100	20×20

Наибольший по размерам генератор (51×51 мм) ГК200-ТС имеет очень высокую температурную стабильность (до $\pm\ 2\times10^{-10}$ при –40…+85°С) и низкие фазовые шумы до –108 дБ/Гц.

ГК 197-ТС с температурной стабильностью (до $\pm5\times10^{-10}$ при –40…+85°С) занимает среднее положение в линейке и является наиболее дешёвым из перечисленных. ГК199-ТС – наименьший по габаритным размерам прецизионный генератор.

Дополнительная информация о новом приборе доступна на сайте АО «МОРИОН».

Тел.: +7 (812) 350-75-72, +7 (812) 350-92-43.
Факс: +7 (812) 332-50-25, +7 (812) 350-15-59.
www.morion.com.ru
sale@morion.com.ru

Широкоформатный сенсорный IPS TFT дисплей RFF700A9-AWH-DNS

Raystar представляет цветной IPS TFT-дисплей RFF700A9-AWH-DNS для широкого диапазона рабочих температур.

RFF700A9-AWH-DNS – это графический широкоформатный (15:9) дисплей с резистивной сенсорной панелью (RTP), разрешение экрана 800×480 пикселей, диагональ 7″. Модуль обладает широким углом обзора благодаря используемой IPS-матрице. Кроме того, его высокая яркость (700 кд/м^2) позволяет пользователю видеть чёткое и резкое изображение при дневном свете и прочих ярких условиях внешней освещённости.

RFF700A9-AWH-DNS работает под управлением микросхем драйверов HX8249-A & HX8678-C и поддерживает интерфейс обмена: 24-bit RGB.

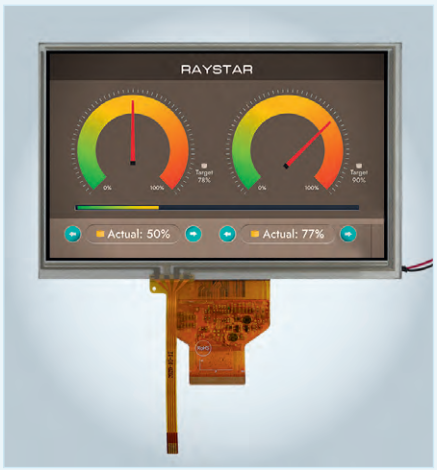
Напряжение питания (VCC) для RFF700A9-AWH-DNS в пределах от 2,7 до 3,6 В (типовое – 3,3 В), напряжение светодиодной подсветки 9,3 В (DC). Модуль работоспособен в диапазоне температур от –30 до +80°C; температура хранения от –30 до +80°C.

Основные характеристики

Размер: 7,0".
Разрешение: 800 × RGB × 480 (TFT) точек.
Размер модуля: 165,8 (Ш) × 106,61 (В) × × 8,0 (Г) мм.
Активная область: 152,40 × 91,44 мм.
Шаг пикселя: 0,1905 × 0,1905 мм.
Тип ЖК-дисплея: TFT.
Углы обзора: 80/80/80/80°.
Интерфейс TFT: 24-битный RGB.
Микросхема драйвера TFT: HX8249-A + HX8678-C или аналогичный.
Соотношение сторон: 15:9.
Тип подсветки: светодиодная.
Сенсорная панель: резистивная.
Поверхность: антибликовое покрытие.

Для заказа доступны различные модели серии RFF700A9

- RFF700A9-AWW-DNN (нормальная яркость; без тач-панели);
- RFF700A9-AWW-DNS (нормальная яркость; RTP – с резистивной тач-панелью);



- RFF700A9-AWW-DNB (нормальная яркость; PCAP – с ёмкостной тач-панелью);
- RFF700A9-AWH-DNN (высокая яркость; без тач-панели);
- RFF700A9-AWH-DNS (высокая яркость; RTP – с резистивной тач-панелью);
- RFF700A9-AWH-DNB (высокая яркость; PCAP – с ёмкостной тач-панелью).

www.komponenta.ru

ПРИБОРЫ И СИСТЕМЫ

R&S®ZNA-K30 – опция измерения коэффициента шума

Компания Rohde&Schwarz анонсирует новую программную опцию для измерения коэффициента шума на векторном анализаторе цепей ZNA. Она будет доступна на приборах с версией ПО от 2.20, и с соответствующей опцией R&S®ZNA-K30. Если в приборе установлена опция работы с преобразованием частоты R&S®ZNA-K4, то при наличии R&S®ZNA-K30 возможно измерение КШ с преобразованием частоты.

Простой пользовательский интерфейс позволяет заполнить все необходимые поля и настроить аппаратные опции для измерения КШ из одного окна, не прибегая к сложным многоуровневым меню и различным разделам настройки измерительной установки.

Меню быстрой настройки R&S®ZNA-K30

В зависимости от характеристик ИУ включение некоторых программных и аппаратных опций оказывает непосредственное влияние на скорость и точность измерений (например, использование опции B161 – альтернативный доступ к опорному приёмнику; B302 – малошумящего усилителя в тракте измерительного приёмника; обратного включения направленного ответвителя). Это влияние и дополнительные рекомендации отображаются непосредственно в окне настройки измерения, что повышает удобство пользования опцией.

Особенности измерений

Как и существующее решение измерения КШ на ZVA, опция ZNA-K30 основывается на измерении абсолютной мощности. Соответственно, для измерений не требуется генератор шума. На новом приборе доступны прежние функции и реализован ряд обновлений и преимуществ:

- переработанный пользовательский интерфейс для измерения усилителей и смесителей;
- удобное меню настройки с автоматизацией конфигурирования измерительной установки;
- полная информация о времени измерения в зависимости от параметров;
- учёт температуры резистора на входе ИУ для получения более точных результатов;
- коррекция побочных каналов приёма;
- коррекция рассогласования, SMARTerCal и калибровка мощности;
- учёт зеркальных каналов при измерении смесителей.

+7 (495) 981-35-60
www.rohde-schwarz.com

Zurich Instruments представляет новое поколение генераторов сигналов для квантовых вычислений

Генератор сигналов SHFSG – прибор, предназначенный для управления сверхпроводящими и спиновыми кубитами. SHFSG работает непосредственно на кубитных частотах без необходимости использования смесителя, фактически являясь первым прибором такого типа на рынке.

SHFSG генерирует программируемые импульсные последовательности на 4 либо 8 выходах с полосой пропускания сигнала 1 ГГц и переменной несущей частотой до 8,5 ГГц. Это необходимо для управления кубитами в квантовых компьютерах. Ранее для этого приходилось использовать комбинацию генератора сигналов произвольной формы (AWG), генератора микроволновых сигналов и смесительной схемы. Благодаря SHFSG устраняется необходимость в трудоёмких и подверженных ошибкам процедурах калибровки сложной системы.

Благодаря интерфейсу ZSync и возможностям динамического секвенирования с низкой задержкой SHFSG поддерживает такие методы обратной связи, как активный сброс (active reset) и квантовая коррекция ошибок. При этом ZSync выполняет точную и воспроизводимую временную синхронизацию между всеми приборами, обеспечивая согласование систем с числом кубитов до 144.

Для генерации сложных сигналов SHFSG требует минимального объёма памяти, благодаря чему сокращается время взаимодействия между приборами, являющееся критичным в процедурах настройки больших квантовых вычислительных систем. Как часть системы управления квантовыми компьютерами (QCCS), SHFSG легко интегрируется в системы с генератором HDAWG и квантовым анализатором SHFQA.

Возможна организация online-демонстрации работы прибора. По всем вопросам обращайтесь в ООО «Криотрейд инжиниринг».

О компании Zurich Instruments

Zurich Instruments производит самые современные приборы для учёных и технологов в передовых лабораториях, которые исследуют процессы, которые зачастую с большим трудом поддаются измерениям. Основными продуктами компании являются синхронные усилители (Lock-In amplifiers), анализаторы импеданса, генераторы сигналов произвольной формы, а также первая коммерчески доступная система управления квантовыми компьютерами QCCS.

+7 (495) 374-6952 (доб. 19)
+7 (926) 001-0714
http://www.cryotrade.ru
www.zhinst.com/products/shfsg-signal-generator

ПРОЕКТИРОВАНИЕ И МОДЕЛИРОВАНИЕ

Испытательный центр АО «ТЕСТПРИБОР» предлагает широкий спектр услуг в области испытаний оборудования и электронной техники

Увеличение видов проводимых работ в испытательном центре – одно из важных направлений развития компании. Испытательный центр постоянно расширяет область своей деятельности, приобретает новое современное оборудование, организует периодическое обучение сотрудников на специализированных курсах и семинарах.

В связи с этим ИЦ предлагает следующие виды работ:

- испытания на определение резонансных частот;
- испытания на воздействие синусоидальной и широкополосной вибрации;
- испытания на прочность при воздействии механических ударов одиночного и многократного действия;
- испытания на воздействие акустического шума;
- испытания на воздействие повышенной и пониженной температур;
- испытания на воздействие повышенной и пониженной влажности;
- испытания на воздействие повышенного и пониженного давления;
- испытания на воздействие статической и динамической пыли (песка);
- испытания на стойкость к воздействию плесневых грибов;
- испытания на воздействие соляного (морского тумана);
- испытания на герметичность;
- рентгенографический контроль.

В процессе испытаний могут обеспечиваться требования ГОСТ РВ 20.57.416, ГОСТ РВ 20.57.305, ГОСТ РВ 20.57.306, ОСТ 11 073.013, КТ-160G/DO-160G, ГОСТ 9.048.

Также на базе испытательного центра проводятся отбраковочные испытания и диагностический неразрушающий контроль электронной компонентной базы, предназначенной для комплектования бортовой аппаратуры космических аппаратов, аппаратуры изделий ВВСТ.

Работы по испытаниям осуществляют аттестованные специалисты, обладающие необходимой квалификацией и опытом проведения испытаний.

Испытания проводятся под контролем ВП МО РФ. По результатам испытаний оформляется протокол.

Приглашаем к сотрудничеству новых партнёров!

+ 7 (495) 657-87-37
www.test-expert.ru

Свобода проектирования

DeltaDesign

В состав Delta Design, обеспечивающей сквозной цикл проектирования печатных плат, входят модули:

- Менеджер библиотек
- Схемотехнический редактор
- Схемотехническое моделирование
- HDL-симулятор
- Редактор правил
- Редактор печатных плат
- Топологический редактор плат TopoR
- Коллективная работа для предприятий

EREMEX +7 (495) 232-18-64 • sales@eremex.ru • www.eremex.ru

Рынок резисторов в России ТОП-50 брендов

Илья Лебедев (ilja78@commarketru.com)

Статья посвящена анализу импорта резисторов.

Введение

В отчёте о рынке конденсаторов замечено, что конденсаторы – это «кровь» любого устройства. Если это так, то резисторы, без сомнения, – «кости», скрепляющие собой все остальные компоненты на плате.

Поставка резисторов – важная составляющая для удержания постоянных клиентов. Стратегию поставки полного БОМа клиенту просто невозможно реализовать без резисторов. Хоть резисторы и являются одной из самых дешёвых групп компонентов на плате, недооценивать их значимость, значит, потерять конкурентные преимущества.

Новой компании заниматься резисторами тяжело: резисторы дешёвые, занимают много места, под них обязательно нужен склад. Это огромная нагрузка для менеджеров по продажам и кладовщиков по строкам отгрузок. Но если хочется завоевать место под солнцем, придётся продавать резисторы.

Проблема в том, что резисторы (особенно чипы) – это дешёвая продукция. На взгляд автора, не стоит рассчитывать на большой доход от продажи резисторов. Эта не та продукция, на которой зарабатывают. Мало кто в полной мере осознаёт, что резисторы, особенно чипы, это, скорее, маркетинг, который помогает отвоёвывать у конкурентов лояльных клиентов или удерживать постоянных.

Старый метод

Российский импорт резисторов

Для начала стоит определиться с группами, по которым надо анализировать импорт в Россию. Предварительно были удалены из анализа:

1. АО «Индезит Интернэшнл». Это, прежде всего, датчики температуры, отправляемые напрямую производителю;
2. огромная (в сравнении с импортом резисторов) поставка АО «Рижский электромашиностроительный завод» для АО «Крона Групп». Это резисторы для электропоездов, прямая поставка;
3. поставки SIEMENS AG;
4. получатели, у которых указаны «Электрический постоянный проволочный резистор (комплектующие для сборки а/м HYUNDAI)» и «Резисторы постоянные для л/а»;
5. пара получателей с указанием «Тензометрический датчик», «Тензопреобразователи давления», «Тензодатчик»;
6. поставки по таможенному коду 8533390000 – прочие резисторы переменные проволочные, включая реостаты и потенциометры. Как незначительный, по открытым данным, всего 0,9 % от общей суммы импорта.

Предварительные данные отражены в таблице 1. Всего для анализа доступно $34,5 млн. Структура брендов отражена в таблице 2. Остальные миллионы делит сотня других брендов. Как и всегда, Россия показывает глобализацию в самом её широком понятии – кого только нет! Но интересно другое (см. табл. 3). На первом месте компания-комплектатор. Компании-комплектаторы обеспечивают, прежде всего, материнские крупные производственные холдинги, а уже потом потребности внешних заказчиков. Холдинг, который обеспечивает компания, является одним из крупнейших производственных холдингов в электронной промышленности, но его нахождение на первом месте очень необычно. Что-то не так. Автор проверил бренды из топ-3, которые импортируются: OSWELL GROUP, YAGEO, TDK (EPCOS).

Любопытно, что OSWELL GROUP участвовала в 2017 году в выставке, которую организовывал «Экспоцентр». Возможно, именно там произошла встреча с компанией, которая в итоге стала первым российским клиен-

Таблица 1. Импорт в 2019 году по кодам ТН ВЭД

Код ТН ВЭД	Итог, шт.	Описание
8533100000	10204024	Резисторы постоянные угольные, композитные или плёночные.
8533401000	7748162	Резисторы переменные прочие, включая реостаты и потенциометры, мощностью не более 20 Вт.
8533210000	6427284	Резисторы постоянные мощностью не более 20 Вт.
8533409000	4579433	Прочие резисторы переменные, включая реостаты и потенциометры.
8533290000	3995374	Прочие резисторы постоянные.
8533310000	1625663	Резисторы переменные проволочные, включая реостаты и потенциометры мощностью не более 20 Вт.
Общий итог	**34579558**	

Таблица 2. Структура импорта брендов в зависимости от объёма

Импорт	Количество брендов	Итог, $ млн
Выше 1 млн	5	12,4
От 100 тыс. до 1 млн	29	6

Таблица 3. Получатели в 2019 году

Секторы конечного потребления оборудования	2018 год, $ млн	Доля рынка, %
Компьютеры и периферия	5731	63,4
Офисное оборудование	412	52,0
Приборостроение	709	37,1
Медицинское оборудование	772	37,7
Промышленный сектор	3237	39,5
Автомобильная промышленность	12865	81,8
Транспорт (неавтомобильный)	2556	54,7
Военное дело и аэрокосмическая промышленность	1566	40,7
Telecom/Datacom	9068	61,8
Потребительский	2064	63,4
Другое	924	36,3
Итого	**39908**	**59,8**

Таблица 4. Первые пять брендов в каждом таможенном коде

Код ТН ВЭД	Изготовитель	Итог, $
8533100000	VISHAY	1943710
	YAGEO CORPORATION	1924215
	WALSIN	981155
	BOURNS	446354
	FENGHUA	398367
8533401000	TDK(EPCOS)	1453828
	BOURNS	940761
	VISHAY	244488
	LITTELFUSE	114835
	SONG HUEI ELECTRIC CO. LTD.	111079
8533210000	TDK(EPCOS)	877440
	YAGEO CORPORATION	729343
	VISHAY	698335
	THINKING ELECTRONIC INDUSTRIAL CO.	153376
	IST	143493
8533409000	TDK (EPCOS)	1290216
	ALBRECHT JUNG GMBH & CO. KG	227685
	BOURNS	195006
	CHINA TOUCHO ELE. TECHNOLOGY CO. LTD	128381
	HAKEL SPOL	125798
8533290000	C.C.OHM ENTERPRISE CO. LTD	158153
	DICONEX DELTA OHM	139771
	TDK (EPCOS)	127451
	VISHAY	118465
	FENGHUA	113495
8533310000	BOURNS	200547
	SUNELECTECH LIMITED	176036
	VISHAY	112487
	MESSIER-BUGATTI	69368
	ELECSOUND ELECTRONICS	67761

том. В описании OSWELL GROUP за 2017 год на сайте выставки значится: «Ведущий поставщик измерительных компонентов трансформаторов тока, шунтирующих датчиков, защёлкивающихся реле, силовых трансформаторов, ЖК-дисплеев, счётчиков, клемм, винтов».

Странно, но никаких резисторов автор на сайте компании не нашёл. В итоге по данному коду компания ввозит какое-то изделие, которое выполняет роль резистора или содержит его как ключевой компонент, но не является резистором на плату в привычном понимании.

Анализ импорта требует очень много практики и знаний об участниках рынка. Только в этом случае возможно получить хотя бы приближённые цифры по рынку. Если отнять у обладателя первого места $800 тыс., то получится вполне внятная цифра. 90% рынка будут занимать всего два бренда – YAGEO и TDK (EPCOS). А компания с первого места переместится на пятое. А что с OSWELL GROUP? Этот бренд вообще удаляется из дальнейшего анализа.

Таблица 4 показывает первые пять брендов в каждом таможенном коде.

В 2008 году компания EPCOS была приобретена (с сохранением номенклатуры выпускаемых изделий) японской корпорацией TDK, поэтому в данной статье эти компании объединены. Как видно, компания TDK (EPCOS) лидирует во всех сферах на территории России (исключение лишь по коду 8533100000: на этот код традиционно приходится большая часть чип-резисторов, и там совсем другие лидеры). Приятно видеть в лидерах YAGEO CORPORATION, так как автор статьи почти 8 лет занимался развитием данного бренда в России. В коде 8533310000 предсказуемый лидер – компания BOURNS, которая и в мире является лидером по производству переменных резисторов.

Как и в любом таможенном коде, часто под видом резисторов ввозится продукция, которая, даже выполняя схожие функции, всё же чаще представляет собой полуфабрикаты в виде почти готовых к сборке модулей. Например, механизм светорегулятора, в котором используются переменные резисторы. Но большинство читателей интересуют цифры импорта, который приходится на компонентный рынок. Для этого нужно взять топ-10 дистрибьюторов и посмотреть, какие бренды они ввозят.

Отличие хорошего менеджера от менеджера просто в том, что хороший всегда ищет пути улучшения. В списке импортёров у автора статьи уже более 130 брокеров, 80 из которых нашлись в списке импортёров резисторов. Зачем брать 10 компаний, если можно взять все 80 и получить полный срез рынка по резисторам среди брокерских брендов? Это автоматически отсечёт неинтересные читателям бренды электротехнического рынка, ремонтного, автомобильного и т.д.

Да, такая статья будет меньше по общим данным, но она будет более точной.

Новый метод

Итак, первым делом автор составил полную версию таблицы получателей в 2019 году и выписал оттуда всех брокеров, которых смог идентифицировать. Всех дистрибьюторов, брокеров, дилеров, посредников автор далее будет именовать термином «реселлеры» (перепродавцы).

Получилось, 79 компаний – реселлеры, две – таможенные брокеры. Таможенных брокеров автор также считает реселлерами по широчайшей линейке поставок, хотя для кого именно они возят, есть только предположения.

В таблице импорта автор оставил только 81 импортёра, остальные были удалены. В результате получилась цифра $11,2 млн. Именно столько импортировал в сумме этот 81 импортёр. В таблице 5 представлены бренды, на которые приходятся эти $11,2 млн. Также в таблицу добавлена ещё одна колонка, в которой представлен объём продаж этих брендов.

Проблема наиболее точного анализа состоит в том, что варисторы и предохранители тоже ввозятся по представленным в таблице 1 кодам, хотя эти компоненты по функциям являются частью защиты цепей. Найти и выделить их не составляет особой проблемы, однако в ручном режиме такая работа потребует несколько сотен часов.

Поэтому автор поступил проще: просто удалил все строки, где было написано слово «предохранитель», а строки, где написано слово «варистор», выделил в отдельную колонку. Это, скорее, промежуточное, компромиссное решение, позволяющее читателю самому

Таблица 5. Итоговая сумма импорта топ-50 брендов, которые импортировал 81 импортёр-реселлер

Названия строк	Продажи через 81 реселлера, $	Варисторы. Продажи через 81 реселлера, $	Общие продажи, $	Доля продаж через российских реселлеров
TDK(EPCOS)	2920904	1646026	3758440	0,78
VISHAY	1684104	5570	3111985	0,54
YAGEO CORPORATION	1378648	2843	2684707	0,51
BOURNS	1083708	79431	1892327	0,57
WALSIN	372675	0	1007588	0,37
FENGHUA	353532	58791	645812	0,55
THINKING ELECTRONIC	271839	262412	277969	0,98
THUNDER COMPONENTS LTD.	236821	0	314886	0,75
VIKING	227147	0	272972	0,83
CADDOCK ELECTRONICS	213078	0	336706	0,63
KLS ELECTRONIC	192207	65245	245121	0,78
TE CONNECTIVITY	185821	0	301539	0,62
PANASONIC	152586	2133	283175	0,54
AMERICAN TECHNICAL	149002	0	164511	0,91
CHINA TOUCHO ELE.	147800	147800	147800	1,00
EBG, RESISTORS ELEKTRONISCHE BAUELEMENTE	124182	0	223642	0,56
DICONEX DELTA	111740	0	415748	0,27
MURATA	108385	2800	211428	0,51
LITTELFUSE	108010	29355	287619	0,38
KOA SPEER	105169	0	143663	0,73
ANAREN	103643	0	161106	0,64
S.I.R. S.R.L. SOCIETA ITALIANA RESISTOR	91228	0	120795	0,76
WEINSCHEL ASSOCIATES	89065	0	114762	0,78
JOYIN	83596	78019	83986	1,00
OHMITE	80185	0	177839	0,45
GUANGDONG HOTTECH	66247	0	97880	0,68
DANOTERM ELECTRIC A/S	59402	0	59402	1,00
FAITHFUL LINK	50504	0	460112	0,11
NXP SEMICONDUCTOR	50275	1174	53659	0,94
SUNTAN	49265	0	87859	0,56
SONG HUEI ELECTRIC	47609	0	153874	0,31
TT ELECTRONICS	45352	158	104405	0,43
JFW INDUSTRIES INC	45261	0	45261	1,00
STACKPOLE ELECTRONICS	45001	0	64151	0,70
BESTBRIGHT ELECTRONICS	44680	27418	52639	0,85
MINI-CIRCUITS	42537	0	58854	0,72
ARCOL	40530	0	81791	0,50
KESTAR ELECTRONIC	34261	34261	34261	1,00
PROSPERITY DIELECTRICS	30778	0	32292	0,95
SUSUMU	27744	0	41490	0,67
ATE-ELECTRONICS	26203	0	31656	0,83
CONTELEC AG	22362	0	38523	0,58
ARAGONESA DE COMPONENTES PASIVOS S.A.	22109	0	35421	0,62
ROYALOHM	21648	0	34707	0,62
DONGGUAN HSIANG-TAI ELECTRONIC	20374	0	46872	0,43
ALLGUY INTERNATIONAL	16929	0	16929	1,00
AVX CORPORATION	15993	12518	27218	0,59
Общий итог	**11400139**	**2455954**	**19045383**	**0,60**

Таблица 6. Примеры отправителей и их получателей – производителей

Наименование отправителя	Наименование получателя	Итог, $
ARROW	1	291505
	2	34900
	3	3127
	4	2612
EPCOS (ZHUHAI FTZ) CO. LTD	1	197384
AVNET	1	12132
	2	5796
	3	4188
DIGI-KEY CORPORATION	1	26289
TTI INC	1	1753
Итого, $	**579685**	

Таблица 7. Импорт по таможенным кодам, сколько всего и сколько приходится только на выделенных реселлеров

	Сумма, млн $		
Названия строк	Реселлеры	Всего	%
8533100000	4,900	10,204	0,480203
8533401000	2,400	7,748	0,309751
8533210000	2,290	6,400	0,357778
8533409000	1,034	4,579	0,225877
8533290000	0,674	3,995	0,168706
8533310000	0,162	1,626	0,099459
Общий итог	**11,484**	**34,500**	**0,332881**

сделать вывод, как использовать данные цифры.

Например, бренд LITTELFUSE – это только варисторы и самовосстанавливающиеся предохранители. 100 000 – это то, что осталось после удаления строк по предохранителям. Остальное идентифицировать быстро нет возможности. В целом по России в сегменте самовосстанавливающихся предохранителей доминируют две компании – LITTELFUSE и BOURNS, в остальных этот фактор не оказывает влияния. Список из 81 реселлера включает всех игроков из топ-25, описанных в отчёте «Центра современной электроники», за вычетом специализирующихся исключительно на российских компонентах. Последняя колонка – это доля продаж данных брендов через российских дистрибьюторов и брокеров. Пусть не смущает, что их всего 81: в сумме эти компании ввозят в страну примерно 95% всех брендов. Если бренда нет, значит, он стопроцентно ввозится напрямую, минуя всех крупных игроков компонентного рынка. Из таблицы видно, что из $34 млн непосредственно на компонентный рынок приходится только $19 млн. В реальности за счёт мелких игроков – на 5% больше, однако это уже вполне в рамках статистической погрешности. Процент поставок через реселлеров будет выше, чем показано в последней колонке. Стоит повториться: это только российские получатели, зарегистрированные в России. Есть ещё зарубежные дистрибьюторы и брокеры. Можно посчитать их на примере TDK (EPCOS). Для подсчёта придётся перечислить их в отдельной таблице 6.

В таблице 6 перечислены только конечные потребители. Хотя это далеко не полный список, даже с этой узкой выборкой процент покупки TDK (EPCOS) через дистрибьюторов, брокеров или напрямую возрастает до 80%. Последняя колонка в таблице верная, но отражает только процент продаж через российских партнёров. Общий процент всех продаж через дистри-

Таблица 8. Производство резисторов в натуральном выражении с 2017 года (оперативные данные в соответствии с ОКПД2)

Годы	2017 январь-декабрь	2018 январь-декабрь	2019 январь-декабрь	2020 январь-ноябрь
Тыс. шт.	140464	126644,7	121648,46	111069,81

бьюторов, российский или глобальный, будет ещё выше.

Итак, есть три точные цифры: $10,8 млн импорта топ-50 брендов, приходящегося на брокеров и дистрибьюторов, $11,2 млн – сумма всех брендов, поставляемых, через брокеров, и $19 млн – общая сумма импорта по этим брендам. Теперь стоит разложить сумму в таблице 7 по таможенным кодам.

Разница в итогах пусть не смущает: 10,8 млн – это только первые 50 брендов, $11,2 млн – это все бренды, которые импортировал 81 реселлер. Объём импорта небольшой в долларовом выражении, однако очень существенный для снабжения клиентов. До половины строк в спецификации клиента в 90% всех спецификаций занимают резисторы. На этой группе много не заработаешь. Это примерно 3% от общей суммы спецификации клиента, но затраты на продажу выше, чем, например, затраты на продажу микроконтроллеров. Стоит ли ими заниматься, решает каждая компания самостоятельно. Иногда проще договориться о специальных условиях с партнёрами, которые уже имеют склад в России.

Производство чип-резисторов в России

В России нет специализированной статистики, позволяющей получить точный срез рынка. Почти все отчёты будут носить обобщённый характер. Практически ни одно российское предприятие за год существования сайта автора не сообщило своих реальных данных. Наиболее точную информацию дают только годовые отчёты предприятий, если они не входят в государственные холдинги. Как только входят, публикации прекращаются. Возникает парадоксальная ситуация. Чем больше государство укрепляет электронную промышленность, тем более закрытой она становится. Чем более закрытой она становится, тем меньше она стремится на гражданский рынок.

Недавно автор прочёл две новости:

1. на ОАО «Ресурс» установлена новая автоматизированная линия, которая позволяет обеспечить выпуск чип-резисторов категории качества ОТК в объёме 50 млн штук в месяц. В проекте участвовала государственная корпорация «Ростех»;

2. завод радиодеталей «Оксид» в Новосибирске, который относится к государственной корпорации «Ростех», ввёл в эксплуатацию производственную линию, где выпускают резисторы в SMD-исполнении. Как рассказал генеральный директор завода Лев Носенко, ежегодно здесь будут выпускать порядка 170 млн штук. Он подчеркнул, что новое оборудование будет использоваться для выпуска SMD-резисторов для поверхностного монтажа типа Р1-12. Такие резисторы устанавливают на различную технику, в том числе на смартфоны, машины и бытовую технику.

Если сложить объём двух производителей, то получится порядка 800 млн штук в год. Средняя цена чип-резистора в корпусе 0603 и 0805 – $0,45 и $0,8 за 1000 штук на FOB (цены для гражданского рынка). Получается, что объём выпуска двух самых современных линий в России равен около $360–640 тыс. в ценах импорта, что составляет максимум 13% от импорта 81 брокера и 6% от всего рынка, по коду 8533100000.

Однако эти максимумы – в случае 100% загрузки линий. Опыт показывает, что 50–70% – уже прекрасное достижение. Автор не думает, что текущая загрузка линий на данный момент превышает 20%. поставка заводом «Ресурс» продукции гражданским предприятиям не превышает 5%. А ведь помимо этих двух предприятий на госзаказ работают и другие, например третий крупный игрок – АО «НПО «ЭРКОН» – тоже имеет линии по производству чип-резисторов. Итоговый рынок госзаказов с их мелкосерийным производством явно недостаточен для загрузки всех линий в России по производству чип-резисторов.

Так как эти две новые линии прежде всего смонтированы для военной приёмки, то сумма за один резистор будет в 5–10 раз выше, чем на гражданском рынке. Эти линии вряд смогут быть переориентированы на производство гражданской продукции. В штучном выражении производительность линий явно недостаточна. Один только «Ледел» потребляет порядка 15–20 млн чип-резисторов в год.

Таблица 9. Средние цены производителей на резисторы по Российской Федерации в 2017–2019 годах

Наименование товара (услуги)	Код по ОКПД2	2017	2018	2019
Резисторы, кроме нагревательных резисторов, шт.	27.90.6	7,3	7,7	10

Надо понимать, что эти небольшие объёмы уже поделены между несколькими предприятиями, которым и так явно тесно и не хватает доли рынка для естественного развития. Естественного развития не будет, так как не хватает производственных мощностей. Этим предприятиям даже и не ставится подобная задача.

Возможно, сейчас у читателей появится явное недоверие к словам автора. Возможно, автор сгущает краски, но вот таблицы 8 и 9 для размышления. Данные официальные, взяты на едином интернет-портале Росстата. База данных, Единая межведомственная информационно-статистическая система (ЕМИСС)

Какие выводы можно сделать на основе государственной статистики:

1. цифра 25% загрузки новых линий преувеличена и сильно;
2. несмотря на все защитные меры, рынок резисторов в регулируемом рынке не растёт или он уже был насыщен нашими производителями на момент запуска новых линий;
3. рынок резисторов в России, согласно Росстату, 1,110 млрд руб., или по среднему курсу 2019 года в 64,6 руб. составляет $17,1 млн. Но это в деньгах. В штуках, по опыту работы автора, на 5 производимых резисторов в России приходится 95 импортируемых.

В общем, в этом десятилетии 81 реселлеру, описанному в данной статье, не стоит опасаться суперсовременных линий по производству чип-резисторов. Да, несомненно, под действием различных защитных мер они полностью вытеснят иностранные бренды из госзаказа, но дальше дело не продвинется в силу описанных ранее причин.

Литература

1. Продвижение российских предприятий электронных компонентов на гражданском рынке. URL: https://commarketru.com/prodvizhenie-rossijskih-predpriyatij-elektronnyh-komponentov-na-grazhdanskom-rynke/.

Граничные вычисления в промышленности

Дмитрий Кабачник (kabachnik@advantix-pc.ru)

В статье рассказывается о концепции граничных вычислений и её связи с облачными вычислениями. Подробно рассматриваются преимущества и недостатки применения технологии для построения ИТ-инфраструктуры предприятия. Особое внимание уделено применению граничных вычислений в промышленной сфере.

Введение

Одной из основных тенденций ИТ-индустрии в последние годы стало постоянное увеличение количества данных, которое генерируется, передаётся и, соответственно, обрабатывается самыми различными электронными устройствами. Касается это в том числе и промышленности, где всё активнее применяются технологии IoT (Internet of Things).

Количество «умных» сенсоров, датчиков и других IIoT- устройств (Industrial Internet of Things) постоянно растёт. Компаниям необходимы новые решения, которые позволят «переварить» такое количество данных. При этом оптимальное использование этих самых данных становится всё более и более актуальным вопросом.

Во многих случаях (особенно в промышленности) использование облачных вычислений является не совсем целесообразным. Ведь передача огромного количества данных, которые генерируются датчиками, контроллерами и другим промышленным оборудованием, создаёт огромный создаёт огромный трафик, снижающий пропускную способность или банально в итоге слишком дорогой. С другой стороны, в современных цифровых производствах полный отказ от облака также невозможен, слишком много удобств создаёт такая централизованная обработка данных. Частичным решением этого вопроса стали так называемые «туманные» вычисления (см. рис. 1). Благодаря этой технологии сбор, хранение и обработка данных происходят в локальной сети между конечным устройством и центрами обработки данных.

Туманные вычисления подразумевают под собой децентрализованную систему, которая фильтрует информацию, передающуюся в ЦОД. Расширением данной концепции стали периферийные или граничные вычисления, которые максимально органично дополняют концепцию облачного использования данных. Основной смысл данной концепции в осуществлении различных вычислений в пределах досягаемости конечных устройств. Применению этой концепции в промышленности в целом и в АСУ ТП в частности посвящена настоящая статья.

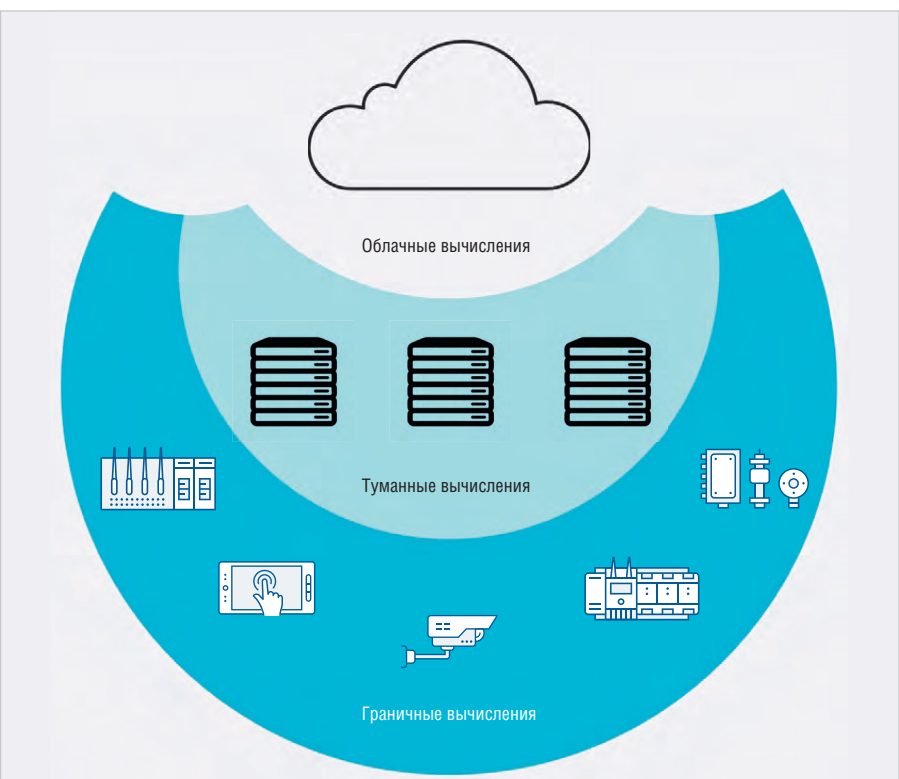


Рис. 1. Концепция облачных, туманных и граничных вычислений

Граничные вычисления

Для начала более подробно рассмотрим само понятие граничных вычислений. Под граничными вычислениями подразумеваются отдалённый мониторинг и обработка данных непосредственно на IoT-устройствах или в пределах их досягаемости.

Самое важное и очевидное отличие граничных вычислений от облачных и туманных заключается в том, что анализ и сбор информации проводятся не в центрах обработки данных с централизованной вычислительной средой, а непосредственно в том месте, где происходит генерация данных.

Сферы применения туманных и граничных технологий во многом пересекаются, поэтому зачастую сложно сказать, по какой именно технологии построена ИТ-инфраструктура предприятия. Главное преимущество обеих концепций – существенное увеличение скорости передачи и анализа данных. Именно поэтому данные технологии применяются там, где важна обработка информации и данных в реальном времени, например в промышленном IoT, машинном зрении, интеллектуальном видеонаблюдении и др.

На производстве или в промышленности граничные вычисления позволяют своевременно реагировать на аварийные или нештатные ситуации, например на поломки и протечки различного оборудования. На такие сигналы необходима максимально быстрая реакция, которую не всегда возможно обеспечить при работе через удалённые облачные сервисы (из-за ограничений, связанных с пропускной возможностью канала).

Также зачастую нет смысла передавать в облако различный «тяжёлый» тра-

фик, например потоковое видео высокого качества, получаемое с систем машинного зрения или видеонаблюдения объекта. Такие данные удобнее и, что немаловажно, зачастую дешевле обрабатывать либо в локальной сети здания, либо непосредственно на месте установки оборудования (актуально для систем машинного зрения). При граничных вычислениях в ЦОД (см. рис. 2) поступают на обработку лишь те данные, которые невозможно или нерационально обрабатывать по-другому.

В первую очередь термин граничных вычислений связан именно с данными IoT или его промышленным вариантом – IIoT (Industrial IoT), которые собираются с удалённых «умных» датчиков, сенсоров, мобильной техники и другого оборудования. Полученные данные анализируются, обрабатываются и передаются в готовом виде операторам на рабочие места. Именно в этом и состоит основное отличие граничных от традиционных распределённых вычислений, которые предназначены для распараллеливания вычислительных мощностей между центрами обработки данных и локальными сетями.

Рис. 2. Крупный центр обработки данных

Объём генерируемой IoT-устройствами информации слишком велик, он накапливается в режиме реального времени и может попросту «забить» канал передачи данных предприятия, будь то Интернет или частная сеть. В случае с IIoT обработка информации особенно критична для промышленных предприятий: каждый час простоя может быть связан с огромными финансовыми потерями. Поэтому важно, чтобы аналитики могли максимально использовать потенциал данных, полученных с помощью таких устройств.

Преимущества и недостатки

Граничные вычисления обладают рядом важных преимуществ. Одним из самых важных именно для промышленности можно назвать столь актуальную сейчас безопасность кон-

Рис. 3. Транспортный встраиваемый компьютер AdvantiX ER-G800 для граничных вычислений и машинного зрения

фиденциальных данных. Если промышленное предприятие будет передавать все сырые данные с устройств IoT в облако, то это создаст риски (ведь, как правило, облако является публичным). При использовании граничных вычислений конфиденциальная информация предварительно обрабатывается на месте, и только данные, соответствующие политике конфиденциальности, передаются в облако для дальнейшего анализа и обработки.

Неоспоримым плюсом граничных вычислений можно назвать и практически нулевую задержку при передаче данных. Ведь вычисления производятся на конечных устройствах, поэтому информации не нужно преодолевать целые сети, чтобы попасть в ЦОД. Сейчас из-за огромного количества данных, передаваемых в облако, обрабатываемых там и передаваемых обратно на периферийные устройства, могут возникать задержки при получении выводов из анализа. Последнее может создать серьёзные последствия для функционирования предприятия. Большие задержки могут привести к простою производства со всеми вытекающими последствиями.

Также важным преимуществом использования граничных вычислений является снятие нагрузки с облака. Тут может быть два основных варианта:
1. компания имеет собственный ЦОД;
2. компания арендует вычислительные мощности у сторонней организации.

При первом варианте компания может переориентировать свой ЦОД на другие задачи или изначально сэкономить при его строительстве. Но создание собственного центра обработки данных не самое дешёвое удовольствие. Далеко не у всех компаний ЦОД есть, даже у производственных. Гораздо чаще встречается второй случай: аренда вычислительных мощностей в виде PaaS (платформа как услуга) или IaaS (инфраструктура как услуга). В этом случае можно говорить о возможной существенной экономии в компании при использовании граничных вычислений.

Ещё одним преимуществом технологии граничных вычислений для промышленных применений является гарантированная надёжность хранения данных. Обработанные на самом устройстве или в непосредственной близости от него данные не будут утеряны в случае отключения устройства от Интернета. При этом работа не остановится и в случае прерывистого или сильно ограниченного сетевого подключения. Это особенно важно при внедрении IoT-технологий в труднодоступных местах или локациях с неустойчивой связью.

Недостатком использования концепции граничных вычислений является сильное усложнение устройства. Это влечёт за собой снижение надёжности и безопасности: любой датчик становится, по сути, полноценным компьютерным устройством, которое может быть взломано.

Главный же недостаток проистекает из предыдущего: это затраты, которые вынуждено будет понести предприятие при внедрении такой технологии. С увеличением сложности устройств пропорционально растёт и стоимость внедрения.

В первую очередь потребуется закупить оборудование. Далее необходимо будет его корректно настроить и поддерживать в рабочем состоянии, что потребует привлечения квалифицированных специалистов и приведёт к расширению штата. Применение облачных технологий в качестве PaaS, IaaS или даже SaaS в этом плане гораздо проще.

Идеального решения, применимого для всех предприятий, в целом не существует. В каждом случае необходимо подходить индивидуально к проектированию ИТ-инфраструктуры предприятия и совмещать существующие облачные, туманные и граничные технологии максимально выгодным способом.

В промышленности

Технология граничных вычислений нашла применение в том числе и в промышленности. Диагностический алгоритм на периферийных или граничных устройствах позволяет проводить постоянный мониторинг самых различных технологических процессов на предмет ошибок или отклонений в работе.

Использование данных, полученных по технологии граничных вычислений, позволяет контролировать работу промышленного оборудования и машин в режиме реального времени. Благодаря быстрой интерпретации информации с помощью аналитических алгоритмов данные о любой возможной неисправности оперативно передаются сотрудникам, отвечающим за бесперебойную работу производства. Аналогичная система может информировать сотрудников, ответственных за качество продукции, например при обнаружении с помощью систем машинного зрения брака на производственной линии.

Системы, построенные по концепции граничных вычислений, в первую очередь нацелены на прогнозирование и предотвращение аварийных или проблемных ситуаций. Подобный подход позволяет реагировать на события до

того, как произойдёт сбой, который может привести к остановке всей производственной линии и огромным финансовым потерям для производства. Если взглянуть на концепцию граничных вычислений с такой точки зрения, то первоначальные вложения в закупку «умных» устройств и средств вычисления становятся оправданными.

Важным преимуществом для промышленности является лёгкая масштабируемость системы граничных вычислений. Передача части аналитики «умным» датчикам и различным сетевым устройствам существенно снижает нагрузку на сеть постоянно генерируемыми данными. Поэтому, когда количество подключённых устройств увеличится, создаваемый ими дополнительный объём данных не приведёт к необходимости немедленного увеличения вычислительного облака (что неминуемо произошло, если бы сбор данных осуществлялся только в облаке).

Учитывая постоянное развитие беспилотных, автономных транспортных средств, можно и их с некоторыми оговорками причислить к промышленному применению технологии граничных вычислений. Такие транспортные средства нуждаются в получении огромного количества данных из окружающего пространства для корректной работы в режиме реального времени. Если использовать только облачные вычисления, то неминуемы различные задержки в работе такого устройства. Это существенно может повлиять на безопасность работы. Трафик, создаваемый большим количеством систем умного и машинного зрения, неминуемо забьёт каналы WAN, которые, как правило, применяются в транспортных средствах. Гораздо разумнее проводить большую часть аналитики непосредственно бортовым компьютером транспортного средства, а в облако и ЦОД отправлять уже наиболее критичную информацию: о неисправностях, ошибках, непредвиденных ситуациях и т.д. Для такого применения идеально подойдут различные бортовые GPU-вычислители (см. рис. 3), предназначенные специально для эксплуатации на транспорте.

Заключение

Важно понимать, что граничные вычисления – это не новое прорывное решение, а лишь один из вариантов реализации ИТ-инфраструктуры. При этом такие вычисления даже не являются конкурентными или альтернативными технологиями, т.к. предназначены для решения разных задач.

Граничные вычисления – это в первую очередь подход, который дополняет или расширяет аналитические возможности, когда оперативная реакция на ошибку может быть крайне важна для функционирования инфраструктуры компании. Больше всего это касается промышленных применений, где простой линии может означать существенные финансовые потери.

Для решения сложных вычислительных задач, с которыми сталкиваются системные интеграторы и организации, облачные вычисления остаются подходящим и вполне актуальным решением. В некоторых случаях полностью оправдывает себя и комплексный подход, в котором комбинируются граничные, туманные и облачные вычисления. Комбинированный подход позволяет достичь максимальной эффективности и при этом сэкономить средства на определённых этапах обработки и хранения информации.

Новый стандарт для проектов «Умный дом» – Connected Home over IP

Часть 1

Виктор Алексеев (victor.alexeev@telemetry.spb.ru)

Концепция «Умного дома» была впервые сформулирована в документе Building Management System (BMS). До настоящего времени основной проблемой этого направления было отсутствие единого международного стандарта. Учитывая это, крупнейшие мировые концерны Amazon, Apple, Google и Zigbee Alliance в декабре 2019 года создали рабочую группу, названную Project Connected Home over IP (CHIP). Основная цель этой рабочей группы заключается в разработке и продвижении единого стандарта протоколов беспроводной связи с открытым кодом, предназначенных для оборудования, используемого в проектах Smart Home. В 2020 году к проекту CHIP присоединились IKEA, Legrand, NXP Semiconductors, Resideo, Samsung SmartThings, Schneider Electric, Signify (ранее Philips Lighting), Silicon Labs, Somfy и Wulian. В данной статье рассмотрены основные базовые принципы, заложенные в основу проекта CHIP.

Общая структура «Умного дома»

Четвёртая промышленная революция всё больше меняет не только производство, но и всю нашу жизнь, включая жилищное строительство. Всё чаще нам встречается термин Smart Home («Умный дом»). Концепция «Умного дома», впервые сформулированная в документе Building Management System (BMS) в 1986 году [1], основана на использовании компьютерной системы, контролирующей всё энергетическое и бытовое оборудование дома.

Прежде всего, «Умный дом» обеспечивает безопасность и комфорт, а также предоставляет множество дополнительных опций, облегчающих повседневные рутинные работы по дому. Немаловажно и то, что современные проекты «Умного дома» способствуют значительной экономии затрат на электричество, воду и отопление.

В последнее время всё возрастающее значение приобретают проекты квартир и персональных домов, предназначенные для проживания людей с деменцией. Количество людей с этим недугом постоянно увеличивается и к 2050 году может достигнуть по всему миру 155 млн человек [2].

Проекты включают в себя интеллектуальные устройства, предназначенные для отслеживания из любой точки мира состояния и действий пожилых людей. Для этого используются камеры видеонаблюдения, дистанционные переговорные устройства, датчики движения и падения человека, автоматизированные тонометры с передачей информации по Интернету, дозаторы лекарств с голосовым напоминанием и другие аналогичные приборы. Для полноценной реализации в подобного рода проектах должно быть реализовано бытовое оборудование, облегчающее жизнь пожилого человека: умные кровати, инвалидные коляски с электрическим приводом, автоматизированное безопасное кухонное и сантехническое оборудование, роботы-пылесосы, голосовое управление освещением, климат-контролем, шторами и системами вентиляции (см. рис. 1).

Рис. 1. Гаджеты с большим экраном и крупным шрифтом помогают пожилым людям управлять бытовыми приборами, не вставая с кресла [3]

Стремительно растущий рынок IoT будет вовлекать всё больше и больше новых продуктов в проекты «Умного дома». Рынок мгновенно реагирует на потребности потребителей. Хорошим примером тут служит фирма Intellias, которая в период пандемии COVID-19 разработала IoT-платформу для интеллектуальных холодильников, обеспечивающую поддержку систем корпоративного удалённого питания. За короткое время платформа стала популярной во многих странах мира, и к ней уже подключились сотни тысяч холодильных установок [4].

По данным Harbour Research, чуть меньше половины всех устройств IoT, которые будут установлены по всему миру в ближайшие 20 лет, придётся на проекты «Умного дома» [5]. Согласно оценкам [6], мировой объём рынка «Умного дома», составлявший в 2020 году примерно $80 млрд, увеличится к 2026 году до $314 млрд.

На первом этапе своего существования (1990-е годы) рост индустрии «Умного дома» сдерживался в основном из-за высокой общей стоимости проектов, сложности проводного монтажа оборудования, отсутствия единого стандарта и относительно низких цен на оплату ЖКХ.

Ситуация кардинально изменилась в начале 2000-х годов в связи с интенсивным развитием глобальных и локальных систем беспроводной связи, когда для коммуникации между датчиками, центральным процессором и исполнительными устройствами внутри дома широко стали использовать сети стандартов WLAN. При этом для удаленного контроля проектов «Умного дома» начали применять беспроводные GSM-модемы.

Современные системы «Умного дома»

В любом из предлагаемых сегодня на рынке вариантов «Умного дома» используется примерно одна и та же базовая схема, показанная на рисунке 2.

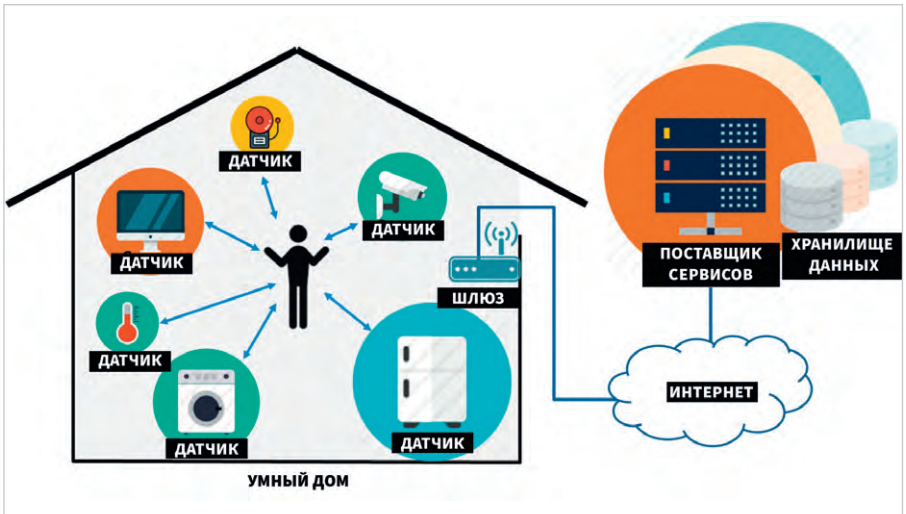


Рис. 2. Типовая базовая структурная схема «Умного дома» [7]

Основная особенность современных проектов «Умного дома», отличающих их от разработок предыдущих поколений, – использование системы беспроводной связи для коммуникации сенсоров и исполнительных устройств с центральным процессором. Интеллектуальные сенсоры и исполнительные устройства подключаются с помощью локальных беспроводных технологий WLAN к центральному контроллеру, который объединяет все устройства «Умного дома» в единую сеть и управляет ими в соответствии с заданной программой.

В структуре «Умного дома» сохраняются также и стандартные проводные интерфейсы электропитания и датчиков. Таким образом, можно пользоваться обычными выключателями, специальным пультом управления или переключать управление в автоматический режим. Связь «Умного дома» на глобальном уровне осуществляется с помощью сетей мобильной связи поколений 2G, 3G, 4G. Поэтому можно контролировать удалённо работу всех систем, находясь в любой точке мира, где есть мобильная связь.

Сегодня различные проекты «Умного дома» позволяют управлять всем оборудованием в трёх основных режимах – вручную, дистанционно и полностью автоматически. Кроме того, поддержка аудиоассистента позволяет также управлять всеми приборами с помощью обычных голосовых команд.

Современные сложные беспроводные системы «Умного дома» обладают множеством разнообразных функций, обеспечивающих управление таким оборудованием как, например:

- охранная и пожарная сигнализации;
- видеонаблюдение в контрольных точках с передачей информации по сети Интернет;
- контроль аварийной протечки водопровода и систем отопления;
- контроль систем электропитания с переключением на резервный источник;
- удалённое управление гаражными воротами, рольставнями, уличным освещением;
- автоматизированный климат-контроль по заданному графику;
- контроль содержания вредных веществ в воздухе помещений (окись и двуокись углерода, летучие органические соединения);
- удалённый контроль и автоматизированное управление кухонным оборудованием;
- робот-пылесос (автоматическая уборка по заданному графику);
- электронный секретарь (обработка телефонных вызовов, календарь запланированных дел и платежей, голосовые напоминания);
- удалённое управление телефоном с громкой связью, телевизором, домофоном, проигрывателем, проектором с помощью голосовых команд или смартфона;
- видеоняня – круглосуточный контроль за младенцем;
- системы климат-контроля в винном погребе;
- удалённый контроль минерального состава и влажности почвы в саду и цветниках (команды контроллера);
- оптимальный автоматизированный режим полива растений в саду и цветниках (команды контроллера);
- возможность масштабирования системы за счёт монтажа дополнительного оборудования.

Потенциал «Умного дома» привлекает огромное количество производителей, системных интеграторов и поставщиков услуг. В результате появляются новые продукты и решения, использующие традиционные технологии и комплектующие. Это, в свою очередь, приводит к невозможности совместной работы датчиков и управляющих устройств от разных брендов.

В простейших системах «Умного дома», таких как «Комплект умный дом Xiaomi Mi Smart Sensor Set», несколько датчиков одного стандартного интерфейса управляются непосредственно самим смартфоном [9].

В более сложных проектах «Умного дома» комплект оборудования может состоять из множества самых различных сенсоров и исполнительных устройств. В настоящее время на рынке доминируют три крупнейшие мировые экосистемы для «Умного дома»: Amazon Alexa, Google Home (Google Assistant) и Apple HomeKit.

Различные производители используют ранее принятую технологию связи между датчиками и управляющим процессором. Чаще всего используются Wi-Fi, Bluetooth (BLE), Zigbee и Z-Wave. Также существуют проекты с использованием LPWAN-технологий нелицензионного диапазона частот ISM: 802.15.4, Thread, LoRa, SIGFOX, Weightless, «ВАВИОТ».

Одним из интересных направлений в конкурентной борьбе за рынок «Умного дома» являются проекты, в которых всё оборудование разбивается на группы устройств, каждая из которых управляется собственным ведущим. Это даёт возможность мелким производителям и стартапам выйти на рынок с продукцией, предназначенной только

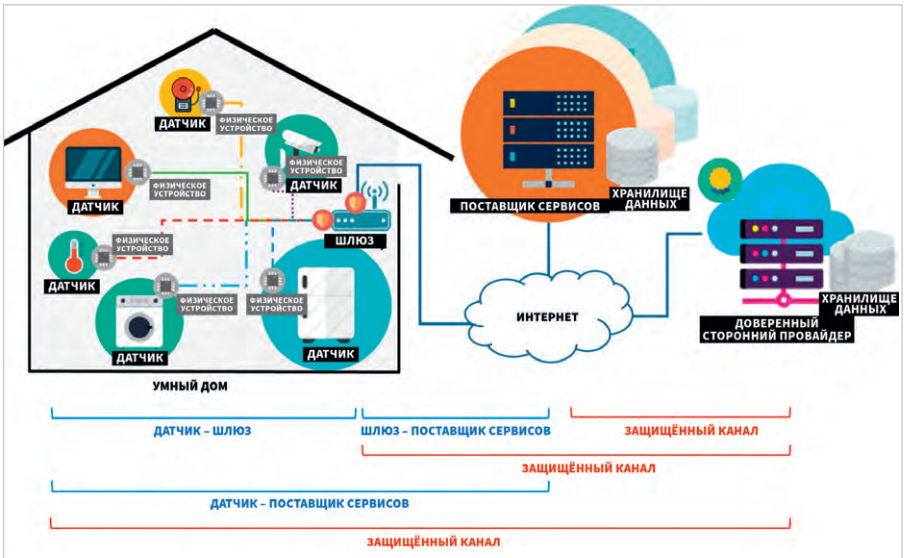


Рис. 3. Схема проекта «Умного дома» с иерархической топологией контроля оборудования [10]

для определённого сегмента. Например, такое бытовое оборудование, как системы отопления и климат-контроля, холодильники, кухонное оборудование, имеют один тип интеллектуальных сенсоров. В системах видеонаблюдения, телевизорах, охранных сигнализациях используются другие сложные автоматизированные датчики. Для управления освещением, замками, шторами и другими аналогичными устройствами используются простейшие датчики с микропотреблением электроэнергии. Для управления этими устройствами можно задействовать различные типы контроллеров.

На рисунке 3 показана схема проекта «Умного дома» с иерархической топологией контроля оборудования.

Сенсорные сети в этом проекте разделены на три класса в зависимости от назначения и технических возможностей: нижний, средний и высший. Интеллектуальный сенсор высшего уровня предназначен для выхода через точку доступа (AP) в сеть Интернет, а также для управления сенсорами среднего уровня. Интеллектуальные сенсоры среднего уровня управляют простейшими датчиками нижнего уровня. Сенсоры среднего класса взаимодействуют только с ближайшими датчиками низшего и высшего классов и не имеют выхода во внешние сети.

Датчик низшего класса общается только с ближайшим к нему сенсором среднего класса. Все сенсоры оснащены уникальными ключами, представляющим собой чип, который нельзя физически скопировать. Сеансы связи предполагают предварительную взаимную аутентификацию сенсоров и согласование ключей. Таким образом, указанная схема является безопасной и эффективной по сравнению с другими методами с одним центральным управляющим микрокомпьютером. Авторы этой работы считают, что предложенная ими схема соответствует требованиям, предъявляемым к нейронным эхо-сетям (ESN, echo state networks) [11], и может быть использована в смешанных сетях.

Нейронные сети ESN позволяют интегрировать в проектах «Умного дома» новые технологии IoT, например автономное управление сенсорами и исполнительными устройствами, киберфизические системы и мобильные узлы. В сетях подобного рода можно отказаться от мощного центрального процессора, поскольку в киберфизических системах (cyber-physical system) [12] вычислительные ресурсы распределены по всей физической системе. При этом вычислительные мощности распределяются по сети в иерархическом порядке в зависимости от назначения и сложности сенсоров. Развитие подобных экосистем, основанных на ESN-сетях, позволит подключать к проектам «Умного дома» отдельными блоками оборудование конкретного назначения, например блоки оборудования безопасности, кухонного оборудования, садово-огородный блок и другие подобные комплексные наборы оборудования.

С развитием IoT-технологий пропорционально увеличивается вероятность угроз безопасности. Поскольку современный «Умный дом» представляет собой сложный программно-аппаратный комплекс с большой базой данных, он в принципе уязвим для различного рода злонамеренных попыток взлома систем безопасности, которые могут причинить серьёзный ущерб и даже угрожать жизни людей, находящихся в доме.

Возможны несколько основных потенциальных вариантов утечки данных на следующих этапах передачи информации: «устройство–устройство» (интеллектуальный сенсор), «устройство–координатор», «координатор–шлюз», «устройство–контроллер для локальной сети», «контроллер поставщика услуг IoT и сервисные службы Интернет». Системы безопасности современных проектов «Умного дома» должны обеспечивать надёжную защиту на каждом из перечисленных этапов передачи информации. Основные хакерские технологии взлома систем IoT достаточно хорошо известны: Exploits, Password Attacks, IoT Worms, Unpatched Devices, Legacy Protocol, Cryptojacking и другие [13]. Методы борьбы с этими технологиями подробно описаны [14–17]. Поэтому в этой статье не будет детально рассмотрен этот вопрос.

Поскольку все проекты «Умного дома» предусматривают выход в глобальные внешние сети, перенасыщенные различными вирусами, проблемы безопасности, связанные с Интернет, также крайне важны для этого направления IoT. Даже опытные пользователи, не говоря уже о детях и пожилых людях, могут кликнуть на ссылку, которая запустит механизм заражения вирусами систем, управляющих оборудованием дома. Поэтому необходимо обеспечить комплексную локальную и облачную защиту от заражения вирусами и сетевых атак.

Проект «Умный дом с подключением по протоколу IP»

Отмеченные ранее глобальные проблемы, связанные с индустрией «Умного дома», признают все ведущие мировые производители, поставщики и интеграторы электроники.

Заметный отрыв трёх лидеров рынка от потенциальных конкурентов для Amazon, Google и Apple создаёт определённое преимущество. Однако для остальных компаний и для индустрии «Умного дома» в целом такая ситуация является крайне неприятной. Определённые нарекания, связанные с допол-

нительными неудобствами при выборе и монтаже оборудования, возникают у потребителей рынка.

Несовместимость технологий и оборудования для всех участников этого рынка, кроме трёх лидеров, создаёт дополнительные проблемы:

- необходимость дополнительных значительных затрат на выбор и использование проприетарных платформ, протоколов и согласующих шлюзов;
- поддержка складских запасов нескольких наименований изделий одного назначения, но от разных производителей для каждой из несовместимых платформ;
- возможное сокращение срока службы комплекта оборудования, обусловленное изменением базовых протоколов владельцами лицензий.

Наиболее ожесточённая конкурентная схватка наблюдалась между группировками, сложившимися вокруг Thread/Weave–Google/Nest, против их соперников, объединившихся под флагом Amazon+Apple. В проектах Amazon устройства Echo и Eero со встроенными концентраторами умного дома используются интеллектуальные устройства на базе ZigBee [18]. В экосистеме Google nest используются устройства, которые связываются между собой с помощью Thread, Weave и Bluetooth LE [19]. Широко распространённая экосистема HomeKit Apple's smart home platform базируется на технологиях Wi-Fi и Bluetooth LE [20].

Остальные поставщики технологий и комплектующих для «Умного дома» заметно отстают от лидеров по объёмам продаж. Они пытаются либо разрабатывать собственные протоколы, либо предлагают роутеры для связи с платформами Google, Amazon и Apple.

Thread и ZigBee (3.0/pro) используют один и тот же стандарт IEEE 802.15.4 на физическом (PHY) канальном подуровне (MAC) (см. рис. 4). Это значит, что можно, вообще говоря, использовать одинаковые устройства в конкурирующих технологиях. Понимая это и видя бесперспективность дальнейшей конкурентной борьбы, соперники решили объединиться и продолжить совместные разработки на благо потребителей всего мира. Таким образом, в декабре 2019 года Amazon, Apple, Google под руководством Zigbee Alliance создали рабочую группу, названную Project Connected Home over IP (CHIP – умный дом с подключением по протоколу IP). Основная цель этой рабочей группы заключается в разработке и продвижении единого стандарта протоколов беспроводной связи с открытым кодом, предназначенных для оборудования, используемого в проектах «Умного дома» [21].

В 2020 году к проекту CHIP присоединились: IKEA, Legrand, NXP Semiconductors, Resideo, Samsung SmartThings, Schneider Electric, Signify (ранее Philips Lighting), Silicon Labs, Somfy и Wulian. Предполагается, что основное руководство проектом будет осуществлять Zigbee Alliance.

В качестве двух основных задач проекта CHIP можно выделить, во-первых, унификацию блоков «Умного дома» различных производителей, а во-вторых, снижение затрат на разработку и монтаж оборудования.

Литература

1. https://memoori.com/evolution-building-management-system-data-connectivity/.
2. https://www.researchgate.net/publication/336325413_IoT_for_smart_homes/link/5e3e00b892851c7f7f25f96e/download.
3. https://www.aarp.org/caregiving/home-care/info-2017/best-buy-tech-gadgets-caregiving-fd.html.
4. https://www.iot-now.com/2021/03/09/108212-case-study-sophisticated-iot-platform-for-billions-of-connected-fridges/.
5. https://harborresearch.com/.
6. https://www.mordorintelligence.com/industry-reports/global-smart-homes-market-industry.
7. https://www.mdpi.com/1424-8220/16/7/1036/htm.
8. https://www.dreamstime.com/photos-images/smart-home.html.
9. https://www.paritet94.ru/gadzhety/umnyj-dom/komplekt-umnyj-dom-xiaomi-smart-home-security-kit-global-ver.
10. https://www.mdpi.com/2073-8994/9/8/143.
11. https://arxiv.org/abs/2012.02974.
12. https://www.researchgate.net/figure/Attack-surface-of-Cyber-Physical-System-CPS-24_fig1_332826219.
13. https://habr.com/ru/company/yota/blog/333850/.
14. https://researchers.mq.edu.au/en/publications/blockchain-for-iot-security-and-privacy-the-case-study-of-a-smart.
15. https://arxiv.org/pdf/1705.06805.pdf.
16. https://link.springer.com/chapter/10.1007/978-981-10-0281-6_70.
17. https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/industries/home-automation.
18. https://www.amazon.com/b/ref=ods_aucc_dp_bp_wwytk2?node=17238426011.
19. https://support.google.com/googlenest/answer/7071794?hl=en&ref_topic=7195641.
20. https://developer.apple.com/support/homekit-accessory-protocol.
21. https://www.connectedhomeip.com/.

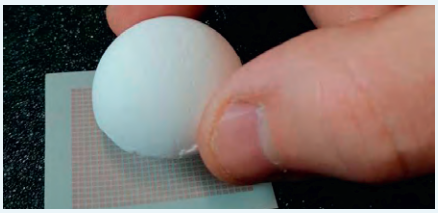
НОВОСТИ МИРА

Электроника 6G из дерева

Из наноцеллюлозы уже сделаны радиолинзы, которые фокусируют сигналы радиопередатчика.

В настоящее время исследователи разрабатывают радиоустройство 6G для демонстрации передачи данных с максимально возможной скоростью. В 6G частота сигнала составляет порядка 300 ГГц, а длина волны такова, что размер антенны не должен превышать 1мм.

Фокусировка сигнала на антенне приёмника является решающим моментом. Для этого необходимы радиообъективы. Наноцеллюлоза как материал для их изготовления имеет много преимуществ: это лёгкий, механически прочный материал с низкой структурой потерь электроэнергии, и она легко доступна. Лёгкость и низкие потери крайне важны. Потери сигнала в материале должны быть минимальными. Лучший из материалов может состоять на 99% из воздуха, и тогда доля потерь будет бесконечно мала. Из целлюлозы уже напечатан материал, похожий на воздух, а это означает, что он чрезвычайно лёгкий. Она хорошо подходит для 3D-печати и обеспечивает необходимую опорную структуру,



образующуюся из нанотрубок, что означает, что в них содержится много воздуха. Водорастворимый и хрупкий электронный компонент, мягко говоря, выглядит странно, но исследователи планируют разработать для линз защитную плёнку.

www.techxplore.com

Интегральная фотоника: перспективы применения в системах связи

Анатолий Ковалёв (генеральный директор АО «ЗНТЦ»)

В статье представлено краткое описание основных направлений и ключевых преимуществ использования технологий интегральной фотоники. Рассмотрены возможности использования фотонной компонентной базы, в том числе AWG мультиплексоров/демультиплексоров в телекоммуникационных и других стратегически значимых отраслях промышленности. Представлено краткое описание полученных АО «ЗНТЦ» результатов в области разработки и производства фотонных интегральных схем.

В современном мире объём передаваемой информации настолько велик, что стандартные системы связи достигли предела и не соответствуют требованиям современной индустрии в части обеспечения необходимого уровня вычислений и пропускной способности. По экспертным оценкам, к 2025 году объём всех данных во всем мире составит 163 ЗБ, что в 10 раз больше, чем общий объём данных по состоянию на 2016 год [1].

Подсчитано, что 90% всех данных в мире было создано за последние несколько лет, и их объём растёт экспоненциально. Если бы эти данные записали на CD-диски, то стопка дисков устремилась бы до Луны и смогла бы вернуться обратно [2]. Кроме того, на обеспечение функционирования Интернета приходится около 10% мировой электроэнергии, при том что потребление энергии каждые 4 года увеличивается в 2 раза. Всё это привело к необходимости разработки новых технологий, превосходящих современные решения, применяемых для производства телекоммуникационных систем и центров обработки данных.

Наиболее эффективно решить задачи организации систем высокоскоростной передачи данных позволяет интегральная фотоника. Интегральная фотоника и оптоэлектроника – это объединение электроники и оптики, позволяющее «принципиально изменить систему передачи данных на расстояниях от миллиметров до тысяч километров» [3]. Несмотря на то что фотоника является сравнительно молодой отраслью, её смело можно считать индустрией будущего.

Значимость результатов внедрения фотоники может быть сопоставима с изобретением полупроводников. Внедрение фотоники позволяет «сохранить действие закона Мура, составляющего базис развития информационных и коммуникационных технологий» [3]. По прогнозам экспертов, к 2027 году рынок фотонных интегральных схем (ФИС) достигнет $3,3 млрд.

Рис. 1. Производственный комплекс

С 90-х годов оптическая технология передачи данных широко используется во всём мире для создания телекоммуникационных сетей, сетей передачи данных, управления, телеметрии. Европейский союз вкладывает большие средства в развитие фотоники. Разработана программа развития фотоники на 2021–2027 годы. Также создан консорциум производителей изделий фотоники и радиофотоники (EPIC), объединяющий более 147 фирм и корпораций. Практически все крупные фирмы и корпорации электронной индустрии мира, включая таких гигантов, как Intel и IBM, сформировали научно-исследовательские и научно-производственные кластеры, занимающиеся фотоникой и оптоэлектроникой.

В США развитие фотоники в основном финансируется за счёт сегмента IT Electronics национальной нанотехнологической инициативы (NNI). Благодаря данным инструментам поддержки в настоящее время иностранными компаниями выпускается широкая номенклатура ФИС, позволяющая зарубежным производителям электронной аппаратуры создавать энергоэффективные защищённые высокопроизводительные системы управления, передачи и обработки информации. Исследования по основным направлениям в области интегральной фотоники ведутся во многих лабораториях мира:

- Andrew M. Weiner et al., Ultrafast Optics and Optical Fiber Communications Laboratory, Purdue University, USA;
- Karry Vahala et al., California Institute of Technology;
- Roberto Morandotti et al,, INRS-EMT, Varennes, Quebec, Canada;
- Yanne K. Chembo et al,, 2FEMTO-ST Institute [CNRS UMR6174], Optics Department, Besancon cedex, France;
- Electro-Optic Materials and Devices Group Lincoln Laboratory (MIT) США.

При этом в настоящее время в России, за исключением полупроводниковых лазеров, отсутствует серийное производство элементов интегральной фотоники – всего спектра: от пассивных элементов до гибридных сборок пассивных с активными элементами. Это однозначно влечёт за собой зависимость отечественных производителей телекоммуникационного оборудования и ЦОД от зарубежных компаний. Применение DWDM-технологий DWDM спектрального уплотнения данных позволит обеспечить высокоскоростную передачу информации, увеличить скорость передачи данных с 50 Гб/с до 10...100 Тб/с, что важно для обеспечения задач цифровой экономики.

Чтобы сформировать условия развития отечественного производства электроники для телекоммуникационной индустрии в России, создан консорциум «Телекоммуникационные технологии» (АНО ТТ). Участники консорциума формируют отечественную экосистему содействия развитию цифровой инфраструктуры и отечественных телекоммуникационных систем. В рамках экосистемы АНО «Телекоммуникационные технологии» Зеленоградский нанотехнологический центр (АО «ЗНТЦ») развивает технологии интегральной фотоники для оптоволоконных систем связи, ЦОДов, сетей распределённых вычислений.

Наличие собственного производственного участка полного цикла и технологий производства позволяет максимально быстро, экономически эффективно разрабатывать и поставлять заказчику фотонные интегральные структуры (ФИС). Эти структуры позволяют создавать телекоммуникационные сети, соответствующие их индивидуальным требованиям гарантированной доступности, интеллектуальных возможностей, производительности, пропускной способности и безопасности.

В настоящее время на площадке АО «ЗНТЦ» отрабатываются технологии производства ФИС, в том числе оптических волноводных AWG мультиплексоров/демультиплексоров для DWDM-систем (см. рис. 1).

ФИС используют оптические методы передачи данных, в частности методы спектрального уплотнения сигнала, позволяющие параллельно передавать информацию по нескольким каналам, тем самым увеличивая не только объём, но и защищённость систем связи.

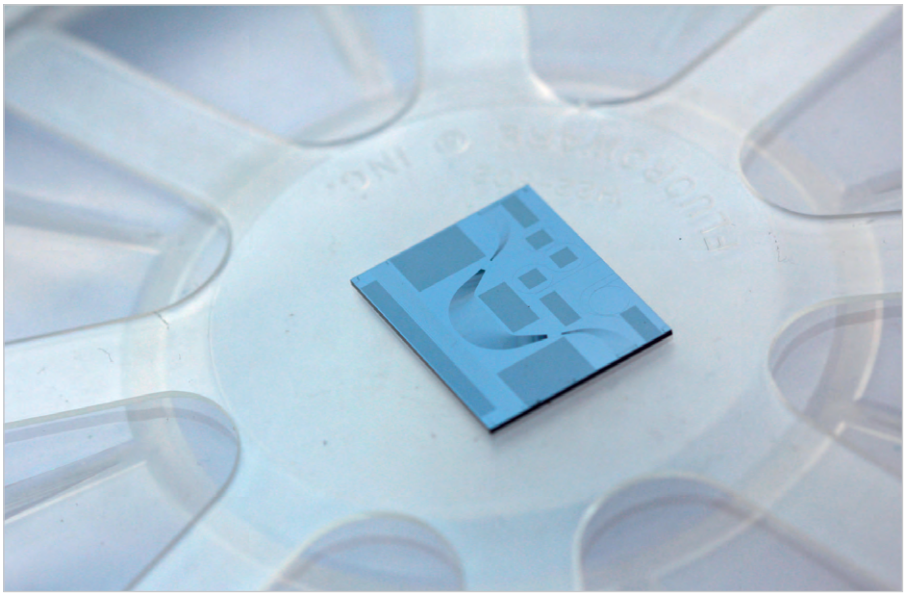


Рис. 2. Кристалл AWG мультиплексора

Получены экспериментальные образцы разрабатываемой продукции (см. рис. 2). Технологии спектрального уплотнения данных позволяют увеличить пропускную способность систем связи в 10–100 раз, обеспечивают возможность создания доверенных и помехоустойчивых систем. Передача данных по оптическим сетям не допускает бесконтактного считывания, т.к. не порождает никаких излучений.

Разрабатываемая фотонная компонентная база позволит создавать устройства для использования в оптической телекоммуникации и квантовой криптографии. С производителями телекоммуникационной аппаратуры согласовываются технические требования и уточняются сферы применения элементов интегральной фотоники.

Элементы интегральной фотоники являются базовыми при проектировании оптических коммутаторов, спектрально-зависимых и независимых переключателей каналов, поляризационных делителей, спектральных модулей ввода-вывода (add-drop фильтров), внешних резонаторов для лазерных диодов (как простейших некоммутируемых, так и коммутируемых для переключения частоты генерации лазерного диода) и др. Актуальность разработки и технологической отладки изготовления оптических мультиплексоров для работы в DWDM-системах определяется как возрастающим объёмом передаваемой информации, так и широким применением данных устройств различной конфигурации в технологических элементах оптических сетей.

Целевыми потребителями разрабатываемых АО «ЗНТЦ» AWG мультиплексоров/демультиплексоров являются компании-производители высокоскоростных и энергоэффективных устройств передачи и обработки телекоммуникационных сигналов. Эти устройства используются для бортовой аппаратуры и наземной инфраструктуры авиационно-космической отрасли, а также в телекоммуникационной отрасли для организации мощных информационных сетей и подключения пользователей к высокоскоростному Интернету, IP-телефонии и IP-телевидению.

По экспертным оценкам, увеличивающиеся требования к доверенности сетевой инфраструктуры приводят к тому, что ключевые элементы телекоммуникационного оборудования должны создаваться на основе отечественных технологий с использованием российской компонентной базы, так как это позволит обеспечить необходимый уровень доверия к сетям связи и их информационную безопасность. В свою очередь, независимость отечественной промышленности от зарубежных компаний будет способствовать интеллектуальному и промышленному росту национальной экономики.

Литература

1. Электронный источник: https://aftershock.news.
2. Электронный источник: https://sci-fact.ru.
3. S. Lin et al, "Efficient, tunable flip-chip-integrated III-V/Si hybrid external-cavity laser array", Optics Ex-press, v.24, no.19, pp.21454-21462 (2016).

Исследование эксплуатационных качеств покрытий для радиочастотных соединителей

Кристиан Рем (HUBER+SUHNER), **Кристиан Дандл, Бернхард Цехентнер, Райнхард Вагнер** (Rosenberger)

В статье приведены результаты исследований контактного сопротивления, износостойкости, гибкости, паяемости и интермодуляционных свойств материалов, применяемых для покрытий радиочастотных соединителей. В ходе испытания анализировались эксплуатационные качества пяти различных покрытий: серебра, белой бронзы (в том числе инновационного материала SURO720), олово-никеля и химического никель-фосфора.

Введение

HUBER+SUHNER AG и Rosenberger Hochfrequenztechnik GmbH & Co. KG являются ведущими поставщиками радиочастотных и оптических компонентов связи: соединителей, кабелей и готовых сборок для телекоммуникаций, приборов космической промышленности, приложений для защиты, тестирования и измерений. Поскольку покрытие из материала остаётся решающим фактором при определении характеристик радиочастотных соединителей, обе компании серьёзно занимаются научно-исследовательскими работами в области разработки новых покрытий. Для этого у компаний имеется соответствующее оборудование.

Чтобы предоставить клиентам подробную информацию о различных покрытиях и их характеристиках, компании HUBER+SUHNER и Rosenberger продолжают очень тесно сотрудничать. Результатом этого сотрудничества стала настоящая статья, которую можно использовать в качестве справочного материала при выборе различных вариантов покрытия.

В данной статье оцениваются традиционные современные покрытия, а также новое запатентованное покрытие SURO720, разработанное HUBER+SUHNER в партнёрстве с Rosenberger.

Чтобы получить более подробные характеристики различных покрытий, используемых в радиочастотных соединителях, в рамках исследования оценивалась устойчивость к коррозии при испытании в соляном тумане в течение 720 ч. В ходе теста анализировались эксплуатационные качества пяти различных покрытий: серебра, белой бронзы, SURO720, олово-никеля и химического никель-фосфора. Помимо этого, исследованы контактное сопротивление, износостойкость, гибкость, пригодность к пайке и пассивные интермодуляционные свойства.

Что касается контактного сопротивления, то лучшие результаты продемонстрировали серебряные покрытия. Чуть хуже показатели у белой бронзы, SURO720 и оловянно-никелевых покрытий. Химическое никель-фосфорное покрытие показало наибольшее контактное сопротивление.

Наилучшая износостойкость была у покрытия никель-фосфор, полученного методом химического восстановления. Покрытие из серебра чрезмерно изнашивается, потому этот материал не рекомендуется для применений с большим количеством циклов соединений и рассоединений. Недостаток твёрдости и износостойкости был отмечен и у никель-фосфорного покрытия – в результате агрессивного воздействия покрытие оказалось очень хрупким.

Для пайки пригодными оказались покрытия из серебра, SURO720 и белой бронзы. Никель-фосфорное покрытие имеет плохую смачиваемость при пайке стандартными припоями. Плохая смачиваемость, вероятно, вызовет проблемы во время пайки, особенно в изделиях, чувствительных к пассивной интермодуляции (ПИМ). Олово-никелевое покрытие можно паять, однако это потребует очень строгого контроля во время нанесения покрытия и пайки деталей, кроме того, проблемы могут возникнуть и во время хранения. Поэтому олово-никель не является идеальным покрытием для паяемых деталей.

Что касается коррозии, моделируемой с помощью 720-часового нахождения в солевом тумане, серебряные покрытия с последующей обработкой против потускнения на основе тиола и химический никель-фосфор показали удовлетворительные результаты.

В то же время никель-фосфорные покрытия лучше справляются с коррозией. Серебряные покрытия практически не показывают ухудшения контактного сопротивления. Олово-никелевые покрытия обесцвечиваются, при этом у них повышается контактное сопротивление.

Без прямого контакта с алюминием стандартное белое бронзовое покрытие подвергается коррозии даже визуально, в то время как новое покрытие SURO720 почти не изнашивается. Кроме того, контактное сопротивление SURO720 незначительно изменяется после испытания на коррозию. Таким образом, SURO720 отвечает самым высоким требованиям с точки зрения устойчивости к коррозии, пригодности к пайке и электрических характеристик, сохраняя при этом значительное экономическое преимущество обычных покрытий перед покрытиями из белой бронзы.

На рынке мобильной связи сформировался тренд на соединители с повышенными требованиями к характеристикам покрытия, особенно к коррозионной стойкости. Соединители, используемые на открытом воздухе, например на удалённых радиоголовках и антеннах, подвергаются экстремальным нагрузкам и должны выдерживать температурные перепады (от арктических зим до тропической жары). Для этих соединителей необходимо покрытие с исключительной коррозионной стойкостью, только так соединители будут соответствовать строгим механическим и электрическим требованиям.

В настоящее время в конструкции соединителей используется множество различных типов покрытий, поэтому необходимо подробное сравнение их преимуществ и недостатков, чтобы выяснить, какое из них обеспечивает оптимальную коррозионную стойкость. Так, компании HUBER+SUHNER AG и Rosenberger провели обширное сравнительное исследование наиболее популярных покрытий радиочастотных соединителей. Также в этом

исследовании участвовали внешние партнёры, таким образом, гарантировалось эффективное управление специальными процедурами тестирования и нейтральное ранжирование результатов тестирования. Результаты обширного исследования, представленные в статье, служат руководством при выборе подходящего покрытия для каждого конкретного применения.

Покрытия

Следующие покрытия наиболее распространены для наружных радиочастотных соединителей (у всех покрытий толщина составляла от 3 до 6 мкм).

Серебро (Ag)

Серебряное покрытие известно выдающимися электрическими характеристиками. Как благородный металл серебро обладает отличной коррозионной стойкостью, но со временем может потускнеть. Тем не менее изменение цвета поверхности, вызванное наличием сероводорода (H_2S), в большинстве случаев не влияет на технические свойства и может быть сведено к минимуму с помощью соответствующей дополнительной обработки против потускнения.

Серебряное покрытие отличается отличной проводимостью, пригодностью к пайке и высокими характеристиками ПИМ. Поэтому этот материал чаще всего выбирают для нанесения покрытия на центральные контакты и внешние контакты радиочастотных соединителей, таких как 7/16, 4.3-10, 4.1-9.5 и NEX10. В некоторых случаях он также используется в качестве покрытия поверхности для корпусирования соединителей и других компонентов.

Белая бронза (CuSnZn)

Белая бронза – тройной сплав меди, олова и цинка. Этот материал известен под разными торговыми названиями, например Sucoplate или Optalloy. Белая бронза – экономичное покрытие с улучшенной износостойкостью по сравнению с покрытием из серебра. Белая бронза представляет собой отличную и недорогую альтернативу серебру с точки зрения проводимости и характеристик ПИМ. Бронза – более дешёвый вариант покрытия для корпусов радиочастотных соединителей, таких как 7/16, 4.3-10, 4.1-9.5 и NEX10.

SURO720

HUBER+SUHNER и Rosenberger разработали улучшенную версию белого бронзового покрытия для применений с высокими требованиями к коррозионной стойкости. Это покрытие имеет такой же внешний вид, электрические и механические свойства, как и стандартная белая бронза, и при этом обладает гораздо лучшей коррозионной стойкостью. Таким образом, новое покрытие SURO720 может заменить все существующие покрытия из белой бронзы, обеспечивая при этом стойкость к коррозии в течение 720 ч, стабильную пайку и характеристики ПИМ без значительного увеличения стоимости.

Олово-никель (SnNi)

Из-за устойчивости к коррозии оловянно-никелевые покрытия, доступные на рынке под различными торговыми марками, активно применяются при производстве высокочастотных соединителей. Олово-никелевое покрытие изобретено ещё в 1950-х годах, однако оно не получило признания на рынке коммерческих коаксиальных электрических соединителей. Этот сплав состоит примерно из 65% олова и 35% никеля. Несмотря на содержание никеля, материал не обладает магнитными свойствами.

Использование оловянно-никелевого покрытия требует осторожности. В дешёвых версиях хром используется для повышения устойчивости к коррозии. Поскольку коммерческое использование хрома (особенно шестивалентного) строго регламентировано, оловянно-никелевое покрытие всегда следует проверять на наличие этого химического элемента.

Химический никель-фосфор (NiP)

Никель-фосфор, нанесённый методом химического восстановления, является одним из наиболее распространённых материалов покрытия для радиочастотных соединителей. Содержание фосфора должно быть меньше 10%, чтобы покрытие оставалось немагнитным. Покрытие из никеля с высоким содержанием фосфора демонстрирует превосходную коррозионную и износостойкость, однако относительно высокое контактное сопротивление может препятствовать использованию этого покрытия для применений с высокими требованиями к проводимости.

HUBER+SUHNER и Rosenberger провели обширные испытания каждого из упомянутых материалов на предмет соответствия рабочим характеристикам радиочастотных соединителей. Результаты этих тестов приведены далее.

Сопротивление контактов

Контактное сопротивление – один из наиболее важных параметров, который может существенно повлиять на высокочастотные характеристики коаксиального соединителя. Сопротивление контакта зависит не только от покрытия, но и от того, как устанавливаются контакты между штекерным и гнездовым соединителями. Проще говоря, сопротивление зависит от того, имеет соединитель стыковой или радиальный контакт со скользящим движением.

Для контактов со скользящим движением контактные сопротивления обычно ниже, поскольку изолирующие оксидные слои на поверхности частично разрушаются из-за износа, вызванного регулярной очисткой поверхности. Разрушаются чаще всего неблагородные металлы, что приводит к обнажению нетронутого металла и хорошему электрическому контакту. Однако скольжение также вызывает и износ покрытия.

Удовлетворительное контактное сопротивление может быть достигнуто только после многократного сопряжения и удаления изолирующих слоёв. Таким образом, были выполнены две разные экспериментальные установки для моделирования контактов без скольжения (установкой стыковых соединителей) и со скольжением и трением поверхностей.

Переходное сопротивление для контактов без скольжения

Для контактов без скольжения серебро имеет самое низкое контактное сопротивление – оно менее 5 мОм даже при слабых усилиях. Покрытия из SURO720 и белой бронзы демонстрируют умеренное контактное сопротивление, достигающее <100 мОм при усилии 1 Н.

Высокое контактное сопротивление имеют покрытия олово-никель (примерно 400 мОм при контактном усилии 1 Н) и никель-фосфор (примерно 100 мОм при контактном усилии 1 Н). Поэтому для приложений, чувствительных к контактному сопротивлению, использовать олово-никель и никель-фосфор не рекомендуется (см. рис. 1).

Эксперименты проводились со скольжением 3 мм и контактными усилиями 1 и 5 Н. Испытания показали, что характеристики различных материалов покрытия практически не изменились. Серебряное покрытие демонстрирует превосходные значения контактно-

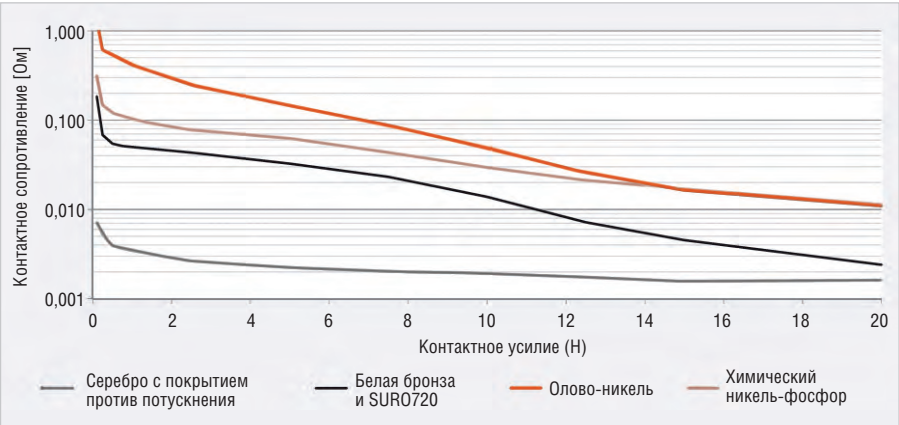


Рис. 1. Контактное сопротивление как функция контактного усилия

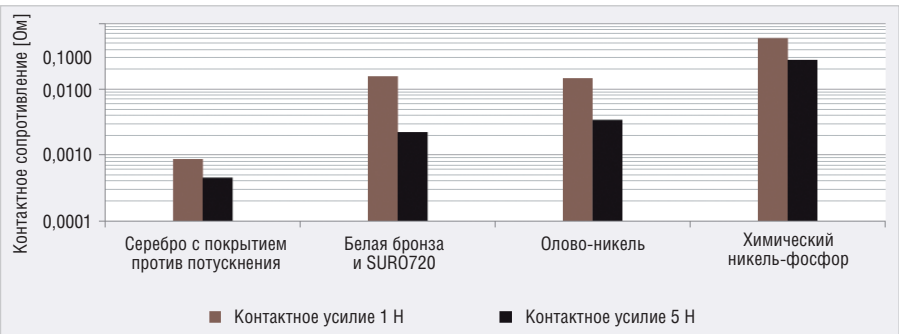


Рис. 2. Контактное сопротивление покрытий при контактном усилии 1 и 5 Н

Таблица 1. Рейтинг контактного сопротивления различных покрытий

Серебро	Белая бронза и SURO720	Олово-никель	Химический никель-фосфор
+ +	+	+	–

Таблица 2. Оценка гибкости различных покрытий, определённой в результате испытания на трёхточечный изгиб

Серебро	Белая бронза и SURO720	Олово-никель	Химический никель-фосфор
+ +	+	+	– –

го сопротивления (<1 мОм) даже при малых контактных усилиях (1 Н).

Покрытия оловянно-никелевые и белая бронза (SURO720) имеют контактные сопротивления в пределах 15 мОм для контактного усилия 1 Н, при 5 Н контактное сопротивление составляет 2–3 мОм. Для покрытия из химического никель-фосфора контактное сопротивление обычно выше: 60 и 30 мОм для контактных усилий 1 и 5 Н соответственно. Появление оксидного слоя приводит к более серьёзному изменению сопротивления в зависимости от количества циклов сопряжения.

Нанесение никель-фосфорного покрытия методом химического восстановления не рекомендуется, если требуется низкое и стабильное контактное сопротивление. Покрытие оловянно-никелевое по этому параметру лучше, чем никель-фосфор, оно сопоставимо с белой бронзой и SURO720 (см. рис. 2).

Таким образом, серебряное покрытие показывает лучшие результаты в отношении контактного сопротивления: это покрытие является предпочтительным, если наличие высокого контактного сопротивления имеет особое значение для конкретного радиочастотного соединителя. Белая бронза, SURO720 и оловянно-никелевое покрытие соответствуют большинству требований к радиочастотным соединителям. Никель-фосфорное покрытие методом химического восстановления имеет высокое и нестабильное контактное сопротивление и не рекомендуется для применений с низким и стабильным контактным сопротивлением (см. табл. 1).

Деформируемость и износ

Если покрытие хрупкое, то из-за деформации или разрушения оно может серьёзно повлиять на общие характеристики радиочастотного соединителя. Пластичность различных покрытий была исследована с помощью испытания на трёхточечный изгиб. Большинство покрытий не повредились и не потрескались после этого испытания. Кроме того, покрытие олово-никель, которое нередко считается хрупким, было деформировано незначительно. Только химическое никель-фосфорное покрытие, известное своей хрупкостью, показало серьёзные повреждения вплоть до отслоения покрытия (см. табл. 2). Износ покрытия радиочастотных соединителей указан для большого числа циклов соединения и рассоединения, например для соединителей 7/16 и 4,3-10 это 500 и 100 циклов соответственно. Износ покрытия становится важной проблемой, которую необходимо учитывать при выборе подходящих покрытий для радиочастотных соединителей.

В частности, важную роль играют нормальная сила в зоне контакта и длина скольжения. Однако коэффициент трения, часто обозначаемый μ, зависит от самого материала контакта и определяется как отношение силы трения между двумя телами и силы, прижимающей их друг к другу. Высокий коэффициент трения приводит к более высоким усилиям, которые приходится прилагать для установки соединителей, и это часто вызывает повышенный износ. В частности, серебряное покрытие демонстрирует высокий коэффициент трения.

Результаты по износу были получены в том же эксперименте, в котором исследовалось сопротивление контакта со скользящим движением. Для каждого типа покрытия было проведено 10 и 25 циклов сопряжения с длиной скольжения 3 мм при контактных усилиях 1 и 5 Н соответственно (см. рис. 3 и табл. 3). Следы износа исследовали с помощью оптической микроскопии.

Износостойкость при контактном усилии 1 Н

При контактном усилии 1 Н большинство исследованных покрытий оставались неповреждёнными после 25 циклов соединения. Только серебряное покрытие показало износ: основной материал обнажился. Эта проблема серебряного покрытия хорошо известна: серебро относительно мягкое и демонстрирует высокий коэффициент трения. Однако некоторые средства дополнительной обработки против

потускнения оказывают смазывающий эффект в первые 5–10 циклов сопряжения, что в целом снижает износ.

Износостойкость при контактном усилии 5 Н

При повышении усилия контакта износ покрытия становится более серьёзной проблемой. При нормальном усилии (5 Н) все покрытия показали повреждения по дорожке износа после 25 циклов соединения. Серебряное покрытие было изношено после 10–15 циклов сопряжения. Коэффициент трения был около 1,2, и только при обработке против потускнения покрытие показало более низкий коэффициент трения – от 0,2 до 1,0 в течение первых 10 циклов сопряжения.

Покрытия из белой бронзы и SURO720 показали умеренное повреждение: обнажение основного материала произошло после 25 циклов сопряжения. Коэффициент трения увеличился с 0,2 до 0,4 после 25 циклов соединений. Покрытие олово-никель имело относительно высокий коэффициент трения (~0,6), также произошло частичное обнажение основного материала. Наилучшие результаты были получены при нанесении никель-фосфорного покрытия методом химического восстановления, при котором после 25 циклов сопряжения обнаружилось лишь очень небольшое нарушение покрытия, а следы воздействия на основной материал и вовсе отсутствовали.

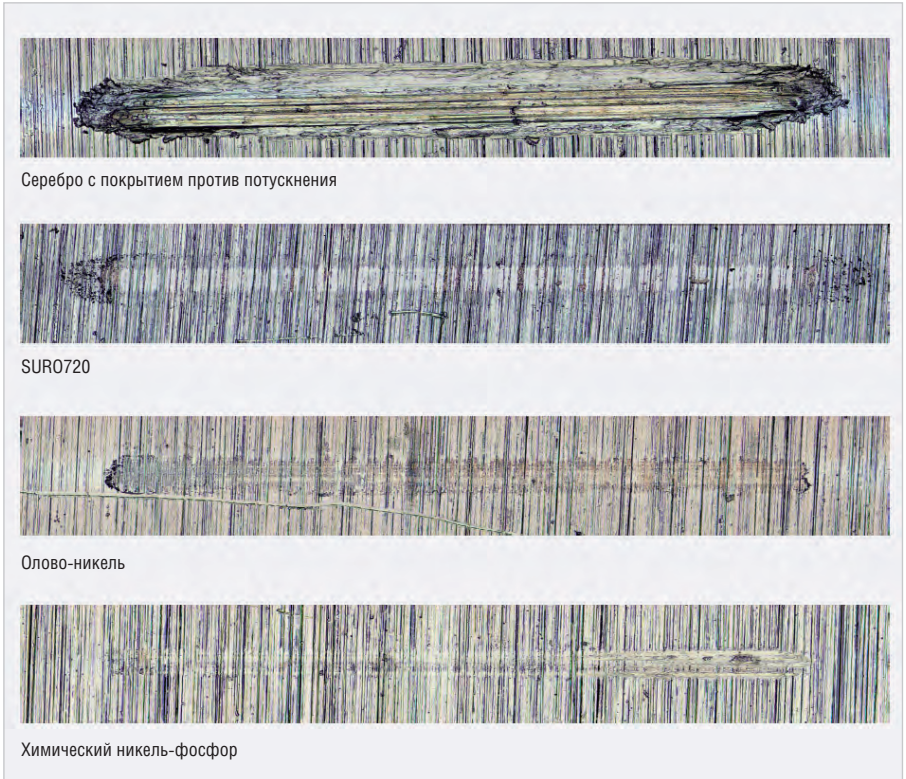


Рис. 3. Следы износа после 25 циклов сопряжения (нормальное усилие 5 Н, скольжение – 3 мм)

Таблица 3. Оценка износа различных покрытий

Серебро	Белая бронза и SURO720	Олово-никель	Химический никель-фосфор
– –	–	–	+

Таблица 4. Паяемость различных покрытий, определяемая балансом смачивания

Серебро	Белая бронза и SURO720	Олово-никель	Химический никель-фосфор
+ +	+ +	–	– –

Пригодность к пайке (паяемость)

В радиочастотные соединители, используемые в кабельных сборках, часто припаивают кабели. Пригодность к пайке – важный параметр, который был протестирован с помощью анализа смачиваемости. Для этого испытания использовался припой $Sn_{96,5}Ag_{3,8}Cu_{0,7}$ (согласно IPC J-STD-006/ISO 9453). Испытания на паяемость проводились на новых образцах, также тестирование проходило и после хранения в течение 10 дней при 40°C и 95% относительной влажности. Таким образом имитировались условия хранения в соответствии с IEC 60068-2-78. Использовались два нормальных состава припоя: 1 (ROL0 согласно J-STD-004, 0,2% хлора) и 2 (ORL0 согласно J-STD-004, 0,5% хлора).

Серебро как благородный металл ожидаемо показывает лучшие результаты в этой категории. Даже после продолжительного хранения смачиваемость остаётся отличной. Белая бронза и SURO720 также показали хорошие результаты смачиваемости. Для белой бронзы и SURO720 характеристики паяемости сравнимы с серебром. После имитации хранения смачиваемость покрытий из белой бронзы немного снижается, но всё же материал имеет хорошую способность к пайке, обеспечивая требуемые электрические и механические характеристики радиочастотных соединителей и кабельных сборок.

В отличие от белой бронзы и SURO720 никель-фосфорное покрытие плохо припаивается и не соответствует требованиям к смачиваемости, определённым протоколом испытаний. Даже при использовании более агрессивного нормального состава припоя 2 (0,5% хлора) требования к смачиваемости не были достигнуты. Олово-никелевое покрытие не подлежит пайке с помощью стандартных процессов. Пайка оловянно-никелевого покрытия зависит от трёх критических факторов:

1. качества электролитической ванны для нанесения покрытия;
2. продолжительности хранения деталей перед пайкой;
3. типа используемого состава припоя.

Тип припоя особенно важен для покрытия олово-никель. В проведённом тесте (см. табл. 4) оловянно-никелевое покрытие можно было спаять только с использованием очень агрессивного припоя, после чего требовалась тщательная очистка. Никель-фосфорное и оловянно-никелевое покрытия не рекомендуются для соединителей, которые требуют пайки кабеля (всех кабельных сборок, чувствительных к ПИМ).

Пассивная интермодуляция (ПИМ)

Для большинства приложений на рынке связи пассивная интермодуляция является решающим критерием при выборе радиочастотных соединителей. В случае нестандартного или магнитного покрытия, прохождение сигнала через соединитель может

Таблица 5. Результаты анализа ПИМ

Покрытие	Начальная ПИМ (дБн)
Серебро (с постобработкой против потускнения)	–177,5
Белая бронза или SURO720	–177,6
Олово-никель	–176,7
Химический никель-фосфор	–178,3

быть нарушено из-за помех, например нежелательных гармоник или интермодуляций. Коррозийное повреждение поверхности также может стать причиной ПИМ. Никелирование само по себе является магнитным и не рекомендуется к использованию для приложений, чувствительных к ПИМ. Однако при определённом процентном содержании фосфора покрытие становится немагнитным. Все покрытия были протестированы на магнитные свойства путём определения ПИМ с использованием соединителя 7/16. Получены следующие значения (см. табл. 5, 6).

720 ч: тест в соляном тумане

Испытание солевым туманом – популярный метод оценки коррозионной стойкости покрытий. Однако есть некоторые сомнения в том, насколько соответствуют создаваемые в процессе испытаний условия реальным коррозионным условиям. Тем не менее испытание нейтральным солевым туманом (согласно ASTM B117) является стандартным методом испытаний. Поэтому оно также было применено в данном исследовании для изучения коррозионных свойств исследуемых покрытий.

Контактное сопротивление после испытания в солевом тумане в течение 720 ч

Применяя результаты испытаний на коррозию к радиочастотным соединителям, очень важно отметить, что области электрических контактов для большинства соединителей, таких как 7/16, 4.3-10 и NEX10, почти всегда защищены уплотнением в сопряжённом состоянии (при соединении). Следовательно, эффект коррозии не влияет на радиочастотные характеристики внутри соединителя, однако повреждает внешнюю поверхность даже на визуальном уровне. Во время испытания контактное сопротивление различных покрытий было измерено даже после появления коррозии. Контактное сопротивление различных покрытий, определённое после 720 ч испытаний в соляном тумане, показано на рисунке 4.

Таблица 6. Рейтинг пассивных интермодуляционных эффектов различных покрытий

Серебро	Белая бронза и SURO720	Олово-никель	Химический никель-фосфор
+ +	+ +	+ +	+ +

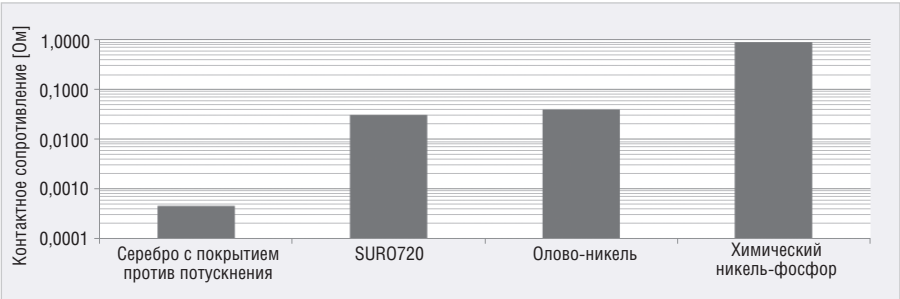


Рис. 4. Контактное сопротивление после испытания в соляном тумане в течение 720 ч в (после одного цикла соединений-разъединений, усилие контакта 5 Н)

Таблица 7. Оценка контактного сопротивления различных покрытий после 720 ч испытания в соляном тумане

Серебро	Белая бронза и SURO720	Олово-никель	Химический никель-фосфор
+ +	–	–	– –

Таблица 8. Визуальная оценка коррозии после испытания в соляном тумане в течение 720 ч

Серебро	Белая бронза и SURO720	Олово-никель	Химический никель-фосфор
+	+	–	+ +

Контактное сопротивление в соляном тумане в течение 720 ч после первого цикла сопряжения при нормальном усилии контакта 5 Н

Среди всех протестированных покрытий образцы с серебряным покрытием (со специальной последующей обработкой против потускнения) показывают лучшие результаты. Контактное сопротивление после коррозии остаётся практически неизменным по сравнению с исходными значениями до коррозии. Покрытие из белой бронзы, включая новое SURO720, и оловянно-никелевое покрытие не обеспечивают стабильного контакта без скользящего движения. Для контактов со скользящим движением контактное сопротивление этих двух типов покрытий после нескольких циклов сопряжения оказывается в 2 раза выше, чем до испытания в солевом тумане, что указывает на значительное ухудшение покрытий из-за коррозии.

Никель-фосфорное покрытие, полученное методом химического восстановления, показало высокое контактное сопротивление перед испытанием на коррозию. Также при стыковом контакте не удалось установить стабильное соединение после испытания солевым туманом. Для контактов с совместным ходом сопротивление контакта после нескольких циклов сопряжения оказалось в 2–4 раза выше, чем до 720-часового испытания в соляном тумане, что указывает на серьёзное ухудшение покрытия (при этом визуально коррозии почти не наблюдается). Результаты приведены в таблице 7.

Визуальная оценка коррозии после 720 ч в испытания в соляном тумане

Для некоторых потребителей наиболее важным является внешний вид покрытия после воздействия агрессивной среды. Все покрытия, рассматриваемые в этой статье, соответствуют требованиям к внешнему виду. Стандартное белое бронзовое покрытие, которое способно выдержать до 48–96 ч воздействия агрессивной среды, было протестировано в солевом тумане 720 ч. Результаты исследования представлены на рисунке 5. Результаты подтверждают, что стандартное покрытие из белой бронзы работает хорошо, по крайней мере до 96 ч. После этого коррозия начинает ухудшать внешний вид, а через 720 ч внешний вид окончательно портится из-за коррозии. Внешний вид исследованных покрытий после 720 ч испытания в соляном тумане показан на рис. 6. Покрытие никель-фосфор показывает наилучшие резуль-

Рис. 5. Стандартная белая бронза (триметалл) после 48, 96 и 720 ч испытаний в соляном тумане

таты: коррозии почти не наблюдается. На серебре с последующей обработкой против потускнения и SURO720 после испытания заметны небольшие пятна коррозии. Однако небольшая коррозия не оказывает значительного влияния на работу соединителей. На оловянно-никелевых покрытиях отчётливо видны пятна коррозии вблизи краёв и особенно – на больших участках, подверженных сильной коррозии. Ржавые участки могут отрицательно повлиять на работу соединителя (см. табл. 8).

Рис. 6. Коррозия образцов после испытания в соляном тумане 720 ч

Коррозия металлических соединителей, установленных в алюминиевый корпус (визуальная оценка)

Радиочастотные соединители часто устанавливают в алюминиевые корпуса. Алюминий является неблагородным металлом с отрицательным потенциалом, поэтому электрохимическая коррозия создаёт серьёзную проблему, если другие металлы находятся в прямом контакте с ним.

Чтобы изучить коррозию, радиочастотные соединители с различными покрытиями были установлены на алюминиевой пластине и затем подвержены действию соляного тумана на 720 ч. При этом использовались винты M3 из нержавеющей стали DIN7986 с цилиндрической головкой с антифрикционным покрытием и без него. Следует учитывать, что алюминий, используемый в этом тесте, не подвергался какой-либо обработке. При этом алюминий, используемый в телекоммуникационном оборудовании, таком как радиоприёмники и антенны, обычно обрабатывается или имеет изоляцию между соединителем и алюминиевой панелью.

Приведённые результаты следует использовать с осторожностью, поскольку в разных приложениях могут быть разные сценарии контакта между соединителем и панелью. Наилучшие результаты показали серебряное покрытие с последующей обработкой против потускнения и никель-фосфорное покрытие. Никель-фосфорные покрытия, нанесённые методом химического восстановления, подвержены незначительной коррозии: едва заметно изменение цвета из-за пассивации поверхности.

Рис. 7. Коррозия образцов после 720 ч испытания в соляном тумане на алюминии (без изоляции)

Посеребрённые покрытия с последующей обработкой против потускнения не изменяют цвет поверхности. Однако на некоторых устройствах есть небольшие пятна коррозии, вероятно, что они появились в результате механического повреждения во время установки соединителей. Олово-никелевые покрытия сильно обесцвечиваются. Белая ржавчина или другие продукты коррозии замечены не были.

В отличие от отдельных соединителей, прошедших 720-часовые испытания в соляном тумане, в соляном тумане белые бронзовые покрытия показывают серьёзную коррозию. Даже улучшенное покрытие SURO720 на основе белой бронзы, которое подверглось коррозии только как отдельная деталь, не смогло противостоять коррозии. Независимо от типа покрытия, необработанный алюминий сильно пострадал от коррозии (см. рис. 7 и табл. 9).

Стоимость

Выбор в пользу того или иного радиочастотного соединителя, конечно же, в первую очередь обусловлен экономическими факторами. Очень важно учитывать стоимость покрытия в процессе проектирования. Покрытие должно отвечать многочисленным техническим требованиям, а

Таблица 9. Визуальная оценка коррозии радиочастотных разъёмов с различным покрытием, установленных на алюминиевых пластинах, после 720 ч испытания в соляном тумане

Серебро	Белая бронза и SURO720	Олово-никель	Химический никель-фосфор
+	– –	-	+

Таблица 10. Сравнение суммарных затрат при использовании различных покрытий

Серебро	Белая бронза и SURO720	Олово-никель	Химический никель-фосфор
+	+ +	+ / –	–

с другой стороны – не обременять финансово.

Стоимость конечного продукта значительно разнится, и цена металла не единственный параметр, который влияет на общую стоимость. Выбранный тип процесса нанесения покрытия также оказывает большое влияние на стоимость. Как правило, покрытия, нанесённые химическим способом, более дороги, чем покрытия, нанесённые традиционном способом электроосаждения. Для соединителей, требующих пайки, сложность и состав припоя, а также необходимость дополнительной очистки также повышают стоимость.

Среди исследованных покрытий белая бронза и SURO720, безусловно, самые экономически оправданные варианты применения. Можно было ожидать, что серебро как благородный металл может быть самым дорогим покрытием, однако на самом деле стоимость серебряных и оловянно-никелевых покрытий находится в одном ценовом диапазоне.

Стоимость оловянно-никелевых покрытий также сильно зависит от экологических норм, поскольку в составе этих покрытий имеются агрессивные химические вещества. Таким образом, правила техники безопасности и утилизации внутри конкретной страны значительно влияют на общую стоимость этого покрытия. Никель-фосфорные покрытия, полученные химическим способом, являются наиболее дорогим вариантом среди исследованных покрытий. Обработка электролита относительно сложна, что приводит к более высокой цене, которая, однако, всё ещё намного ниже по сравнению с покрытием из золота (см. табл. 10).

Заключение

Из-за различных преимуществ и недостатков каждого типа покрытия невозможно дать общую рекомендацию и сказать, что тот или иной тип покрытия является лучшим решением на все случаи жизни. Разработчик должен учитывать индивидуальные требования к радиочастотному соединителю и выбирать покрытие, исходя из технических и экономических требований. Результаты настоящего исследования должны служить справочным руководством по выбору правильного типа покрытия для конкретного применения (см. табл. 11).

Серебро

Покрытия из серебра с их превосходными коррозионной стойкостью и электрическими свойствами будут подходящим вариантом для большинства радиочастотных соединителей. Использование серебряных покрытий может быть ограничено, если имеются повышенные требования к износу или предполагается большое количество циклов соединения и разъединения.

Серебро также является лучшим выбором для покрытия электрических контактов, чувствительных к пассивной интермодуляции. Однако у серебра есть недостаток: со временем оно может потускнеть из-за сероводорода, который в большинстве случаев не влияет на технические свойства, и его влияние может быть снижено с помощью обработки против потускнения.

Белая бронза

Белые бронзовые покрытия теперь являются современным и предпочтительным вариантом, если нужно экономичное покрытие с приемлемыми электрическими свойствами и коррозионной стойкостью не менее 96 ч.

SURO720

SURO720 – это улучшенная версия белого бронзового покрытия, которая обеспечивает гораздо более высокий уровень стойкости к коррозии и соответствует большинству требований радиочастотных соединителей в течение 720-часового коррозионного испытания. Однако из-за электрохимического различия прямого контакта с алюминием следует избегать.

Одним из основных преимуществ SURO720 по сравнению с покрытием на основе никеля является его превосходная способность к пайке. Поскольку большинство антенных соединителей имеют форму стабильных кабельных сборок, устойчивых к ПИМ, SURO720 является решением, которое можно использовать как для фильтрующих, так и для антенных соединителей. С точки зрения стоимости, ПИМ, паяемости, коррозии и механических свойств, SURO720, по-видимому, имеет преимущество по сравнению с другими вариантами покрытия.

Олово-никель

Олово-никелевые покрытия сопоставимы с SURO720 по уровню стойкости к коррозии. Однако несколько более высокая стоимость, а также плохая паяемость оловянно-никелевых покрытий препятствуют широкому использованию этого покрытия. По коррозионной стойкости и электрическим свойствам олово-никель уступает серебру. Это покрытие демонстрирует лучшую износостойкость по сравнению с серебром, но не достигает износостойкости никель-фосфорных покрытий, полученных химическим способом. По совокупности свойств и стоимости покрытие олово-никель не имеет каких-либо существенных преимуществ по сравнению с другими хорошо зарекомендовавшими себя покрытиями радиочастотных соединителей.

Химический никель-фосфор

Никель-фосфорные покрытия, полученные методом химического восстановления, обладают превосходной износостойкостью. Этот вид покрытий является предпочтительным для радиочастотных соединителей, которые рассчитаны на большое количество циклов соединений и в то же время имеют низкие требования к контактному сопротивлению. Однако высокая стоимость, плохие электрические свойства, низкая способность к пайке и хрупкость являются недостатками этого покрытия.

Устойчивость к коррозии визуально кажется удовлетворительной, однако контактное сопротивление явно ухудшается в результате 720-часового испытания солевым туманом: области электрических контактов подвергаются

Таблица 11. Сводная таблица результатов испытаний

			Серебро (с покрытием против потускнения)	Белая бронза (SURO720)	Олово-никель	Химический никель-фосфор
После коррозийного теста (720 ч в солевом тумане)	Контактное сопротивление		+ +	–	–	– –
	Визуальное	Без примесей (без дополнительных материалов)	+	+	–	+ / +
		На алюминии	+	– –	–	+
Контактное сопротивление			+ +	+	+	–
Гибкость			+ +	+	+	– –
Абразивный износ			– –	–	–	+
Способность смачиваться			+ +	+ +	–	– –
Пассивная интермодуляция			+ +	+ +	+ +	+ +
Относительные затраты			+	+ +	+ / –	–

коррозии. Поскольку никель является магнитным по своей природе и может привести к большим проблемам с ПИМ, процентное содержание олова и фосфора очень важно в покрытиях на основе никеля.

Если концентрация никеля становится выше, чем указано в спецификации, соединитель может показывать плохие характеристики ПИМ, и это может быть обнаружено только в том случае, если специальные тесты будут проведены на собранном оборудовании. Последнее может привести к огромному экономическому ущербу.

Кроме того, никель и его соединения могут вызывать аллергические реакции. Поэтому в некоторых странах и областях применения его использование ограничено. Также следует тщательно оценить отсутствие оксида хрома ($Cr_{(VI)}$), используемого в процессе нанесения покрытия. Поэтому для каждого применения следует тщательно продумывать использование никельсодержащего покрытия.

Информация и рекомендации, содержащиеся в этой статье, основаны на тестах, которые HUBER+SUHNER и Rosenberger считают надёжными и выполненными с максимальным профессионализмом. Однако точность и полноту предоставляемой информации авторы статьи не гарантируют.

НОВОСТИ МИРА

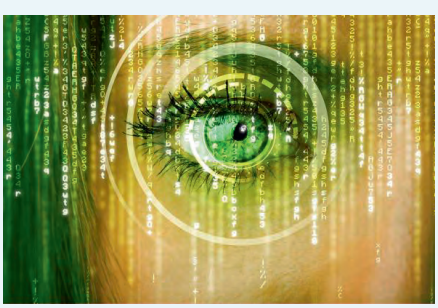
Исследователи видят новые векторы угроз по мере роста Интернета вещей

В настоящее время зарегистрировано около 8,6 миллиарда подключений устройств Интернета вещей, но к 2026 году, по прогнозам исследовательской компании ABI Research, это число почти утроится и достигнет 23,6 миллиарда. В последнем техническом документе фирмы исследуется, как экспоненциальный рост подключений к Интернету IoT откроет новую эру угроз и уязвимостей. В то же время надвигающиеся пробелы в безопасности открывают огромный потенциал для игроков в области безопасности Интернета вещей.

Опасения по поводу безопасности Интернета вещей широко распространены. Пробелы в безопасности простираются от незащищённых устройств до производителей оригинального оборудования (OEM-производителей) и поставщиков, часто предпочитающих принимать риск, а не устранять его, а также функциональных устройств IoT-типа безопасности, которые делают приоритетом доступность и не могут одновременно обеспечить конфиденциальность. На рынке существует ограниченное количество решений для обеспечения безопасности Интернета вещей, в значительной степени из-за фрагментированного характера самого Интернета вещей.

Точно так же, как количество подключений к интернету Интернета Вещей должно вырасти взрывными темпами, должны возрасти возможности получения дохода в сфере безопасности Интернета вещей. Данные ABI Research Market показывают, что к 2026 году общая выручка в этом пространстве достигнет 16,8 миллиарда долларов США.

Огромное количество новых подключений к Интернету вещей в течение следующих 5 лет, расширенные некоторых рынков Интернета вещей (например, коммунальные услуги, промышленность, инфраструктура и умные города), увеличение числа подключённых пользователей и активов наряду с возросшими потребностями в подключении, вызванными пандемией COVID-19, – всё это является справедливым предиктором цифровой безопасности в целом. Однако объём доходов от безопасности Интернета вещей не всегда коррелирует с объёмом подключений Интернета вещей, и ожидается, что на некоторых рынках доходы будут непропорциональными. Это связано с многоаспектным характером требований к безопасности и управлению, которые обеспечивают основу для ключевых операций и ценных услуг, в том числе для операций разведки и аналитики, управления жизненным циклом и предиктивного обслуживания, обновления встроенного ПО, а также целостности устройств и данных.



ABI Research прогнозирует, что цифровые службы безопасности войдут в уравнение рентабельности инвестиций (ROI) в ближайшие 3 года, поскольку как поставщики безопасности, так и игроки Интернета вещей осознают необходимость защищать ключевые приложения монетизации, связанные с их стратегиями Интернета вещей.

www.abiresearch.com

Соединители SMA с предельной частотой до 34 ГГц. Эволюция продолжается

Кива Джуринский (kbd.istok@mail.ru)

Рассмотрены основные направления эволюции соединителей SMA: расширение диапазона рабочих частот и повышение надёжности контакта между вилкой и розеткой. Показаны особенности коаксиальной линии, конструктивные и электрические параметры стандартных соединителей SMA (предельная частота 18 ГГц), соединителей Super SMA (предельная частота 27 ГГц) и оптимизированного Super SMA (предельная частота 32...34 ГГц).

Соединители SMA

Соединители SMA (SubMiniature A) были разработаны в США в 1958 году. С 1968 года их выпускают по стандарту MIL-C-39012 для применения в военной аппаратуре. В этом соединителе с волновым сопротивлением 50 Ом применена коаксиальная линия размерами 4,15/1,27 мм, заполненная фторопластом, и резьбовое соединение (американская дюймовая резьба 0,250-36 UNS) вилки и розетки (см. рис. 1) [1].

Соединители SMA миниатюрны, имеют достаточно высокий уровень параметров, технологичны в изготовлении. В связи с этим их широко применяют в радиоэлектронной аппаратуре для военной, аэрокосмической, телекоммуникационной, медицинской и других областей техники. В настоящее время в устройствах СВЧ-соединители типов SMA и N составляют около 50% от всех применяемых радиочастотных соединителей. Гарантированной предельной частотой кабельных соединителей SMA принято считать 18 ГГц в сочетании с полужёстким радиочастотным кабелем и 12,4 ГГц – с гибким кабелем [1]. Основные параметры соединителей SMA приведены в таблице 1.

Соединители SMA были созданы более 60 лет назад, однако работы по их совершенствованию не прекращаются и в настоящее время. Основной целью этих работ является увеличение жёсткости конструкции соединителей для повышения надёжности контактирования вилки и розетки, а также расширение диапазона рабочих частот. Недостаточная жёсткость конструкции соединителя SMA обусловлена небольшой (менее 0,23 мм) толщиной стенки розетки в области её сочленения с вилкой. Предельную частоту соединителя SMA можно увеличить, если использовать в полной мере возможности его коаксиальной линии. Действительно, теоретическая предельная частота, $f_{пред}$ (ГГц), при которой в коаксиальной линии соединителя с внутренним диаметром наружного проводника D, диаметром центрального проводника d и диэлектрической проницаемостью изолятора ε ещё не возникают нежелательные волны высшего типа, равна [1]:

$$f_{пред} \cong \frac{190,85}{\sqrt{\varepsilon}\,(D+d)}.$$

Для соединителя SMA $f_{пред}$ приблизительно равна 26,5 ГГц. Поэтому Southwest Microwave, Amphenol RF, Molex, Radiall и другие зарубежные компании поставили задачу максимально использовать возможности коаксиальной линии соединителя SMA и расширить его диапазон рабочих частот с 18 до 26...27 ГГц.

Созданные различными компаниями в начале 2000-х годов соединители с предельной частотой 26...27 ГГц имеют следующие названия: SMA 26,5 GHz, SMA 27 GHz, Super SMA, SMA HF Interface, EPSMA, High Performance SMA, Optimized SMA, Extended-Frequency SMA. В данной статье эти соединители названы Super SMA.

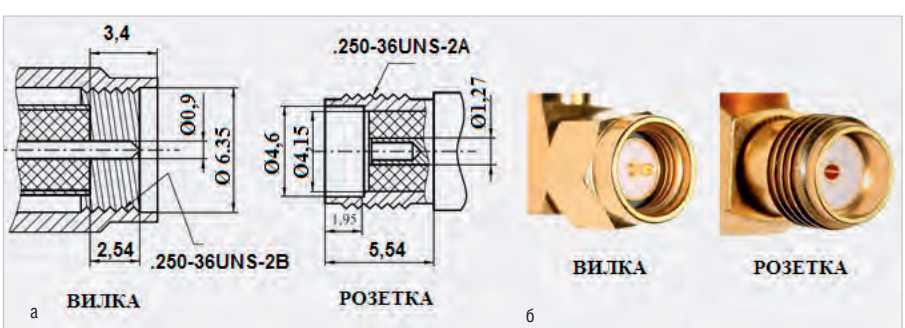


Рис. 1. Вилки и розетки соединителей SMA: а) интерфейс; б) внешний вид

Таблица 1. Основные параметры соединителей SMA и Super SMA

Параметры соединителей	SMA	Super SMA
Рабочий диапазон частот, ГГц	0–18	0...(26...27)
Максимальный КСВН прямых кабельных соединителей (в диапазоне частот, ГГц) в зависимости от типа кабеля	1,2...1,5 (0–18)	1,25 (0...26)
Максимальная величина потерь прямых соединителей, дБ (в диапазоне частот, ГГц)	0,30 (0...18)	0,30 (0...18)
Допустимая пропускаемая мощность, Вт (на частоте, ГГц)	110 (10), 70 (18)	110 (12,4...18)
Рабочее напряжение на уровне моря, В	335	335
Экранное затухание (на частотах f, ГГц), дБ	–60…–(90 – f)	–(100 – f)
Сопротивление изоляции, МОм, не менее	5000	5000...10000
Гарантированное количество соединений и рассоединений	500	500
Рабочий диапазон температур,°С	–65…+165	–55…+165

Соединители Super SMA

Внутренняя геометрия соединителей Super SMA для обеспечения низкого коэффициента отражения оптимизирована с использованием моделирования методом конечных элементов. Работы по созданию соединителей SMA с предельной частотой до 27 ГГц проводились по двум направлениям:

1. изменение внутренней геометрии соединителя за счёт применения изолятора с меньшей, чем у фторопласта, диэлектрической проницаемостью;
2. повышение точности размеров и чистоты обработки поверхности коаксиального канала соединителя.

Например, компания Southwest Microwave в розетке Super SMA заменила фторопластовый изолятор с диэлектрической проницаемостью 2,05...2,1 материалом с диэлектрической проницаемостью 1,82 [2]. Благодаря этому

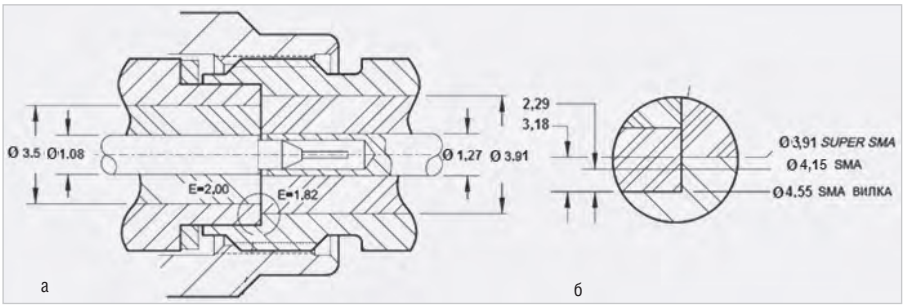


Рис. 2. Вилка и розетка соединителя: а) в сочленённом состоянии; б) размеры области контакта вилки и розетки

Рис. 3. Соединители Super SMA

внутренний диаметр наружного проводника был уменьшен с 4,1 до 3,91 мм при сохранении прежнего наружного диаметра внутреннего проводника 1,27 мм (см. рис. 2).

Внутренний диаметр внешнего проводника вилки Super SMA, заполненного фторопластом, был уменьшен с 4,1 до 3,5 мм, поэтому диаметр центрального проводника вилки для сохранения волнового сопротивления, равным 50 Ом, также был уменьшен с 1,27 до 1,08 мм. Следует отметить, что внутренний диаметр внешнего проводника в вилке соединителя выбран таким же, как в соединителе 3,5 мм с воздушной коаксиальной линией.

Наряду с расширением частотного диапазона это позволило увеличить на 38% (с 0,23 до 0,318 мм) ширину области контакта розетки и вилки и повысить жёсткость конструкции. Поэтому соединители Super SMA неслучайно называют ещё «толстостенными соединителями».

В результате перечисленных нововведений коаксиальная линия пары вилка-розетка соединителей Super SMA в сочленённом состоянии получилась ступенчатой, в отличие от «гладкой» (без ступенек) коаксиальной линии соединителей SMA. Внешний вид соединителей Super SMA вилка и розетка показан на рисунке 3.

Соединители Super SMA совместимы со всеми стандартными соединителями типов: SMA, 3,5 мм и 2,92 мм, особенно с соединителями 3,5 мм, имеющими воздушную коаксиальную линию с размерами проводников 3,5/1,52 мм [1]. Кроме того, эти соединители имеют высокий уровень экранного затухания за счёт надёжного «360-градусного» контакта вилки и розетки.

Применение соединителей SMA с предельной частотой до 27 ГГц открыло новые возможности совершенствования изделий микроэлектроники СВЧ:

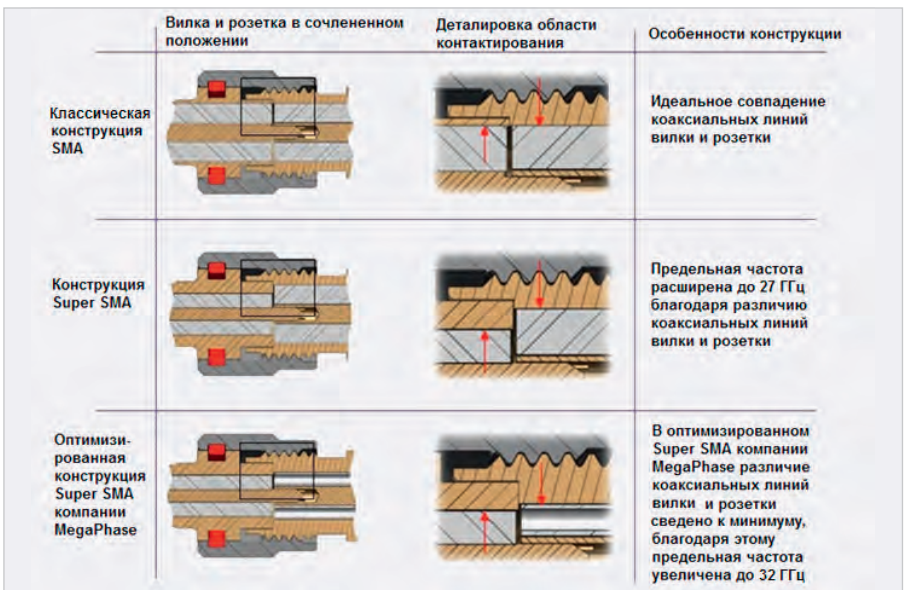


Рис. 4. Сравнение конструкций соединителей SMA, Super SMA и Super SMA компании MegaPhase

расширение частотного диапазона, снижение уровня КСВН, повышение уровня экранного затухания, повышение надёжности и воспроизводимости параметров.

Соединители с предельной частотой 32 ГГц компании MegaPhase

В работе [1] было отмечено: «Эволюция соединителей SMA продолжалась в течение более чем 50 лет. Не исключено, что в ближайшее время появятся новые разработки этих соединителей». Это предсказание сбылось в июне 2020 года с появлением сообщений о создании компанией MegaPhase (США) оптимизированного соединителя Super SMA с предельной частотой 32 ГГц [3-6]. Компания MegaPhase известна своими разработками и производством высоконадёжных коаксиальных СВЧ-кабелей и соединителей для различных радиотехнических и оптико-электронных устройств. При оптимизации соединителя Super SMA компания MegaPhase, несомненно, использовала опыт других компаний. Но если в соединителе Super SMA коаксиальная линия вилки имела меньшие размеры, чем коаксиальная линия розетки, и общая коаксиальная линия вилки и розетки в сочленённом состоянии была ступенчатой, то в оптимизированном соединителе компании MegaPhase были максимально выровнены размеры коаксиальной линии. При этом за основу были взяты размеры коаксиальной линии вилки.

Детали конструкции разработанного соединителя компания не раскрывает, лишь приводит сравнение коаксиальных линий соединителей SMA, Super SMA и оптимизированного Super SMA (см. рис. 4) [3, 4].

Компания MegaPhase разработала соединители вилка и розетка прямыми, предназначенными для работы с кабелем серии AL141 собственного производства (см. рис. 5) [6]. Частотная зависимость КСВН кабельных соединителей компании MegaPhase приведена на рисунке 6 [3–6].

Компания MegaPhase гарантирует разработку и поставку соединителей, кабелей и кабельных сборок в течение 2...4 недель (см. рис. 7) [7].

Рис. 5. Оптимизированные соединители Super SMA вилка и розетка компании MegaPhase

Кабельная вилка с предельной частотой 34 ГГц от компании Amphenol RF

Приблизительно в это же время компания Amphenol RF объявила о создании прямых кабельных соединителей SMA вилка № 901-10708, работающих на частотах до 34 ГГц [8, 9]. Эти соединители предназначены для паяного соединения с полужёстким кабелем RG-405 (0,085″). Соединитель № 901-10708 имеет следующие параметры:

- максимальный КСВН в диапазоне частот 0...34 ГГц – 1,05+0,09*f*, где *f* – частота, ГГц (1,35 макс.);
- испытательное напряжение 1000 В;
- диапазон рабочих температур от – 65 до 165°С;
- допустимое количество соединений и рассоединений – 500.

Внешний вид соединителя показан на рисунке 8. Корпус соединителя изготовлен из латуни и покрыт износостойким золотом, центральный проводник выполнен из бериллиевой бронзы и также покрыт износостойким золотом. Стопорное кольцо и соединительная гайка изготовлены из нержавеющей стали, а изолятор – из полимера PTFE (аналогом этого материала является отечественный фторопласт Ф4). Габаритные размеры соединителя – 13,26×8,0 мм, а ориентировочная стоимость одного соединителя $8,28.

Благодаря лёгкой, компактной и вибростойкой конструкции и расширенному диапазону рабочих частот эти соединители найдут применение в беспроводной инфраструктуре 5G, радарных системах, системах гражданского и военного назначения.

Заключение

Зарубежные компании постоянно совершенствуют соединители, разработанные много десятилетий тому назад. Необходимость создания новых соединителей SMA продиктована особенностями их применения. Стандартные соединители SMA, к которым так привыкли разработчики устройств микроэлектроники СВЧ, имеют гарантированный

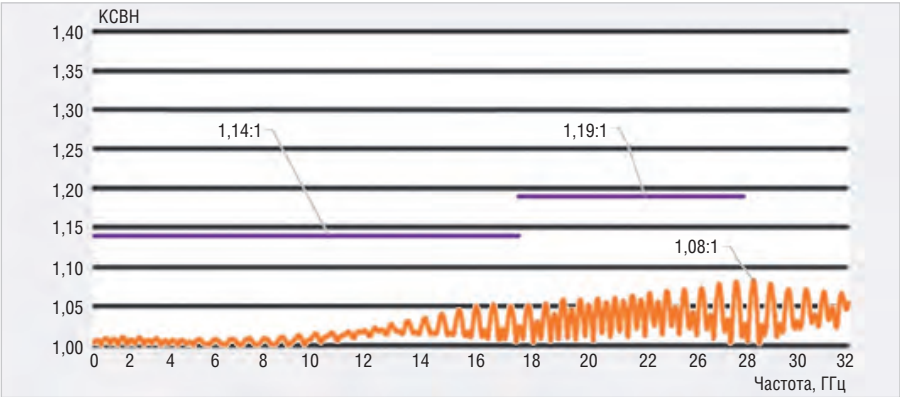


Рис. 6. Частотная зависимость КСВН кабельных соединителей компании MegaPhase. Сплошными линиями обозначены уровни КСВН стандартных соединителей Super SMA

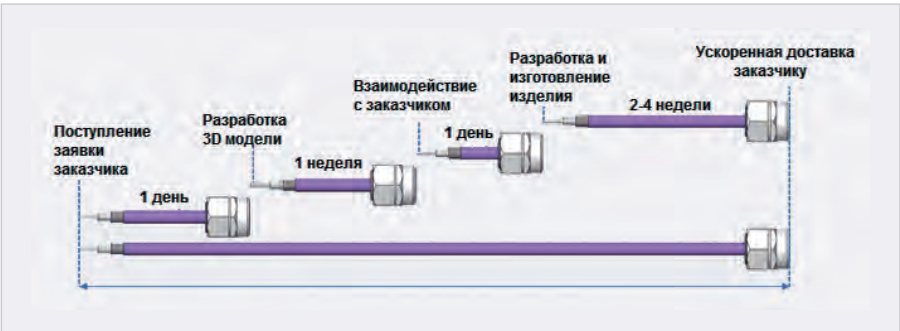


Рис. 7. Схема разработки и поставки изделий компанией MegaPhase

рабочий диапазон 0...18 ГГц. Для изделий, работающих в К-диапазоне частот (18...26 ГГц), уже необходимы соединители 3,5 мм или 2,92 мм с воздушной коаксиальной линией, в которых центральный проводник закреплён в тонкой диэлектрической опорной шайбе. Но такие соединители более повреждаемы при многократных соединениях, чем соединители SMA, заполненные фторопластом. Этим было обусловлено создание соединителей Super SMA с предельной частотой 27 ГГц и в дальнейшем – оптимизированных соединителей Super SMA с предельной частотой 32...34 ГГц компаниями MegaPhase и Amphenol RF

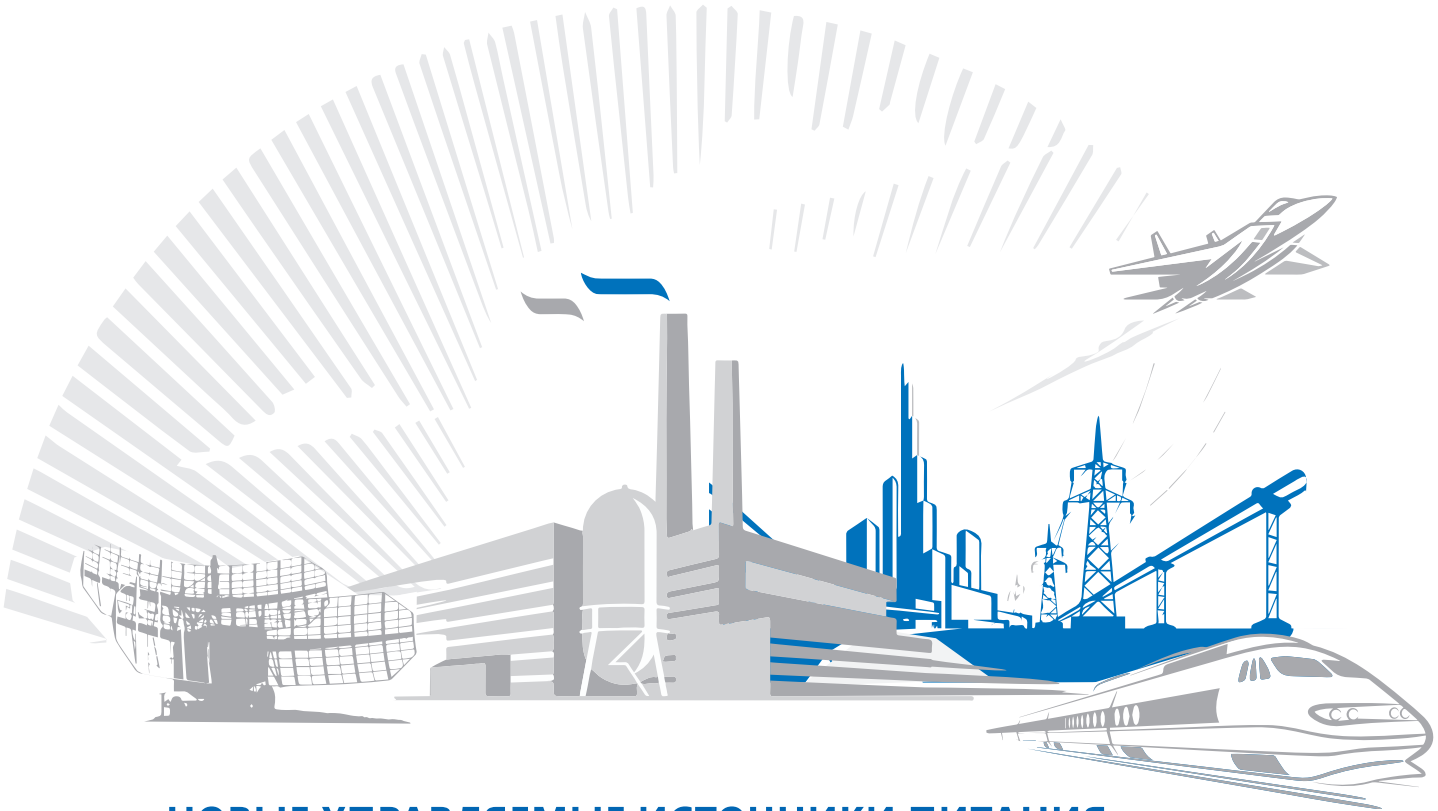
Но все-таки следует заметить, что эти соединители с изменённой коаксиальной линией не являются соединителями SMA, это соединители других типов. Общие с соединителями SMA, у них только резьба 0,250-36 UNS на корпусе и присоединительные размеры, что делает их механически совместимыми между собой. Но зарубежные компании любят вставлять слово SMA в название соединителей даже других типов: SMA 3,5 мм, SMA 2,9 мм.

Рис. 8. Кабельная вилка № 901-10708 с предельной частотой 34 ГГц компании Amphenol RF

Литература

1. *К.Б. Джуринский.* Современные радиочастотные соединители и помехоподавляющие фильтры. Изд-во ЗАО «Медиа Группа Файнстрит» С-Петербург, 2014.
2. Super SMA Series DC to 27.0 GHz Southwest Microwave, Inc., www.southwestmicrowave.com.
3. Mega Phase Launches a 32 GHz Optimized Super SMA Connector, July 15, 2020. www.megaphase.com
4. Mega Phase Launches a 32 GHz Optimized Super SMA Connector. Microwave Journal, July 21, 2020.
5. Optimized Super SMA Connectors/ Excellent performance through 32 GHz. www.megaphase.com.
6. Super SMA Connector – Mega Phase | RF Connector, www.everythingrf.com
7. Connectors Overview – Mega Phase, www.megaphase.com.
8. Frequency Cable Mount Connectors supporting up to 34 GHz. Electronics Media, July 8, 2020.
9. High-frequency SMA connectors reduce frequency range limitations, www.connectortips.com.

TDK·Lambda



НОВЫЕ УПРАВЛЯЕМЫЕ ИСТОЧНИКИ ПИТАНИЯ ДЛЯ РАЗЛИЧНЫХ ОТРАСЛЕЙ ПРОМЫШЛЕННОСТИ

Серия GXE

- Входное напряжение **85–265 В AC или 120–370 В DC**
- Выходная мощность **600 Вт**
- Выходные напряжения **24** или **48 В DC**
- КПД до **95%**
- Высота 1U
- Запуск при **–40°C**
- Гарантия **7 лет**

- **Конвективное охлаждение**
- **Режим стабилизации напряжения или стабилизация тока**
- **Аналоговый порт:** сигналы on/off, DC-OK, AC-Fail, Power-Fail, 0–100% выходной ток, 20–120% выходное напряжение
- **Цифровой порт** (Modbus RTU, на RS-485): установки выходных параметров + регулировка фронта нарастания, настройки защит. Считывание температуры, времени наработки прибора
- Варианты исполнения: в кожухе или без, с конформным покрытием платы или без

Увеличение мощности высокоэффективных усилителей СВЧ инверсного класса F

Мьо Мин Тхант, Виталий Романюк (Национальный исследовательский университет «МИЭТ»)

Проведено сравнение схем двухканальных сумматоров мощностей с синфазными, противофазными и квадратурными каналами. Схемы усилителей с суммированием мощностей созданы на основе однотактного усилителя СВЧ инверсного класса F, на GaN-транзисторе структуры HEMT частоты 4 ГГц, с КПД 88% и выходной мощностью 13 дБм. Отмечены достоинства и недостатки различных усилителей с суммированием мощности по эффективности, уровню шума, величине высших гармоник в спектре выходной мощности, согласованием с источником колебаний.

Введение

Для СВЧ-усилителей мощности с увеличенным КПД применяют полигармонические режимы работы транзисторов [1], из которых наиболее эффективен инверсный класс F [2]. Выходная мощность усилителя на одном транзисторе определяется параметрами его конструкции и полупроводника, из которого он изготовлен. Простейшим способом увеличения мощности усилителя является разделение его напряжения на два канала, мощности в которых усиливаются и далее суммируются. Входные напряжения каналов могут быть синфазными, противофазными, квадратурными.

В настоящей работе разработана схема высокоэффективного усилителя мощности инверсного класса F на транзисторе структуры HEMT, изготовленном на базе GaN, и проведено сравнение трёх вариантов суммирования мощностей:

- деление и суммирование мощности с помощью синфазных каналов;
- применение делителей и сумматоров с противофазными каналами;
- использование квадратурных каналов.

Режимы работы транзисторов оптимизированы по максимуму коэффициента полезного действия $\eta = P_1/P_0$ и КПД добавленной мощности:

$$PAE = (P_1 - P_{BX})/P_0,$$

где P_1 – выходная мощность первой гармоники, P_{BX} – входная мощность усилителя, P_0 – мощность, потребляемая транзисторами из источника питания.

Однотактный усилитель мощности инверсного класса F на GaN-транзисторе структуры HEMT

В качестве основы разработана схема усилителя на одном интегральном GaN-транзисторе структуры HEMT длиной затвора 0,25 и шириной 200 мкм [3]. Рабочая частота усилителя 4 ГГц, входная мощность 10 дБм. Электрическая схема однотактного усилителя приведена на рис. 1.

В схеме, помимо разделительных ёмкостей C_1, C_3, блокировочной индуктивности L_2, имеется входная C_2, L_1 и выходная, согласующие цепи L_3, C_4. Блокировочным элементом цепи смещения, а также формирователем формы выходного тока транзистора является отрезок линии TL1 длиной около четверти длины волны входной частоты. Для формирования формы напряжения на стоке включена подсхема S1, показанная на рис. 2, содержащая последовательно соединённые параллельные резонансные контуры [4]. Контур LC1 настроен на частоту 4 ГГц, а LC2 – на вторую гармонику 8 ГГц.

Путём выбора режима работы транзистора по постоянному току и применения четвертьволнового отрезка линии в цепи смещения получена форма тока стока транзистора, содержащая, кроме первой, достаточно выраженную третью гармонику. Помимо этого, в спектре выходного тока имеется небольшая вторая гармоника I_{d2}. Высокое значение модуля импеданса транзистора на частоте второй гармоники $Z(2\omega_{BX})$, где ω_{BX} – входная частота, привело к созданию напряжения на стоке, в спектре которого существенны две гармоники: первая U_{d1} и вторая $U_{d2} = I_{d2}Z(2\omega_{BX})$ (2).

Зависимости от времени тока стока и напряжения на стоке однотактного усилителя приведены на рис. 3. КПД однотактного усилителя η = 88%, PAE = 84% на частоте 4 ГГц при коэффициенте усиления K_p = 12,3 дБ. Так как в полигармонических усилителях выходной ток и выходное напряжение транзистора содержат высшие гармоники, для получения высокого КПД требуется выполнения условия $P_1 >> P_n$, n – номер высшей гармоники (2, 3, 4, ...) [5].

На рис. 4 показан спектр выходной мощности однотактного усилителя. В спектре выходной мощности однотактного усилителя мощности высших

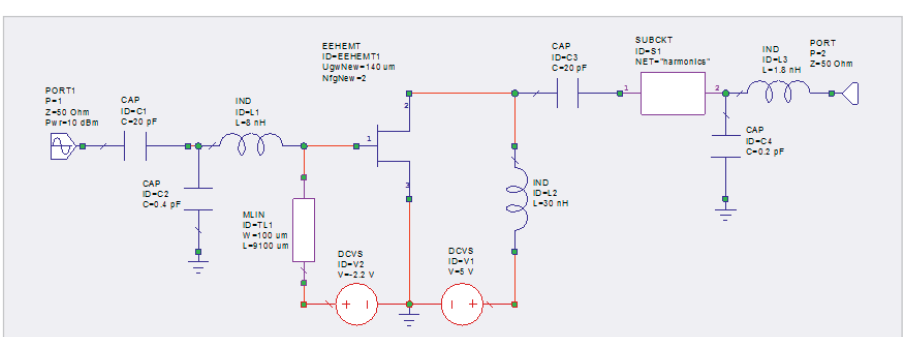


Рис. 1. Электрическая схема усилителя мощности инверсного класса F на одном GaN-транзисторе

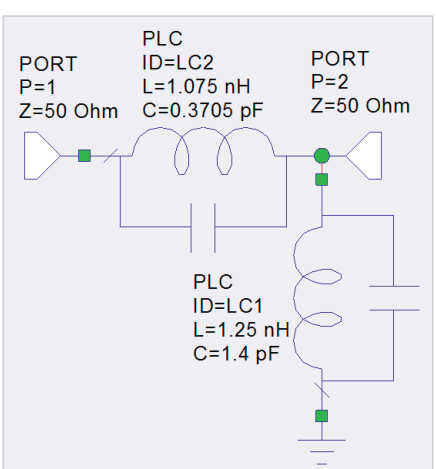


Рис. 2. Схема выходной формирующей цепи

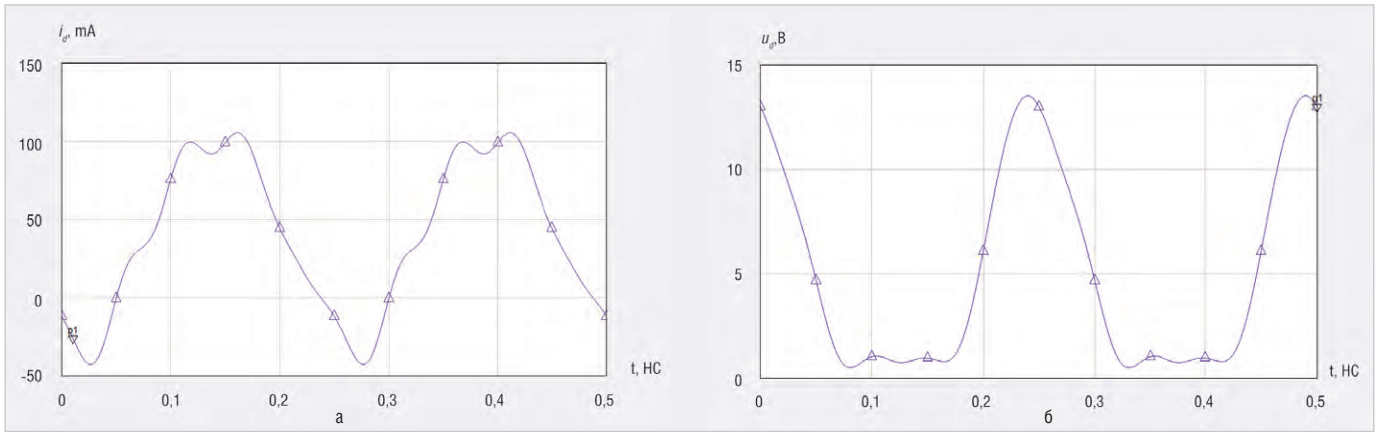


Рис. 3. Зависимости в однотактном усилителе инверсного класса F: а) от времени тока стока; б) от напряжения на стоке

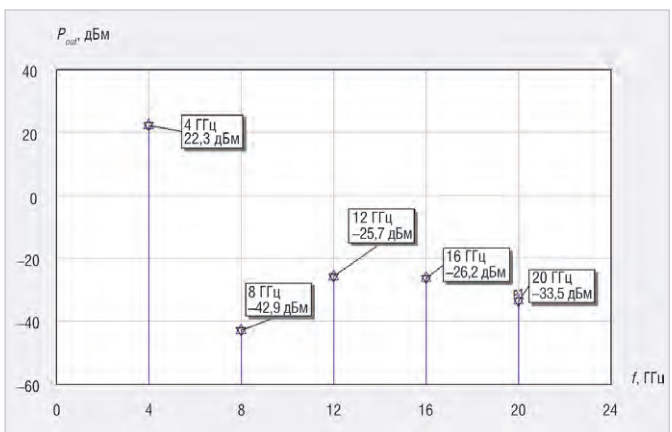


Рис. 4. Спектр выходной мощности однотактного усилителя инверсного класса F

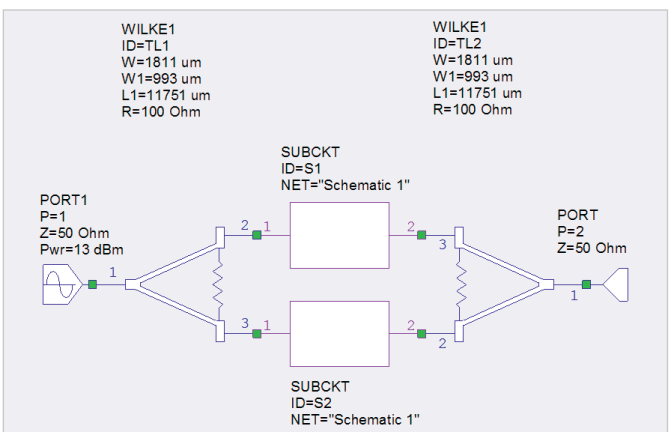


Рис. 5. Сумматор мощностей с синфазными каналами

гармоник существенно меньше первой: наибольшая из высших гармоник, третья, меньше основной на 48 Дб, вторая гармоника меньше первой на 65 дБ.

Выходную мощность усилителей класса F увеличивают в двухканальных схемах. Для деления и суммирования мощностей применяют мостовые устройства: мост Уилкинсона (синфазные каналы), кольцевой мост (противофазные каналы), квадратный мост (квадратурные каналы).

Усилитель мощности с синфазными каналами

Схема усилителя с синфазными каналами приведена на рис. 5. В качестве делителя и сумматора мощностей использован мост Уилкинсона. В каждом канале имеется подсхема Shematic 1, соответствующая однотактному усилителю (см. рис. 1). Входная мощность усилителя с синфазными каналами 13 дБм, коэффициент усиления мощности равен 12,12 дБ.

Усилитель мощности с противофазными каналами (двухтактный усилитель)

Двухтактный усилитель выполнен на кольцевых мостах (см. рис. 6). С помощью первого моста входные колебания разделяются на два равных по мощности канала, напряжения на входе сдвинуты по фазе на 180°. На втором кольцевом мосте мощности каналов суммируются. Подсхемы Schematic 1 соответствуют однотактному усилителю, схема которого представлена на рис. 1. Выходная мощность первой гармоники двухтактного усилителя равна 25,27 дБ.

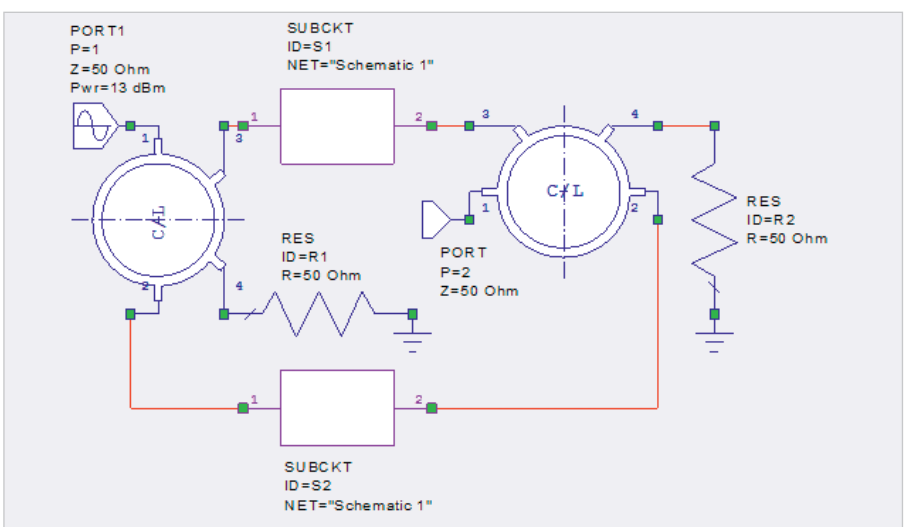


Рис. 6. Двухтактный усилитель мощности

Квадратурный усилитель мощности

На базе усилителя на одном транзисторе составлена схема квадратурного усилителя, в которой входная мощность с помощью первого квадратного моста делится пополам на два канала. При этом входные напряжения сдвинуты по фазе на 90°. Мощность каждого канала усиливается с помощью однотактных усилителей, схема которых соответ-

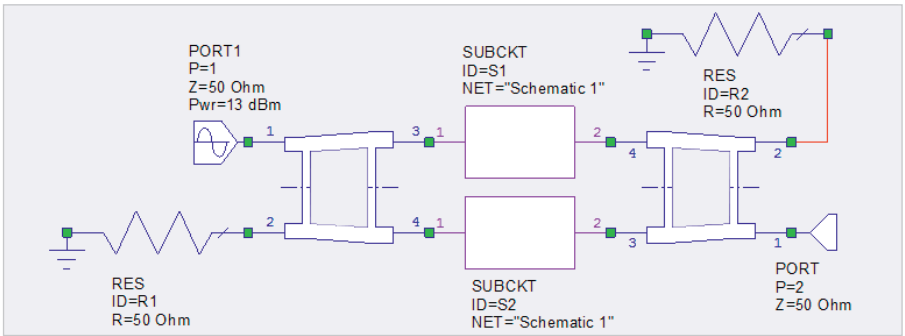


Рис. 7. Схема квадратурного усилителя

ствует рисунку 1 и суммируется на втором квадратном сумматоре (см. рис. 7). Коэффициент усиления мощности квадратурного усилителя 12,27 дБ при входной мощности составляет 13 дБм.

Сравнение вариантов суммирования мощностей

В комплексе программ Microwave Office (MWO) измерены основные параметры усилителей с суммированием мощностей: КПД добавленной мощности PAE, коэффициент шума в режиме большого сигнала, спектр выходной мощности, коэффициент отражения от входа усилителя. Зависимость PAE от частоты для трёх типов усилителей с суммированием показана на рис. 8. Коэффициент шума в зависимости от частоты измерен в нелинейном режиме работы программы MWO [6] (см. рис. 9). Для измерения коэффициента отражения от входа усилителя между источником входных колебаний и усилителем включён двойной направленный ответвитель, который изображён на рисунке 10.

Амплитуда тока I_{in}, измеряемого амперметром AMP1 на сопротивлении R_1, позволяет судить о падающей мощности, амплитуда тока I_{out} амперметра AMP2 – об отражённой мощности. Модуль коэффициента отражения $|\Gamma| = I_{out}/ I_{in}$. Коэффициент шума усилителей с синфазными и противофазными каналами примерно одинаков и соответствует шуму одиночного усилителя. Наиболее шумящим оказался усилитель с квадратурными каналами. При частоте входных колебаний 4 ГГц коэффициент шума ~4 дБ.

Измеренные в MWO параметры усилителей с суммированием мощности и однотактного усилителя приведены в таблице. Там же показаны рассчитанные КПД η, входная мощность однотактного усилителя 10 дБм, усилителей с суммированием 13 дБм.

В таблице приняты следующие обозначения: $\Delta P_{1-2} = P_1 - P_2$, $\Delta P_{1-3} = P_1 - P_3$, P_1, P_2, P_3 – мощности соответствующих гармоник. По результатам моделирования в MWO можно сделать следующие выводы:

- наряду с двойным увеличением выходной мощности, КПД усилителей с суммированием лишь немного отличается от η одиночного усилителя. Наибольший КПД в усилителе с синфазными каналами η = 88%, наименьший КПД в квадратурном усилителе равен 85%;
- существенное преимущество квадратурного усилителя в наименьшем коэффициенте отражения от входа усилителя. Даже при плохо настроенном однотактном усилителе (|Γ| = 50%) коэффициент отражения квадратурного усилителя |Γ| < 2%. Этот результат соответствует другим публикациям [5];
- уровень наибольших спектральных составляющих высших гармоник (второй и третьей) в усилителях с суммированием несколько меньше, чем в одиночном усилителе. Наименьшая величина высших гармоник в квадратурном усилителе: мощность второй гармоники меньше основной на 67,5 дБ, мощность третьей гармоники – на 52 дБ, в то время как в одиночном усилителя эти показатели равны 65 и 50 дБ.
- коэффициент шума в режиме больших сигналов наибольший в квадратурном усилителе.

Заключение

Разработана схема однотактного усилителя мощности на интегральном GaN-транзисторе структуры HEMT, имеющая КПД 88%, на частоте 4 ГГц с выходной мощностью 22,3 дБм. Проведено сравнение трёх вариантов суммирования мощностей однотактных усилителей: с синфазными, противофазными и квадратурными каналами, построенными на базе однотактного усилителя.

Наибольший КПД наблюдается в усилителе с синфазными каналами на мостах Уилкинсона, этот КПД не меньше, чем в одиночном усилителе. Достоинство усилителя с квадратурными каналами – существенно меньший коэффициент отражения, чем в одиночном и других видах усилителей с суммированием. Кроме того, в спектре выходной мощности квадратурного усилителя меньший уровень высших гармоник. Однако квадратурный усилитель имеет недостаток – более высокий уровень шума в режиме больших амплитуд колебаний.

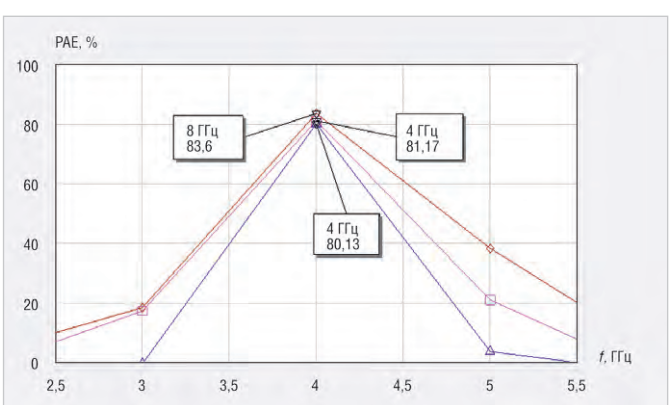


Рис. 8. Зависимость от частоты КПД добавленной мощности усилителей инверсного класса F с двумя каналами (◊ – синфазными, □ – противофазными, Δ – квадратурными)

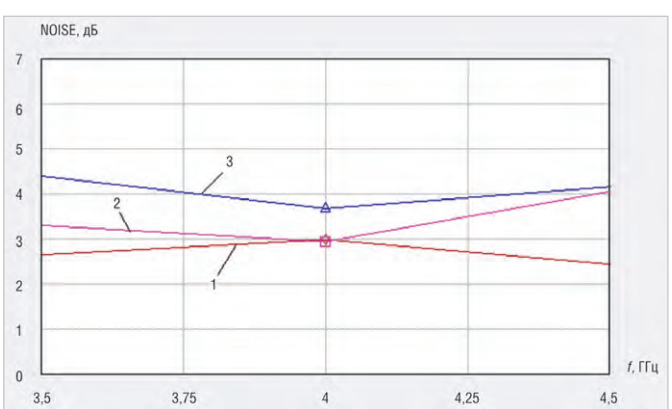


Рис. 9. Зависимость коэффициента шума усилителей с суммированием мощности от частоты (1 – синфазные каналы, 2 – противофазные, 3 – квадратурные)

Литература

1. *Тхант М. М., Романюк В. А.* Монолитные микроволновые интегральные схемы высокоэффективных усилителей мощности (обзор литературы). Успехи современной радиоэлектроники. 2019. № 6. С. 52–65.
2. *Гадзиковский А. Г.* Усилители мощности инверсного класса F – эффективное средство улучшения энергетических характеристик радиопередатчиков. Вестник ЮУрГУ. Компьютерные технологии, управление, радиоэлектроника. 2018. Т. 18. № 1. С. 75–82.
3. *Гуминов Н. В., Тхант М. М., Романюк В. А., Шомахмадов Д. П.* Сравнение характеристик и параметров СВЧ-транзисторов структур HEMT, изготовленных из GaAs и GaN. Известия вузов. Электроника. 2019. № 24(1). С. 43–50.
4. *Rassokhina Y.V., Krizhanovski V.G., Colantonio P., Giofre R.* Invearse class-F power amplifier using slot resonators as a harmonic filter. International Journal of Microwave and Optical Technology. 2014. № 9(1). 49–53.
5. *Dellier S., Dehaene T. and Peragin E.* GaN High-Efficiency S-band Power Amplifier with Power Flexibility from 1 to 10 Watts. 2014 IEEE Topical Conference on Power Amplifiers for Wireless and Radio Applications (PAWR). 2014.
6. *Бахвалова С. А., Романюк В. А.* Основы моделирования и проектирования радиотехнических устройств Microwave Office. СОЛОН-Пресс. М. 2016.

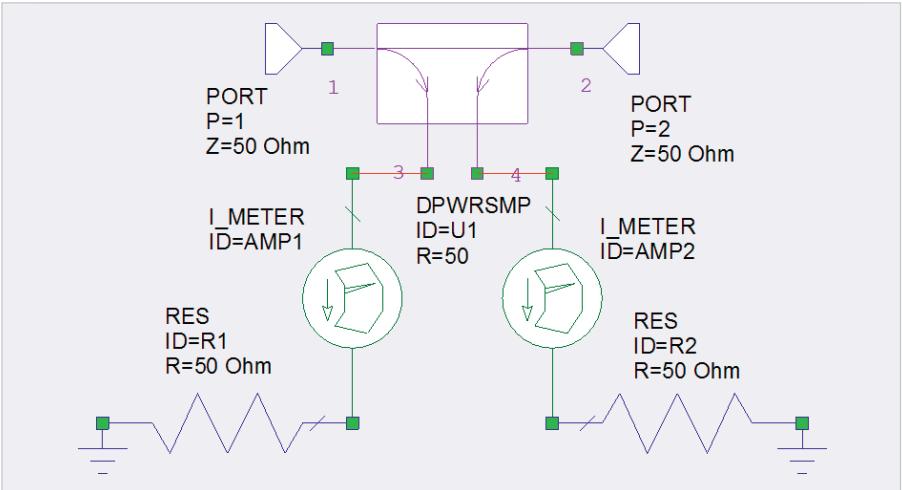


Рис. 10. Схема для измерения коэффициента отражения от входа транзистора

Параметры усилителей

Усилители	Выходная мощность P_1, дБм	η , %	PAE, %	NOISE, дБ	IГI, %	$\Delta P_{1\text{-}2}$, дБ	$\Delta P_{1\text{-}3}$, дБ
Однотактный	22,3	88	84	3	50	65	48
С синфазными каналами	25,1	88	83,6	3	44	64	49
Двухтактный	25,3	85	81	3	49	67	46
Квадратурный	25,3	85	80	3,7	1,9	67,5	52

Миллиомметр с графическим LCD Nokia-5110

Алексей Кузьминов (compmicrosys@mail.ru)

В статье приведена аппаратная и программная реализация цифрового миллиомметра на базе нового микроконтроллера EFM8LB12 со встроенным 14-разрядным высокоскоростным SAR АЦП, ИУ INA333 и ОУ OPA334. Погрешность измерения миллиомметра составляет не более 1%. Показания миллиомметра выводятся на популярный графический дисплей Nokia-5110 (84×48 пикселей), установленный в корпусе размером 102×54×30 мм. В статье приводятся принципиальные схемы, разводка и фотографии плат, изображения самого устройства, позволяющие изготовить прибор самостоятельно.

Введение

Часто требуется измерить достаточно малое сопротивление (миллиомы) некоторых относительно низкоомных объектов или компонентов (вторичных обмоток силовых трансформаторов, катушки индуктивности с небольшим количеством витков, токоизмерительных резисторов, шунтов и т.п.). Для измерения таких малых сопротивлений выпускаются специализированные приборы, называемые миллиомметрами.

Стоимость подобных приборов довольно высока и начинается от $300 у приборов с не особенно высокой точностью. Более точные приборы стоят в несколько раз дороже. В то же время опыт, полученный автором при конструировании цифрового вольтметра с высоким разрешением [1], и метод, применённый для измерения напряжений, натолкнул на идею: а нельзя ли сконструировать миллиомметр, применив подобные принципы для измерения малых сопротивлений?

Небольшая стоимость вольтметра [1], простота схемы и достаточно высокая точность измерений позволили предположить, что такой миллиомметр будет ненамного сложнее по схеме и, кроме того, возможно, будет обладать невысокой стоимостью и достаточно приемлемой точностью измерения малых сопротивлений.

Дальнейшее изложение будет построено следующим образом. Вначале будет объяснен принцип измерения сопротивления, применённый в миллиомметре, затем будут приведены принципиальные схемы, разводка плат и фотографии плат и внутреннего устройства прибора. Далее будут описаны программные средства, применённые в приборе, и дано руководство по его настройке и использованию. После этого будут приведены примеры измерений прибором малых сопротивлений (до 0,5 мОм).

Предварительные замечания

Чтобы понять принципиальные схемы миллиомметра, приведённые далее, на рисунке 1 показана упрощённая схема, поясняющая принцип измерения сопротивления тестируемого резистора Rx. Этот принцип основан на измерении напряжения U_{Rx} на резисторе Rx, через который пропускается определённый ток I_{Rx} (также измеряемый). Сопротивление Rx вычисляется по закону Ома:

$$Rx = \frac{U_{Rx}}{I_{Rx}}.$$

Для исключения погрешности измерений из-за падения напряжения на проводах, возникающего при прохождении по ним относительно большого тока (до 0,5 А), используется хорошо известная двухконтурная измерительная схема Кельвина. Измеряемый резистор подключается к этим контурам с помощью специализированных зажимов, которые также именуются как зажимы Кельвина (в схеме используются зажимы марки LCR-90).

Для формирования тока I_{Rx} используется стабилизатор напряжения, показанный на рисунке 1 в виде отдельного блока. На вход стабилизатора V_{in} подаётся напряжение питания, условно показанное как $V_п$. Стабилизатор может включаться и выключаться с помощью сигнала «on/off», подаваемого на одноимённый вход. Кроме того, на вход V_{ref} стабилизатора подаётся опорное напряжение V_{ref}. В качестве V_{ref} в данном случае используется выходное напряжение внешнего источника опорного напряжения (ИОН) номиналом 2,5 В. Любой стабилизатор имеет также измерительный вход V_{refi}, на который подаётся напряжение V_{refi}, сравниваемое с опорным V_{ref}. И, наконец, стабилизатор имеет выход V_{out}, напряжение на котором V_{refm} и используется для формирования тока I_{Rx}. Отличительной особенностью стабилизатора является способ подключения напряжения к измерительному входу V_{refi}. Обычно к этому измерительному входу подключается выходное напряжение стабилизатора V_{refm}, которое и стабилизируется. Но в данном случае к этому входу, как видно из схемы, подключено напряжение, взятое с контакта зажима с образцовым резистором, т.е. V_{refi}. Таким образом, стабилизатор выдаёт такое выходное напряжение V_{refm}, чтобы напряжение V_{refi} было равно опорному V_{ref}, поскольку именно напряжение, поданное на измерительный вход V_{refi}, сравнивается с опорным.

В первом контуре (сигнал V_{refm}–R_x–$R_{обр}$–«земля») ток $I_{Rобр}$ проходит через измеряемый резистор Rx и последовательно соединённый с ним образцовый

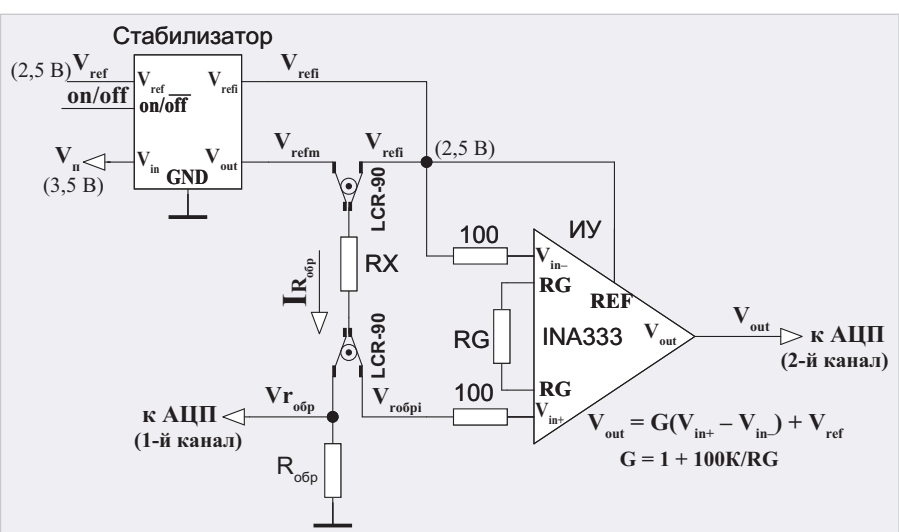


Рис. 1. Упрощённая схема миллиомметра

резистор $R_{обр}$. Силовые провода (V_{refm}) и провод, соединяющий нижний (по схеме) зажим с $R_{обр}$, должны иметь относительно большое поперечное сечение (не менее 0,5 мм^2). Для определения тока I_{Robp} напряжение с образцового резистора $V_{робр}$ подаётся на один из входов АЦП МК (назовём его условно как первый канал АЦП). Зная напряжение $V_{робр}$ и номинал образцового резистора $R_{обр}$, можно определить ток I_{Robp} (см. далее), который также проходит через измеряемый резистор Rx.

Второй контур (сигнал V_{refi}–R_x–V_{robri}) предназначен для измерения падения напряжения на измеряемом резисторе Rx. В этот контур включён инструментальный усилитель (ИУ – INA333), работающий в дифференциальном режиме. Сигнал V_{robri} через стоомный резистор подаётся на неинвертирующий вход ИУ (V_{in+}), а сигнал V_{refi} – на вход опорного напряжения ИУ (REF) и через 100-омный резистор – на инвертирующий вход ИУ (V_{in-}). Провода для сигналов V_{refi} и V_{robri} (в связи с пренебрежимо малым током в этом контуре) могут быть меньшего сечения (лучше не менее 0,1...0,05 мм^2). Для установки коэффициента усиления G ИУ к его входам RG подключён резистор RG. Коэффициент усиления ИУ (согласно справочному листку на ИУ INA333) G = 1 + 100К/RG. Выходное напряжение ИУ (V_{out}) подключается к условно второму каналу АЦП МК. Это напряжение для классического ИУ, построенного на трёх ОУ (а именно так устроен ИУ INA333), как известно, определяется формулой:

$$V_{out} = G(V_{in+} - V_{in-}) + V_{ref}. \quad (1)$$

Здесь следует сделать некоторое отступление относительно способа включения ИУ. В наиболее часто используемом способе включения вход REF ИУ заземляется, вход V_{in-} также подключается к «земле» через какой-либо токоограничивающий резистор небольшого номинала (например, 100 Ом), а измеряемый сигнал подаётся на вход V_{in+} также через небольшой токоограничивающий резистор. Однако такой способ включения имеет два существенных недостатка. Во-первых, при таком способе пришлось бы образцовый резистор подключать к выходу стабилизатора (т.е. к V_{refm}), а измеряемый резистор – между образцовым и «землёй». В этом случае при измерении напряжения на образцовом резисторе с помощью АЦП возникли бы проблемы, поскольку АЦП измеряет напряжение относительно «земли» (а не относительно V_{refm}). Во-вторых, напряжение на измеряемом резисторе измерялось бы АЦП относительно «земли», и при малом номинале измеряемого резистора (миллиомы) это напряжение было бы также мало́ (даже учитывая усиление ИУ). Малые напряжения относительно «земли» при их измерении АЦП имеют максимальную погрешность, поскольку вблизи «земли» интегральная нелинейность максимальна, да и вообще АЦП очень плохо измеряет малые напряжения относительно «земли». При способе включения, показанном на рисунке 1, из опорного напряжения вычитается малое напряжение на измеряемом резисторе, в связи с чем результирующее напряжение очень близко к опорному. Чем ближе измеряемое напряжение к опорному, тем точнее оно измеряется АЦП, поскольку АЦП сравнивает измеряемое напряжение с опорным, а не с «землёй». Кроме того, интегральная нелинейность АЦП минимальна, если измеряемое напряжение близко к опорному. Помимо этого, при способе включения ИУ, показанном на рисунке 1 (т.е. ИУ как бы «перевёрнут» по сравнению со стандартным способом включения), напряжение на образцовом резисторе измеряется АЦП с минимальной погрешностью, поскольку это напряжение также близко к опорному.

Поскольку потенциал сигнала V_{refi} всегда выше потенциала сигнала $V_{робрi}$, приведённая формула (1) может быть переписана в виде:

$$V_{out} = G(V_{in+} - V_{in-}) + V_{ref} = -G(V_{in-} - V_{in+}) + V_{ref}. \quad (2)$$

Из (2) можно найти разность потенциалов (напряжение) на резисторе Rx:

$$V_{in-} - V_{in+} = \frac{V_{ref} - V_{out}}{G}. \quad (3)$$

Реальное напряжение V_{out}, если оно измеряется АЦП, может быть получено по его безразмерному показанию (обозначим его как U_{out}), умноженному на опорное напряжение V_{ref}:

$$V_{out} = V_{ref} \times U_{out}. \quad (4)$$

Здесь следует сделать некоторое уточнение. Пусть имеется 14-разрядный АЦП, и пусть его передаточная характеристика идеальна. Тогда при подключении к его входу опорного напряжения V_{ref} его показания в двоичном коде будут равны $U_{out2} = 11111111111111_2$ (т.е. 14 двоичных единиц). Безразмерное показание АЦП, выраженное рациональным десятичным числом, U_{out10}, можно найти, разделив U_{out2} на $(2^{14} - 1)$: $U_{out10} = U_{out2}/(2^{14} - 1) = 1$. Другими словами, в этом случае $U_{out} = 1$. Если же вход АЦП заземлить, то безразмерное показание АЦП будет нулевым: $U_{out} = 0$.

Аналогично по безразмерному показанию АЦП ($U_{робр}$) определяется реальное напряжение ($V_{робр}$) на образцовом резисторе:

$$V_{робр} = V_{ref} \times U_{робр}. \quad (5)$$

Ток I_{Robp}, проходящий через образцовый резистор $R_{обр}$, может быть найден по формуле:

$$I_{Robp} = \frac{V_{робр}}{R_{обр}}. \quad (6)$$

Измеряемое сопротивление резистора Rx может быть найдено как разность потенциалов ($V_{in-} - V_{in+}$), делённая на проходящий ток I_{Robp}, а с учётом (3–6) получим формулу для вычисления Rx по показаниям АЦП (U_{out}, $U_{робр}$), номиналу образцового резистора $R_{обр}$ и, коэффициенту усиления G ИУ:

$$Rx = \frac{1 - U_{out}}{G \times U_{робр}} \times R_{обр}. \quad (7)$$

Интересной особенностью формулы (7) является отсутствие в ней опорного напряжения V_{ref}. Это означает, что, во-первых, оно в принципе может быть любым (конечно, в разумных пределах), и, во-вторых, что его абсолютное значение не играет никакой роли, лишь бы оно было стабильно во время измерения (не более 1 с, см. далее). Формула (7) и была использована для всех расчётов в программе для МК. Конкретные значения номиналов образцовых резисторов $R_{обр}$ и коэффициентов усиления G будут указаны далее.

Принципиальные схемы

Условно схему платы миллиомметра (см. рис. 2) с дополнительными устройствами (см. рис. 3) можно разбить на две части: цифровую и аналоговую. В цифровую часть входят: два интерфейса для сопряжения МК с компьютером для его (МК) программирования, интерфейс с LCD, несколько сигналов (бит состояния), предназначенных для управления работой МК, и несколько сигналов, предназначенных для управления МК внешними устройствами.

Первый вариант программирования МК – с помощью USB DEBUG адаптера, который сопрягается с компьютером по интерфейсу USB, а с МК – по двухпроводному интерфейсу C2. Для этого предназначен трёхконтактный штыревой разъём XB, на который выведены два сигнала – RST/C2CK и C2D – и «земля». Для сопряжения используется кабель, который одним концом (ответная трёхконтактная вилка) подключается к разъёму XB, а второй его конец подключается к самому USB DEBUG адаптеру. Схему такого кабеля можно найти в [2]. Цепочка R1R2C1 используется для штатной работы интерфейса C2.

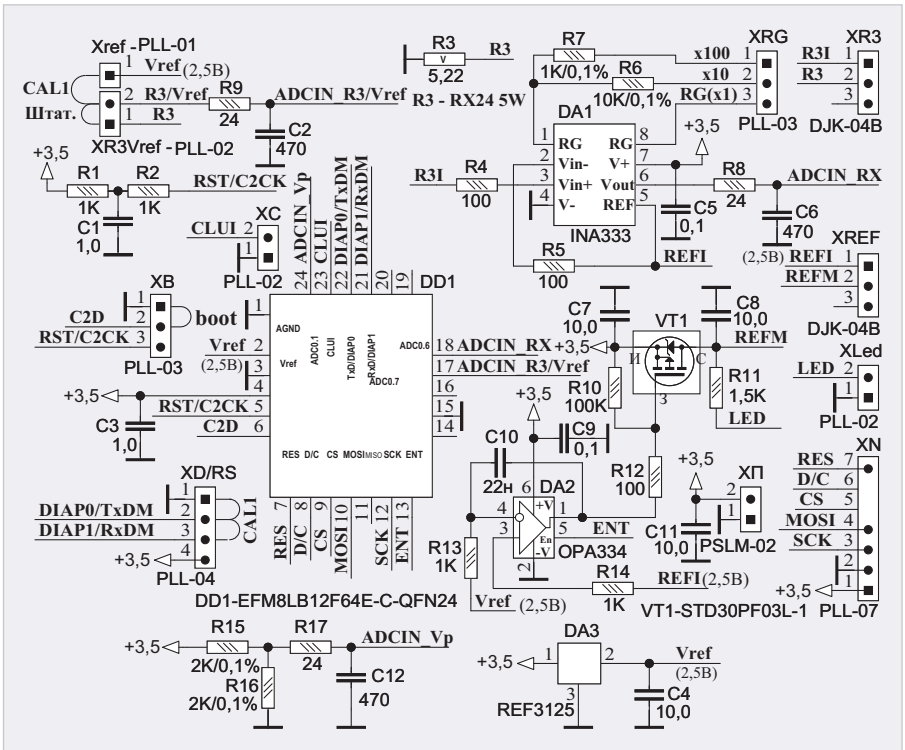


Рис. 2. Принципиальная схема платы миллиомметра

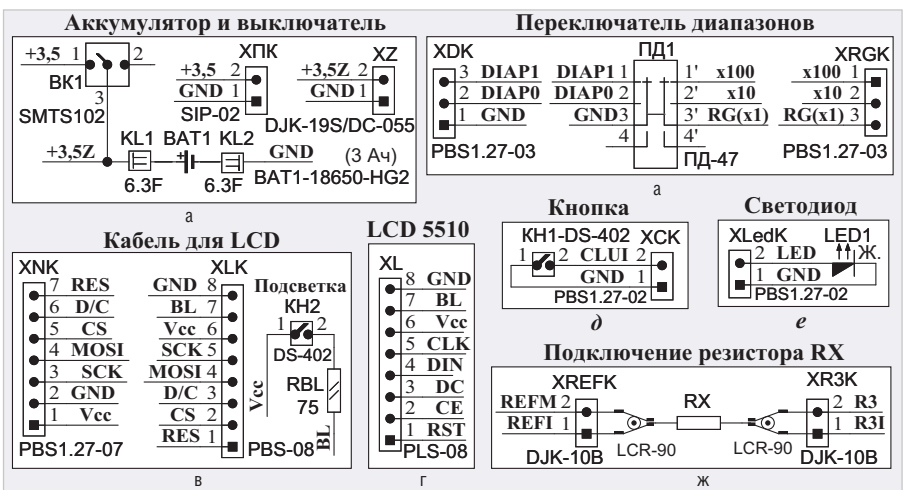


Рис. 3. Схемы дополнительных устройств миллиомметра

Второй вариант программирования МК – по интерфейсу RS-232 с помощью COM-порта компьютера (COM1). Для сопряжения используется 4-контактный штыревой разъём XD/RS, на который выведены два сигнала – TxDM RxDM – питание (+3,5 В) и «земля». К этому разъёму подключается преобразователь уровней интерфейса RS232-TTL, а к нему – кабель сопряжения с COM-портом компьютера. Все схемы и подробное описание этого режима программирования можно найти в [3]. Для перевода МК в данный режим программирования необходимо замкнуть перемычкой контакты 1–2 разъёма XB (эта перемычка показана пунктиром).

Для сопряжения МК с LCD-5110 используется интерфейс SPI и семиконтактный штыревой разъём XN, на который выведены сигналы SPI, питание (+3,5 В) и «земля». К этому разъёму одним концом (ответная семиконтактная вилка – XNK, см. рис. 3в) подключается кабель, который вторым концом (ответная восьмиконтактная вилка – XLK, см. рис. 3в) подключается к разъёму LCD (XL, см. рис. 3г). Дисплей оборудован подсветкой – четыре светодиода синего цвета, расположенные по углам LCD. Для того чтобы «зажечь» светодиоды, необходимо на контакт BL (BackLight, седьмой контакт разъёма XLK) подать напряжение питания V_{cc} (шестой контакт XLK) через токоограничивающий (до 20 мА) резистор RBL. Это осуществляется с помощью кнопки DS-402 (КН2, см. рис. 3в) красного цвета, которая установлена на лицевой поверхности корпуса прибора.

Управление режимами работы МК осуществляется сигналами DIAP0 и DIAP1, логические состояния которых (лог. 0 или лог. 1) определяют тот или иной режим работы. Эти сигналы выведены на штыревой разъём XD/RS. К контактам 1–3 этого разъёма одним концом (трёхконтактная ответная вилка) подключается кабель, который вторым концом припаян к движковому переключателю ПД1 (см. рис. 3б). Здесь следует заметить, что объединение в одном разъёме (XD/RS) сигналов для программирования МК по интерфейсу RS–232 и сигналов управления не приведёт к какой-либо коллизии: при программировании МК прибор не работает и ничего не измеряет, а при измерениях он отключён от интерфейса RS–232.

Сигнал CLUI (лог. 0) запускает миллиомметр в режиме измерения, если он появляется после включения питания. Этот сигнал (и «земля») выведен на двухконтактный штыревой разъём XC, к которому подключается один из концов кабеля (ответной двухконтактной вилкой), а второй его конец соединяется с двухконтактной кнопкой КН1 (см. рис. 3д). При нажатии кнопки CLUI = лог. 0, при отпускании CLUI = лог. 1. Если кнопка нажата и удерживается в нажатом состоянии перед включением питания, а после включения питания отпускается, то миллиомметр переходит в режим установки нуля по выбранному диапазону измерения (см. далее). Для управления работой стабилизатора используется управляющий сигнал ENT (подаваемый МК), состояние которого включает (лог. 1) или выключает (лог. 0) стабилизатор.

Аналоговая часть включает в себя следующие устройства. Прецизионный измерительный резистор R3, напряжение на котором измеряется АЦП МК, ИУ INA333 (DA1), посредством которого измеряется падение напряжения на измеряемом резисторе, ИОН REF3125 (DA3) с выходным напряжением V_{ref}=2,5 В и стабилизатор на базе операционного усилителя (ОУ) OPA334 (DA2) и мощного полевого p-канального транзистора STD30PF03L-1 (VT1).

Сигнал V_{ref} подключён ко второму выводу МК DD1 (P0.0/V_{ref}). Этот же сигнал выведен на одноконтактный штыревой разъём X_{ref}. Конденсатор C4 блокировочный; он необходим для штатной работы ИОН. Для измерения напряжения на R3 это напряжение (сигнал R3) подаётся на первый контакт двухконтактного разъёма $XR3V_{ref}$. В штатном режиме работы

его контакты 1–2 замыкаются перемычкой, в результате чего напряжение (на R3) со второго контакта (сигнал $R3/V_{ref}$) через RC цепочку R9C2 подаётся на 17-й вывод МК (ADC0.7) – сигнал ADCIN_R3/V_{ref}. В режиме калибровки полной шкалы АЦП (см. далее) перемычка с разъёма $XR3V_{ref}$ снимается, и второй контакт разъёма $XR3V_{ref}$ соединяется с контактом разъёма X_{ref} проводом с двумя ответными гнёздами на его концах. В результате опорное напряжение V_{ref} через цепочку R9C2 подаётся на вход АЦП ADC0.7 МК (сигнал ADCIN_R3/V_{ref}).

ИУ INA333 (DA1) включён по схеме, аналогичной рисунку 1. В зависимости от диапазона измерения к его входам RG (выводы 1, 8) подключается либо резистор R7 (1 кОм), в этом случае коэффициент усиления G =1+100К/1К = 101, либо резистор R6 (10 кОм), тогда G=1+100К/10К =11, либо ничего не подключается, т.е. выводы 1, 8 свободны; в этом случае G=1.

Для установки того или иного коэффициента усиления служит движковый переключатель ПД-47 (ПД1, см. рис. 3б) с двумя группами контактов (три положения, два направления). Для установки коэффициента усиления G на плате предусмотрен трёхконтактный штыревой разъём XRG. К этому разъёму подключается кабель, на одном конце которого расположена ответная трёхконтактная вилка XRGK (которая и подключается к разъёму XRG), а второй его конец припаян к контактам 1'–3' ПД1 (см. рис. 3б). Помимо установки коэффициента усиления ИУ, ПД1 с помощью второй группы контактов (1–3) устанавливает в то или иное состояние биты диапазонов DIAP0 и DIAP1 МК. Для этого служит трёхпроводный кабель, который одним концом припаян к контактам 1–3 ПД1 (см. рис. 3б), а на втором его конце установлена трёхконтактная вилка XDK, которая подключается к контактам 1–3 разъёма XD/RS (см. рис. 2). В первом (нижнем по схеме на рис. 3б) положении ПД1 все его контакты разомкнуты, в связи с чем биты DIAP0 и DIAP1 находятся в состоянии лог. 1, а коэффициент усиления ИУ G=1. Во втором (среднем) положении замыкаются контакты 2–3 и 2'–3', бит DIAP0 устанавливается в состояние лог. 0 (DIAP1=лог. 1), а коэффициент G=11 (см. ранее). В третьем (верхнем по схеме) положении замыкаются контакты 1–3 и 1'–3', в связи с чем бит DIAP1 = лог. 0 (DIAP0 =1), а G = 101.

Есть ещё одна (технологическая) комбинация: бит DIAP0 и DIAP1. Оба бита устанавливаются в состояние лог. 0. Комбинация используется для калибровки полной шкалы АЦП МК (см. далее). Для этого с разъёма XD/RS снимается ответная трёхконтактная вилка кабеля, соединяющего этот разъём с переключателем ПД1, и на три контакта (1–3) надевается трёхконтактная перемычка, соединяющая все три контакта, т.е. заземляющая сигналы DIAP0 и DIAP1. Эта перемычка показана пунктиром справа от разъёма XD/RS (см. рис. 2).

Измеряемый резистор RX подключается к зажимам Кельвина LCR-90, к которым одним концом припаяны два двухпроводных кабеля, ко вторым концам которых припаяны двухконтактные разъёмы – вилки DJK-10B (XREFK и XR3K, см. рис. 3ж). Эти две вилки вставляются в розетки DJK-04B (XR3 и XREF, см. рис. 2), установленные на лицевой поверхности корпуса прибора. К этим розеткам припаяны два двухпроводных кабеля, которые своим вторым концом впаяны в плату. Силовой контур, через который течёт большой ток, – REFM-RX-R3, измерительный контур, предназначенный для измерения напряжения на RX, – REFI-RX-R3I. Сигнал REFI подключён к выводу REF ИУ DA1 (5-й вывод) и через резистор R5 – к входу V_{in-} ИУ DA1 (2-й вывод), а сигнал R3I через резистор R4 подключён к входу V_{in+} (3-й вывод DA1), т.е. именно так, как это организовано на рисунке 1.

Напряжение с выхода ИУ V_{out} (6-й вывод DA1) через цепочку R8C6 подаётся на 18-й вывод МК (ADC0.6) – сигнал ADCIN_RX. Блокировочный конденсатор C5 служит для штатной работы ИУ DA1.

В состав стабилизатора входит ОУ OPA334 (DA2) и мощный p-канальный полевой транзистор STD30PF03L-1 (VT1). В отличие от стандартной схемы стабилизатора положительного напряжения на ОУ и n-канальном полевом транзисторе, на сток которого подаётся входное напряжение, а с истока снимается стабилизированное, в данном случае использован p-канальный транзистор, который «перевёрнут», т.е. входное напряжение (+3,5 В) подаётся на его исток, а стабилизированное снимается с его стока. Такое включение p-канального транзистора имеет одну особенность. В стандартной схеме для открытия n-канального транзистора требуется подать на его затвор напряжение выше напряжения истока (т.е. выше входного напряжения) на 1...4 В (пороговое). В данной же схеме (см. рис. 2), во-первых, на стоке напряжение (выходное – около +2,5 В) более отрицательно по отношению к напряжению истока (входное – +3,5 В), т.е. p-канальный транзистор работает в штатном режиме. Во-вторых, на затвор транзистора для его открытия требуется подать напряжение не выше входного, а ниже его на те же 1...4 В (т.е. более отрицательное по отношению к напряжению истока). С этим легко справится ОУ DA2, т.к. напряжение его питания – +3,5 В. Транзистор STD30PF03L-1 имеет низкое пороговое напряжение (около 1 В), поэтому схема будет работать даже при сильном разряде аккумулятора (до 2,7 В). Как видно из схемы, на инвертирующий вход ОУ (4-й вывод DA2) через резистор R13 подаётся опорное напряжение V_{ref}, а на неинвертирующий вход (3-й вывод DA2) подаётся не выходное напряжение стабилизатора (REFM), а напряжение REFI, т.е. то, которое получается в месте контакта зажима (с разъёмом XREFK) с измеряемым резистором (см. рис. 3ж). Другими словами, стабилизатор устанавливает опорное напряжение V_{ref} именно в месте контакта RX с зажимом (напряжение REFI). Выходное напряжение ОУ (1-й вывод DA2) через резистор R12 подаётся на затвор транзистора VT1. При подключении нагрузки к выходу стабилизатора его выходное напряжение (REFM) будет падать, а вместе с ним упадёт и напряжение REFI, и поскольку оно подключено к неинвертирующему входу ОУ DA2 (через резистор R14), снизится и выходное напряжение ОУ. Это приведёт к тому, что напряжение затвора транзистора также снизится, транзистор приоткроется, вернув выходное напряжение REFM, а за ним и напряжение REFI на прежний уровень. При отключении нагрузки всё произойдёт с точностью до наоборот. Конденсатор C10 предотвращает самовозбуждение ОУ DA2.

ОУ DA2 имеет вход разрешения (En – Enable) – 5-й вывод DA2, низкий уровень (лог. 0), на котором отключает выход ОУ, т.е. переводит его в высокоимпедансное состояние. В этом случае затвор VT1 оказывается подключённым к истоку через резистор R10, что приведёт к закрытию транзистора. Если на вход En DA2 подан высокий уровень (лог. 1), то выход ОУ включится, что приведёт к работе стабилизатора в штатном режиме. Как видно из схемы, номинал R12 (100 Ом) на 3 порядка ниже номинала R10 (100 кОм), поэтому влияние R10 на включение транзистора ничтожно мало. Включение и выключение стабилизатора осуществляется сигналом ENT, подаваемым с МК (13-й вывод DD1).

К выходу стабилизатора через двухконтактный штыревой разъём XLed (см. рис.2)

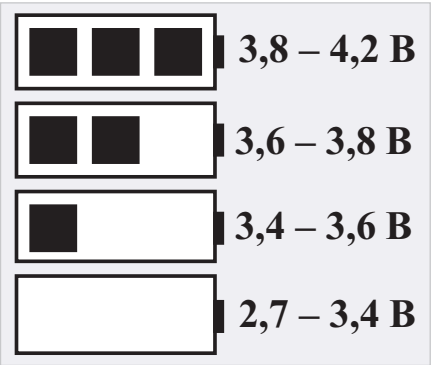


Рис. 4. Показания степени разряженности аккумулятора на экране миллиомметра

и двухпроводный кабель с ответным разъёмом XLedK (см. рис. 3е) подключён светодиод. Светодиод расположен на лицевой панели корпуса и сигнализирует о наличии напряжения на выходе стабилизатора. Он загорается только в процессе измерения (не более 1 с).

Напряжение питания платы с условным значением +3,5 В поступает с двухконтактного цангового штыревого разъёма XP. На самом деле, напряжение полностью заряженного аккумулятора составляет +4,2 В, а разряженного (но ещё находящегося в штатном режиме работы) – +2,7 В. К разъёму XP одним концом с ответным гнездом XPK (см. рис. 3а) подключается двухпроводный кабель питания, который своим вторым концом припаян к 1-му выводу выключателя питания BK1 (+3,5 В, 2-й вывод XPK), а провод GND (1-й вывод XPK) припаян к клемме KL2, соединённой с минусом аккумулятора (BAT1). Эта клемма надета на лепесток, приваренный к минусу BAT1. Аналогичная клемма KL1 надета на лепесток, приваренный к плюсу BAT1. Эта клемма (сигнал +3,5Z) соединена проводом с выводом 3 выключателя BK1 и одновременно с выводом 2 гнездового разъёма DJK-19S (XZ). 1-й вывод разъема XZ (сигнал GND) соединён с клеммой KL2. Клеммы KL1 и KL2 – нажимные, размером 6,3 мм.

Разъём XZ предназначен для зарядки аккумулятора зарядным устройством. Этот разъём (DJK-19S) припаян на специальную плату (её разводка приведена в дополнительных материалах к статье), которая двумя винтами M2 крепится к днищу корпуса. Конец разъёма выведен наружу на торец корпуса. К этому разъёму подключается ответная вилка DJK-11K (2,5×0,7-L9) двухпроводного кабеля, который своим вторым концом припаян к плате зарядного устройства на базе TP4056. Сама плата зарядного устройства приклеена гибкой теплопроводящей прокладкой с двусторонним липким слоем к игольчатому радиатору с площадью поверхности около 70 см^2 (см. далее).

Для определения состояния аккумулятора в схеме используются два резистора R15 и R16, точка соединения которых через цепочку R17C12 подаётся на ещё один вход АЦП МК – ADC0.1 (24-й вывод DD1, сигнал ADCIN_Vp). Напряжение в точке соединения резисторов делителя напряжения питания (в 2 раза) измеряется АЦП МК, и в зависимости от его значения на дисплей выводится условное изображение аккумулятора с тремя сегментами, соответствующими напряжениям (см. рис. 4).

Все резисторы (кроме R3) и конденсаторы (керамические) – для поверхностного монтажа, размером 0603 (кроме C4, C7, C8, C11 – их размер 0805). Резистор R3 пятиваттный в металлическом корпусе. Все разъёмы (кроме XP, XR3 и XREF) штыревые с шагом 1,27 мм (PLL-0X), разъём XP цанговый с шагом 2,54 мм (PSLM-02).

Разводка плат и фотографии устройства

Разводка плат выполнена в программе SprintLayOut 6.0. В дополнительных материалах к статье приведён файл разводки в формате *.lay6, в котором присутствует разводка обеих плат: основной платы с МК и миниатюрной платы для установки разъёма подключения зарядного устройства.

На рисунке 5 приведены разводка и фотография (перед распайкой компонентов навесного монтажа) основной платы миллиомметра. Кружками на разводке показаны места с двусторонней пайкой. Разводка платы с разъёмом для подключения зарядного устройства в связи с её простотой не приводится.

Конструкция прибора

По фотографии прибора в открытом корпусе размером 102×54×30 мм (см. рис. 6) можно составить представление о его внутреннем устройстве. Корпус состоит из двух половин. На первой расположена лицевая панель прибора. В ней прорезано окно для дисплея, плата которого укреплена по углам пластиковыми полосками, приклеенными к боковым поверхностям корпуса губчатой лентой с двусторонним липким слоем. На лицевой стороне также расположены: светодиод, кнопка чёрного цвета для инициализации процесса измерений, кнопка красного цвета для включения подсветки и выключатель питания. Для ручки движкового переключателя диапазонов прорезано прямоугольное окно. На этой же стороне укреплены разъёмы (гнёзда) для подключения измерительных зажимов Кельвина, к которым припаяны провода с ответными разъёмами (штекеры). На внутренней стороне второй половины корпуса расположены: аккумулятор, приклеенный полосками губчатой ленты с двусторонним липким слоем; движковый переключатель, к которому припаяны две латунные стойки с внутренней резьбой M2,5, прикрученные к корпусу с обратной стороны винтами M2,5 впотай; плата с разъёмом для зарядки аккумулятора, прикрученная к корпусу с обратной стороны двумя винтами M2 впотай и гайками (см. далее). Транзистор припаян к медной пластине размером 25×15×1,5 мм, в

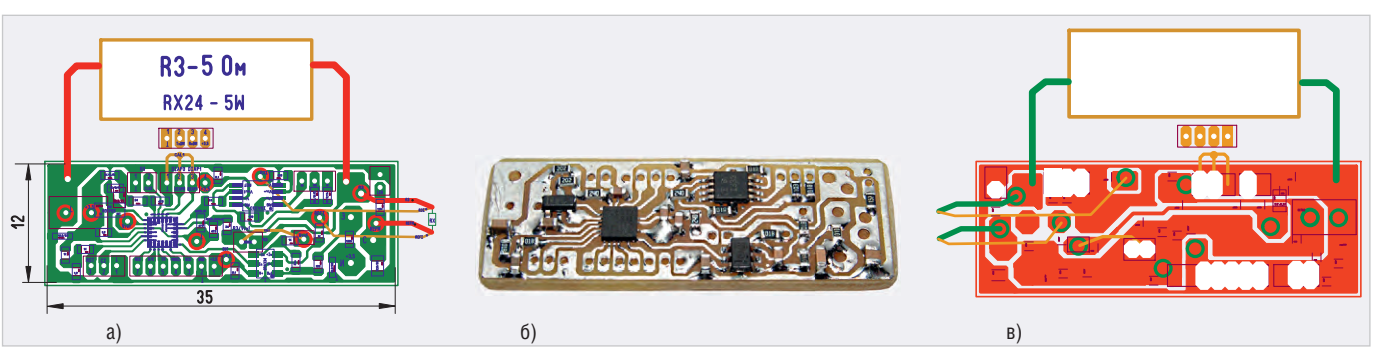


Рис. 5. Плата миллиомметра: а) разводка; б) внешний вид; в) платы со стороны компонентов для поверхностного монтажа, разводка платы со стороны навесных компонентов

которой просверлено отверстие и нарезана резьба М3. Эта пластина крепится к внутренней поверхности второй половины корпуса винтом М3 впотай. Все три вывода транзистора впаяны в плату со стороны расположения компонентов для поверхностного монтажа. Образцовый резистор впаян в плату и держится на своих выводах. Плата не имеет крепёжных отверстий, т.к. она держится на достаточно жёстких выводах транзистора. Обе половины корпуса защёлкиваются двумя торцевыми пластинами.

Зарядка аккумулятора прибора

Как уже упоминалось ранее, для зарядки аккумулятора используется специальная плата на базе микросхемы TP4056, оборудованная разъёмом microUSB для подключения к ней устройства для зарядки телефона с выходным напряжением 5 В. К выходным контактам устройства на TP4056 припаян двухпроводный кабель, а на другой его конец – ответный разъём DJK-11K (2,5×0,7-L9, см. рис. 7). Провода в месте пайки кабеля к плате укреплены каплей термоклея. Иначе от частого изгибания кабеля провода в месте пайки могут отломиться. Этот кабель подключён к разъёму зарядки прибора DJK-19S (XZ, рис. 3а), распаянном на небольшой плате (см. рис. 6, сверху). Разъём microUSB от зарядного устройства подключён к плате. При зарядке аккумулятора питание прибора должно быть выключено, а зарядное устройство подключено к сети. При правильном подключении на плате включится красный светодиод и начнётся зарядка аккумулятора. По завершении зарядки (когда аккумулятор зарядится до напряжения 4,2 В) красный светодиод погаснет и включится синий.

На плате с TP4056 по умолчанию установлено максимальное значение зарядного тока 1 А. Такой ток обеспечивают далеко не все зарядные устройства. Кроме того, при токе 1 А плата с TP4056 достаточно сильно нагревается и может выйти из строя от перегрева. Поэтому если использовать зарядное устройство для телефона (или других аккумуляторов), обеспечивающее ток 1 А или более, то плату необходимо установить на радиатор. Автор использовал игольчатый радиатор с площадью поверхности около 70 см^2. Плата приклеена к радиатору гибкой термопрокладкой с двусторонним липким слоем (см. рис. 7). Если же зарядное устройство обеспечивает ток не более 0,5 А, то в радиаторе нет необходимости.

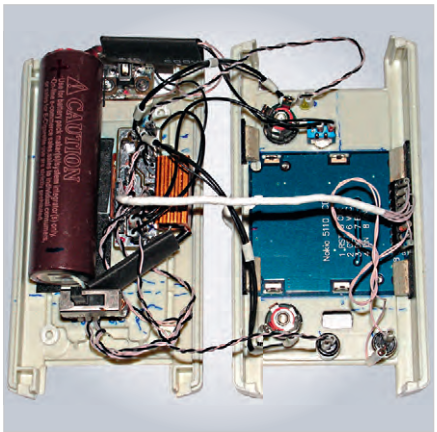


Рис. 6. Внутреннее устройство миллиомметра

Рис. 7. Зарядка аккумулятора прибора

Программные средства и управление работой прибора

Используемый для измерений необходимых напряжений в миллиомметре метод передискретизации и осреднения для увеличения разрешающей способности четырнадцатиразрядного SAR-АЦП (встроенного в МК EFM8LB12) подробно описан в [1]. Вывод информации на ЖКИ условно можно разбить на две части. Первая часть состоит в подготовке информации к выводу, т.е. получения необходимых для вывода цифр с помощью функции Си sprintf(). Об этом подробно описано в [1]. Вторая часть касается непосредственно вывода цифр на дисплей LCD-5110. В отличие от вывода цифр на семисегментный ЖКИ [1], вывод цифр на графический дисплей LCD-5110 существенно отличается. Далее описана организация такого вывода.

С программной точки зрения дисплей состоит из так называемых строк шириной 8 пикселей, соответствующих 8 битам или 1 байту. В LCD-5110 таких строк шесть (6×8 = 48 пикселей по вертикали). Строки нумеруются от 0 до 5. Помимо строк имеются также столбцы. Таких столбцов в LCD-5110 – 84. Столбцы нумеруются слева направо от 0 до 83.

Каждая цифра представляет собой прямоугольное поле пикселей определённого размера. В LCD-5110 это поле имеет размер 24×16 пикселей, т.е. три строки (3 байта) по 16 столбцов (размер поля выбран автором). Значение тех или иных битов поля определяется шрифтом и соответствующей цифрой (символом). Существуют специальные программы, которые формируют значения бит поля в зависимости от символа и шрифта. Автор использовал бесплатную программу GLCD Font Creator 1.2.0.0. Для цифр использовался шрифт Clarendon Condensed жирный размером 26. У этого шрифта каждый символ цифры как раз занимает поле из 24×16 пикселей.

Вывод цифр на дисплей в программе осуществляется по столбцам. Например, для того чтобы вывести один символ на дисплей LCD-5110, необходимо указать номер строки (в данном случае это 3), начиная с которой будет выводиться столбец, и указать начальный номер столбца (от 0 до 83). При выводе каждого байта номер строки автоматически увеличивается на 1, поэтому после вывода трёх байт необходимо установить номер строки в начальное состояние (3) и выводить следующие 3 байта. При этом номера столбцов автоматически инкрементируются. После вывода всех 16 столбцов цифра появится на экране.

На дисплей выводятся пять цифр, занимающих 5×16=80 пикселей, а оставшиеся 4 пикселя занимает десятичная точка шириной 4 пикселя, что в сумме составляет 84 пикселя – вся ширина экрана LCD-5110. Цифры и десятичная точка выводятся на три последние строки (с третьей по пятую).

Помимо цифр, на две верхние строки (нулевую и первую) выводятся символы «mΩ» и пиктограмма аккумулятора, показывающая степень его разряженности, в соответствии с рисунком 4. Символы «m» и «Ω» занимают поле 16×16 пикселя, а один из символов разряженности аккумулятора (их четыре) – 16×32 пикселей. Для символа «Ω» использован шрифт Symbol PS, жирный, размер 16; для символа «m» – шрифт Times, жирный, размер 14. Для символов аккумулятора использован шрифт Arial, жирный, размер 26. В этом шрифте символы цифр 0, 1, 2 и 3 соответственно заменены на рисунки аккумулятора: пустой, с одним «горящим» сегментом, с двумя и тремя.

Подпрограммы вывода информации на дисплей (по сравнению с остальной

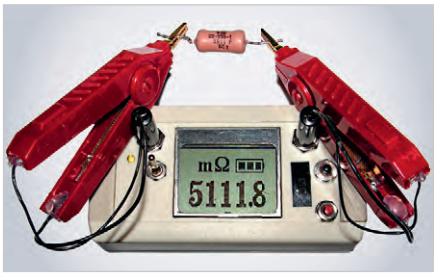


Рис. 8. Измерения на первом диапазоне. Резистор 5,11 Ом, 1% (С2-29В-1)

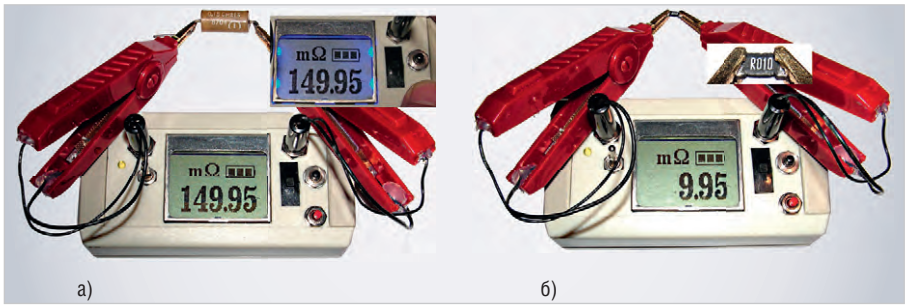


Рис. 9. Измерения на втором диапазоне. Резисторы: а) С5-16МВ 1 Вт, 0,15 Ом, 1%; б) SMD 2512 0,01 Ом, 1%

частью программы) примитивно просты. Формула (7) для расчёта измеряемого сопротивления Rx также проста, и запрограммировать её в МК не составляет большого труда. Поэтому ниже будет описана только суть работы подпрограмм, используемых в миллиомметре, и способ их запуска.Таких подпрограмм три: подпрограмма калибровки полной шкалы АЦП МК, подпрограмма установки нуля прибора в выбранном диапазоне, подпрограмма штатной работы прибора. Кроме того, дополнительно используется подпрограмма индикации уровня зарядки аккумулятора.

Подпрограмма калибровки полной шкалы АЦП может быть запущена только в открытом корпусе прибора (см. рис. 6). Эту подпрограмму требуется запустить всего один раз:

- снять с разъёма XD/RS (см. рис. 2) ответный разъём кабеля;
- подключить к контактам 1–3 разъёма XD/RS 3-контактную перемычку – ответный разъём с тремя контактами, соединёнными между собой;
- снять двухконтактную перемычку с контактов разъёма $XR3V_{ref}$;
- соединить второй контакт разъёма $XR3V_{ref}$ с контактом разъёма X_{Ref} (для этого необходимо изготовить однопроводный кабель с двумя гнёздами на его концах);
- включить питание прибора.

Подпрограмма измерит опорное напряжение V_{ref} в безразмерном виде, т.е. АЦП покажет значение, близкое к единице (например, у одного экземпляра МК это значение было равно 0,9998). Далее вычисляется обратное значение (которое в данном случае будет равно 1/0,9998≈1,0002), которое в виде коэффициента К=1,0002 запишется во флеш-память МК и прочитается из неё. Далее будет произведено повторное измерение напряжения, которое будет умножено на К и выведено на дисплей. Показания на дисплее должны быть: «1.0000». Если на дисплее получено такое показание, то это будет означать, что калибровка полной шкалы произведена правильно. В противном случае необходимо произвести калибровку заново, выключив и включив питание прибора. После калибровки полной шкалы необходимо вернуть все разъёмы в первоначальное состояние и закрыть корпус прибора. На этом калибровка полной шкалы закончена. Запуск подпрограммы установки нуля для каждого диапазона измерений необходимо проводить в следующей последовательности:

1. подключить к прибору штекеры от зажимов и соединить их измерительные контакты между собой;
2. не включая питания, нажать чёрную кнопку и, не отпуская её, включить питание. Далее кнопку отпустить. Подпрограмма прочитает из флеш-памяти коэффициент К, полученный при калибровке полной шкалы АЦП. С учётом этого коэффициента подпрограмма произведёт измерение сопротивления (в данном случае это сопротивление равно нулю). Результат будет выведен на дисплей. Показания на дисплее должны быть нулевыми в каждом диапазоне. Подпрограмма вычислит разницу между нулём и измеренным сопротивлением, запишет эту разницу в виде коэффициента (К0 – для первого диапазона, К1 – для второго и К2 – для третьего);
3. выключить питание и включить заново. Затем нажать и отпустить чёрную кнопку. Программа прочитает из флеш-памяти записанные ранее коэффициенты (К, К0, К1 и К2), измерит сопротивление (нулевое, т.к. зажимы закорочены) и с учётом коэффициентов выведет результат на экран дисплея. Показания прибора также должны быть нулевыми. В противном случае необходимо произвести повторно установку нуля (п. 2). Во время измерения кратковременно (не более чем на 1 с) загорится и погаснет светодиод;
4. произвести установку нуля во всех трёх диапазонах.

На этом установка нуля прибора заканчивается. Для запуска подпрограммы измерения сопротивления резисторов в штатном режиме работы необходимо:

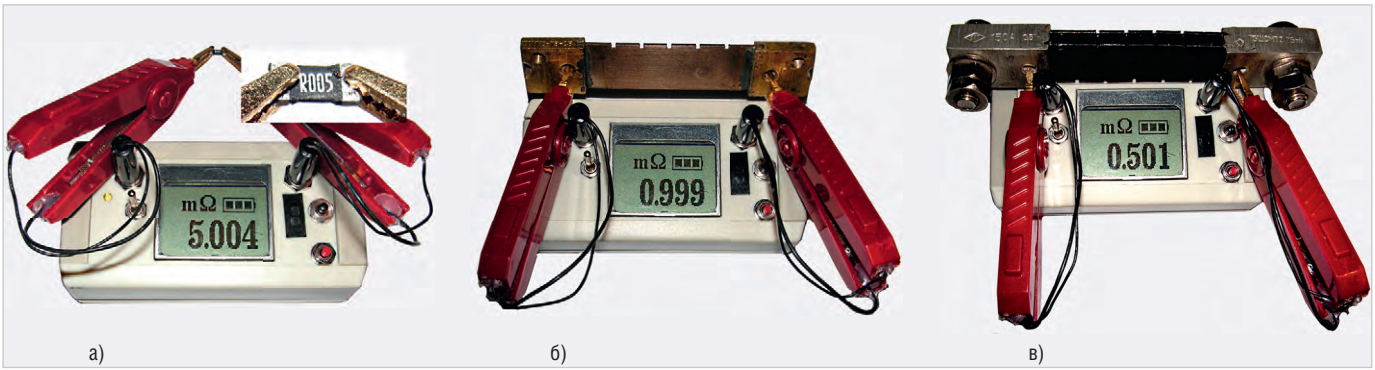
- подключить измеряемый резистор к зажимам;
- установить нужный диапазон измерения;
- включить питание прибора;
- нажать и отпустить чёрную кнопку.

Программа прочитает из флеш-памяти записанные ранее коэффициенты (К, К0, К1 и К2), измерит сопротивление подключённого резистора и с учётом коэффициентов выведет результат на экран дисплея. Во время измерения кратковременно (не более чем на 1 с) загорится светодиод, а показания останутся на дисплее.

Подпрограмма для индикации уровня зарядки аккумулятора работает следующим образом. Максимальное напряжение, до которого заряжается аккумулятор, как было упомянуто ранее, составляет 4,2 В. Минимально допустимое напряжение, при котором аккумулятор функционирует в штатном режиме, составляет 2,7 В. Однако прибор адекватно работает, если напряжение питания составляет не менее 3,4 В, поэтому были выбраны следующие граничные напряжения: 2,7, 3,4, 3,6 и 3,8 В (см. рис. 4).

Для определения выходного напряжения аккумулятора $U_{БАТ}$ (см. рис. 2) это напряжение (сниженное в 2 раза делителем R15-R16) подаётся на вход первого канала АЦП МК (ADC0.1). Подпрограмма измеряет это напряжение. Если 2,7 В ≤ $U_{БАТ}$ ≤ 3 ,4 В, то индицируется «пустой» символ аккумулятора. Если 3,4 В < $U_{БАТ}$ ≤ 3,6 В, то индицируется символ с одним сегментом. Если 3,6 В < $U_{БАТ}$ ≤ 3,8 В – с двумя. Если $U_{БАТ}$ > 3,8 В – с тремя. При измерениях необходимо следить за состоянием аккумулятора, и если индицируется один сегмент, аккумулятор следует подзарядить.

Если для измерения напряжений U_{out} и $U_{Робр}$, использующихся в расчёте значения измеряемого сопротивления Rx по формуле (7), производится 64-кратное осреднение результатов 1024 показаний АЦП



а) б) в)

Рис. 10. Измерения в третьем диапазоне. Резисторы: а) SMD 2512 0,005 Ом, 1%; б) шунт 75ШСММ3-75-0,5 – 75 А, 75 мВ, класс 0,5, 1 мОм, 0,5%; в) шунт 75ШСМТ2-150 А, 75 мВ, класс 0,5, 0,5 мОм, 0,5%

(осреднённых с децимацией), то для измерения значения $U_{БАТ}$ производится восьмикратное осреднение. Это сделано в связи с тем, что высокая точность измерения $U_{БАТ}$ не нужна, а восьмикратное осреднение требует в 8 раз меньше времени (т.е. почти на порядок), чем 64-кратное. А это дополнительное время, которое входит в общее время прохождения большого тока (0,5 А). Оно снижено в 8 раз для того, чтобы аккумулятор меньше разряжался.

Если время измерения Rx не превышает 1 с, то каждое измерение потребует 0,5 А·с. Ёмкость аккумулятора составляет 3 А·ч, однако если принять во внимание разрядную характеристику аккумулятора, то при токе разряда, равном 0,2 ёмкость С будет равна 0,2×3000 мА = 600 мА, ёмкость аккумулятора при разряде до напряжения 3,4 В составит, по разным оценкам, от 2 до 2,5 А·ч. Если взять минимальное значение 2 А·ч=7200 А·с и разделить на 0,5 А·с, то получим 14 400, т.е. около 14 000 измерений. Другими словами, полностью заряженный аккумулятор позволяет произвести около 14 000 измерений, после чего его уже следует подзарядить.

Потребление тока миллиомметром только при индикации показаний составляет около 15 мА, т.е. существенно меньше, чем во время измерения (500 мА). Также следует отметить, что потребление тока только в режиме индикации для миллиоомметра (15 мА) в 3 раза выше, чем потребление тока вольтметром (5 мА), описанным в [1]. Утроенное потребление тока – следствие утроенной тактовой частоты процессора МК (72 МГц – в миллиомметре против 18 МГц – в вольтметре [1]). Однако утроение тактовой частоты процессора МК снизило время измерения (когда протекает ток 0,5 А) до 1 с (при частоте 18 МГц это время составляет 3 с).

Как было указано ранее, при подсветке потребление тока дисплеем LCD-5110 составляет около 25 мА (20 мА потребляет подсветка и 5 мА – дисплей без подсветки), так что существенного разряда аккумулятора от подсветки не произойдёт. Программа для миллиомметра в уже готовом загрузочном *.hex-формате приведена в дополнительных материалах к статье.

Результаты измерений

Для проверки работоспособности приборов автор подобрал несколько резисторов однопроцентной точности разного номинала и два шунта класса 0,5. Результаты измерений показаны на рисунках 8–10.

Результаты измерений оказались неожиданными. Относительные погрешности всех без исключения измеренных значений полностью укладываются в относительные погрешности резисторов (1%) и шунтов (0,5%). Конечно, предполагалось, что прибор должен измерять подобные сопротивления, но откуда взялась такая невероятная чувствительность и достаточно приемлемая точность, особенно при измерении сопротивлений шунтов (см. рис. 10)?

Учитывая формулу (7), можно прийти к выводу, что сопротивление измеряемого резистора Rx зависит от четырёх параметров: от результатов измерений двух напряжений U_{out} и $U_{Rобр}$, от коэффициента усиления ИУ G и номинала $R_{обр}$. Если не учитывать погрешности измерений напряжений U_{out} и $U_{Rобр}$, то остаётся два параметра: G и $R_{обр}$. Как следует из справочного листка на ИУ INA333, типовая (максимальная) погрешность установки коэффициента G при G = 1 составляет 0,01% (0,1%), при G = 10 – 0,05% (0,25%), при G = 100 – 0,07% (0,25%). Установка коэффициента G осуществляется резисторами R6 и R7 (см. рис. 2), имеющими погрешность 0,1%. Сопротивление образцового резистора $R_{обр}$ было измерено более точным прибором с погрешностью около 0,1%. Если принять среднее значение погрешности установки коэффициента G равным $\delta G \approx 0{,}1\%$ и сложить его с погрешностями $\delta(R6/R7) = 0{,}1\%$ и $\delta R_{обр} \approx 0{,}1\%$, то получим, что осреднённая погрешность измерения прибором сопротивления Rx будет равна $\delta Rx = \delta G + \delta(R6/R7) + \delta R_{обр} \approx 0{,}3\%$. Но даже если принять максимальную погрешность $\delta G = 0{,}25\%$, $\delta R_{обр} = 0{,}5\%$ и $\delta(R6/R7) = 0{,}1\%$, то получим $\delta Rx = 0{,}85\%$, т.е. не более 1%, причём во всех трёх диапазонах. На основе приведённых рассуждений можно сделать вывод, что погрешность δRx лежит где-то между 0,3 и 0,85%. Таким образом, результаты (см. рис. 8–10) показывают, что измерения малых сопротивлений прибором достаточно адекватны.

Заключение

В заключение хотелось бы отметить достаточно приличную точность измерения прибором малых сопротивлений. Простота схем и в связи с этим несложная разводка, а также малый размер плат позволили расположить прибор в небольшом корпусе. Кроме того, это определило возможность лёгкого повторения устройства. Стоимость всех комплектующих прибора, по подсчётам автора, не превышает $10.

Литература

1. *Кузьминов А.* Цифровой вольтметр с высоким разрешением. Современная электроника. 2020. № 8–9. 2021. № 1–2.
2. *Кузьминов А. Ю.* Связь между компьютером и микроконтроллером. Современные аппаратные и программные средства. М. Перо. 2018.
3. *Кузьминов А.* Программирование микроконтроллеров EFM8 с помощью встроенного загрузчика программ. Радио. 2018. № 12.

Практика использования встроенного АЦП в ПЛИС семейства MAX10

Часть 3. Цифровой вольтметр/термометр на базе АЦП ПЛИС MAX10

Павел Редькин (г. Ульяновск)

Предлагаемая статья содержит информацию по практическому применению аппаратного модуля АЦП, входящего в состав ПЛИС семейства MAX10 производства Intel (Altera). В третьей части статьи изложенная в предыдущих частях справочная информация иллюстрируется на примере рабочего проекта ПЛИС с АЦП, реализующего функции цифрового вольтметра и цифрового термометра с выводом результатов измерений на индикатор и во внешние устройства.

Функции проекта ПЛИС

Описанный в статье проект ПЛИС, реализующий обслуживание IP-ядра модуля АЦП в ПЛИС, является тестовым. Он разработан для ПЛИС 10M08SAE144C8G из состава отладочной платы Altera MAX10 FPGA. Проект предназначен для исследования АЦП, а также для отладки взаимодействия модуля АЦП в ПЛИС и цифровой части ПЛИС и внешних по отношению к ПЛИС устройств. Вместе с тем этот проект вполне успешно реализует функции цифрового вольтметра и цифрового термометра, используя для реализации последней функции встроенный температурный датчик модуля АЦП в ПЛИС.

Проект ПЛИС в виде архивного файла MAX_10_ADC_1.zip можно загрузить с сайта журнала.

Проект ПЛИС позволяет производить исследование любого из каналов АЦП, однако аппаратно для исследования АЦП больше всего подходит его канал 7, входные цепи которого на отладочной плате Altera MAX10 FPGA снабжены потенциометром для обеспечения возможности регулировки входного измеряемого напряжения АЦП.

В качестве входного измеряемого напряжения для АЦП в ПЛИС можно использовать внешнее постоянное напряжение в диапазоне от 0 до +3,3 В относительно аналогового общего провода (обозначение цепи ⏚ на схеме рисунка 10 во 2-й части статьи), поступающее на вход повторителя напряжения на операционном усилителе (ОУ) U4C с контакта 7 разъёма J4 (цепь Arduino_A6 на схеме рисунка 10). С помощью перемычки в джампере J7 можно альтернативно подать на вход ОУ регулируемое напряжение с движка потенциометра R16. Выход ОУ U4C через фильтрующую RC-цепочку R92, C59 подключён к универсальному входу АЦП в ПЛИС ADCIN7 (канал 7 АЦП). Резистор R84, образующий нижнее плечо предварительного делителя входного напряжения на 2, автор в ходе экспериментов с АЦП из отладочной платы демонтировал. Кроме того, в отладочную плату были внесены следующие доработки:

- удалены элементы R73, C46, подключённые к выделенному входу АЦП ANAIN1 (выводу 3 ПЛИС U2);
- выделенный вход АЦП ANAIN1 (вывод 3 ПЛИС U2) соединён методом навесного монтажа с цепью Arduino_A6 в точке контакта 1 джампера J7.

Проведённые доработки обеспечивают возможность использования в проекте выделенного входа ПЛИС.

Для «ручного» управления режимом и состоянием АЦП в собранном на основе отладочной платы макете предусмотрены кнопки управления SB1...SB6, которые позволяют выбирать канал АЦП для преобразований по кольцу и задавать уровни цифровых сигналов управления АЦП.

Все текущие параметры режима АЦП и результаты преобразований проект ПЛИС отображает на подключённом к ПЛИС ЖКИ: состояние АЦП (включено/отключено) «VAL_ADC=ON/OFF», запуск/останов АЦП «ADC=Pusk/Stop», выбранный для преобразований канал АЦП «CHAN=xx», где xx – номер канала в диапазоне от 0 до 20, текущий результат АЦП в битах и милливольтах «ADC_OUT=yyyy bit» и «U=zzzz mV», значение температуры кристалла ПЛИС со знаком в °C «T= mmmm C» в случае, если для преобразований выбран канал встроенного температурного датчика TSD (канал 17). Обновление показаний ЖКИ осуществляется каждые 0,5 с. Никакого усреднения результатов АЦП для вывода на индикацию в проекте ПЛИС не производится: на индикацию поступает просто каждый пятисоттысячный результат при измерении внешнего напряжения или каждый двадцатипятитысячный – при измерении температуры.

Текущее состояние сигналов command_startofpacket_ADC и command_endofpacket_ADC, с помощью которых осуществляются запуск и останов АЦП, помимо индикации на ЖКИ («ADC=Pusk/Stop») дублируется штатными светодиодами отладочной платы D5 и D4 соответственно. Свечение светодиода указывает на высокий (активный) уровень соответствующего сигнала. Светодиод D1 используется для индикации секундного ритма.

Для выдачи результатов АЦП в проекте ПЛИС одновременно используются три способа: индикация результата АЦП на ЖКИ в битах, милливольтах и °C (последнее только в случае выбора для преобразований канала 17 температурного датчика TSD), выдача результата АЦП из ПЛИС в параллельном виде в битах, выдача результата АЦП из ПЛИС в последовательном виде в битах. Выдача результатов АЦП в параллельном и последовательном виде реализована для обеспечения возможности детального, в том числе статистического, исследования АЦП, поскольку через эти интерфейсы выдаётся результат каждой производимой АЦП выборки. Индикация результата АЦП на ЖКИ реализована в проекте ПЛИС для обеспечения общей визуальной оценки АЦП.

Структура проекта ПЛИС

Исходные коды проекта ПЛИС написаны на языке описания аппаратных

средств Verilog HDL. Структурно проект ПЛИС состоит из исходного файла модуля верхнего уровня MAX_10_ADC_1.v и нескольких исходных файлов модулей более низкого уровня: файла модуля обслуживания ЖКИ 12864ZW LCD_12864.v, файла модуля формирования единичного импульса разрешения звука от нажатия кнопки buzzer_butt.v, файла модуля фильтра дребезга контактов кнопки noise_filter_butt.v, файла модуля выдачи результата АЦП в последовательном виде ADC_rezult_serial.v, файла модуля преобразования выходного кода АЦП в значение температуры в °С со знаком Code_Temper_conv.v, а также двух файлов, сгенерированных в ходе создания проекта инструментом Qsys: файла IP-ядра модуля АЦП ADC_Core_1.qip, файла IP-ядра модуля PLL ALTPLL1.qip, каждый с исходными файлами более низкого уровня. Полная файловая структура проекта ПЛИС показана на рисунке 24 (2-я часть статьи). Проект занимает около 1/3 ресурсов ПЛИС 10M08SAE144C8G по логике и около 1/2 – по линиям ввода-вывода.

В модуле верхнего уровня реализована главная функция проекта ПЛИС – осуществление аналого-цифровых преобразований, а также несколько сервисных функций: опрос кнопок управления, задание значений управляющих сигналов АЦП по результатам этого опроса, вывод текущих настроек АЦП и результатов преобразований на ЖКИ, вывод результатов преобразований через цифровые интерфейсы, генерация внутренних синхросигналов, генерация звуковых сигналов, управление светодиодами.

Выбор канала АЦП для преобразований осуществляется кнопкой SB4 по кольцу от 0 до 20.

Кнопкой SB1 можно управлять значением сигнала command_valid_ADC по кольцу, то есть каждое нажатие на кнопку приводит к инверсии текущего значения сигнала. Сигнал command_valid_ADC, по сути, задаёт состояние АЦП: включено или отключено. Опытным путём было установлено, что выбор канала для преобразований всегда нужно производить при отключённом АЦП, то есть при низком уровне сигнала command_valid_ADC. В противном случае возможны сбои в установлении частоты синхросигнала АЦП. Так, вместо синхросигнала с частотой 50 кГц, автоматически генерируемого IP-ядром АЦП при выборе канала встроенного температурного датчика TSD, может ошибочно генерироваться синхросигнал с большей в несколько раз частотой.

Листинг 5

```
// Фиксация результата АЦП по фронту сигнала
// готовности результата АЦП  command_ready_ADC
// при условии активного уровня сигнала
// валидности из АЦП response_valid_ADC
always @(posedge command_ready_ADC)
begin
  if (response_valid_ADC)
        begin
                rezult_ADC <= dout_ADC;
        end
end
```

Листинг 6

```
parameter  U_ref_mV = 3300;  // опорное напряжение АЦП в милливольтах
                             // для пересчета результата АЦП в мВ
// умножение результата АЦП в битах на опорное напряжение в милливольтах,
    // чтобы получить результат в милливольтах
     rezult_ADC_U_ref <= rezult_ADC * U_ref_mV;

    // деление результата умножения на  2**12,
    // что эквивалентно лог сдвигу вправо на 12 разрядов
         rezult_ADC_mV <= (rezult_ADC_U_ref >> 12);

     rezult_ADC_mV_tis <= rezult_ADC_mV / 1000;
     Temp2_data <= rezult_ADC_mV % 1000;
     rezult_ADC_mV_sot <= Temp2_data / 100;
     Temp3_data <= Temp2_data % 100;
     rezult_ADC_mV_des <= Temp3_data / 10;
     rezult_ADC_mV_ed <= Temp3_data % 10;
```

Кнопки SB2, SB3 управляют по кольцу значениями сигналов command_startofpacket_ADC, command_endofpacket_ADC соответственно. Однако поскольку в проекте ПЛИС мы используем IP-ядро АЦП без программы упорядочения (sequencer), значения указанных сигналов не должны никак влиять на ход преобразований. В нашем проекте преобразования автоматически запускаются только при установке сигнала command_valid_ADC и останавливаются только при сбросе этого сигнала. Значения сигналов command_startofpacket_ADC, command_endofpacket_ADC при этом могут быть произвольными, управление ими в текущей версии проекта ПЛИС реализовано для будущих версий.

Кнопки SB5, SB6 в текущей версии проекта ПЛИС не используются, они зарезервированы для будущих версий.

Все кнопки SB1-SB6 работают на замыкание между цифровым входом ПЛИС и цифровым общим проводом. В проекте ПЛИС задана подтяжка всех цифровых входов подключения кнопок к плюсу питания внутренними резисторами. Дребезг при нажатии на кнопки устраняется в проекте ПЛИС с помощью модуля фильтра дребезга контактов кнопки noise_filter_butt.v.

Аналого-цифровые преобразования при выборе любого канала, кроме канала встроенного температурного датчика TSD (канал 17), и установке сигнала command_valid_ADC осуществляются циклически, в автоматическом режиме с частотой выборок 1 МГц. При осуществлении выборок от TSD в канале 17 преобразования также осуществляются циклически, в автоматическом режиме, но уже с частотой 50 кГц. При осуществлении преобразований в любом канале фиксация результата АЦП производится по фронту сигнала готовности результата АЦП command_ready_ADC, поступающего из IP-ядра АЦП, при условии, что также поступающий из IP-ядра АЦП возвратный сигнал валидности результата АЦП response_valid_ADC находится на активном (высоком) уровне. Указанное действие реализуется с помощью языковой конструкции модуля, приведённой в листинге 5. В этом модуле dout_ADC – это 12-разрядная цепь (wire) выходов данных IP-ядра АЦП, а rezult_ADC – 12-разрядный регистр (reg) хранения текущего результата преобразования. Зафиксированное при каждом преобразовании в регистре rezult_ADC значение используется для дальнейшей обработки.

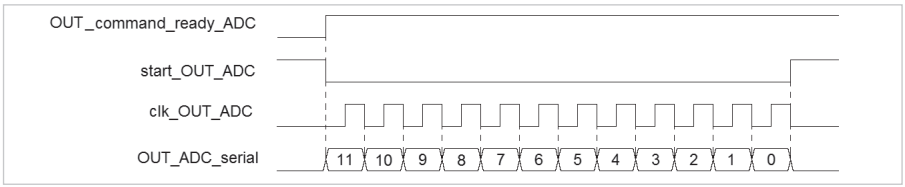


Рис. 29. Формат последовательной выдачи результата АЦП из ПЛИС

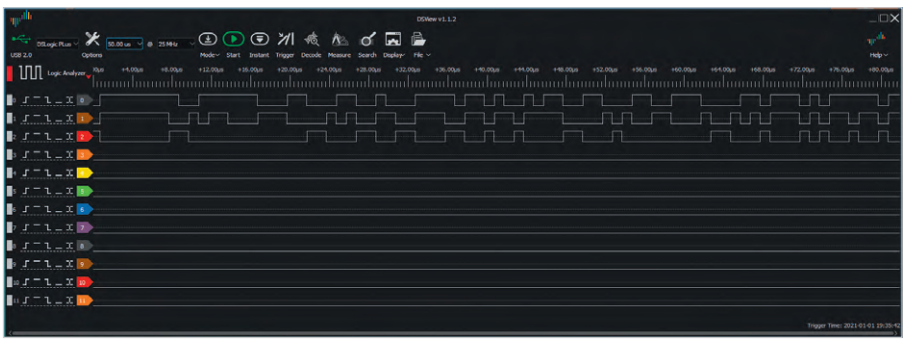


Рис. 30. Результаты АЦП для универсального входа ПЛИС на интервале 50 мкс для нулевого входного сигнала

Для пересчёта результата преобразования из битов в милливольты с последующим его преобразованием из двоичного в двоично-десятичное представление в проекте ПЛИС используется языковая конструкция, приведённая в листинге 6. В качестве исходных данных для пересчёта и преобразования представления здесь используется содержимое регистра rezult_ADC.

Для повышения точности преобразований значение parameter U_ref_mV, в авторском варианте проекта равное 3300, может быть скорректировано, исходя из конкретного значения напряжения опорного напряжения АЦП в милливольтах.

Выдача результата АЦП в последовательном виде во внешние устройства реализована с помощью модуля нижнего уровня, исходный текст которого содержится в файле ADC_rezult_serial.v. Формат последовательной выдачи в проекте ПЛИС в общих чертах воспроизводит распространённый формат SPI режима 0 (бит полярности SPOL = 0, бит комбинации фазы SPHA = 0). При этом ПЛИС является ведущим (master) устройством на шине и генерирует опорный синхросигнал. Сигнал принимаемых данных MISO в последовательном интерфейсе отсутствует, поскольку АЦП в ПЛИС не принимает извне никаких данных, сигналу передаваемых данных MOSI в проекте ПЛИС соответствует выход OUT_ADC_serial, сигналу синхронизации SCLK в проекте ПЛИС соответствует выход clk_OUT_ADC с частотой 25 МГц, сигналу выбора ведомого устройства /SS в проекте ПЛИС соответствует выход start_OUT_ADC. Однократная последовательная выдача 12-разрядного слова результата АЦП производится по каждому положительному фронту сигнала готовности результата АЦП OUT_command_ready_ADC, который представляет собой копию сигнала command_ready_ADC, выведенную из ПЛИС.

Временные диаграммы формата последовательной выдачи показаны на рисунке 29.

Параллельная выдача результата АЦП в проекте ПЛИС реализована в виде 12-разрядной параллельной выходной шины OUT_rezult_ADC_bus, слово данных на которой обновляется по каждому положительному фронту сигнала готовности результата АЦП OUT_command_ready_ADC. В качестве исходных данных для обновления шины здесь используется содержимое регистра rezult_ADC.

Преобразование выходного кода АЦП в значение температуры в °C со знаком реализована в проекте ПЛИС с помощью модуля нижнего уровня, исходный текст которого содержится в файле Code_Temper_conv.v. В основе модуля лежит таблица соответствия температуры выходному коду АЦП от температурного датчика TSD, взятая из [1, Table 4]. Каждому значению аргумента – 12-разрядного выходного кода АЦП code_ADC – в таблице сопоставлено пять 8-разрядных значений: двоичное значение модуля температуры в °C temper_mod_C, двоичное значение сотен модуля температуры в °C temper_mod_sot_C, двоичное значение десятков модуля температуры в °C temper_mod_des_C, двоичное значение единиц модуля температуры в °C temper_mod_ed_C, двоичное значение знака температуры temper_znak_C. Такой подход позволяет избежать необходимости дополнительного преобразования в проекте ПЛИС из двоичного в двоично-десятичное представление. Выдаваемые модулем Code_Temper_conv.v значения сотен, десятков и единиц модуля температуры и знака температуры поступают на индикацию после преобразования в модуле верхнего уровня в ASCII-формат, которое заключается в прибавлении к каждому байту десятичного числа 48.

Модуль обслуживания ЖКИ, исходный текст которого содержится в файле LCD_12864.v, сразу после включения питания ПЛИС производит аппаратный сброс подключённого к ПЛИС ЖКИ 12864ZW (длительность сброса 0,2 с, задаётся константой VALUE_END_RESET), начальную инициализацию ЖКИ, затем в течение 3 с на ЖКИ выводится начальная заставка, содержащая информацию о проекте ПЛИС и его версии. Время вывода начальной заставки задаётся константой VALUE_END_BOOT. После окончания индикации заставки начинает производиться циклический последовательный вывод на индикацию четырёх групп 8-разрядных регистров знакомест: data_LCD1_0_reg – data_LCD1_15_reg, data_LCD2_0_reg – data_LCD2_15_reg, data_LCD3_0_reg – data_LCD3_15_reg, data_LCD4_0_reg – data_LCD4_15_reg. Каждая группа включает по 16 регистров (по числу символов в строке ЖКИ) и соответствует одной строке ЖКИ (всего четыре строки: 1...4). Содержимое всех регистров обновляется одновременно в начале каждого цикла индикации содержимым соответствующих им 8-разрядных входов модуля обслуживания ЖКИ: data_LCD1_0 – data_LCD1_15, data_LCD2_0 – data_LCD2_15, data_LCD3_0 – data_LCD3_15, data_LCD4_0 – data_LCD4_15. На этих входах модуль верхнего уровня выставляет данные в произвольные моменты времени, поскольку разными входами в модуле верхнего уровня управляют разные цифровые автоматы. Цикл индикации (интервал обновления информации на ЖКИ) равен 0,5 с (задаётся константой VALUE_ZIKL). Синхронизация модуля обслуживания ЖКИ осуществляется внутренним синхросигналом с частотой 1кГц, поступающим из модуля верхнего уровня.

Помимо информационных сигналов проект ПЛИС выдаёт на выводы ПЛИС несколько контрольных и технологических сигналов: контрольный сигнал с выхода PLL sys_pll_control, сигнал возврата IP-ядром валидности АЦП OUT_response_valid_adc, сигнал возврата IP-ядром запуска преобразований OUT_response_startofpacket_adc, сигнал возврата IP-ядром останова преобразований OUT_response_endofpacket_adc.

Исследование измерителя напряжения в ПЛИС

Для исследования модуля АЦП с помощью вышеописанного проекта ПЛИС использовался многоканальный логический анализатор, описание которого можно загрузить по ссылке [2], а ПО поддержки – по ссылке [3].

Для грубой оценки количества эффективных разрядов АЦП, то есть таких, которые кодируют собственно входной сигнал, а не внутренние шумы АЦП, соединяем накоротко вход внешней аналоговой цепи выбранного канала АЦП № 7 (контакт J4-7) с аналоговым общим проводом, затем задаём канал 7 в качестве активного и запускаем преобразования. Снятая через параллельный интерфейс с помощью логического анализатора последовательность результатов АЦП для входных выборок 1 MSPS на интервале времени 50 мкс показана на рисунке 30. Как можно видеть из рисунка, младшие три разряда выходного кода АЦП при нулевом напряжении на аналоговом входе дают хаотические всплески единиц, не привязанные по времени ни к каким периодическим сигналам, кроме внутреннего синхросигнала модуля АЦП (1 МГц). Эти всплески отражают влияние на результат преобразования внутренних шумов АЦП. При напряжении полной шкалы 3300 мВ цена младшего значащего разряда АЦП (MSP, разряд 0) составляет 0,805 мВ, разряда 1 – 1,61 мВ, разряда 2 – 3,22 мВ. Следовательно, максимальная величина всплесков в пересчёте на эквивалентный уровень напряжения при одновременно единичных трёх младших разрядах может составлять до 5,635 мВ.

Аналогичная оценка для канала 0 (выделенный вход АЦП) даёт результат, показанный на рисунке 31. Единичные всплески в разряде 2 здесь происходят реже, чем в предыдущем случае, но также имеют место. Очевидно, в канале 7 шума во входной сигнал добавляет буферный ОУ, который в плане шумовых свойств вовсе не является прецизионным.Таким образом, как для выделенного, так и для универсального входов АЦП по результатам грубой оценки имеем только девять эффективных разрядов. Шумовые свойства АЦП ПЛИС семейства MAX10 на практике оставляют желать лучшего.

Таблица 11. Результаты оценки ошибок смещения нуля и усиления АЦП

Характеристика входного напряжения	Показания ЖКИ макета, мВ	Показания контрольного вольтметра, мВ	Модуль разности показаний, мВ	Доля разности показаний от полной шкалы, %	Примечание
Канал 0 АЦП (выделенный вход АЦП в ПЛИС)					
Нулевое напряжение – замыкание входа АЦП на общий провод	1	–0,2	1,2	0,037	Ошибка смещения нуля
Точка в районе середины шкалы	1703	1700,7	2,3	0,069	Ошибка усиления в середине шкалы
Точка в районе максимума шкалы	3258	3259,3	1,3	0,039	Ошибка усиления у максимума шкалы

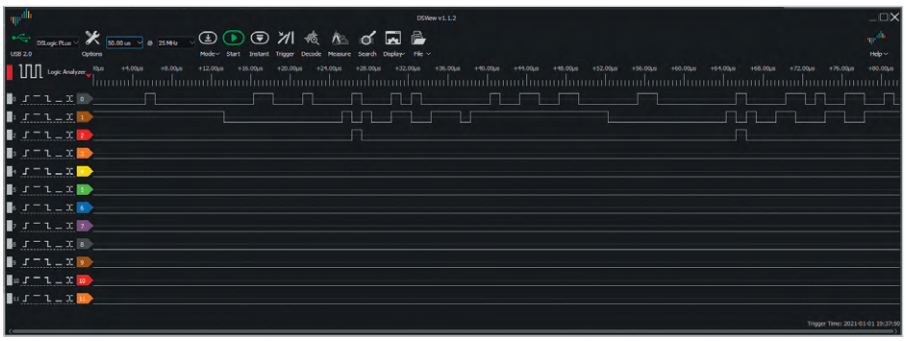


Рис. 31. Результаты АЦП для выделенного входа ПЛИС на интервале 50 мкс для нулевого входного сигнала

Для оценки ошибок смещения нуля и усиления АЦП были произведены измерения напряжения на входе внешней аналоговой цепи выбранного канала 0 АЦП (вывод 3 ПЛИС U2) в нескольких точках в пределах полной шкалы (0...+3,3 В) с помощью контрольного эталонного вольтметра-мультиметра производства RIGOL модели DM3058E, имеющего разрешение $5\frac{1}{2}$ разряда на пределе измерения напряжения 20 В постоянного тока (паспортная погрешность измерений не более 0,02%). Полученные результаты измерений вместе с результатами АЦП, взятыми из показаний ЖКИ макета, приведены в таблице 11. Как можно видеть из таблицы 11, ошибки смещения нуля и усиления в середине и в районе максимума шкалы вполне укладываются в пределы, указанные в таблице 2 (часть 1). Однако из-за внутренних шумов АЦП индицируемые на ЖКИ результаты АЦП постоянно «прыгают» в пределах нескольких милливольт, что затрудняет корректную оценку ошибок смещения нуля и усиления.

По результатам проведённых оценочных исследований можно сделать вывод, что параметры АЦП в ПЛИС семейства MAX10 являются довольно средними как в плане точности, так и в плане скорости. Модуль АЦП в ПЛИС семейства MAX10 по своим характеристикам примерно соответствует 12-разрядными АЦП в большинстве микроконтроллерных семейств. Применение АЦП в ПЛИС MAX10 можно рекомендовать для приложений, не требующих большой точности и скорости: контроль питающих напряжений, оцифровка узкополосных сигналов с неприцизионных датчиков, оцифровка звука со средним качеством и т.п. Для высокоскоростных и высокоточных приложений АЦП в ПЛИС MAX10 рекомендован быть не может.

Оценочное исследование измерителя температуры, выполненного на основе встроенного температурного датчика TSD, показало, что при положительной температуре данный измеритель даёт ошибку порядка 5...7°C, что, впрочем, вполне укладывается в пределы, указанные в таблице 2 (часть 1).

Литература

1. Intel® MAX® 10 Analog to Digital Converter User Guide. Updated for Intel® Quartus® Prime Design Suite: 19.1/ UG-M10ADC | 2020.03.17. https://www.intel.com/content/dam/www/programmable/us/en/pdfs/literature/hb/max-10/ug_m10_adc.pdf.
2. DSLogic Plus USB-based Logic Analyzer. https://www.dreamsourcelab.com/doc/DSLogic_Plus_Datasheet.pdf.
3. https://www.dreamsourcelab.com/download/.

О некоторых особенностях формирования межчастотного корреляционного признака

Владимир Бартенев (bartvg@rambler.ru)

Рассматривается задача классификации объектов в РЛС по их продольному размеру на основе межчастотного корреляционного признака. Оптимальный для этой задачи классификатор строится на основе оценки максимального правдоподобия модуля межчастотного коэффициента корреляции, сравниваемого с порогом. Однако есть два способа формирования этой оценки: с использованием независимых выборок наблюдений от обзора к обзору и коррелированных выборок от импульса к импульсу в одном обзоре. Об особенностях такого формирования межчастотного корреляционного признака и пойдёт речь в этой статье.

В работах [1, 2, 3] показано, что для классификации отражённых сигналов обнаруженных объектов по их продольному размеру можно использовать характер флюктуаций отражённых сигналов на разных несущих частотах. В частности, в основе этого сигнального признака классификации лежит взаимосвязь значения нормированного межчастотного коэффициента корреляции с линейными размерами объекта: чем больше размер объекта, тем меньше межчастотный коэффициент корреляции.

Для того чтобы сформировать межчастотный коэффициент корреляции, используют наиболее эффективный алгоритм в виде оценки модуля максимального правдоподобия (ОМП) межчастотного коэффициента корреляции, которая выполняется в соответствии с формулой (1) [2].

Где $\hat{R}$ – оценка модуля межчастотного коэффициента корреляции, т.е. число накоплений по независимым выборкам наблюдения, например обзорам РЛС. $Z1_j = x1_j + iy1_j, Z2_j = x2_j + iy2_j$ в (1) – комплексные выборки классифицируемых эхо-сигналов на входе в двух частотных каналах. Квадратурные компоненты классифицируемых флюктуирующих сигналов имеют нормальное распределение, при этом без уменьшения общности подхода, так как данный алгоритм нечувствителен к изменению мощности сигналов мешающих отражений, дисперсия их равняется единице и среднее – нулю.

$$\hat{R}(\Delta F) = \left| \sum_{j=1}^{N} Z1_j * Z2_j^* \right) / \left(\sum_{j=1}^{N} Z1_j * Z1_j^* \right) * \left(\sum_{j=1}^{N} Z2_j * Z2_j^* \right) \Big| = \frac{\sqrt{\left(\sum_{j=1}^{N} x1j * x2_j + y1_j * y2_j \right)^2 + \left(\sum_{j=1}^{N} x2_j * y1_j - x1_j * y2_j \right)^2}}{\sqrt{\left(\sum_{j=1}^{N} x1_j * x2_j + y1_j * y1_j \right)^2 + \left(\sum_{j=1}^{N} x2_j * y2_j - x2_j * y2_j \right)^2}} \quad (1)$$

$$\hat{R}(\Delta F) \le R_{\text{пор}} \quad (2)$$

$$\hat{W}(\hat{R}) = 2(N-1)(1-\hat{R}^2)^{N-2} \hat{R} (1-\hat{R}^2)^N \sum_{k=0}^{N-1} \frac{(\hat{R}\hat{R})^{2k} \Gamma(N+k)}{(1-\hat{R}^2)^{N+k} \Gamma(N-k) \Gamma^2(k+1)} \quad (3)$$

$$W(\hat{R}) = 2(\hat{R})(1-\hat{R}^2)^{N-2}(N-1) \quad (4)$$

$$P(R_{пор}) = 1 - (1 - R_{пор}^2)^{N-1} \quad (5)$$

Решение о том, что классифицируемый объект протяжённый принимается, если (2).

Проиллюстрируем работу предлагаемого способа на конкретном примере, прибегнув как к аналитическому расчёту, так и к моделированию с помощью системы MATLAB [4].

Осуществим классификацию протяжённого объекта, используя две выборки наблюдений с межчастотным коэффициентом корреляции, равным 0. Корреляционный порог в расчётах будем менять от 0,1 до 0,9. Независимое число накоплений N возьмём равным 8 и 16.

Для нахождения вероятности правильной классификации протяжённого объекта по непревышению оценкой порога нужно воспользоваться распределением Уишарта. В работе [3] получено распределение (3), где Г() – гамма функция.

Для протяжённых объектов с = 0 и распределение (3) можно представить в более простом виде (4).

Используя (4), можно получить формулу для вероятности правильной классификации протяжённых объектов как вероятность непревышения порога (5).

Для верификации данной формулы было проведено моделирование с помощью системы MATLAB [4] классификатора ОМП с расчётом для разных значений порога $R_{пор}$ и N =16 и 32 (см. рис. 1 и 2 соответственно).

Результаты моделирования хорошо совпадают с аналитическими расчётами (см. рис. 1 и 2).

Все вышеприведённые исследования выполнены для независимых выборок наблюдений и получены, например, принимая отражённые сигналы от обзора к обзору РЛС. Однако представляет интерес и другой способ формирования модуля межчастотного коэффициента корреляции, когда обрабатываются сигналы в виде коррелированной пачки импульсов на каждой частоте в одном обзоре.

К сожалению, аналитически рассчитать вероятность правильной классификации протяжённого объекта в этом

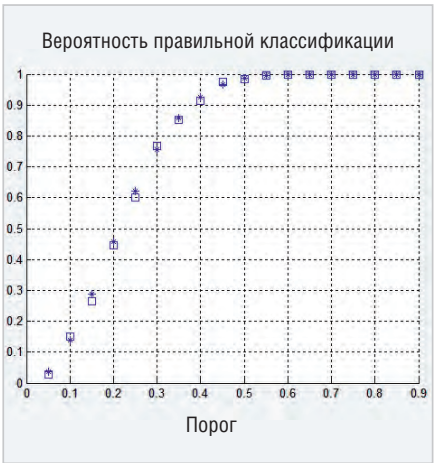


Рис. 1. Зависимость вероятности правильной классификации протяжённых объектов от порога $R_{пор}$ для N = 16 в классификаторе ОМП (звёздочки – аналитика, квадраты – моделирование)

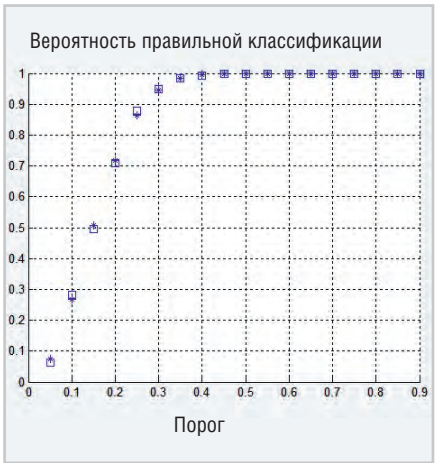


Рис. 2. Зависимость вероятности правильной классификации протяжённых объектов от порога $R_{пор}$ для N = 32 в классификаторе ОМП (звёздочки – аналитика, квадраты – моделирование)

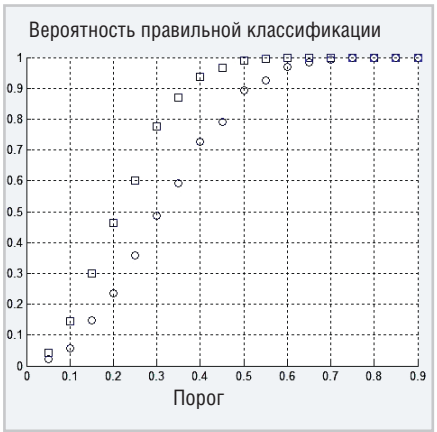


Рис. 3. Зависимость вероятности правильной классификации протяжённых объектов от порога $R_{пор}$ для N = 16 в классификаторе ОМП для коррелированных выборок наблюдений с межпериодным коэффициентом корреляции 0 (квадраты) и 0,7 (кружки)

Рис. 4. Зависимость вероятности правильной классификации протяжённых объектов от порога $R_{пор}$ для N = 16 в классификаторе ОМП для коррелированных выборок наблюдений с межпериодным коэффициентом корреляции 0 (квадраты) и 0,9 (кружки)

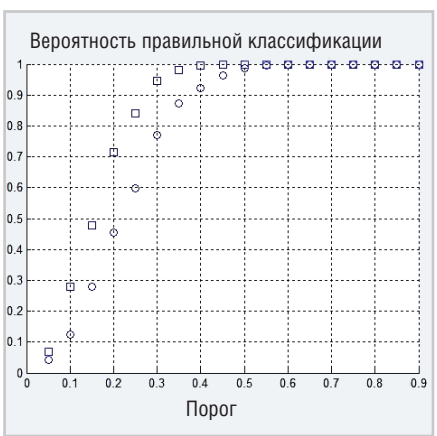


Рис. 5. Зависимость вероятности правильной классификации протяжённых объектов от порога $R_{пор}$ для N = 32 в классификаторе ОМП для коррелированных выборок наблюдений с межпериодным коэффициентом корреляции 0 (квадраты) и 0,7 (кружки)

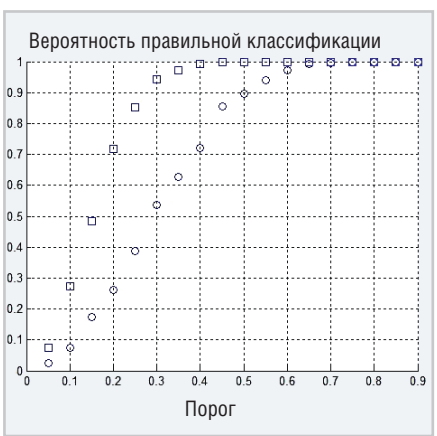


Рис. 6. Зависимость вероятности правильной классификации протяжённых объектов от порога $R_{пор}$ для N = 32 в классификаторе ОМП для коррелированных выборок наблюдений с межпериодным коэффициентом корреляции 0 (квадраты) и 0,9 (кружки)

случае не представляется возможным, и результаты были получены только моделированием в MATLAB. Для этого использовалась модель отражённых сигналов на каждой частоте в виде коррелированной пачки импульсов с нормально распределёнными квадратурными составляющими и имеющих корреляционную функцию гауссовой формы. Межпериодный коэффициент корреляции задавался 0,7 и 0,9, для числа импульсов в пачке – 16 и 32. Результаты моделирования представлены на рис. 3–6.

Таким образом, проведённое исследование полностью подтверждает положительный эффект от применения предложенного способа для классификации протяжённых объектов с использованием межчастотного корреляционного признака. Например, для независимых выборок наблюдения при N=16 для порога, равного 0,5, обеспечивается вероятность правильной классификации 0,99. Коррелированность же выборок наблюдения заметно снижает эффективность классификации. Так, при тех же 16 выборках наблюдений, но коррелированных с межпериодным коэффициентом корреляции 0,7, вероятность правильной классификации для порога 0,5 равна 0,9, а для межпериодного коэффициента корреляции 0,9 – около 0,7. Повысить эффективность классификации для коррелированных выборок можно или их декорреляцией, или увеличением их числа. Так для 32 коррелированных выборок с межпериодным коэффициентом корреляции 0,9 вероятность правильной классификации для порога 0,5 равна 0,9.

Литература

1. *Bartenev V.* Radar objects classification using inter frequency correlation coefficient. Report on the International conference RADAR 2016. China, Oct. 2016
2. *Бартенев В.Г.* Патент «Способ классификации и бланкирования дискретных помех» № 2710894, Опубликован: 14.01.2020, Бюл. № 2.
3. *Бартенев В.Г.* О распределении оценки модуля коэффициента корреляции// Современная электроника, 2020. № 8,
4. *Потемкин В.Г.* “Справочник по MATLAB” Анализ и обработка данных. http://matlab.exponenta.ru/ml/book2/chapter8/.

Современный подход к измерению импульсных радиопомех с использованием амплитудно-вероятностного распределения

Дмитрий Богаченков (dmitry.bogachenkov@rohde-schwarz.com),
Николай Лемешко (nlem83@mail.ru)

В статье рассматривается современный подход к определению характеристик импульсных радиопомех с использованием амплитудно-вероятностного распределения. Рассмотрены источники помех с нестационарными спектрально-энергетическими характеристиками, проанализированы требования стандартов к средствам измерений, имеющим функцию построения амплитудно-вероятностного распределения. Рассмотрены схемы установок для измерений амплитудно-вероятностного распределения. В качестве примера рассмотрены новые возможности измерительных приёмников Rohde&Schwarz ESW, позволяющих значительно ускорить испытания на эмиссию излучаемых радиопомех для оборудования некоторых типов.

Введение

В настоящее время проблема электромагнитной совместимости (ЭМС) является одной из важнейших в радиоэлектронике. Этому способствовали следующие факторы:

- повышение пространственной насыщенности, из-за чего электронные устройства, существенно разнящиеся по функциональности, типу обрабатываемых сигналов и другим характеристикам располагаются всё ближе друг к другу;
- расширение полосы помехоэмиссии за счёт увеличения тактовых и других характерных частот;
- снижение мощности полезных сигналов за счёт совершенствования компонентной базы и перехода к более низким технологическим нормам.

Одновременно видоизменяется и само содержание практических задач обеспечения электромагнитной совместимости. В простейшем случае электромагнитная обстановка (ЭМО), в которой работают технические средства (ТС), является стационарной и характеризуется регулярными спектральными составляющими, в совокупности которых можно выделить узкополосные и шумовые составляющие [1]. При формировании ЭМО всегда можно выделить несколько источников излучений, определяющих уровень эмиссии на заданной частоте. Если картина помехоэмиссиии от некоторого устройства неизменна во времени, то она может быть полностью охарактеризована наиболее простым способом, например пиковыми или средними значениями напряжённости поля, измеренными в регламентированных условиях.

Однако в общей совокупности эксплуатируемых электронных устройств лишь небольшая их доля формирует электромагнитные излучения со строго стационарными характеристиками. Такие устройства, как радары с импульсным излучением, СВЧ-печи на основе магнетронов с нестабилизированной частотой, характеризуются широким диапазонам весьма динамичного изменения помехоэмиссии, для которого отмеченные выше характеристики не дают исчерпывающего её описания. Для исправления такой ситуации в теории ЭМС было введено понятие амплитудно-вероятностного распределения (АВР) радиопомех – распределения вероятности времени, в течение которого амплитуда помехи превышает установленный уровень [2].

Для измерений радиопомех с нестационарными спектрально-энергетическими характеристиками должны использоваться приборы, которые позволяют оценивать их амплитудно-вероятностное распределение. При этом наиболее важно проводить такие исследования для тех ТС, которые могут создавать помехи системам связи с цифровыми видами модуляции. Это обусловлено тем, что для них воздействие помех с нестационарными спектрально-энергетическими характеристики сопровождается увеличением минимально допустимых защитных отношений, что должно учитываться, в частности, при частотном планировании радиосетей и решении практических задач межсистемной ЭМС. Так, например, экспериментальные исследования, проведённые для сигналов DVB-T2 при воздействии узкополосных помех, показали, что при некоторых скоростях смещения по частоте в пределах занимаемой полезным сигналом полосы частот защитные отношения требуют увеличения на 12...15 дБ [3].

Учитывая практическую важность вопроса, рассмотрим некоторые аспекты измерений импульсных радиопомех с использованием АВР.

Типовые источники помех с нестационарными спектрально-энергетическими характеристиками

Электромагнитная обстановка в некоторой области пространства для заданной полосы частот обычно определяется несколькими источниками излучений. Если среди них имеется хотя бы один, отличающийся нестационарными спектрально-энергетическими характеристиками, то вся ЭМО приобретает характер нестационарной. Типовыми источниками помех с такими свойствами являются:

1. устройства генерации высокочастотных колебаний на основе магнетронов, работающих в нестабилизированном режиме. Типичным ТС этой группы являются СВЧ-печи бытового и промышленного назначения, излучение которых наиболее часто соответствует несущей, модулированной по частоте суммой нескольких гармоник. Для таких устройств отношение полосы излучения к его центральной частоте обычно лежит в интервале 5...20%;
2. передатчики радиолокационных станций (РЛС), использующие режим импульсного излучения [4]. При наличии кругового обзора его периодичность оказывает влияние на АВР

и должна учитываться при измерениях;

3. средства радиосвязи, в которых используется псевдослучайная перестройка рабочей частоты (ППРЧ), например для обеспечения скрытности передачи информации. Периодичность перестройки частоты обычно лежит в интервале от 0,1 до 10 мс [5], и быстродействие средств измерений АВР радиопомех оказывается достаточным для осуществления такого анализа;
4. средства радиосвязи, применяющие автоматическое управление несущей частотой для повышения качества передачи данных, например в условиях сложной электромагнитной обстановки [6];
5. любые другие ТС для генерации и обработки радиосигналов с выраженной цикличностью функционирования.

Среди перечисленных имеются технические средства, формирующие импульсные помехи с периодичностью около 1 с. К этой категории могут относиться, например, некоторые типы РЛС. При этом результаты измерений фактически не зависят от частоты повторения импульсов. Известно [2, 7], что для точных измерений одиночных и редко повторяющихся импульсов измерительные приёмники должны обладать большим запасом по линейности трактов, для которых требуемый коэффициент перегрузки превышает 40 дБ. Столь значимые требования приводят к увеличению стоимости измерительных приёмников и в целом технически трудно реализуемы. Применение АВР для анализа редко повторяющихся импульсных помех способно дать значительно более полное их описание.

Источники помех с нестационарными спектрально-энергетическими характеристиками могут характеризоваться наличием выраженных узкополосных спектральных составляющих (УСС) либо их отсутствием. Если в совокупной картине помехоэмиссии присутствуют УСС, то можно говорить об одном из трёх видов их изменчивости:

- частоты УСС постоянны, а их амплитуды изменяются;
- амплитуды УСС постоянны, частоты варьируются;
- изменяются и частоты, и амплитуды УСС.

Если же в спектре помехоэмиссии УСС отсутствуют, то такую классификацию нестационарности спектрально-энергетических характеристик использовать нельзя. В то же время АВР является универсальным способом представления информации о характере распределения амплитуд помех, не привязанным к конкретным их типам.

Требования стандартов к функциональности средств измерений с определением АВР радиопомех

В отечественной нормативно-технической базе требования к средствам измерений, имеющим функцию определения АВР, установлены стандартами [2, 7]. Они предписывают выполнять измерения АВР радиопомех в диапазоне частот от 1 до 18 ГГц, но допускают возможность использования такого анализа радиопомех и на более низких частотах. АВР измеряют для одной или нескольких частот в этом диапазоне, для градации амплитуд используют те же единицы, которые применяются для указания уровней помехоэмиссии. При этом определение АВР рассматривается

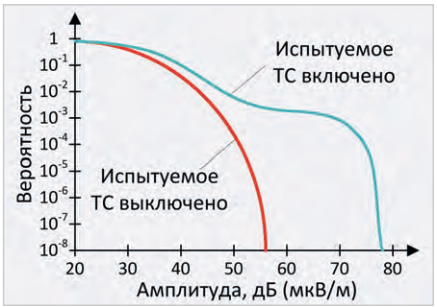


Рис. 1. Типовой вид АВР для собственных шумов средства измерений и помех, формируемых испытуемым ТС

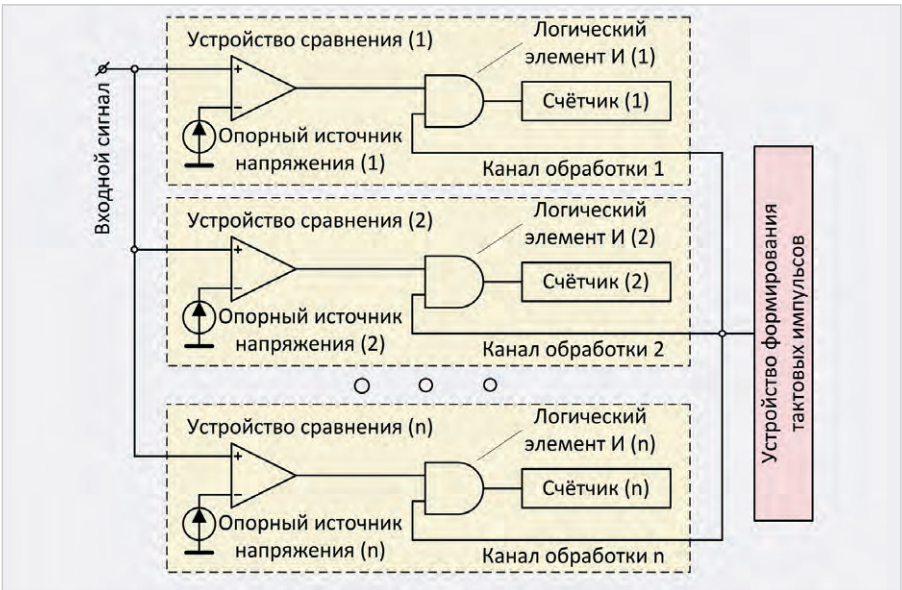


Рис. 2. Блок-схема устройства измерения АВР без АЦП

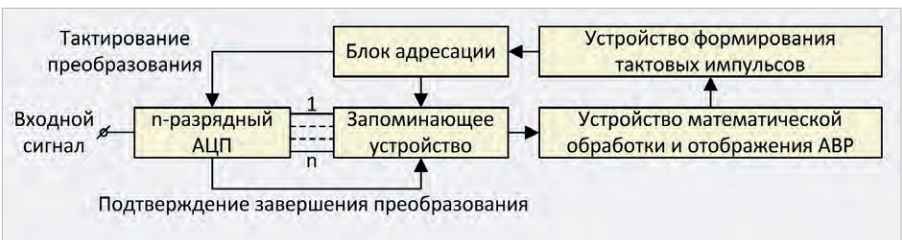


Рис. 3. Блок-схема устройства измерения АВР с использованием АЦП

как вспомогательная функция средств измерений. Для определения АВР обычно используется сигнал с детектора огибающей, характеризующий текущее значение уровня радиопомех.

Средство измерений в режиме определения АВР должно иметь динамический диапазон амплитуд свыше 60 дБ при точности определения амплитуд не хуже 2,7 дБ и минимальном значении измеряемой вероятности 10^{-7}. Максимальное время измерения помехи должно составлять не менее 120 с для обеспечения достоверности построения вероятностного распределения. Измерение прерывистых помех допускается проводить, если фактическое время нечувствительности прибора составляет менее 1% всего времени измерения. Измерение АВР должно проводиться при не менее чем двух уровнях амплитуды, причём вероятности, соответствующие всем предварительно выбранным уровням, должны определяться одновременно.

Разрешение при предварительном выборе амплитуд должно быть не ниже 0,25 дБ, скорость выборки — не менее 10 млн отсчётов/с при полосе разрешения 1 МГц. При использовании схем измерений с аналого-цифровым преобразователем (АЦП) рекомендуется использовать средства отображения информации с разрешением по амплитуде менее 0,25 дБ, количество амплитудных уровней для отображения зависит от разрешающей способности АЦП.

В приложениях G [2] и Ж [7] приведено следующее обоснование некоторых из перечисленных требований к определению АВР. Динамический диапазон амплитуд определяется как интервал всех возможных значений амплитуд, необходимый для измерения АВР. Верхний предел динамического диапазона должен быть больше пикового уровня измеряемой помехи, а нижний — меньше нормы помех, установленной для конкретного испытуемого устройства. В соответствии с CISPR 11 норма помех (пиковое значение) для промышленных, научных, медицинских и бытовых высокочастотных устройств группы 2 класса В установлена равной 110 дБ (мкВ/м), а «взвешенная» норма составляет 60 дБ (мкВ/м). Следовательно, динамический диапазон должен быть больше 60 дБ, включая запас 10 дБ.

Частота выборки определяется, исходя из следующих соображений. Для диапазона частот E, в котором обычно проводятся измерения АВР, импульсная полоса пропускания измерительного приёмника составляет 1 МГц, исходя из чего скорость выборок выбирается на порядок большей, что позволяет зарегистрировать редко повторяющиеся амплитуды радиопомех.

В CISPR 11 определено максимальное время удержания 120 с при измерениях помех от микроволновых печей для приготовления пищи с применением измерителя с пиковым детектором. Поэтому время измерения при определении АВР должно быть не менее данного значения. Из-за ограниченности памяти измерителей и диапазонов счётчиков допускаются периодические измерения при условии, что общее время пауз между измерениями составляет менее 1% полного времени измерения.

Из временных факторов оценивается и минимальное значение вероятности при построении АВР. Для получения статистически достоверного результата при расчёте АВР может потребоваться до 100 циклов измерений [2]. Для определения минимальной вероятности АВР это значение соотносят с количеством выборок, получаемых за один цикл измерений, что приближённо даёт значение 10^{-7}.

Наконец, последнее требование, касающееся амплитудного разрешения средства отображения АВР, обусловлено следующими соображениями. Амплитудное разрешение при отображении результатов распределения амплитуд зависит от динамического диапазона и разрешающей способности АЦП. Разрешение отображения становится менее 0,25 дБ при использовании 8-битового АЦП и динамическом диапазоне, равном 60 дБ. Таким образом, основные требования, предъявляемые к устройствам для измерения АВР радиопомех, определены потребностями практики и особенностями харак-

Анализатор спектра и сигналов высшего класса FSW

Новый стандарт анализа в миллиметровом диапазоне

3 года гарантии

Анализ импульсных сигналов ЛЧМ и ППРЧ

5G 6G WLAN

Разработка современных и перспективных стандартов радиосвязи

Защита пользовательских данных

Тестирование спутниковой связи

www.rohde-schwarz.com/ru

ROHDE&SCHWARZ

Make ideas real

Реклама

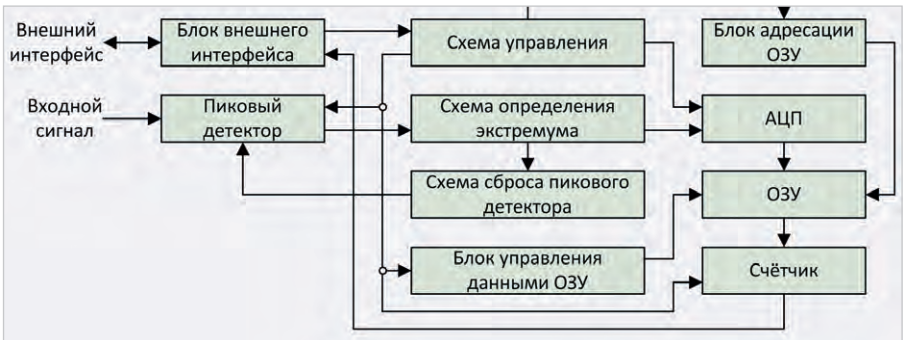


Рис. 4. Блок-схема устройства измерения АВР [8]

Рис. 5. Внешний вид измерительного приёмника R&S ESW44

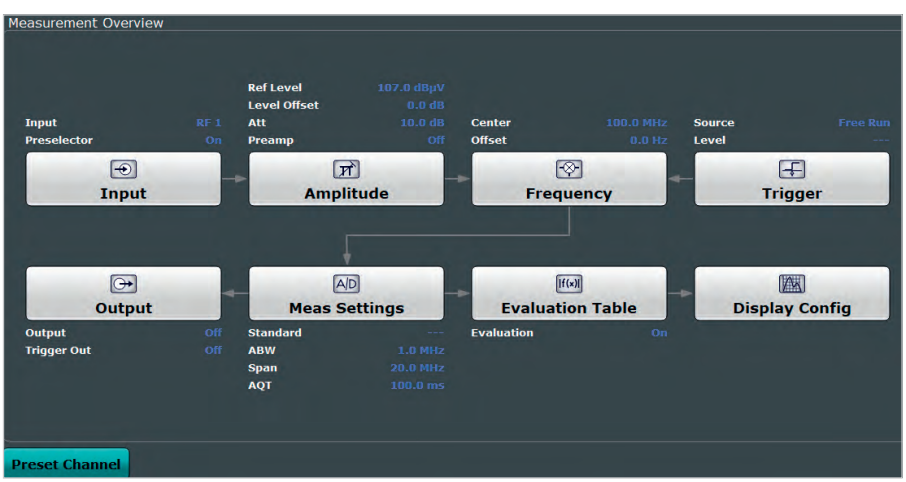


Рис. 6. Окно конфигурирования опции R&S ESW-K58 Multi CISPR APD

тера помехоэмиссии некоторых тестируемых объектов.

На рисунке 1 в качестве примера представлен график типовых АВР. Если испытуемое ТС выключено, то в отсутствие других источников помех АВР будет отражать для текущей частоты настройки статистические свойства собственных шумов линейного тракта средства измерений и антенны. Такой шум имеет тепловую природу и является широкополосным со статистически постоянной спектральной плотностью и удельной энергией. АВР для собственного шума средства измерений в координатах «амплитуда-вероятность» не имеет резких изгибов и характеризуется выпуклостью вверх, в то время как АВР радиопомех испытуемого ТС имеет обычно два изгиба, как это показано на рисунке 1.

Способы и схемы измерений АВР

Рассмотренные стандарты [2, 7] не устанавливают требования к алгоритмам определения АВР, однако в качестве справочной информации содержат блок-схемы типовых устройств для таких измерений. На рисунке 2 представлена блок-схема устройства измерения АВР без использования АЦП. В ней количество каналов анализа равно числу амплитудных уровней, для которых строится АВР. Каждый канал анализа имеет в своём составе устройство сравнения (компаратор), сопоставляющее входное напряжение с уровнем опорного источника, напряжение которого и определяет опорное значение амплитуды. Для обеспечения эквидистантности выборок по времени для всех каналов предусмотрено тактирование, частота которого должна быть, как следует из требования стандартов, не ниже 10 МГц. Превышение входным напряжением опорного значения вызывает появление на выходе компаратора высокого уровня, соответствующего логической единице, и каждый тактовый импульс обеспечивает регистрацию такого события счётным устройством. Счётчики должны иметь достаточное количество разрядов – для измерений длительностью 120 с при тактовой частоте 10 МГц общее количество обработанных выборок составит 1,2 млрд, что требует не менее чем 31 разряд двоичного кода для каждого счётчика. Учитывая высокую разветвлённость, система синхронизации такого устройства строится на основе особых технических решений.

На рисунке 3 представлена блок-схема для построения АВР с использованием АЦП. В ней запоминающее устройство фиксирует весь объём выборок в двоичном коде. В типовом случае применяется 8-битный АЦП, и тогда требуемый для измерений длительностью 120 с минимальный объём памяти составляет 1,2 Гбайт. В случае использования 12-битного АЦП этот объём увеличивается до 4,8 Гбайт. Для задания адреса записи и считывания используется специальный блок адресации, который по каждому следующему тактовому импульсу формирует новый начальный адрес для записи. Запись осуществляется по импульсному сигналу завершения оцифровки, вырабатываемому АЦП.

Построение функции АВР осуществляется путём последовательного считывания и математической обработки выборок. В некоторых случаях используются модификации данной схемы, в которых данные записываются в байтовые блоки, т.е. в группы по 8 бит, и тогда появляется возможность использования «лишних» разрядов для записи контрольной суммы каждой выборки, а схема несколько усложняется.

Помимо приведённых в стандартах [2, 7], имеются и альтернативные схемы для построения АВР радиопомех. Примером является схема [8], представленная на рисунке 4 и предназначенная для анализа помех с малой частотой повторения. Принцип её работы в целом аналогичен устройствам измерения АВР на основе АЦП. Координацию функционирования осуществляет схема управления. При осуществлении каждой оценки пиковый детектор включается на короткое время, и напряжение на его выходе нарастает. Предельное его значение фиксирует схема определения экстремума, которая сразу после этого обеспечивает разряд ёмкости (сброс) пикового детектора. Напряжение на выходе схемы определения экстремума оцифровывается при помощи АЦП, результаты оцифровки записываются в оперативное запоминающее устройство. Счётчик обеспечивает последовательное прочитывание записанных значений и формирует функцию АВР непосредственно в ходе осуществления измерений.

Как видно из представленных схем измерений АВР, они все оперируют с отсчётами огибающей на промежуточной частоте. Наиболее рациональным вариантом реализации измерений АВР является использование не отдельных устройств, а соответствующих программных опций современных измерительных приёмников, в частности R&S ESW-K58 Multi CISPR APD. Эта опция функционирует на базе измерительных приёмников высшего класса серии R&S ESW (см. рис. 5).

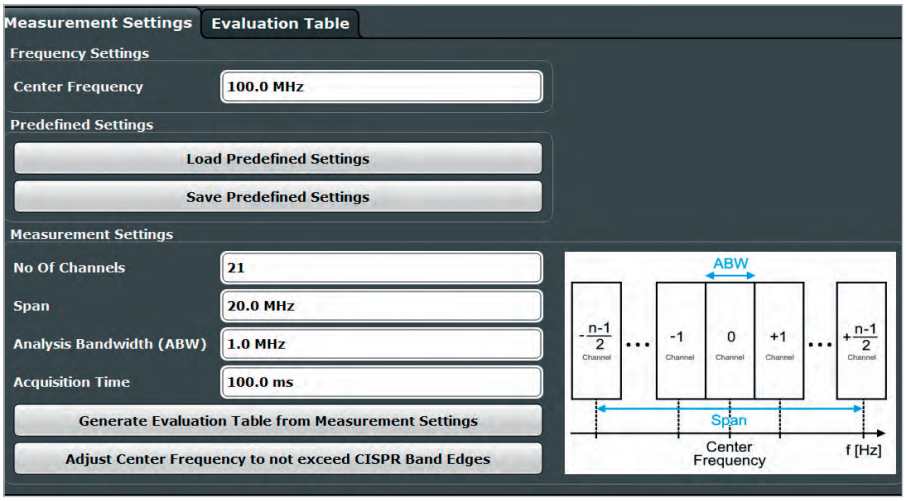


Рис. 7. Вкладка настройки режима измерений АВР

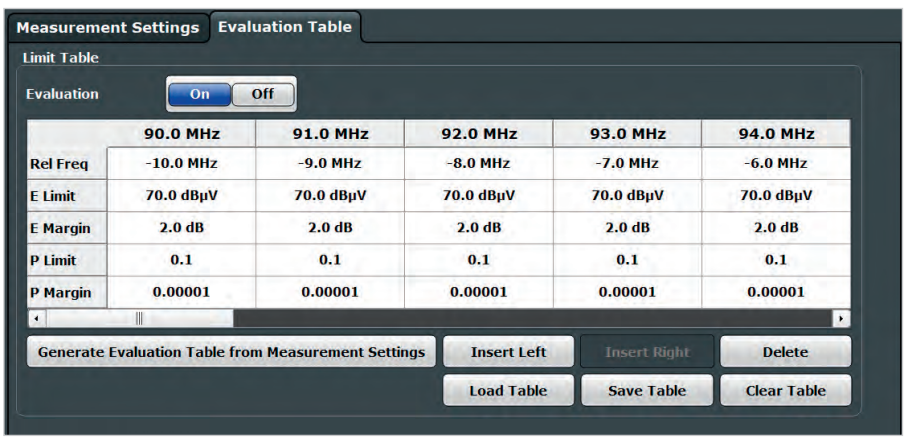


Рис. 8. Вкладка для задания данных для оценки результатов измерений

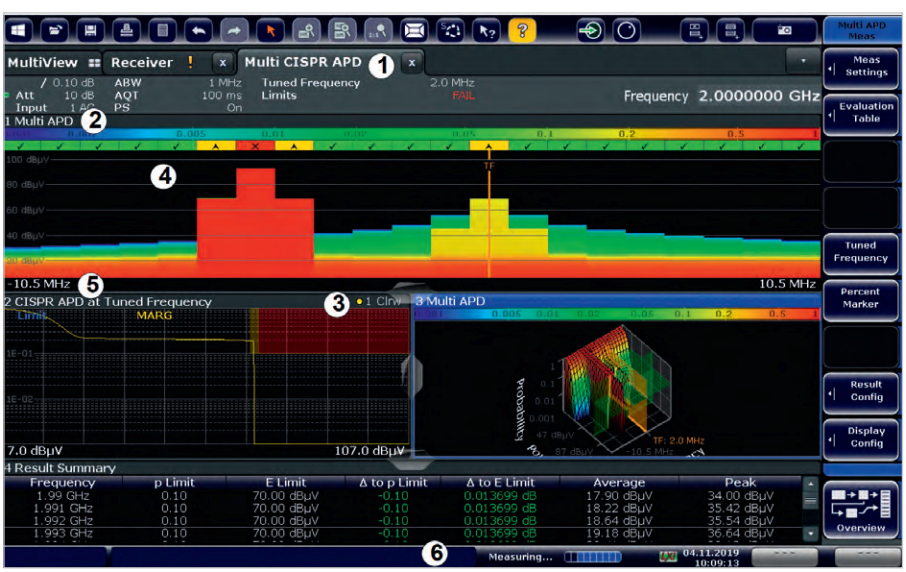


Рис. 9. Окно отображения результатов измерений опции R&S ESW-K58

Функциональность и особенности использования опции R&S ESW-K58 Multi CISPR APD

Опция R&S ESW-K58 Multi CISPR APD предназначена для расширения измерительных возможностей классического измерительного приёмника с функцией измерений АВР путём проведения таких измерений одновременно в 67 каналах с полосой 120 кГц и в 21 канале с полосой 1 МГц [9, 10]. Измерительные функции опции в части построения АВР строго соответствуют требованиям стандарта CISPR 16-1-1 и, например, в соответствии с CISPR 11 предназначены для проведения сертификационных испытаний СВЧ-печей. Основные особенности функции многоканального измерения АВР состоят в одновременности измерений во многих каналах и в форме представления результатов измерений.

Multi CISPR APD является отдельным исполняемым на измерительном приёмнике приложением, которое запускается после выбора соответствующего режима измерений, и они начинаются с настройками по умолчанию. Настройка режимов измерений и отображения их результатов осуществляется в окне приложения (см. рис. 6). Оно включает и стандартное конфигурирование линейной части измерительного приёмника – установку настроек по входу, включая использование преселектора, предусилителя, а также защиты от импульсов высокой мощно-

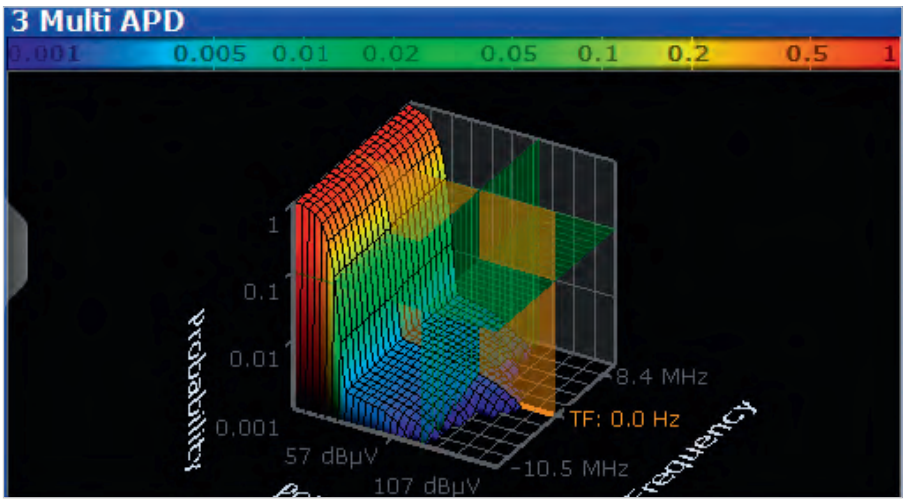


Рис. 10. 3D-диаграмма АВР

сти. Допускается проведение измерений с использованием внешних смесителей, расширяющих доступный для R&S ESW диапазон частот. Стандартным для приборов R&S ESW способом устанавливаются амплитудные и частотные параметры: опорный уровень, шаг сетки по частоте и амплитуде, ослабление встроенного аттенюатора, характеристики изменения частоты и амплитуды при стандартных операциях их перестройки.

Настройки предусматривают возможность использования запуска анализа по внешнему сигналу, подаваемому на вход на лицевой панели прибора R&S ESW после достижения им заданного уровня, а также использование внутреннего сигнала запуска для управления другими техническими средствами.

Настройка режима измерений осуществляется при помощи вкладки, форма которой показана на рисунке 7. Здесь задаются центральная частота, количество каналов и полоса анализа для каждого из них, а также время сбора данных при измерениях. Имеется возможность сохранения настроек и вызова ранее заданных конфигураций.

Для каждой полосы построения АВР могут быть заданы критерии автоматического анализа на вкладке, показанной на рисунке 8. Данные для ограничительных линий в каждом канале могут быть загружены из файлов установленного формата либо сохранены.

В окне, показанном на рисунке 6, дополнительно могут быть заданы типы используемых измерительных преобразователей, например, антенн и токовых пробников с автоматическим пересчётом результатов измерений к конечным единицам при помощи калибровочных таблиц.

После завершения настроек и осуществления измерений АВР их результаты могут быть отображены в разных формах. Доступная для R&S ESW-K58 Multi CISPR APD визуализация позволяет строить трёхмерное амплитудно-вероятностное распределение, в котором третьей координатой является частота. Это обусловлено тем, что

каналы анализа с заданными пользователем характеристиками расположены вплотную друг к другу, и их количество весьма велико. Пример окна отображения результатов измерений показан на рисунке 9, где цифрами отмечено несколько областей. В области 1 показаны основные настройки при измерении АВР, включая общий результат тестирования, получаемый путём сопоставления измеренных в каждом канале АВР с нормами, заданными пользователем. Цифрой 2 обозначена строка заголовка окна с отображаемыми результатами измерений, причём приборы R&S ESW поддерживают отображение нескольких окон одновременно. В общем случае в строке указывается тип детектора, режим развёртки, а также номер и цвет полученной кривой. В области 3 представлено измеренное АВР для одного из измерительных каналов, на график которого нанесены установленные для него же нормы.

В области 4 показаны основные результаты измерений. Здесь красным цветом отмечены уровни и частотные каналы, в котором АВР вышли за установленные нормы. Фактически это вид на 3D-диаграмму АВР в плоскости амплитуд и частот. В строках 5 и 6 представлена информация о частотном диапазоне, для которого строилось многоканальное АВР, и степень завершённости процесса измерений.

На рисунке 10 представлен вид 3D-диаграммы АВР, которая строится в категориях амплитуд, вероятностей и частот. Более тёплые цвета соответствуют большей вероятности. Частоты отсчитываются как смещения относительно номинала, задаваемого в области 1 окна, показанного на рисунке 9. Для упрощения анализа результатов измерений они сводятся в таблицу, показанную в нижней части окна. Таким образом, описываемая опция предоставляет возможность получения исчерпывающей информации о характере помехоэмиссии на основе анализа многоканального АВР, измеренного в соответствии с пользовательскими настройками.

Заключение

Как следует из изложенного, современный подход к измерению импульсных радиопомех с использованием амплитудно-вероятностного распределения реализуется на аппаратно-программной платформе измерительных приёмников высшего класса, предназначенных для сертификационных испытаний на ЭМС. Построение АВР выполняется в соответствии с пользовательскими настройками и почти полностью автоматизировано, как это было показано на примере функциональности опции R&S ESW-K58 Multi CISPR APD.

Одновременное построение АВР для заданного количества частотных каналов исключает необходимость проведения последовательных измерений для каждой из частот, что кратно экономит время при испытаниях ТС. Важно также отметить, что АВР позволяет более точно измерить истинные средние и пиковые значения напряжённости электромагнитного поля радиопомех, чем классические измерения. Ввиду этого можно ожидать расширения номенклатуры ТС, для которых будут требоваться измерения АВР радиопомех. Это подтверждает и тот факт, что в новую, третью редакцию стандарта CISPR 32, охватывающую испытания по ЭМС для мультимедийных устройств, предложено ввести такое требование для измерений помехоэмиссии на частотах выше 1 ГГц [11].

Литература

1. *Бузов А.Л., Быховский М.А., Васехо Н.В. и др.* Управление радиочастотным спектром и электромагнитная совместимость радиосистем. Под ред. Быховского М.А. — М.: Эко-Трендз. 2006. 376 с.
2. ГОСТ CISPR 16-1-1–2016 «Требования к аппаратуре для измерения радиопомех и помехоустойчивости и методы измерений. Часть 1-1. Аппаратура для измерений радиопомех и помехоустойчивости. Измерительная аппаратура». М.: Стандартинформ, 2017. 79 с.
3. *Лемешко Н.В., Захарова С.С.* Действие нестационарных узкополосных радиопомех на сигналы цифровой эфирной передачи данных. Труды НИИР, сборник научных статей / Под ред. Бутенко В.В. М.: НИИР, 2017. №2. С.43-48.
4. *Ширман Я.Д., Багдасарян С.Т., Маляренко А.С. и др.* Радиоэлектронные системы. Основы построения и теория. Под ред. Ширмана Я.Д., М.: Радиотехника. 2007. 512 с.
5. Интернет-ресурс https://www.bluetooth.com (дата обращения 18.02.2021)
6. *Zaidi A., Athley F., Medbo J.* 5G Physical Layer. Principles, Models and Technology Components. Academic Press, 2018. 302 p.
7. ГОСТ Р 51318.16.1.1-2007 «Совместимость технических средств электромагнитная. Требования к аппаратуре для измерения параметров индустриальных радиопомех и методы измерений. Часть 1-1. Аппаратура для измерения параметров индустриальных радиопомех и помехоустойчивости. Приборы для измерения индустриальных радиопомех». М.: Стандартинформ, 2008. 58 с.
8. *Переверзев Л.А., Хамадулин Э.Ф.* Измерение импульсных радиопомех с использованием амплитудно-вероятностного распределения. Интернет-ресурс https://mks.ru/library/conf/biomedpribor/2000/sec09_14.html (дата обращения 18.02.2021)
9. Интернет-ресурс https://www.microwavejournal.com/articles/33725-rohde-schwarz-has-added-new-timesaving-functions-to-its-high-end-rs-esw-emi-test-receiver (дата обращения 18.02.2021).
10. R&S®ESW-K58 Multi CISPR APD. User Manual. 1179.0880.02-01. p.102.
11. *Pettit J.* New and Proposed Changes to CISPR SC I Standards. Интернет-ресурс https://interferencetechnology.com/new-and-proposed-changes-to-cispr-sc-i-standards/ (дата обращения 24.02.2021).

НОВОСТИ МИРА

Аналоговый пьезоэлектрический голосовой акселерометр

VA1200 от Vesper – это пьезоэлектрический голосовой MEMS-акселерометр, который обеспечивает высокоточную оцифровку голоса (VPU) в наушниках, TWS (True Wireless Stereo), VR (Виртуальная реальность), AR (дополненная реальность), смарт-очках. акселерометр VA1200 может использоваться для улавливания голоса пользователя через костную проводимость. Используя это устройство в сочетании со стандартным микрофоном, можно добиться превосходного снижения фонового шума и шума ветра. В отличие от традиционного микрофона, датчик VA1200 полностью невосприимчив к окружающим звукам и улавливает только голос пользователя в виде колебаний, распространяющихся через кости черепа и отфильтровывает фоновые шумы, такие как шум ветра, музыка, шум метро и шум толпы.

Крошечное устройство (2,90×2,76×0,9 мм) снабжено высокоточным VPU, автоматическим отключением звука, функцией голосовой аутентификации. Устройство может работать в экологически суровых условиях, поскольку устойчиво к пыли и влаге.

www.circuitdigest.com

Способ адаптивного корреляционного обнаружения

Владимир Бартенев (bartvg@rambler.ru)

Рассматривается задача корреляционного обнаружения флюктуирующих коррелированных сигналов на фоне некоррелированного шума. Один способ корреляционного обнаружения реализуется с помощью умножения и когерентного накопления сигналов с фиксированным порогом. В другом предложенном способе после умножения и когерентного накопления используется адаптивный порог. Расчёт порогов для вероятностей ложных тревог на выходе этих корреляционных обнаружителей для малых выборок наблюдения произведён аналитически, а вероятности правильного обнаружения рассчитаны моделированием в системе MATLAB. Данные результаты в радиолокационной практике получены впервые. На способ адаптивного корреляционного обнаружения получен патент.

Введение

Задача обнаружения коррелированных сигналов на фоне некоррелированных случайных процессов по дискретным выборкам конечного объёма возникает во многих технических приложениях. Известен способ корреляционного обнаружения принимаемых сигналов, когда две выборки наблюдения, принятые на двух разных несущих частотах, перемножаются, их произведение накапливается и модуль накопленного произведения сравнивается с фиксированным порогом [1]. Полученная таким образом оценка модуля межчастотного коэффициента корреляции сравнивается с порогом, на основании чего принимается решение о наличии принятых коррелированных сигналов. Данный способ позволяет осуществлять эффективное обнаружение коррелированных сигналов, тем не менее данному способу свойственен недостаток, проявляющийся в отсутствии стабилизации ложных тревог при изменении уровня шума, на фоне которого производится корреляционное обнаружение.

Для стабилизации ложных тревог при корреляционном обнаружении предлагается способ [2], который включает в себя формирование оценки модуля коэффициента корреляции на основе выборок наблюдений, принятых на двух несущих частотах. Также способ включает сравнение оценок с порогом, который с целью стабилизации ложных тревог при изменении уровня шума делают адаптивным, формируемым как произведение коэффициента, определяющего вероятность ложной тревоги, на суммарную оценку мощности шума на двух несущих частотах. Анализ эффективности подобных устройств, особенно для малых выборок наблюдения и низких вероятностей ложных тревог, с помощью статистического моделирования, затруднителен. Нелинейная операция умножения приводит к изменению вида распределений на выходе этих устройств и существенному усложнению анализа с помощью аналитических выкладок.

Если при нахождении характеристик обнаружения точность расчёта вероятности правильного обнаружения допускает моделирование, то для малых вероятностей ложных тревог точность расчёта с помощью статистического моделирования становится недопустимо низкой. По этой причине и была предпринята попытка впервые найти аналитические выражения для расчёта низких вероятностей ложных тревог для нелинейных устройств с умножителем на входе и адаптивным порогом при использовании малых выборок наблюдений.

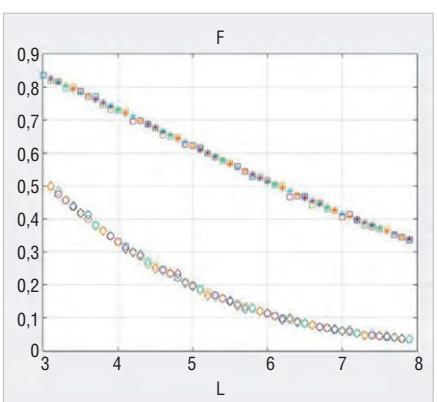


Рис. 1. Вероятность ложной тревоги для корреляционного обнаружения с фиксированным порогом в зависимости от порога L для N=4

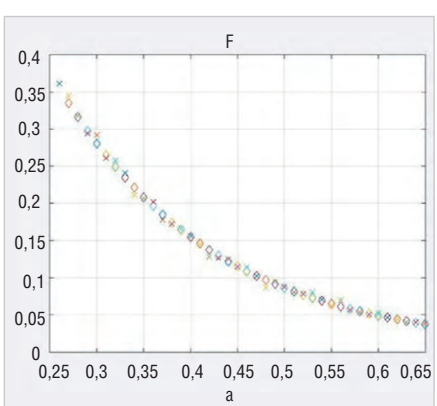


Рис. 2. Вероятность ложной тревоги для предложенного корреляционного обнаружения с адаптивным порогом для N=4 в зависимости от константы a, умноженной на суммарную оценку мощности шума

Вероятность превышения порога огибающей шума на выходе умножителя с когерентным накопителем и фиксированным порогом

Рассмотрим коррелятор с фиксированным порогом и покажем, что при изменении уровня шума изменяется вероятность ложной тревоги на его выходе. Для расчёта вероятности ложной тревоги для коррелятора с фиксированным порогом воспользуемся следующим выражением (1), где $\hat{R}$ – оценка модуля коэффициента корреляции, N – число накоплений по независимым выборкам.

$$Z1j = x1_j + iy1_j, Z2_j = x2_j + iy2_j -$$

комплексные выборки сигналов на входе умножителя, разнесённых по частоте в виде аддитивной смеси шума и коррелированного сигнала. Квадратурные компоненты шума имеют нормальное распределение, при этом мощность (дисперсия) равна σ^2, и среднее распределение, равное 0. Обнаружение сигналов в корреляторе с фиксированным порогом осуществляется путём сравнения полученной оценки модуля

Пороги для корреляторов с фиксированным и адаптивным порогами при разных ложных тревогах и разных N

N	4	8	16	4	8	16
10^{-1}	6,196	8,674	12,2	0,474	0,474	0,20
10^{-4}	15,684	20,093	26,59	2,2045	2,2045	0,5225

коэффициента корреляции с порогом $R_{ПОР}$, $\hat{R} > R_{ПОР}$.

Покажем, что изменение мощности шума σ^2 приводит к изменению вероятности ложной тревоги. Для этого, применяя методику нахождения вероятности ложной тревоги $F(R_{пор})$ из [3], получим выражение (2).

В данное выражение входит гамма-функция $\Gamma(N)$, модифицированная функция Бесселя $K_N(\hat{R}_{ПОР})$ порядка N и мощность шума σ^2.

Расчёты по формуле (2) для N=8, приведённые на рис. 1, показывают, что даже незначительные изменения мощности шума на входе (от 0 до 3 дБ) приводят к заметному росту вероятности ложной тревоги. Для верификации аналитических расчётов на графике имеются результаты и моделирования коррелятора с фиксированным порогом в MATLAB. Совпадение аналитики и моделирования подтверждает отсутствие стабильной вероятности ложной тревоги в корреляторе с фиксированным порогом. Ромбики (моделирование) и кружочки (аналитика) на графиках рисунка 1 соответствуют мощности шума 0 дБ, квадратики (моделирование) и звёздочки (аналитика) – мощности шума 3 дБ.

Вероятность ложной тревоги на выходе умножителя с когерентным накопителем и адаптивным порогом

Чтобы устранить указанный недостаток, предлагается производить дополнительно оценку мощности шума на двух несущих частотах, т.е. z1 и z2 (см. (3) и (4)).

Суммирование оценок мощности Z_s=(z1+z2) и умножение на коэффициент, определяющий вероятность ложной тревоги α, позволяет сделать порог адаптивным.

Считая независимыми оценки модуля коэффициента корреляции и оценки мощности шума, можно получить выражение для вероятности ложной тревоги предложенного адаптивного коррелятора, см. (5).

Считая, что оценка мощности Z_s имеет распределение χ^2, вероятность ложной тревоги $F(\alpha)$ примет вид (6).

$$\hat{R} = |(\sum_{j=1}^{N} Z1_j * Z2_j^*)| = \sqrt{(\sum_{j=1}^{N} x1_j * x2_j + y1_j * y2_j)^2 + (\sum_{j=1}^{N} x2_j * y1_j - x1_j * y2_j)^2} \quad (1)$$

$$F(R_{ПОР}) == \frac{(R_{ПОР}/\sigma^2)^N K_N(R_{ПОР}/\sigma^2)}{2^{N-1}\Gamma(N)} \quad (2)$$

$$z1 = \sum_{i=1}^{N-1} Re(Z_{1i}) Re(Z_{1i}) + Im(Z_{1i}) Im(Z_{1i}) \quad (3)$$

$$z2 = \sum_{i=1}^{N-1} Re(Z_{2i}) Re(Z_{2i}) + Im(Z_{2i}) Im(Z_{2i}) \quad (4)$$

$$F(\alpha) = \int_0^{\infty} P(Z_S) dZ_S \int_{\alpha Z_S}^{\infty} P(R) dR \quad (5)$$

$$F(\alpha) = \int_0^{\infty} \frac{Z_S^{N-1} e^{-z_S/2\sigma^2}}{\Gamma(N)(2\sigma^2)^N} \frac{(\alpha Z_S/\sigma^2)^N K_N(\alpha Z_S/\sigma^2)}{\Gamma(N)(2)^{N-1}} dZ_S \quad (6)$$

$$F(\alpha) = \sqrt{\pi} a^{2N} \Gamma(3N) / 2^{(4N-1)} \Gamma(2N+1/2)\Gamma(N) {}_2F_1(\frac{3N+1}{2}, \frac{3N}{2}; 2N+1/2; 1-4\alpha^2) \quad (7)$$

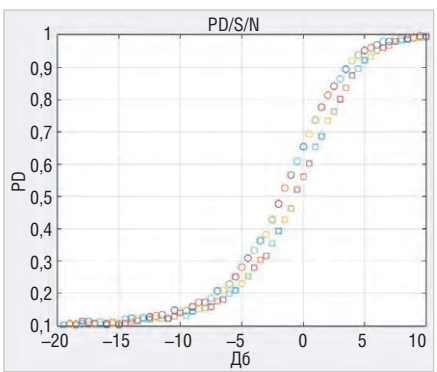


Рис. 3. Вероятность правильного обнаружения PD для корреляторов с фиксированным и адаптивным порогом для N=4 в зависимости от соотношения сигнал/шум (дБ) для вероятности ложной тревоги 0,1 и коэффициента корреляции 0,9

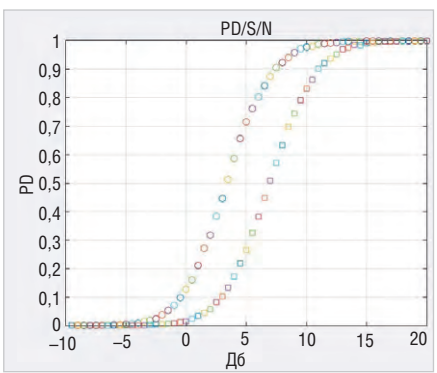


Рис. 4. Вероятность правильного обнаружения PD для корреляторов с фиксированным и адаптивным порогом для N=4 в зависимости от соотношения сигнал/шум (дБ) для вероятности ложной тревоги 0,0001 и коэффициента корреляции 0,9

После взятия интеграла получаем (7), где ${}_2F_1$: гипергеометрическая функция. Полученное выражение (7) говорит о главном – в нём отсутствует мощность шума σ^2. В таблице указаны пороги для корреляторов с фиксированным (два левых столбца) и (два правых столбца) адаптивным порогами при разных ложных тревогах и разных N.

Характеристики обнаружения сравниваемых способов корреляционного обнаружения

Дальнейший анализ производился не только аналитическим расчётом по полученной формуле, но и для верификации моделированием корреляционного обнаружения с адаптивным порогом в MATLAB.

Результаты аналитических расчётов и моделирования показали хорошее совпадение (см. рис. 2), что позволяет сделать вывод о корректности полученного аналитического выражения (7). Ромбики на графиках рисунка 2 соответствуют аналитике, крестики – моделированию. Главный результат, изменение уровня шума в корреляторе с адаптивным порогом, не влияет на вероятность ложной тревоги.

Коррелятор с адаптивным порогом по эффективности сравнивался с коррелятором с фиксированным порогом расчётом характеристик обнаружения флюктуирующего коррелированного сигнала. Это было сделано с помощью моделирования в системе MATLAB. На рисунках 3–8 приводятся кривые для вероятности правильного обнаружения флюктуирующего сигнала с коэф-

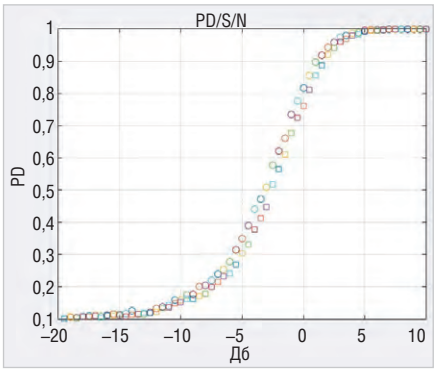


Рис. 5. Вероятность правильного обнаружения PD для корреляторов с фиксированным и адаптивным порогами для N=8 в зависимости от сигнал/шум (дБ) для вероятности ложной тревоги 0,1 и коэффициента корреляции 0,9

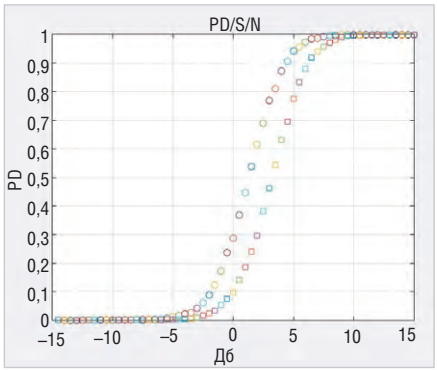


Рис. 6. Вероятность правильного обнаружения PD для корреляторов с фиксированным и адаптивным порогом для N=8 в зависимости от соотношения сигнал/шум (дБ) для вероятности ложной тревоги 0,0001 и коэффициента корреляции 0,9

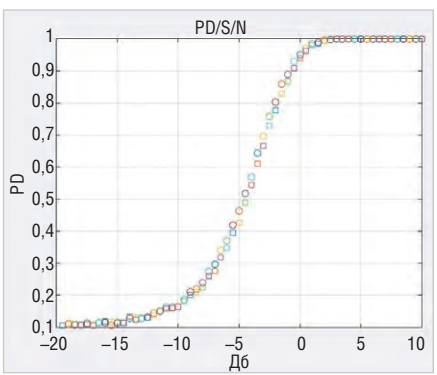


Рис. 7. Вероятность правильного обнаружения PD для корреляторов с фиксированным и адаптивным порогом для N=16 в зависимости от соотношения сигнал/шум (дБ) для вероятности ложной тревоги 0,1 и коэффициента корреляции 0,9

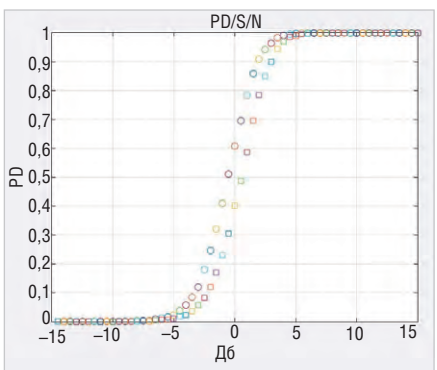


Рис. 8. Вероятность правильного обнаружения PD для корреляторов с фиксированным и адаптивным порогом для N=16 в зависимости от соотношения сигнал/шум (дБ) для вероятности ложной тревоги 0,0001 и коэффициента корреляции 0,9

фициентом корреляции 0,9 для двух рассматриваемых устройств при N=4, N=8 и N=16 для вероятности ложной тревоги 0,1 и вероятности ложной тревоги 0,0001. Кружочки на графиках рисунков 3–8 соответствуют коррелятору с фиксированным порогом, квадратики – коррелятору с адаптивным порогом.

Показано, что эффективность в пороговом сигнале для вероятности правильного обнаружения 0,5 и вероятности ложной тревоги 0,1 и 0,0001 несколько выше у коррелятора без стабилизации ложных тревог, особенно для меньшей вероятности ложной тревоги. Это своего рода плата за инвариантные свойства адаптивного коррелятора к изменениям мощности шума, при этом обеспечивается стабилизация вероятности ложной тревоги на выходе. Следует заметить, что эти потери снижаются при увеличении выборки наблюдений.

Таким образом, проведённое исследование в системе MATLAB полностью подтверждает положительный эффект от применения предложенного коррелятора со стабилизацией ложных тревог. Важно подчеркнуть, что полученное впервые аналитическое выражение для вероятности ложной тревоги адаптивного коррелятора позволит более обстоятельно исследовать его свойства для разных малых выборок наблюдения в широком диапазоне вероятностей ложных тревог.

Литература

1. *Бартенев В. Г.* Новые результаты анализа эффективности устройств корреляционного типа. Современная электроника. 2017. № 1.
2. *Бартенев В. Г.* Патент № 2743027 по заявке № 2019141461. Способ адаптивного обнаружения по корреляционному признаку. 2021. Бюл. № 5.
3. *Бартенев В. Г.*, *Бартенев М. В.* Способ нахождения вероятностных характеристик на выходе нелинейных систем. Цифровая обработка сигналов. 2013. № 4.
4. *Потёмкин В. Г.* Справочник по MATLAB. Анализ и обработка данных. URL: http://matlab.exponenta.ru/ml/book2/chapter8/.

НОВОСТИ МИРА

Осциллограф для монтажа в стойку от RIGOL

Компания RIGOL Technologies объявила о расширении своей технологической платформы UltraVision II. Осциллограф DS8000-R для монтажа в стойку обеспечивает полосу пропускания до 2 ГГц и такую же функциональность что и проверенный осциллограф серии MSO8000 от RIGOL.

Ультратонкая компактная конструкция (высота 1U на 1/2 ширины стойки) позволяет устанавливать два осциллографа DS8000-R на стандартной высоте стойки 1U. Имея в общей сложности восемь каналов с частотой 2 ГГц в 1U стоечного пространства, DS8000-R обеспечивает непревзойдённую плотность размещения оборудования. Он может управляться локально с помощью монитора HDMI, мыши и клавиатуры, а также удалённо с помощью веб-управления. Тактовая частота дискретизации и синхронизация триггеров позволяют RIGOL предоставлять мощные решения для многоканального высокоскоростного сбора сигналов, таких как сбор переходных событий в физике высоких энергий и автоматизированное тестирование промышленных систем. Цифровые осциллографы DS8000-R имеют четыре аналоговых канала с полосой пропускания 350 МГц, 1 ГГц и 2 ГГц с отличной частотой дискретизации в реальном времени до 10 Гс/с, глубиной памяти до 500 миллионов точек/с и высокой скоростью захвата сигналов 600 000 фреймов/с. DS8000-R включает в себя цифровой осциллограф, анализатор спектра, генератор произвольной формы сигнала (опционально), цифровой вольтметр, шестизначный счётчик и сумматор, а также анализатор протокола (опционально). DS8000-R может использоваться для мониторинга сигналов в экстремальных условиях окружающей среды с его способностью выдерживать рабочие температуры до –40°C.

www.signalintegrityjournal.com

19-я МЕЖДУНАРОДНАЯ ВЫСТАВКА ЭЛЕКТРОНИКИ

ChipEXPO-2021

КОМПОНЕНТЫ | ОБОРУДОВАНИЕ | ТЕХНОЛОГИИ

ВЫСТАВКА ПРОЙДЕТ

14-16.09

В ТЕХНОПАРКЕ ИННОВАЦИОННОГО ЦЕНТРА

СКОЛКОВО

ТЕМАТИЧЕСКИЕ ЭКСПОЗИЦИИ:

- Экспозиция Департамента радиоэлектронной промышленности Минпромторга России, включая:
  - экспозицию предприятий, являющихся изготовителями изделий, включенных в единый реестр российской радиоэлектронной продукции (Постановление Правительства РФ №878)
  - экспозицию разработок, созданных в рамках государственной программы «Развитие электронной и радиоэлектронной промышленности на 2013-2025 годы» (Постановление Правительства РФ №109)
  - экспозицию разработок, обеспечивающих выполение приоритетных национальных проектов.
- Дивизионы кластера «Радиоэлектроника» ГК «Ростех»
- Квалифицированные поставщики ЭКБ
- Участники конкурса «Золотой Чип»
- Стартапы в электронике
- Консорциумы и дизайн-центры по электронике
- Корпорация развития Зеленограда

ОФИЦИАЛЬНАЯ ПОДДЕРЖКА:

Sk Сколково · Государственная Дума · Минпромторг России · Ростех · Росэл · Российская Академия Наук

ОРГАНИЗАТОРЫ:

ЗАО «ЧипЭКСПО» Москва,121351, ул. Ярцевская, д.4. Тел.: +7 (495) 221-50-15
E-mail: info@chipexpo.ru http://www.chipexpo.ru

Кому нужна электронная индустрия?

Алексей Галицын (a.a.galitsyn@gmail.com),
Андрей Железнов (zhelandr@mail.ru)

В статье рассматриваются различные аспекты безопасности России перед лицом экономических санкций со стороны ведущих мировых экономик. Обосновывается необходимость срочного обеспечения технологической независимости в ключевых направлениях развития микроэлектроники, телекоммуникаций, а также в сфере финансов.

Введение

Данная статья основана исключительно на проверенных с точки зрения Закона РФ № 538-ФЗ фактах, которые авторы могут подтвердить документально, и является последней из серии статей [1–6] коллектива авторов Консорциума «Физико-техническая корпорация», все проекты которого были отвергнуты Департаментом радиоэлектронной промышленности (ДРЭП) Минпромторга РФ. Что характерно, именно этот департамент несёт ответственность за импортозамещение, осуществляемое в целях безопасности электронного оборудования государства. В этой связи нам хотелось бы обратить внимание чиновников ДРЭП Минпромторга РФ, создающих крючкотворные законы о «балльной» оценке «отечественности» электронного оборудования, на то, что безопасность электронной техники – это не диссертация по экономике, безопасность не измеряется в процентах – она или есть, или её просто нет! А вот «безнадёжность» сложных, причём невосстанавливаемых электронных устройств (то есть вероятность их отказа: $Q(t) = 1 - P(t)$, где $P(t)$ – вероятность безотказной работы устройства) будет практически обратно пропорциональна произведению вероятностей $P_i(t)<1$ безотказной работы всех (n) его отечественных компонент: $P(t)= P_1(t)\times P_2(t)\times...\times P_n(t)$. Именно так, с гарантированной государством (при отсутствии конкуренции Pi=0,9) вероятностью отказа Q=0,999974, «погиб» ремонтопригодный советский гражданский автопром (при P_i=0,9 и n=100 $Q=1-0{,}9^{100} = 0{,}999974$).

Чтобы напомнить читателям, о чём, собственно, шла речь в отвергнутых Департаментом проектах, перечислим некоторые из них:

1. «Зонт» от сверхманёвренного гиперзвука» позволил бы создать реальную защиту от сверхманёвренного гиперзвукового оружия и сделать российское сверхманёвренное гипероружие (простой заменой электронного блока!) на порядок более точным;
2. «Настольная» ядерная энергетика» позволила бы сделать холодный ядерный синтез «настольным», а ионные двигатели – компактными;
3. «Интернет Вещей Будущего» – спасти и вывести на мировой рынок полупроводниковую индустрию страны, открыв ей (за счёт интеллектуальных преимуществ) мировой рынок Интернета Вещей (IoT) (рынок $7,0...10,0 трлн/год, четверть бюджета США);
4. «Российская рентгенолитография и РФА-спектрометрия»: первая – создать рентгенолитографию с кратно большей радиационной светосилой пучков наноразмерной ширины, вторая – обеспечить чувствительность рентгенофлуоресцентного анализа (РФА) на уровне масс-спектроскопических и атомно-абсорбционных методов анализа при себестоимости на порядок меньшей;
5. «Невидимая» и «неубиваемая» военная радиосвязь взамен смертоносной (для собственной армии) «китайской» радиосвязи – дать армии массовую дешёвую развед- и помехозащищённую радиосвязь, принципиально недоступную для кибератак и обладающую уникальной живучестью;
6. «Цифровая трансформация предприятий» – создать технологическую платформу интернет-коммуникаций повышенного качества («сеть поверх сети», в том числе сервис IP-TV и защищённая телефония) на базе сетевой технологии «IPv17» с ассоциативной маршрутизацией, гарантированной доставкой пакетов и исключением возможности организации дестабилизирующих воздействий на сетевую инфраструктуру;
7. «Аппаратная криптозащита киберсистем» – на недоступном для конкурентов уровне защитить информационные ресурсы, национальную цифровую валюту (см. далее), киберфизические системы, критическую инфраструктуру, а также осуществлять сертификацию и защиту товарного рынка при помощи криптосредств нового типа.

На основе именно таких проектов, базирующихся на так называемых «предельных технологиях» – технологиях, обладающих новыми качествами и опережающих современные научные достижения в своей области (в которых получается то, что считается невозможным), и должно давным-давно начаться возрождение новой полупроводниковой индустрии страны (загрузка полупроводниковых фабрик и рентабельное производство массовой конкурентоспособной продукции даже на отсталой технологической базе), а главное, создание и загрузка десятков дизайн-центров целенаправленным проектированием на кристаллах качественно новых криптосистем, электронных финансов, систем управления, систем телекоммуникаций, телефонии и связи для гражданских и военных применений.

Впрочем, сейчас об экономике электронной индустрии даже и вопрос не стоит – электронную индустрию надо просто спасать любой ценой и расплачиваться за 30 лет реального физического уничтожения отрасли, продукция которой (пока) априори неконкурентоспособна, но жизненно необходима для будущего страны, что наглядно показано в настоящей статье.

К сожалению, по этому вопросу у разных людей существуют совершенно разные и даже диаметрально противоположные мнения. Существует, например, суждение «в народе», что микроэлектронная индустрия в России погибла навсегда, восстановить её невозможно, а возрождать бессмысленно, ведь у народа и так есть и смартфоны, и телевизоры, и компьютеры.

Есть и суждение, что теперь у всех технических специалистов страны и у всех российских учёных в области микроэлектроники одномоментно изменилось сознание, и что они в результате этого «за

год» наверстают наше 30-летнее отставание от мировой цивилизации [7], при том что от электронных технологий (Cadence, Synopsys, Agilent, TSMC и SoC-комплектующих, etc.) российских разработчиков теперь, скорее всего, просто-напросто отключат [8-10].

Авторы уверены: чтобы публиковать оценочные суждения по тому или иному предмету, надо иметь и профессиональные знания в обсуждаемой предметной области, и моральное право на это (иначе люди будут считать тебя, мягко говоря, «чудаком»). Существует, например, суждение о «шпионских закладках» в «чайниках и утюгах» китайского производства. Как это ни смешно для подавляющего большинства людей, такое суждение (если все правильно понимать) имеет право на существование. И далее в статье будет показано, что ничего удивительного в этом нет!

Причины, побудившие авторов написать данную статью

Так почему же и на каком таком основании авторы осмелились и не смогли не сказать публично, может быть в последний раз и хотя бы кратко, эти несколько слов правды? Да потому что, к сожалению, подавляющее большинство специалистов в области микроэлектроники – это сотрудники госструктур, вынужденные молчать под давлением своего руководства.

К сожалению, российские чиновники и раньше, и сейчас, по-видимому, недооценивают то, что электронная индустрия, в отличие, например, от гражданского автопрома, это реальное глобальное оружие, стратегически не менее серьёзное, чем атомное. Поэтому очень важно, кто-же реально им (ей) управляет.

Теперь атомное оружие – это даже не оружие сдерживания, а способ бессмысленного возмездия и, гипотетически, полного уничтожения цивилизации. А вот реальное сдерживание и удушение нашей страны будет вестись совершенно другими средствами.

Представим локальные конфликты по всему периметру России, реально поддержанные деньгами и тактическим оружием НАТО, наряду с запретом на передачу технологий, одномоментной парализацией средств связи и управления, приостановлением всех финансовых транзакций. Это то, что реально и в кратчайшие сроки может экономически и политически уничтожить Россию, сохранив для будущих победителей в целости и сохранности (в том числе от радиации) все её природные ресурсы. И это вполне реальный сценарий. И к нему уже всё готово, а первый удар в этом сражении примут на себя гражданские и военные средства управления и связи, а также электронная платёжная и финансовая системы страны.

Но главное, почему авторы были вынуждены написать эту последнюю заключительную статью (специалисты всё и без того понимают), так это потому, что в то время, когда между США и Китаем развернулась жёсткое противостояние и жестокая борьба за лидерство в области электронной индустрии и индустрии телекоммуникаций, когда абсолютно всем стало совершенно очевидно, что именно этой отраслью будет определяться лидерство в будущей мировой цивилизации, оказалось, что для российского чиновничества даже самой этой проблемы целых 30 лет не существовало, да и теперь как бы не существует. Выходит, эта проблема должна «рассосаться» как бы сама собой в мутной воде министерств и институтов развития страны.

Несколько слов об авторах данной статьи

Авторы осмелились написать эту заключительную статью на том простом основании, что несколько десятилетий тому назад научным руководителем дипломного проекта одного из них (Алексея Галицына) был самый авторитетнейший специалист отрасли, д.т.н., профессор Игорь Павлович Степаненко, заведующий кафедрой микроэлектроники МИФИ, основоположник полупроводниковой техники и микроэлектроники СССР, автор фундаментальной монографии «Основы теории транзисторов и транзисторных схем» [11](впоследствии при переиздании результаты, полученные в дипломной работе автора данной статьи, вошли в эту монографию). Научным руководителем кандидатской диссертации автора статьи был основоположник отечественной микро- и наносхемотехники [12-14], д.т.н., профессор Андрей Геннадьевич Алексенко (награждён звездой Героя Социалистического Труда за получение фотографий с поверхности планеты Венера и кометы Галлея), по инициативе которого, направленной в Политбюро ЦК КПСС, был построен город микроэлектроники Зеленоград и создано советское микроэлектронное производство.

И ещё потому, что диссертационная работа самого автора данной статьи в 1982 году была посвящена разработке программируемых в условиях эксплуатации матричных схем (FPGA или по-русски – ПЛИС). В настоящее время добрая половина электронного оборудования в мире и 90% оборудования в России проектируется именно с применением таких СБИС. К сожалению, иностранного производства – фирм Altera и Xilinx, учреждённых в США в 1984 году, а ныне гигантов мировой электронной индустрии. Только в последние годы в стране, наконец-то, появились аналоги устаревших импортных FPGA производства КТЦ «Электроника» (г. Воронеж). Также автор данной статьи участвовал в разработке первых советских микроЭВМ («Электроника-60» – полный аналог микро-ЭВМ «LSI-11» фирмы DEC), он же написал и первую в СССР техническую книгу о микропроцессорах никому в то время неизвестной фирмы Intel [15] (технический бестселлер 80-х) или, как теперь оказалось, книгу о технических основах информационной эры. Кроме того, его подписи стоят на кальках аппаратуры космического сегмента системы ГЛОНАСС, который был запущен в эксплуатацию ещё в середине 80-х, тогда как наземный сегмент страна стала создавать только в 10-х годах нового тысячелетия, навсегда потеряв при этом мировой рынок гражданских навигационных систем и неся всё это время десятки, если не сотни миллиардов рублей расходов на поддержание в рабочем состоянии спутниковой группировки, в то время как США (за GPS-приёмники) ежегодно получали сотни миллиардов долларов прибыли.

Осмелились ещё и потому, что второй автор данной статьи Андрей Железнов имеет не менее серьёзный технический бэкграунд: в своё время закончил физматшколу-интернат при МГУ им. Ломоносова; закончил МФТИ (Московский физико-технический институт), факультет управления и прикладной математики, специальность «Системы автоматического управления», кафедра «Управление и эффективность спецсистем» (стратегические и тактические системы авиационного вооружения); работал (с 3-го курса МФТИ) 10 лет в головном институте авиационных вооружений НИИАС; был (с 25 лет) руководителем группы НИИАС по исследованию и оптимизации облика стратегической крылатой ракеты Х-90, имевшей уже тогда (по данным

открытых публикаций в СМИ и книгам о гиперзвуковых системах) высоту полёта 30 000 м, скорость – 4,5...5 Махов (скоростей звука), два самонаводящихся ядерных блока.

Далее был (с 28 лет) начальником лаборатории перспективных комплексов бортового оборудования (включая пилотажно-навигационный комплекс, комплекс обороны, комплекс вооружения и др.) КБ УВЗ им. Н. И. Камова (соосные боевые вертолёты «Ка-50» «Чёрная акула», «Аллигатор» и др.), занимавшейся разработкой облика скоростного боевого перспективного вертолёта.

В 2006–2007 годах руководил разработкой и внедрением цифровых систем циркулярной связи для ЦУП (Центра управления полётами «РОСКОСМОСА» (г. Королев)). Именно эти системы обеспечивали взаимодействие операторов ЦУП при управлении МКС и другими космическими аппаратами в 2008–2020 годах.Этот человек, будучи сторонником реальных реформ, гораздо раньше, чем многие, ещё в 1989 году, смог осознать, к чему может привести перестройка при неправильном управлении экономикой, и даже лично попытался предостеречь М. С. Горбачёва и предупредить надвигающуюся на страну экономическую катастрофу. К тому времени реальные преобразования в СССР действительно назрели. И начатые Горбачёвым реформы были совершенно необходимы.Но при этом большинство ведущих экономистов СССР обосновывали целесообразность «псевдореформ» на основе вашингтонского консенсуса, в которых невидимая рука рынка должна была всё в экономике исправить и расставить по местам (и «расставила», как теперь оказалось).В 1990 году Андрей Железнов подготовил «Программу регулируемого перехода к рынку» и в 1990–1991 годах был создателем и руководителем-координатором рабочей группы, которая продвигала эту Программу [16]. Правда под рынком в ней подразумевалась конкуренция, а не «базар». Программа регулируемого перехода к рынку сделала бы СССР лидером мировой экономики.

В состав рабочей группы входили несколько генералов КГБ СССР (кстати, один из них закончил МИФИ и начинал работать в научной лаборатории Института атомной энергии им. Курчатова), несколько членов-корреспондентов АН СССР (в том числе по экономике), зам. председателя Госкомиссии СССР по реформе, начальник отдела Госплана СССР, депутат ВС СССР, доктора наук по социологии и политологии.

У группы весной 1991 года появился прямой выход на Президента СССР М. С. Горбачёва и Председателя ВС СССР А. И. Лукьянова.

8 мая 1991 года (в Кремле, в субботу, за день до Дня Победы) состоялась встреча участников группы с М. С. Горбачёвым. Это была непротокольная беседа, длившаяся 3,5 часа: 1,5 часа в диалоге с Горбачёвым был автор данной статьи, 1,5 часа – член-корреспондент РАН Львов, 0,5 часа – общая дискуссия.

Кроме членов группы присутствовали только Председатель Верховного Совета СССР А. И. Лукьянов и Президент Научно-промышленного союза СССР А. И. Вольский.

Так или иначе, программу и работу группы одобрили. В мае-июне 1991 года даже реализовали разработанные группой срочные меры, и Горбачёв не только избежал втягивания его в программу «Согласие на шанс», но и принял решение провести реальное реформирование экономики, отвергнув программы, навязанные из-за рубежа, т.е., по сути, СССР получил реальную возможность реформирования, резкого роста и усиления экономики.

Если бы не ГКЧП и его последствия, с осени 1991 года в СССР должна была реализовываться «Программа регулируемого перехода к рынку». СССР сейчас имел бы самую мощную в мире экономику и один из самых высоких в мире уровней жизни. Однако история не терпит сослагательных наклонений. СССР был разрушен.

Но вернёмся к технике. Так уж заведено, что технику создают люди, а она, в свою очередь, или защищает, или уничтожает людей. В любом случае, от качества электронной техники в итоге зависит жизнь людей, а её качество зависит от тех, кто, в каких условиях и под чьим руководством эту технику создаёт. В данной статье мы в основном будем рассматривать технические проблемы, но, увы, вынуждены будем затронуть и вопросы того, как создаётся электронная техника в нашей стране – одно без другого не бывает.

Что же можно сказать о безопасности электронных средств управления, связи и обеспечения финансовых транзакций с точки зрения их уязвимости и перспектив противостояния разного рода угрозам по оценке разработчиков радиоэлектронной аппаратуры, этих странных людей, несмотря ни на что не покинувших Родину и занимающихся «лженаукой» кибернетикой?

Безопасность электронного оборудования

Микроэлектроника развивается стремительно и непрерывно. Нравится нам или нет, но согласно Закону Мура стоимость микроэлектронных ресурсов (стоимость миллиона операций в секунду, мегабайта оперативной памяти, гигабайта долговременной памяти) соответственно непрерывно снижается: каждые 10 лет информационные ресурсы дешевеют в ... 100 (!) раз.Следовательно, если комплект «стандартного оборудования для шпионажа», например для передачи информации на пролетающий шпионский спутник, в 1980 году стоил немыслимые 1 млн долларов, то он мог стоить 10 тыс. долларов в 1990 году, 100 долларов – в 2000 году, 1 доллар – в 2010 году и... 0,01 доллара – в 2020 году.

И цена определяла «тактику» его внедрения: можно предположить, что в 1990 году оно уже было серийно встроено во все комплекты оборудования ценой 1 млн долл. (тогда речь шла уже о дополнительных электронных узлах). В 2000 году оно было, как можно предположить, встроено во все комплекты стоимостью 10 тыс. долларов (речь шла уже о «шпионских закладках», сделанных на кристалле микросхем), в 2010 году оно могло быть встроено в оборудование стоимостью 100 долларов, а в 2020 году – уже везде.

Начиная с 2000 года, «шпионский канал» активизируют только по мере необходимости, посредством передачи извне соответствующего управляющего кода. Причём можно предположить, что все «шпионские» устройства давно встроены в микроэлектронные кристаллы серийных микросхем, потому что их самих просто дешевле выпускать массово, активизируя «шпионский канал» извне по мере необходимости, а российские чиновники иногда неожиданно узнают и даже потом людям в прессе зачем-то сообщают, что ими обнаружены «шпионские закладки» в чайниках и утюгах китайского производства.

Вопрос: как можно с помощью традиционных «спецпроверок» (рентгеноскопии) и «специсследований» (контроля RF-спектра) в современных условиях обнаружить «шпионские закладки» (и даже какой в этом смысл?) при современном уровне микроэлектронных технологий и количестве серий микросхем? Тем более что акти-

визируются они и выходят на связь только по команде «сверху».

Ответ: практически никак! То же самое можно сказать и о незадекларированных возможностях сложной вычислительной техники, подключаемой к Интернету, которую тоннами закупают почти все режимные структуры. При современном уровне сложности однокристальных и других устройств, содержащих сотни миллионов транзисторов, при современном уровне сложности системного программного обеспечения обнаружить незадекларированные возможности в импортных микропроцессорах практически невозможно. И поверьте, авторы этих строк знают, о чём говорят. Это теперь даже теоретически невозможно, т.к. по уровню сложности такая задача не проще, чем заново разработать и изготовить процессор!

В плане шпионских закладок очень интересен вопрос об информационной безопасности при применении на спецсетях силовых структур импортного или российского оборудования, реально спроектированного на базе иностранных спецмикросхем связи, потенциально имеющих шпионские закладки на кристалле, более того, являющегося системной копией импортного оборудования. Оно собрано в России, но по зарубежным рекомендациям, на импортном оборудовании.К сожалению, такие случаи имеют место и совсем не редки даже в аппаратуре ФСО, и оптимизм ведомства в том плане, что сети ФСО выхода в открытые сети не имеют, не вполне оправдан, поскольку всего один шпион может поставить всю эту сеть под контроль. И касается это не только силовых структур, а всех электронных устройств и сетей так называемой критической инфраструктуры. В этой ситуации достаточно вспомнить печальную (для России) историю завербованного зарубежными спецслужбами генерал-лейтенанта ГРУ СССР Полякова, сдавшего ЦРУ целое поколение (8000 человек) советской резидентуры за рубежом.

TCP/IP и IP-телефония

Особенное удивление вызывает российская мода на использование в наземных военных и аэрокосмических системах связи и управления протоколов TCP/IP (Transmission Control Protocol – Internet Protocol), тем более что они были разработаны в DARPA (Агентство перспективных оборонных исследований) в США в 1972–1982 годах.

Эти протоколы являются идеальным средством шпионажа против России (поскольку позволяют «подготовленным» серверам дублировать и передавать любую проходящую через них информацию в любом «нужном» направлении), а системы на основе этих протоколов могут быть легко парализованы, так как в них заложена эта возможность. Как следствие, они могут «зависнуть» в любой самый неподходящий момент, в чём заинтересованы потенциальные враги России.

Тем не менее протокол TCP/IP активно используется в критической инфраструктуре. Зарубежные спецслужбы это устраивает, поскольку упрощает и удешевляет шпионаж. Да и российские коррупционеры довольны, поскольку эти протоколы можно бесплатно скачать из Интернета, сделав при этом вид, что ты заплатил за их разработку огромные деньги.

Но если вдруг неожиданно в не самый подходящий момент произойдёт потеря управления космическими аппаратами, и при этом произойдёт авария, да ещё не дай бог с гибелью людей, что тогда?

Вместе с тем сами США и Европа применяют в своих новейших авиационно-космических разработках протоколы совсем другой группы. Называется эта группа протоколов TTP (Time-Triggered Protocol).

В числе авиационно-космических изделий, на которых применили эту новую группу протоколов TTP: Global-7500; F-16; Boeing-787; A-380 и др.Более того, за рубежом этот TTP-протокол принят как стандарт протоколов для критически важных систем, это так называемый стандарт SAE AS6003.

Сейчас в России повсюду внедряется IP-телефония. Повторим, что это идеальное средство для шпионажа против России со стороны зарубежных спецслужб.

Между тем интересно, что дальность по проводам до ближайшего концентратора в IP-телефонии – 100 м (причём четыре провода специального высокочастотного сетевого кабеля). А в обычной цифровой телефонии – 5000...7000 м (причём два провода обычного телефонного кабеля). Как говорится, почувствуйте разницу!

Всё это, а главное – возможность внешнего управления «живучестью» таких сетей связи, говорит о том, что IP-телефония хороша как некое дополнительное средство, но отнюдь не как основное. При помощи IP-телефонии можно легко снять секретную информацию и транспортировать её за рубеж из любого учреждения или предприятия России, в котором она присутствует. Как снимается информация? Очень просто!

Техника «съёма» информации

Дело в том, что в современных системах цифрового кодирования речи применяется так называемый «комфортный шум». В ситуации, когда абонент молчит, возникает эффект так называемого «ватного уха». И слушающий абонент испытывает дискомфорт, поскольку постоянно думает, что связь прервалась. Чтобы этого избежать, в моменты, когда абонент молчит, в канал добавляется так называемый «комфортный шум». В то же время особенности человеческого слуха таковы, что человек не слышит шумовых помех, которые маскируются громко звучащей речью. И именно это позволяет реализовать передачу на любые расстояния снятой с объекта «секретной информации» посредством сигнала [1]. При этом в канале возникнет «псевдокомфортный шум». На фоне речи он будет незаметен, а при отсутствии речи роль его будет даже положительна (правда, не с точки зрения информационной безопасности, а с точки зрения «комфорта» слушающего). Таким образом, на фоне одного открытого разговора можно снимать и транспортировать один секретный разговор (ведущийся через АТС или в других организациях).

Обычный цифровой телекоммуникационный канал между АТС Е1 (2 Мбит/с) является носителем 30 цифровых речевых каналов. Таким образом, мы приходим к интересному выводу о том, что, имея всего один цифровой канал Е1 между АТС (а меньше не бывает, только больше), можно «увести» в сторону 30 секретных речевых каналов. Очевидно, используя нехитрые (скорее даже примитивные) цифровые методы, можно транспортировать снятую секретную информацию за рубеж или (и) в посольства зарубежных стран.

Стоит это при современном уровне развития микроэлектроники малые доли цента! Согласитесь, учитывая, что годовой бюджет зарубежных спецслужб исчисляется огромными суммами, можно ли предположить, что они не воспользовались такой очевидной копеечной возможностью? Вряд ли...

Тем временем в России процветает массовая сборка якобы собственных

цифровых АТС. Производятся они на базе зарубежных спецмикросхем связи, несомненно, содержащих на уровне кристаллов шпионские закладки. Более того, они повторяют архитектуру зарубежных цифровых систем связи (конкретно – АТС производства SIEMENS, Германия). Но при этом спроектированы-то они в России (!).

Вопрос тогда в том, а что же, собственно, спроектировано в России? – А в России спроектирован дизайн. То есть внешне АТС не похожа на импортную АТС, а внутри она вся импортная. И она уже получила сертификат информационной безопасности! И дан сертификат такой солидной структурой как ФСБ России. Опираясь на этот сертификат безопасности связи, её уже успешно внедряют во все силовые структуры! В их числе ФСБ, Министерство обороны России и др.! На самом деле, это, конечно, несомненный успех разведки, правда, не российской, а BND (немецкой разведки).

Россия на современных импортных сборочных линиях сама массово собирает цифровые АТС из зарубежных (потенциально содержащих шпионские закладки на кристалле) спецмикросхем связи, по архитектуре повторяющие известную импортную АТС, а потом сама же внедряет их в силовых и других жизненно важных структурах, например американские цифровые АТС Avaya внедрены даже в концерне воздушно-космической обороны «Алмаз-Антей».

Отказ на линии «ЮГ» Ростелекома

Зимой 1998–1999 годов в ТЦМС-22 (Территориальный центр междугородной связи 22), отвечающем за связь на направлении «ЮГ» Ростелекома (Москва, Тула, Орёл, Курск, Белгород и т.д.), один из авторов данной статьи, Андрей Железнов, вместе со специалистами его предприятия и Ростелекома проверяли, как будет работать разработанная и производимая его компанией цифровая АТС с кольцом АТС, расположенных вокруг Москвы, на тот самый не самый приятный случай. В процессе проверки специалисты ТЦМС-22 решили показать, как качественно это сделано у них на других системах. Речь зашла не об ЦАТС на «кольце», а о цифровых каналах связи, идущих на «ЮГ».

Они с гордостью показали рабочую станцию Hewlett-Packard. Показали на экране в графической форме трассу, идущую на ЮГ. Андрей Железнов посмотрел на это и задал всего один вопрос: «А кто писал эту прекрасную программу?». Они ответили: «Специалисты SIEMENS!». «Значит, специалисты SIEMENS контролируют вашу сеть лучше, чем вы, и они могут выключить её в любой момент, когда сочтут нужным?» – спросил Андрей Железнов. Специалисты ТЦМС-22 тогда подняли его на смех, сказав, что «этого не может быть, потому что этого не может быть никогда».

Год спустя (как раз началась 2-я чеченская война) вдруг вырубилось всё направление «ЮГ» Ростелекома. Вдруг ли? Попытки перезапустить оборудование оказались безуспешными. Попытки применить ЗИП не помогли. Призвали на помощь специалистов SIEMENS из Москвы, но и они ничего не смогли сделать. Тогда руководители Ростелекома связались с руководством SIEMENS в Мюнхене и сказали: «Сами понимаете, началась война, поэтому, если связь в ближайшее время не заработает, то руководство Ростелекома уволят (это в лучшем случае) или посадят (в худшем случае)». Руководители SIEMENS успокоили: «Всё нормально, всё будет хорошо!». И через полчаса связь заработала! Но главный и самый важный факт заключается в том, что российские специалисты не смогли восстановить связь самостоятельно!

Надо полагать, что проверка незадекларированных возможностей в оборудовании, поставленном фирмой SIEMENS, прошла успешно. «Успешно» с точки зрения немецкой разведки. Понятное дело, что Ростелеком имеет несколько глобальных линий цифровой связи («ЮГ», «СЕВЕР», «ЗАПАД», «ВОСТОК» и др.). На самом деле, по крайней мере в тот период, разные направления были сделаны на импортном оборудовании разных производителей. Правда, это распределение было довольно странным, скорее подозрительным: направление «ЮГ» построено на оборудовании немецкой SIEMENS; направление «СЕВЕР» построено на оборудовании американской AT&T; направление «ЗАПАД» построено на оборудовании французской ALCATEL; направление «ВОСТОК» построено на оборудовании японской NEC. Интересно, что это поразительно совпадает с военной активностью упомянутых стран в годы Первой мировой войны, Гражданской войны и Второй мировой войны.

Современные технологии шпионских закладок в современных цифровых АТС позволяют прослушивать телефонные разговоры и разговоры в помещениях и передавать их в штабы, расположенные на расстоянии в десятки тысяч километров. Во время войны в Ираке и Югославии связь в этих странах вообще отключили по команде извне, а ракеты на административные объекты наводились по пеленгу заранее установленных в них (закупленных их администрациями) средств радиосвязи стандарта Tetra. Кстати, а какой стандарт беспроводной связи используется российским Министерством обороны?

Несколько лет назад в США объявлено о создании кибервойск (нового рода вооружённых сил армии США, который должен вести войну в информационном пространстве) и объявлена задача: выведение из строя систем управления и связи в любой стране мира в любой необходимый момент времени. При этом было объявлено, что вся предварительная работа на территории главного потенциального противника уже проведена:

- Агентство национальной безопасности США (АНБ) (с бюджетом в несколько раз больше, чем ЦРУ) контролирует фактически все каналы телефонной связи в мире, полностью накапливает, систематизирует и анализирует все данные, циркулирующие в сети Интернет;
- Администрация Президента РФ, центральный аппарат ФСБ используют телефонную связь, базирующуюся на цифровой АТС HiCom, произведённой фирмой SIEMENS, теснейшим образом связанной с немецкой разведкой;
- большинство предприятий ракетно-космической промышленности России установили цифровые АТС DEFINI TY, произведённые американской компанией Avaya (ранее она называлась LUCENT, а ещё ранее – AT&T), которая теснейшим образом связана с ЦРУ и другими спецслужбами США;
- вся инфраструктура связи в России (сети Ростелекома и базовая сеть областных филиалов СВЯЗЬИНВЕСТА) полностью переведена на импортное оборудование;
- вся мобильная связь России поколения 5G (базовые станции и телекоммуникационное оборудование) на несколько лет вперёд законтрактована аппаратурой китайской (радует, что не американской!) компании Huawei.

ПАТРОНАЖ ТПП РФ

21-24
СЕНТЯБРЯ 2021
САНКТ-ПЕТЕРБУРГ
КВЦ «ЭКСПОФОРУМ»

Radel

XXI МЕЖДУНАРОДНАЯ ВЫСТАВКА

РАДИОЭЛЕКТРОНИКА & ПРИБОРОСТРОЕНИЕ

- ЭЛЕКТРОННЫЕ КОМПОНЕНТЫ И КОМПЛЕКТУЮЩИЕ
- ПЕЧАТНЫЕ ПЛАТЫ И ДРУГИЕ НОСИТЕЛИ СХЕМ
- СВЕТОДИОДНЫЕ ТЕХНОЛОГИИ
- РАЗРАБОТКА И ПРОИЗВОДСТВО ЭЛЕКТРОННЫХ УСТРОЙСТВ
- РОБОТОТЕХНИКА
- КОНСТРУКТИВЫ
- МАТЕРИАЛЫ
- ТЕХНОЛОГИИ
- ПРОМЫШЛЕННОЕ ОБОРУДОВАНИЕ И ИНСТРУМЕНТЫ
- КОНТРОЛЬНО-ИЗМЕРИТЕЛЬНЫЕ ПРИБОРЫ И ЛАБОРАТОРНОЕ ОБОРУДОВАНИЕ

ОРГАНИЗАТОР ВЫСТАВКИ:

FarEXPO PROFESSIONAL EXHIBITION & CONGRESS ORGANIZER

radelexpo.ru **(812) 718-35-37**

Может быть, в Администрации Президента РФ, Совете безопасности РФ, Минобороны РФ, ФСБ РФ, Военно-промышленной комиссии просто не знают об этом?

Безопасность микропроцессоров

В годы застоя в СССР был запущен грандиозный проект «ЕС-ЭВМ» («Единая система ЭВМ», копия семейства ЭВМ IBM-360/370, фирма IBM, США). Ради этого огромного проекта – «ЕС-ЭВМ» – в СССР прекратили, а по сути «убили» (вместо того, чтобы воспроизвести в интегральном исполнении), дальнейшее развитие советских ЭВМ семейства БЭСМ, вполне классных машин с массой наработанного собственного серьёзного программного обеспечения (включая системы трассировки 20-слойных печатных плат, разработки и трассировки матричных СБИС, моделирование разного рода процессов и т.п.). И это была самая крупная и (по мнению авторов) самая успешная экономическая диверсия против СССР, сравнимая по своим экономическим и историческим последствиям разве что с «антиалкогольной компанией» М. С. Горбачёва.Затем в СССР решили развивать «СМ-ЭВМ» («Серия малых ЭВМ», копий семейства PDP-11/70 фирмы DEC, США). Хотя разработчикам вычислительной техники уже было понятно, что, как только ты начинаешь копировать что-либо, ты заведомо обрекаешь себя на отставание, и хорошо, если на годы, а не навсегда, т.к. развивать чужие системы невозможно, а потому бессмысленно! Безответственность и тупость чиновников (которых отбирали из неудавшихся инженеров) привели к тому, что в СССР тогда было выработано ошибочное решение о том, что все перспективные бортовые вычислители (включая работающие в режиме реального времени (!) бортовые вычислители боевых самолётов и ракет) должны были быть программно совместимыми с СМ-4 (медлительная микропоследовательностная машина, в которой каждая команда выполняется посредством выполнения десятков микрокоманд). Под эту, «благородную» на первый взгляд, идею «единения», «зарезали» фактически все собственные перспективные разработки Минэлектронпрома СССР, который как раз в это время начинал выпуск микроЭВМ «Электроника НЦ-80», фактически не уступавшей американским. У неё, правда, был один очевидный «недостаток»: она была самостоятельной отечественной разработкой.

Получилось всё это в виду недооценки руководством СССР (но не специалистами! [12-15]) роли микроэлектроники и микропроцессорной техники для страны в целом (о кибербезопасности тогда вообще никто не задумывался), отсутствия единого центра координации работ в области микропроцессорной техники и её программного обеспечения, отраслевого «разделения труда», ведомственной раздробленности заказчиков, стремления одних министерств развиваться за счёт других и постоянных «оглядок власти на Запад». Но главное, потому что в то время большинство тем Минэлектронпрома (производившего микросхемы и транзисторы) финансировалось на вторичной основе. Тогда деньги выделялись первично профильным министерствам (Минавиапрому, Минобщемашу, Минрадиопрому, Минпромсвязи и т.д.), а уже потом эти ведомства, если считали нужным (!), выделяли часть из этих средств Минэлектронпрому, который по их заказу делал то, что им нужно.

А в США тем временем не «клали все яйца в одну корзину», а работали системно, развивая конкуренцию. Так, на рынке ЭВМ все эти годы работали следующие фирмы: в области ЭВМ для автоматизации медленно текущих операций работала DEC; в области ЭВМ для финансовых операций конкурировали IBM и NCR; в области ЭВМ для реального времени – Hewlett-Packard и Perkin Elmer; в области суперЭВМ – Cray, Control Data и Convex; в области рабочих станций – Hewlett-Packard и Silicon Graphics; в области персональных ЭВМ – IBM и Apple и т.д.Зато в СССР в области ЭВМ и большинства других изделий электроники конкуренции не было. Только вот сам СССР «почему-то» развалился.

Но вернёмся в современную российскую реальность. Изготовить отечественный микропроцессор теперь можно, но только за рубежом (fabless-производство, и то «до поры – до времени»), т.к. собственная микроэлектронная промышленность России разрушена. То, что есть, устарело. В лучшем случае мы имеем устаревшие импортные производственные линии. Производить микропроцессоры современного уровня сложности на них не только не рентабельно, а просто физически невозможно. Все расходные материалы этих линий импортные. А если нам перестанут их поставлять?

Вся обеспечивающая подотрасль для микроэлектроники тоже разрушена, её не существует!

Ещё одним «проколом» как отечественных (в том числе и авторов данной статьи), так и зарубежных разработчиков первых микропроцессоров было то, что они не могли даже предположить, что кто-нибудь когда-нибудь покусится на их детища и помимо их воли и воли пользователей начнёт запускать в микропроцессорные системы вирусы и прочие злонамеренные программы. В то время разработчики честно боролись за повышение производительности, снижение себестоимости, а решение всех проблем, связанных с безопасностью кибернетических систем, было (ошибочно, как теперь оказалось!) отдано на откуп программистам.Как результат, теперь мы имеем то, что имеем: весь мир неустанно борется с вирусами и киберпреступностью, а сама она превратилась в ужасную напасть для одних и в отдельную прибыльную отрасль техники, сделавшую долларовыми мультимиллиардерами других.

Тем не менее (даже значительно позднее, уже понимая весь драматизм ситуации по части кибербезопасности) весь мир упорно шёл проторённым, консервативным путём. Максимум, на что программисты (и то в целях самосохранения) поначалу «разрешили» пойти разработчикам классических зарубежных микропроцессоров, так это на введение NX-бита страниц памяти для борьбы с вредоносными программами (аналогичные, но значительно более глубоко продуманные комплексные средства защиты есть в процессорах «Эльбрус») [17].

В простейшем случае NX – атрибут страницы памяти (NX-бит: от англ. no execute – запрет исполнения кода на странице) в архитектурах x86 и x86-64 был добавлен для защиты системы от ошибок в непрофессионально написанных программах и от использующих эти ошибки вирусов, троянских коней и прочих вредоносных программ. А добавлен он был только потому, что для программистов это было просто «чёрной дырой» в безопасности программного обеспечения: ведь организация злоумышленниками преднамеренного переполнения программного стека в непрофессионально написанных программах с последующей передачей

управления в не предназначенную для исполняемых команд область памяти была классическим и самым массовым способом передачи управления вредоносным программам, в результате чего злоумышленники получали контроль над уязвимой системой.

Поскольку в современных компьютерных системах память разделяется на страницы, имеющие определённые атрибуты, разработчики процессоров добавили ещё один атрибут, обеспечивающий запрет исполнения кода на странице: такая страница может быть использована для хранения данных, но не программного кода. При попытке злоумышленников передать управление на страницу с запретом исполнения программного кода будет инициировано прерывание, ОС получит управление и завершит выполнение «подозрительной» программы. Смешно сказать, но на этой «ерунде» возникла целая индустрия киберпреступности и (соответственно) индустрия кибербезопасности.

К сожалению, и теперь, и тем более в будущем (после создания компиляторов, операционных систем и наработки колоссального количества прикладного программного обеспечения для стандартных архитектур) достаточно сложно внедрять в вычислительные системы, казалось бы, очевидные, простые, но требующие и аппаратной, и программной поддержки элементы безопасности, такие как защищённый прямой доступ к памяти с шифрованием данных для критически важных функций, защищённая загрузка и защищённое обновление кода, контроль доступа к защищённым ресурсам, аутентификация сеансов, защита наборов инструкций, на которые не должны выполняться переходы при ветвлениях, сохранение функции адреса возврата в отдельном «теневом» стеке после передачи управления и извлечение его перед выходом из функции, поддержка встроенного в накопитель оборудования inline-шифрования (Inline Encryption), осуществляющего прозрачное шифрование и расшифровку на основе заданных ключей и алгоритмов шифрования при вводе/выводе информации с дисков и т.д, и т.п.

Многое в части кибербезопасности, конечно, делается уже сейчас, причём максимальная эффективность защиты достигается как раз там и тогда, когда разработчики имеют как возможность модернизировать вычислительную систему на структурном уровне процессоров (модифицировать сам кристалл), так и возможность модифицировать (а зачастую создавать заново) её системное (OS, компиляторы) программное обеспечение.Например, в микропроцессорах «Эльбрус» уже используются защищённые вычисления, основанные на контекстной защите памяти на базе тегированной архитектуры, обеспечивающей стойкость к компьютерным вирусам и быструю отладку программ, а аппаратно поддерживаемая двоичная компиляция обеспечивает совместимость этой системы с другими платформами на уровне исполняемых кодов.

Для реализации всего этого потребовалась определённая поддержка и со стороны аппаратуры, операционной системы, и со стороны систем языкового программирования: компиляторов, редакторов связей, отладчиков. Предложенная разработчиками реализация обеспечивает полную и эффективную модульную защиту программного обеспечения (поддержанную аппаратурой и компилятором) и может служить основой для защиты системы от компьютерных вирусов, а достичь этого (а также обеспечить возможность дальнейшего развития этой «экосистемы») оказалось возможным исключительно благодаря тому, что и идеология, и архитектура, и структура микропроцессора, и его программное обеспечение (OS, компиляторы, компоновщики, загрузчики, отладчики) изначально разрабатывались в России, причём как всегда за копейки и «не благодаря, а вопреки». И всей этой истории около 50 лет.

Защита передаваемой информации

При передаче информации через открытые, незащищённые передающие среды важное значение приобретает её криптокодирование. Основной задачей криптографии является шифрование информации у источника её происхождения и дешифрования её в приёмнике при помощи ключей шифрования (не путать с квантовой «криптографией», используемой на волоконно-оптических линиях связи, которая не шифрует информацию, а делает её просто физически принципиально недоступной именно для несанкционированного «съёма»).

Формирование, распределение и защита от компрометации ключей осуществляется по-разному, в зависимости от области применения, среды передачи и класса проектируемых систем: системы массового обслуживания, спецсистемы и т.п. При передаче через незащищённую среду по открытым каналам связи любую информацию (текстовую, цифровую и т.п.) сначала преобразуют в двоичный поток бит, затем шифруют его (по тем или иным алгоритмам шифрования) двоичным кодом (ключом шифрования), передают зашифрованный двоичный поток по каналам связи, принимают и дешифруют этот поток при помощи двоичных же кодов (ключей дешифрования) с помощью соответствующих алгоритмов дешифрования, а затем восстанавливают исходную информацию в текстовом, цифровом или ином виде.

В системах массового обслуживания, передающих информацию через открытые (широковещательные) среды, совершенно отдельными проблемами являются передача (распределение) открытых ключей корреспондентам, принимающим зашифрованный поток информации, и формирование ими (на основе этих открытых ключей) ключей закрытых, при помощи которых осуществляется дешифрование цифрового потока на принимающей стороне, а также проблема защиты передаваемых ключей от компрометации [18].

Сам процесс шифрования и дешифрования осуществляется посредством примитивных логических операций в двоичном формате, над двоичной информацией, с использованием двоичных ключей, но для реализации криптоалгоритмов и алгоритмов работы с ключами (вычисление, аутентификация, верификация, генерация, распределение ключей, защита их от компрометации и т.п.) в настоящее время используют весьма сложные алгоритмы и весьма ресурсоёмкую процессорную «десятичную арифметику». Но разве не странно тратить вычислительные ресурсы и время на переход из одной системы счисления в другую и использовать ресурсоёмкие вычислительные процедуры в десятичной системе счисления, когда всё это можно сделать аппаратно (т.е. на несколько порядков быстрее) в двоичной системе на уровне булевых функций и двоичной арифметики?

Современные достижения в области дискретной стохастической криптографии позволяют создавать криптографические технологии совершенно нового типа, аппаратно (без потерь на про-

цессорную десятичную арифметику), в реальном масштабе времени решающие криптографические задачи на качественно новом техническом уровне и обеспечивающие информационную безопасность без снижения производительности компьютерных систем, что крайне актуально для обеспечения, а также ликвидации и в настоящем, и в будущем отставания технологий обеспечения безопасности от современного уровня развития техники. И такие технологии в стране есть.

Данные технологии, уничтоженные, помимо прочих [1-6], Департаментом радиоэлектронной промышленности Минпромторга РФ, могли бы обеспечить не только надёжный, эффективный и единый, универсальный (криптографического уровня стойкости) безбумажный и бесконтактный подход к маркировке, идентификации и сертификации товарной продукции во всех отраслях производства, что позволило бы не только обеспечить защиту товарного рынка и всех (!) сегментов экономики от контрафактной, фальсифицированной и недоброкачественной продукции, но и обеспечить загрузку полупроводниковых фабрик страны социально значимой продукцией, что, кстати, в своё время было принудительно сделано в Китае для подъёма его полупроводниковой индустрии.

При этом рутинный и малоэффективный «бумажный» ведомственный контроль за маркировкой и сертификацией товарной продукции был бы заменён эффективным электронным гражданским контролем, а взаимодействие средств электронной маркировки продукции со средствами электронного гражданского и государственного контроля за её качеством и продажей (реализацией) осуществлялось бы бесконтактно, радиочастотным способом. Помимо этого, возможно последующее масштабное распространение этой универсальной технологии на задачи защиты (с криптографическим уровнем стойкости) национальной цифровой криптовалюты, удостоверяющих документов, а также на другие приложения в сфере обеспечения безопасности как физических объектов, так и (что не менее, а даже более важно) информационных процессов.

Подобные технологии позволяют осуществлять на недоступном для конкурентов уровне решение огромного комплекса производственных, экономических и социальных задач: обеспечить вывод на качественно новый уровень безопасности цифровой техники и киберфизических систем, в первую очередь – устройств с дефицитом аппаратных ресурсов, где другие способы защиты просто неприменимы.

Выводы

Нет сомнений, что несмотря на все организационные (часто выдуманные чиновниками) и реальные технические трудности и аппаратная дискретная стохастическая криптография, и программно-аппаратные (реализованные на структурном уровне организации процессоров и компиляторов) средства противодействия киберугрозам постепенно внедряются и рано или поздно всё же будут внедрены в технику будущего во всём мире и позволят вычислительным комплексам и системам, поддерживающим безопасность не только на программном, но и на структурном и архитектурном уровнях, эффективно защититься от вредоносных программ и прочих киберугроз, создаваемых хакерами и киберпреступниками.

Другой вопрос: как защититься от закладок и незадекларированных возможностей потенциального противника, закупая у него технологии и электронное оборудование, с учётом усложнения всей этой техники с годами? Ведь по мере усложнения электронной техники (100-кратное усложнение каждые 10 лет) эта проблема будет только усугубляться и усугубляться, став в скором времени не только неразрешимой, но и необратимой. Существовать (что нам пока ещё разрешают США) на импортной технике стране ещё можно, а вот развивать саму эту технику – уже нет: это не только архисложно, но и бессмысленно, потому что бесперспективно. Как научиться её использовать, блокируя заложенные противником незадекларированные возможности и «шпионские закладки», да ещё не зная, кто из нынешних торговых партнёров (США или Китай) в будущем будет более опасен для России? По-видимому, никак!

Защититься от иностранного вмешательства в работу киберсистем в час «Ч» можно, только используя собственные процессоры (причём без использования в них чужих IP-блоков), собственные криптосистемы, собственные средства безопасности и собственные программные средства, «совместимые» с зарубежными разве что на уровне файловых систем, а также синтаксиса и семантики языков высокого уровня.

Электронные финансы – новый стимул развития российской электронной индустрии

При немыслимом (сотни триллионов долларов) размере внутреннего и внешнего госдолга США, во время пандемии их «печатный станок» вновь заработал и начал печатать новые доллары триллионами в месяц и «надувать» ими уже не какие-нибудь «доткомы» или «ипотеку», а свой последний (ничего другого уже не существует) оплот – финансовый сектор (попутно наводняя и мировой финансовый рынок «резаной зелёной бумагой»), что свидетельствует о неизбежности суверенного дефолта доллара (а соответственно, и резервных валют) в ближайшем обозримом будущем и перехода Человечества на новые, именно цифровые валюты (цифровой доллар, цифровой юань и т.п.), что сейчас уже является велением времени (технически апробировано на криптовалютах) и к чему и США, и Китай (в отличие от России) технологически уже готовы (у них есть системы-прототипы на уровне группы крупнейших банков).

И если раньше ЦБ России «не было позволено» даже думать о цифровых валютах, то в нынешней преддефолтной ситуации как с долларом, так и с самой государственностью США наличие хотя бы прототипа собственной национальной цифровой валюты – это уже вопрос жизни и смерти для России как государства. Но при этом следует понимать, что самое важное качество любой валюты – это её технологическая защищённость, причём как на данный момент, так и на исторически обозримую перспективу (!). Ведь в основном именно по этому признаку будет выбираться будущая мировая цифровая валюта.

Поскольку электронные криптоденьги намного эффективнее обычных выполняют роль универсального средства обращения (и не только его!), потребность экономики в них столь высока, что участники сферы обращения готовы были принять даже столь сомнительное средство, как Bitcoin. Но так как все существующие криптовалюты выполняют все пять функций «денег Маркса» (включая накопление капитала), то они обладают одинаковыми недостатками и имеют одинаковый печальный исход – нулификацию, т.е. финансовый крах. Но главным недостатком существующих криптовалют является отсутствие персонифициро-

ванного эмитента, что даже в будущем не позволит осуществлять целенаправленную эмиссию цифровых денег ни владельцам мировых валют, ни владельцам валют национальных, т.е. осуществлять ими осознанное и целенаправленное управление экономикой.

Такие возможности может предоставить стране национальная (государственная) цифровая валюта, технологический прототип которой обязательно должен быть создан и в России на случай дефолта доллара и резервных валют, на случай резкого ужесточения санкций (например, отключения транзакций SWIFT, VIZA, MasterCard и т.п.) или разрыва тех или иных международных договоров по независящим от России причинам.

Ведь в ту секунду (в тот день и час «Ч»), когда доллар да и все прочие фиатные валюты «вдруг» перестанут существовать (суверенный дефолт), главный «эмитент» мировых фиатных валют сможет защититься от владельцев валют с помощью военной силы, т.е. ракет (не потому ли отменен ДРСМД?), флота (не потому ли, казалось бы, бессмысленный американский флот по численности превосходит все остальные?) и кибервойск (а не для этого ли США и нужны кибервойска?).

Но что делать остальным странам, когда годом раньше или годом позже, но дефолт доллара все же произойдёт? Слишком огромен (приближается к триллиарду долларов) и несопоставим с размерами реальной экономики этот пузырь американского (и мирового) финансового рынка, и неизвестно, по какой именно причине и в какой момент он лопнет, и активы из финансового сектора экономики вдруг «низвергнутся» в реальный сектор и «затопят» его – слишком много в мире накопилось внутренних и межгосударственных противоречий. Не хотелось бы быть пророком, но, с грустью вспоминая анекдот про «коммунизм» и «Олимпиаду-80», мы опасаемся, как бы вместо ранее объявленной Зимней Олимпиады 2022 года в Пекине, в Китае не случился «коммунизм»: глобальный дефолт доллара, евро и других валют, т.е. «крах капитализма».

Во время глобального дефолта экономически одномоментно проиграют все (огромный финансовый пузырь лопнет, все «долги» будут списаны, коммерческие банки рухнут, накопленная населением «резанная зелёная бумага» аннулирована), и мир начнёт жизнь с «чистого листа».Но те (страны), чья экономика устоит, а технология государственных электронных финансов окажется прочнее, они и выйдут победителями из этой схватки и станут владельцами всех денег мира. После этого у победителя на мировой арене уже не будет никаких конкурентов долгие столетия, а вот остальные страны (проигравшие) будут вынуждены использовать финансовые технологии победителей, т.е. де факто станут их колониями, и история повторится сначала.

Как развивать экономику национальных государств «с нуля» (или не «с нуля»), «до дефолта» (или «после»), если каждое из них начнёт создавать свою национальную цифровую валюту и даже получит возможность «печатать» её в неограниченных количествах (пропорционально потребностям экономики)? Как вводить такие цифровые деньги в хозяйственный оборот?

В условиях открытой экономики, т.е. свободного обмена всех (в том числе и цифровых) валют и трансграничного движения капитала, все вброшенные, но невостребованные пустые «фантики» (в обмен на ресурсы) мгновенно «превратятся» в валюты более успешных и сильных государств, произойдёт очередной виток инфляции, рынок слабых стран заполнится дешёвыми иностранными товарами из более развитых государств, что дестабилизирует производство стран отсталых и замедлит рост их экономики. Опять всё пойдёт по тому же кругу: начнут развиваться сильные страны и эксплуатировать слабых. Всё это пройдено всеми и уже не раз.

Таким образом, мы приходим к выводу, что всё вернётся просто к аннулированию финансовых пузырей, законных и незаконных накоплений населения, переоценке ценностей и возвращению к основе основ – реальному производству. Так какой, спрашивается, смысл ждать глобального дефолта, очередного разрушения производства и как разорвать этот замкнутый круг?

Единственное разумное решение в данной ситуации (когда «невидимая рука рынка» явно уже с ней не справилась!) это заблаговременно, одновременно с переходом на национальную цифровую валюту встать на новый инвестиционный путь развития. Но инвестиционный совсем не в том упрощённом смысле, в котором его понимают финансисты и банкиры: «Вот вам деньги – вернёте в тройном размере, а ещё будете платить ренту... всю оставшуюся жизнь!».

Каким предлагается сделать российский цифровой рубль

Автор «финансового» раздела данной статьи (Алексей Галицын) заранее извиняется перед ЦБ РФ и Минфином за свою финансовую необразованность, а также за посягательство на святая святых –американский доллар и российский рубль. Но, видимо, время пришло и уже пора что-то делать, т.к. техническая подготовка к введению официальной национальной (государственной) цифровой валюты требует времени, но позволит России в критический момент, момент мировой паники, в час «Ч», когда произойдёт суверенный дефолт доллара и «вдруг» окажется, что под ним нет никакого обеспечения, а все финансовые транзакции (SWIFT, VIZA, MasterCard e.t.c.) будут остановлены, мгновенно запустить двух- или даже трёхконтурную систему электронного денежного обращения в стране.

К примеру, в СССР за две пятилетки мобилизационной экономики и индустриализации (по сути, подготовивших страну к Великой Отечественной войне) безо всяких там инвестиций было построено более 9000 (!) заводов, и не в последнюю очередь – благодаря введению в стране двухконтурной системы обращения. Да и сразу после войны (даже под угрозой ядерного нападения) СССР не поддался ни на какие уловки ФРС (в плане суверенитета советского рубля).

Тем не менее эмитируемые государством безналичные деньги обеспечивали развитие страны (фактически это было осознанное целенаправленное инвестирование), независимое от рыночного спроса-предложения. Наличные же деньги обеспечивали рыночные операции, а золото и валюта – внешнеторговые. Наличные и безналичные деньги были взаимно неконвертируемы: безналичными нельзя было дать взятку, а инфляции (без «ссудного процента») не могло быть в принципе.

Смысл нового государственного инвестирования в России должен заключаться в том, что эмиссия денег государством (вся или частично) должна осуществляться в развитие страны, а деньги должны вкладываться именно в это развитие посредством инвестирования цифровых денег (в трёх разных контурах) в перспективные инвестиционные (инновационные) проекты, создающие новые реальные ценности,

востребованные промышленностью и населением.

Причём инвестируемые цифровые деньги, будучи эффективным средством обращения, некоторое время (год, два, три) после их эмиссии не должны быть средством накопления, а должны стать средством, стимулирующим товарообмен, в цифровой форме это сделать достаточно просто. Таким средством и должен стать инвестиционный «российский цифровой рубль».

Формула российского цифрового рубля

Даже сейчас, соблюдая все «законы МВФ» (как это делает «законопослушный» Китай), т.е. вплоть до дефолта доллара, не увеличивая «незаконно» рублёвую денежную массу, а просто последовательно замещая «старые рубли» новыми «цифровыми рублями» (а после глобального дефолта денежную массу цифровых рублей можно будет в тот же день и увеличить... «сталинским» методом), можно и сейчас вводить в оборот «цифровой рубль». Более того, нужно обязательно убрать «функцию накопления» у распределяемых целевым образом, эмитируемых (инвестируемых – в указанном выше смысле слова) государством («бюджетных») цифровых денег «квазибезналичного контура» посредством введения по ним «отрицательной электронной» процентной ставки, что резко увеличит оборот денег и товаров (ускорит продвижение товаров) и кратно (что давно доказано) ускорит экономическое развитие страны. В то же время выбывающую (из-за отрицательной процентной ставки) общую стоимость всей цифровой валюты можно будет периодически восстанавливать осознанной целевой эмиссией новых цифровых денег (и запуском новых, востребованных обществом проектов) на вполне законных основаниях.

Таким образом, все эмитируемые государством новые цифровые деньги пойдут не на кредитование банков-паразитов и разгон инфляции (посредством ключевой ставки ЦБ, ссудного процента коммерческих банков и банковского кредитного мультипликатора), а на скорейшее создание востребованной обществом продукции. При этом функцию средств накопления начнут выполнять не спекулятивные виртуальные финансовые, а реальные активы (товары, природные ресурсы, интеллектуальная собственность и даже... золото), которые будут свободно обмениваться на цифровую валюту «квазиналичного» контура. Цифровые деньги оставят нетронутым все финансовые институты прошлого (в т.ч. и «ссудный процент»), но, как это ни странно звучит, постепенно заставят все эти институты «служить добру» (реальным нуждам экономической жизни), а не «злу» (закабалению людей), т.к. коммерческим банкам придётся конкурировать с дешёвыми и быстрыми «короткими» и «длинными» цифровыми деньгами, разумно эмитируемыми государством, и самим, до минимума сокращать свой паразитический ссудный процент, и (вынужденно!) оказывать реально полезные людям финансовые услуги.

Цифровые валюты ближайших конкурентов

Вскоре после начала работы над цифровым юанем (2014 год) Центробанк Китая (НБК) объединил усилия с Банком международных расчётов (БМР) и Международным валютным фондом (МВФ): Европейский центральный банк, Банк Англии, ФРС США, Банк Канады, Банк Японии, а также ЦБ Швеции и Швейцарии совместно с Банком международных расчётов уже определили основные требования к национальным цифровым валютам. В декабре 2019 года ЦБК заключил партнёрство с семью крупными государственными компаниями и банками, чтобы начать масштабное тестирование цифрового юаня. Госбанки КНР уже конвертировали часть своих депозитов в НБК в цифровую валюту и определили секторы экономики для её продвижения.

Анонимность транзакций будет пониматься лишь в контексте транзакций контрагентов, а у НБК будет доступ к информации обо всех операциях. К концу 2020 года НБК завершил разработку необходимых норм и правил, а регулятор предложил поправки в законодательство, которые предусматривают легализацию цифрового юаня и запрещают выпуск привязанных к нему токенов.

Победа в этой гонке позволит Китаю укрепить позиции юаня на мировой арене и сломить доминирование доллара, создав лучший продукт. Если старый добрый USD работает на древней инфраструктуре, то цифровой юань изначально создан для новой, цифровой, а платёжная система на основе цифрового юаня способна заменить морально устаревшую систему SWIFT на базе доллара. Полномасштабный запуск цифрового юаня (и, соответственно, начало его распространения по всему миру) предположительно состоится на зимних Олимпийских играх в Пекине в 2022 году, откуда «электронные кошельки с цифровым юанем» разлетятся по всему земному шару.

В серьёзности намерений китайцев, а также в том, что они своей настойчивостью, сплочённостью и целеустремлённостью добьются лидерства в мире, сомневаться не приходится, ведь согласно уже принятому компартией Китая плану социально-экономического развития страны на 14-ю пятилетку задачей Китая на ближайшие 5 лет будет превращение его в технологическую супердержаву путём создания самодостаточной замкнутой технологической экосистемы, не оставив всем конкурентам на планете никаких шансов. Для этого ежегодное финансирование всех НИОКР в стране будет увеличено в 17,5 раз (!) по сравнению с предыдущей пятилеткой (когда по технологическому уровню Китай практически сравнялся с США).

Первостепенные задачи, стоящие перед российской электронной индустрией

Раньше России можно было печатать фиатные деньги на любом допотопном печатном станке. Работать с юридическими и физическими лицами тоже было можно на любой непонятно какой импортной технике через коммерческие банки, это был их коммерческий риск! Но вот строить новую валютно-финансовую систему страны, систему национальных цифровых денег (когда, по сути, каждая транзакция будет проходить через ЦБ), и любые (все) риски будут приходиться на ЦБ и его «кибернетику», строить такую национальную систему на иностранных процессорах с уязвимостями и незадекларированными возможностями (ведь это даже не система по учёту налогов) просто недопустимо!

Строить новую цифровую валютно-финансовую систему страны можно только на безопасном цифровом оборудовании, поэтому стране жизненно необходима не только собственная процессорная техника, но и новая цифровая, защищённая аппаратной и квантовой криптографией государственная облачная платформа хранения, обработки и передачи данных. И создавать её надо уже сейчас, заблаговременно и комплексно (наряду с цифровой национальной валютой), а не потом, когда доллара «вдруг» не станет (!).

Наиважнейшее качество любой национальной цифровой валюты – её технологическая защищённость. На сегодня это сложный комплексный вопрос создания целой экосистемы, который должна решить отечественная электронная индустрия. В первую очередь от возможного иностранного вмешательства должна быть защищена (посредством полной замены процессорных и телекоммуникационных средств на отечественные) внутренняя (цифровая электронная) транспортная инфраструктура (маршрутизаторы, серверы, ВОЛС – на квантовые ВОЛС и т.п.), кроме того, заменена вся управляющая электроника на объектах критической инфраструктуры, и ещё должна быть создана защищённая государственная цифровая облачная инфраструктура и, соответственно, собственные защищённые системы хранения данных. Но для этого все эти отечественные технические средства должны быть созданы именно как элементы единой защищённой технической системы (не путать с РАО ЕС).

И момент для создания подобной инфраструктуры (системы) в государственном масштабе (по крайней мере, для госсектора) к настоящему времени с технической точки зрения полностью назрел, поскольку:

- во-первых, именно сейчас, с появлением облаков, качественно изменяется глобальная архитектура систем, что приводит к отмиранию архаичных (т.е. исторически созданных совсем для другого) процессоров (x86 и x86-64) и операционных систем (типа Windows, где есть много ещё не найденных уязвимостей и изначально заложены незадекларированные возможности), причём у страны есть шанс сразу перейти на более простую и более адекватную новой архитектуре самих систем, причём отечественную операционную систему и на отечественную аппаратную платформу;
- во-вторых, в стране уже создана и активно развивается экосистема «Эльбрус», следующее поколение которой уже «не за горами», оно будет в 300 раз быстрее и по производительности практически догонит зарубежные платформы. Но главное в этом то, что эти машины не будут содержать «незадекларированных» возможностей и будут иметь программное обеспечение и операционную систему с поддерживаемой на аппаратном уровне защитой от вирусов и других вредоносных программ. Т.е. это будет полностью контролируемая отечественными разработчиками, а главное развиваемая экосистема, которая должна быть вписана в глобальную отечественную (!) облачную архитектуру;
- в-третьих, именно сейчас Россия (с её-то просторами) весьма далеко продвинулась в области практической квантовой криптографии, точнее в области создания принципиально недоступных для потенциального противника транспортных волоконно-оптических криптосистем, а кроме того, в РКЦ впервые в мире был даже разработан квантово защищённый блокчейн – инструмент для создания распределённой базы данных, в которой практически невозможно подделать записи. Методы квантовой криптографии позволили защитить блокчейн от угроз, связанных с появлением квантового компьютера, потенциального «убийцы» классического интернет-трафика и всех

известных на сегодня, основанных на нем информационных и банковских сервисов. Далеко продвинулись и методы аппаратной дискретной стохастической криптографии, необходимые для защиты как самих технических средств, так и информационных процессов;

- в-четвертых, мировая полупроводниковая индустрия вышла на уровень «систем на кристалле» (System on Chip – SoC). На этом уровне развития полупроводниковая фабрика, производя кристалл, фактически будет производить функционально законченное изделие (электронную часть вещи или системы). Поэтому сегодня не приходится надеяться на западный мир, который осознал, что производить (в ущерб себе) и поставлять в Россию даже микросхемы прошлого века (не говоря уж о SoC), значит, терять огромные рынки и вооружений, и гражданской техники. Поэтому других альтернатив, кроме как инициировать собственные разработки SoC, у России в общем-то и нет (и никакой Китай ей в этом не поможет!).

Технической основой национальной цифровой валютно-финансовой системы и современных систем управления критической инфраструктурой (как было показано ранее) могут быть только технические средства, разработанные отечественными разработчиками (в частности процессоры не должны иметь в своем составе иностранных IP-блоков). Поэтому чем раньше страна поймёт и чем раньше вложит именно в электронную индустрию весь свой интеллект и всю свою оставшуюся финансовую «мощь», тем больше шансов у неё останется сохранить свой суверенитет и в итоге не стать колонией и отсталой страной третьего мира несмотря на наличие у неё атомного оружия. И именно сейчас, именно в электронной отрасли для нашей страны будет решаться вопрос: «To be, or not to be».

Особая роль и вклад экономистов в обеспечение безопасности

Сегодня при наличии гигантских природных ресурсов, при наличии людей и неплохих мозгов у самих этих людей в России уже которое десятилетие не наблюдается никакого развития и экономического роста якобы потому, что нет каких-то инвестиций. Но что такое инвестиции, да и откуда им взяться, инвестициям, в планово убыточную российскую электронную индустрию? Тем не менее с деньгами на электронную индустрию у РФ как раз проблем никогда и не было: «Денег у нас очень много», – обмолвился однажды глава «Роснано» [19]. При желании, а также при наличии политической воли не только нанотехнологии, но и обыкновенная микроэлектроника в стране могла бы уже быть не хуже, чем, например, в Германии.

Но в России на основании утверждённых экономистами бизнес-планов 20 лет подряд, всеми институтами развития, массово, триллионами, финансировались национальные бизнес-проекты по разработке электронной техники на «безопасной» импортной элементной базе, а госпредприятия закупали импортное программное обеспечение и импортные процессоры. Именно так «осваивались» триллионы. Типичный пример этому – «разработка» гипер-процессора «Кристофари» и будущего «российского» искусственного интеллекта на его основе.

В России вместо организации разработок систем на кристалле (SoC), т.е. формирования высокорентабельной добавочной стоимости, на народные деньги закупались планово убыточные полупроводниковые фабрики, с которыми теперь никто не знает что вообще и делать: фабрикам просто нечего производить, а затраты на их содержание огромны [20]. К счастью, «виноватый» во всём этом уже найден. Им оказался разработчик процессоров [21]. Но, как сказано в басне Крылова, по-видимому, он «виноват лишь в том, что хочется мне кушать...». Впрочем, какова истинная цель столь «жёсткой» скупки теперь «отечественных» и якобы безопасных процессоров и операционной системы, известно исключительно «экономистам»..., наука этого не знает.

Экономика и безопасность страны прочно связаны друг с другом. По текущему состоянию экономики России видно, что наши экономисты не в состоянии решить ни системные проблемы экономики, ни, соответственно, проблемы безопасности страны, потому что проблемы эти заключаются совсем не в том, от чего господа-экономисты предлагают страну «лечить» [16, 22]. Конечно, некоторые учёные-экономисты многое знают и что-то могут, некоторые даже очень многое, например, Андрей Рэмович Белоусов, 1-й вице-премьер Правительства России, но таких в стране немного.

Но даже лучшие учёные-экономисты могут решать только задачи параметрического анализа экономики в целом (на основе данных Росстата), а задачи параметрического и структурного синтеза (тем более, касающиеся конкретных технологических отраслей и их взаимодействия) они ни решать, ни решить принципиально не в состоянии). А ведь если допущены ошибки на структурном уровне, то никаким параметрическим анализом и управлением (в т.ч. законами и запоздалым латанием дыр народными деньгами) ситуацию уже не отрегулировать.

Если мы имеем проблемы в химической промышленности, то кого мы пригласим для обсуждения этих проблем и поиска решения? Пригласим химиков: теоретиков, практиков, организаторов. Если мы имеем проблемы в металлургии – пригласим металлургов. Если проблемы в обороне – пригласим военных и т.д. Так почему же такой сложнейшей технической, столь динамично развивающейся и комплексной отраслью, как нанотехнологии, электронная индустрия и вычислительная техника, были поставлены управлять вообще мало что понимающие во всём этом «ура-экономисты»?

Заключение

Реальные инновации, реальные системы, реальные прорывные и конкурентоспособные технологии создаются не чиновниками, не экономистами, а людьми совсем другого рода, в иной, научной и рыночной среде.

Но миллионы людей, среди которых сотни тысяч уникальных специалистов, покинули Россию. Только по официальной оценке РАН, если в 2013 году было 20 тыс. уехавших учёных, то в 2016 их стало уже 44 тыс., и это число к 2020 году лишь увеличилось.

Сотни перспективнейших проектов в области электроники, которые давно могли бы «поднять с колен» полупроводниковую индустрию страны (примеры тому – Китай, Южная Корея и т.п.), десятилетиями лежали, лежат и будут лежать «под сукном» у российских чиновников [1–6,23].

И главное, что теперь должна понять страна: отдавая последние деньги в руки новоявленных «ура-экономистов от электроники», ни по риторике ни по делам ничем не отличающихся от предыдущих [24], она проводит последний, причём смертельный экономический эксперимент. Пора, наконец, осознать,

что время глашатаев-болтунов, «ура-экономистов» и «ура-патриотов» закончилось. Началась Третья Мировая Электронная Война.

Литература

1. *Галицын А.* Неуправляемые боевые роботы и беспилотники. Современная электроника. 2020. № 9.
2. *Галицын А., Рождественский А., Рождественский Д.* Системы управления с «предвидением». Современная электроника. 2019. № 9.
3. *Галицын А.* Туманный Интернет вещей. Современная электроника. 2020. № 3.
4. *Егоров Е., Егоров В., Галицын А.* Явление и последствия волноводно-резонансного распространения и взаимодействия радиационных потоков. Часть 1,2. Современная электроника. 2020. № 1,2.
5. *Егоров Е., Егоров В., Галицын А.* Элементный анализ планарных нано-структур на базе рентгеновской эмиссии индуцированной высокоэнергетическим возбуждением. Современная электроника, 2021, №5
6. *Галицын А.* IoT-радиопроцессор с крипто-кодированием структуры радиосигнала. Современная электроника. 2019. № 7.
7. *Шпак В.* «О первом годе реализации Стратегии развития электронной промышленности до 2030 года». Интернет-портал YOUTUBE : https://www.youtube.com/watch?v=PK1vTyfmBJw&feature=share&fbclid=IwAR3f_O9AdopQUcz3sPC43IxfOHZUp_OV1wymBfBGLKQpXE_0N6d6IOHzulg.
8. В США пригрозили ответить России «не просто санкциями». Портал Лента.RU, Новости, 2021: https://lenta.ru/news/2021/02/21/ciber/.
9. *Андреев С.* Технологии под ударом. Зачем США ввели санкции против российской промышленности. Интернет-портал LIFE, 2019: https://life.ru/p/1359926.
10. *Королев И.* Российские электронщики объявлены врагами США: 119 имен и компаний. Интернет-портал CNEWS,2020: https://www.cnews.ru/news/top/rossijskie_elektronshchiki_obyavleny_vragami.
11. *Степаненко И.* Основы теории транзисторов и транзисторных схем. Издание 3-е, переработанное и дополненное, М. Энергия, 1973, 608 р.
12. *Алексенко А.* Основы микросхемотехники. М. Советское радио, 1971, 352 р.
13. *Алексенко А., Шагурин И.* Микросхемотехника: Учеб. пособие для вузов. Издание 2-е, переработанное и дополненное. М. Радио и связь, 1990, 496 с.
14. *Алексенко А. Графен, М.* Бином, 2014. 176 с.
15. *Алексенко А., Галицын А., Иванников А.* Проектирование радиоэлектронной аппаратуры на микропроцессорах. М. Радио и связь, 1984, 270 с.
16. *Железнов А.* Системные вопросы разрушения экономики СССР и России. Часть 1,2. Журнал «СВЕРХНОВАЯ РЕАЛЬНОСТЬ», 2008, №3, 2009,№4.
17. *Трушкин К.* Что такое «Эльбрус»? Официальный сайт компании МЦСТ, 2020: http://www.elbrus.ru/.
18. *Смоленцев С.* Информационные технологии. Защита информации в корпоративных сетях. Издательство ГМА им. Адмирала С. О. Макарова, 2009, 201 с.
19. *Чубайс А.* Выступление на собрании «Роснано». Интернет-портал YOUTUBE : https://www.youtube.com/watch?v=_lzr2UXAI1g
20. *Гатинский А.* Шувалов объявил о выделении заводу «Ангстрем-Т» почти 21 млрд руб. Интернет-портал РБК: https://www.rbc.ru/business/27/05/2019/5cebf51b9a79475a3786f801.
21. Baikal Electroniks. О компании. Официальный сайт компании «Байкал Электроникс»: https://www.baikalelectronics.ru/about/
22. *Ханин Г.* Как спасти от краха экономику России? Троицкий вариант. М. Наука, 2019, № 277, с. 15. Интернет-портал trv-science.ru: https://trv-science. ru/2019/04/23/kak-spasti-ot-kraxa-ekonomiku-rossii/.
23. *Галицын А.* Технология широкополосной высокозащищенной радиосвязи (C-UWB): что лежит «под сукном» у российских чиновников. М, Первая миля, Техносфера, 2008, № 1.
24. *Садыркин П.* «Роснано» создавали для технологического прорыва. Почему его не случилось даже через 13 лет. Интернет-портал LENTA.RU: https://lenta.ru/articles/2021/01/27/ rosnano/.

НОВОСТИ МИРА

К 2025 году число eSIM в мире достигнет 3,4 миллиарда

Исследование предполагает, что внедрение фреймворков eSIM от поставщиков потребительских устройств, таких как Apple и Google, ускорит рост ESIM. Исследование Juniper Research показало, что количество ESIM, установленных в подключённых устройствах, увеличится с 1,2 миллиарда в 2021 году до 3,4 миллиарда в 2025 году, что составляет рост на 180%. ESIM – это модули, встроенные непосредственно в устройства, которые обеспечивают сотовую связь и хранят несколько профилей операторов сети. Исследование независимо оценило внедрение eSIM и спрос в потребительском, промышленном и государственном секторе и прогнозирует, что к 2025 году на потребительский сектор будет приходиться 94% мировых установок eSIM. Исследование предполагает, что внедрение платформ eSIM от поставщиков потребительских устройств, таких как Apple и Google, ускорит рост ESIM в потребительских устройствах, опередив промышленный и государственный секторы. Глобальное развёртывание ESIM во всех потребительских вертикалях увеличится на 170% в течение следующих четырёх лет, а широкое внедрение будет зависеть от поддержки сетевых операторов. Чтобы помочь рынку, производители устройств должны оказать давление на операторов, чтобы они поддерживали платформы eSIM и ускоряли созревание рынка. Однако фрагментация поставщиков оборудования на рынке устройств сотовой связи IoT потребует от каждой вертикали принятия комбинации беспроводных технологий, оборудования и инструментов управления. В свою очередь, в отчёте прогнозируется, что появятся специализированные поставщики, которые обеспечат надёжные форм-факторы eSIM для промышленных сред. Разработка промышленных форм-факторов позволит поставщикам хорошо заработать на

рынке, поскольку установки eSIM в этих вертикалях вырастут с 28 миллионов единиц в 2021 году до 116 миллионов к 2025 году. Авторы исследования отметили, что обеспечение удобства для конечного пользователя должно оставаться главным приоритетом для поставщиков платформ управления eSIM. Для этого они должны обеспечить уровень обслуживания, сопоставимый с тем, который наблюдается при использовании традиционных SIM-карт.

www.eenewswireless.com

РОССИЙСКАЯ НЕДЕЛЯ ВЫСОКИХ ТЕХНОЛОГИЙ

Минцифры России

Комитет Государственной Думы Федерального Собрания Российской Федерации по образованию и науке

ТОРГОВО-ПРОМЫШЛЕННАЯ ПАЛАТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ufi Approved International Event

Expo Rating

СВЯЗЬ

«Информационные и коммуникационные технологии»

15–18 июня 2021

33-я международная выставка

Организатор

ЭКСПОЦЕНТР

При поддержке:
- Министерства цифрового развития, связи и массовых коммуникаций РФ
- Комитета Государственной Думы ФС РФ по образованию и науке

Под патронатом ТПП РФ

Россия, Москва, ЦВК «ЭКСПОЦЕНТР»

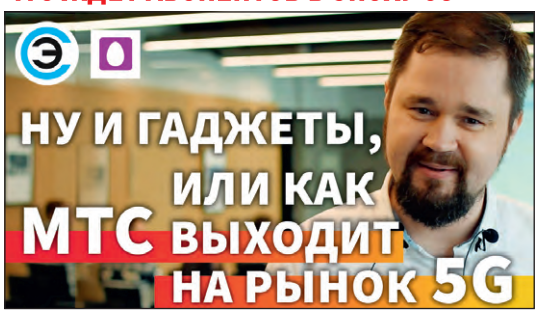
www.sviaz-expo.ru

12+ Реклама

YouTube

Смотрите на YouTube-канале СОВРЕМЕННАЯ ЭЛЕКТРОНИКА

ЧТО ЖДЁТ АБОНЕНТОВ В ЭПОХУ 5G



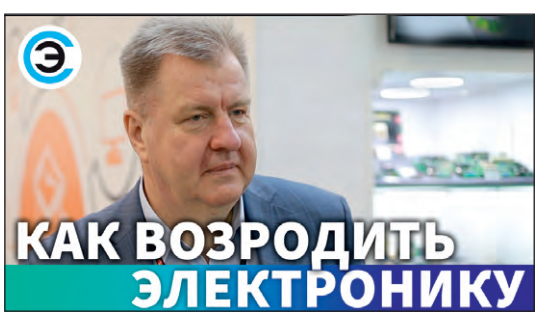
МТС
«...мы готовим набор гаджетов для консьюмерского рынка...»

СКОЛЬКО ГОЛОВ У СОВРЕМЕННОГО ГОРЫНЫЧА

Базальт СПО
«...у этой рабочей станции 8 ядер и 32 Гб оперативной памяти...»

8 апреля редакция журнала побывала в гостях у компании «Астра Линукс» на отраслевой практической конференции «Цифровая трансформация системы образования: импортозамещение в сфере IT». Мероприятие было интересным, а уж о его актуальности, в свете «отлучения» нашей страны от высоких технологий, и говорить не стоит.
На конференции мы познакомились и пообщались с представителями компаний, своими усилиями создающих надёжную, а главное – независимую отечественную IT-инфраструктуру.

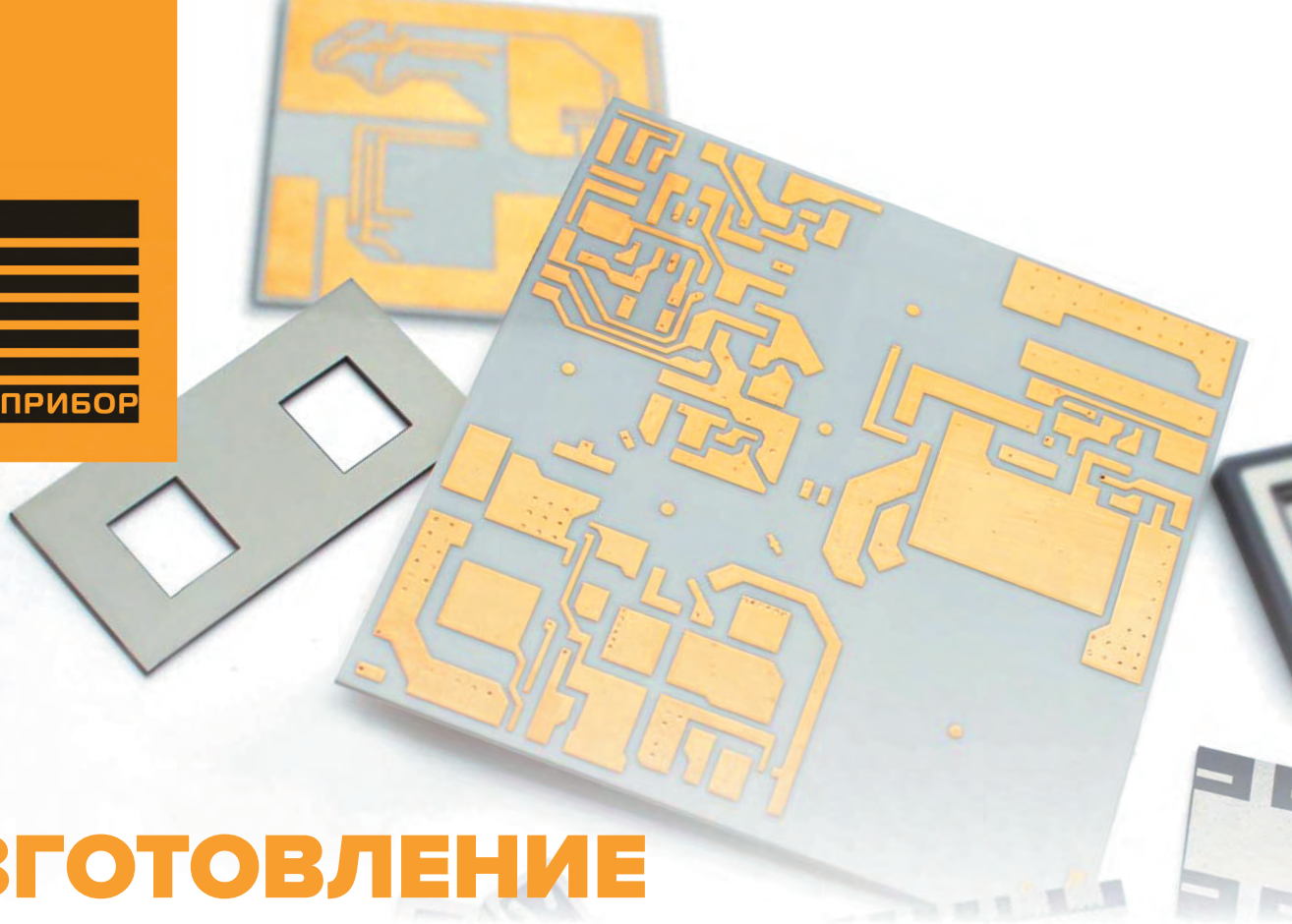
Скоро на нашем канале смотрите множество новых интервью, в том числе взятых на прошедшей в столице выставке ExpoElectronica-2021, в которых мы расскажем вам о перспективах отечественной электроники, о новых разработках и о том, насколько страшны для России технологические санкции.



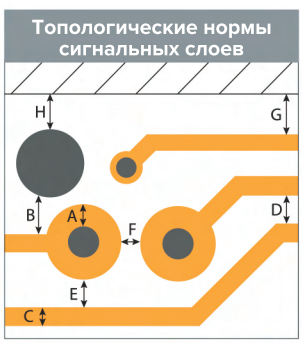
Как возродить электронику.
Павел Куцько,
Генеральный директор АО «НИИЭТ»

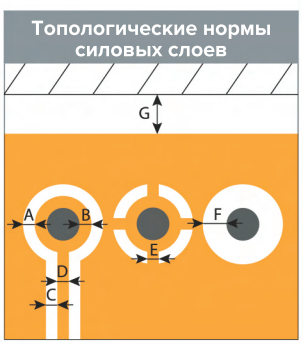
Технологическая независимость России – миф или реальность?
Светлана Легостаева, АНО «ВТ»

ТЕСТПРИБОР



ИЗГОТОВЛЕНИЕ
КЕРАМИЧЕСКИХ ПЛАТ И ПОДЛОЖЕК





АО «ТЕСТПРИБОР» осуществляет изготовление и поставку металлизированных керамических подложек на основе алюмооксидной керамики (Al_2O_3) и алюмонитридной керамики (AlN), которые предназначены для электрической изоляции конструкций, узлов и элементов различных электронных устройств.

Керамические подложки могут иметь как одно- или двухстороннюю сплошную металлизацию, так и топологический рисунок, сформированный в соответствии с техническими требованиями заказчика.

ХАРАКТЕРИСТИКА	ЕД. ИЗМЕРЕНИЯ	ЗНАЧЕНИЕ			
		Al_2O_3 92%	Al_2O_3 96%	Al_2O_3 99,6%	AlN
Цвет	–	Черный	Белый	Белый	Серый
Плотность	г/см^3		3,72	3,89	3,30
Влагопоглощение	%	0	0	0	0
Теплопроводность	Вт/(м•К)	14	28	29	180 – 220
КТЛР (20 – 1000 °С)	10^{-6}/ °К	7,1	6,8 – 8,0	7,2 – 8,2	6,2
Диэлектрическая проницаемость (1 МГц)	–	9,8	9,0	9,75	
Тангенс угла диэлектрических потерь (1 Мгц)	–	0,0024	0,0002	0,0001	0,0003
Напряжение пробоя	кВ/мм		15,0	25	15,0
Предел прочности при изгибе	МПа	400	300	400	260
Модуль упругости	ГПа	310	330	390	320
Прочность на сжатие	МПа		2100		–
Твердость	кг/мм^2		14 ÷ 15		1110
Удельное объемное электрическое сопротивление (20 °С)	Ом•см		10^{13}		10^{15}

+7 (495) 657-87-37 | tp@test-expert.ru | www.test-expert.ru | 125480, г. Москва, ул. Планерная, д. 7А