

# Экспресс-информация ПО ЗАРУБЕЖНОЙ ЭЛЕКТРОННОЙ ТЕХНИКЕ

Итоги выставки  
AutoSens-2019

Пьезоэлектрические  
MEMS-микрофоны  
корпорации Vesper  
Technologies

Защищенная загрузка  
с поддержкой  
FPGA в доверенных  
вычислительных архитектурах

Тайваньский стартап  
бросает вызов Google  
в области технологии  
распознавания жестов



1 Компетентное мнение



4 Итоги выставки AutoSens-2019



13 Пьезоэлектрические MEMS-микрофоны корпорации Vesper Technologies



17 Защищенная загрузка с поддержкой FPGA в доверенных вычислительных архитектурах



21 Тайваньский стартап бросает вызов Google в области технологии распознавания жестов



27 Новейшие исследования в области перспективных материалов



32 Аккумулятор, который можно сгибать, растягивать и скручивать



35 Главное авиационное командование ВВС США – об искусственном интеллекте



38 Безнагревная технология для производства гибкой электроники



41 Платформа Microchip Trust призвана упростить аппаратную безопасность Интернета вещей



45 Глоссарий

## Издатель

АО «ЦНИИ «Электроника»

## Главный редактор

Алена Фомина, д. э. н., доц.

## Заместитель главного редактора

Виктория Французова

## Научный референт

Валерий Мартынов, д. т. н., проф.

## Выпускающий редактор

Полина Корсунская

## Авторы материалов

Михаил Макушин,  
Елена Миронова,  
Анастасия Хомчик,  
Иван Черепанов

## Над выпуском работали

Григорий Арифудин,  
Людмила Железнова,  
Анастасия Никитина

## Реклама

publish@instel.ru  
+7 (495) 940-65-24

## Адрес редакции

127299, г. Москва,  
ул. Космонавта Волкова, д. 12  
+7 (495) 940-65-24  
www.instel.ru  
publish@instel.ru

Экспресс-информация  
по зарубежной электронной  
технике издается с 1971 г.,  
в электронной версии – с 2003 г.

Издание зарегистрировано  
в Федеральной  
службе по надзору  
за соблюдением  
законодательства в сфере  
массовых коммуникаций  
и охране культурного наследия  
(свидетельство ПИ № 77-13626  
от 20 сентября 2002 г.).



## КОМПЕТЕНТНОЕ МНЕНИЕ

Несмотря на то что тема искусственного интеллекта (ИИ) в последнее время широко обсуждается, его четкого и однозначного определения как на общетеоретическом уровне, так и во взаимосвязи с реальными технологическими решениями, методами, методиками и подходами, до сих пор не существует. Под понятием «искусственный интеллект» подразумевается открытое множество технологических решений, методик и методов, включая машинное и глубокое обучение, распознавание объектов и их признаков и т. д., причем отдельные позиции могут сами по себе и не быть элементами ИИ. Задача разработки подобного определения (определений) весьма важна в свете перехода к цифровой экономике.

Проблемы ИИ хорошо видны на примере автомобильной промышленности и военной авиации. На недавно состоявшейся выставке AutoSens-2019 был сделан прогноз, что автономные транспортные средства четвертого уровня (обращающиеся к человеку только в непредусмотренных программным обеспечением случаях) будут создаваться при полном и тщательном учете требований безопасности. При этом автомобиль, управляемый ИИ, достигнет уровня интуитивности, присущей людям – то есть понимания контекста управления и того, что он действительно управляет транспортным средством, – по крайней мере через 10 лет, а скорее всего – в пределах 20–30 лет. Одна из самых больших проблем ИИ – нехватка обучающих данных, в частности аннотированных. Обучающие данные необходимо помечать метаданными, но это занимает много времени. Предпринимаются попытки автоматизации данного процесса, например за счет глубокого обучения. Интерес представляет модель генеративно-сопоставительной сети (generative adversarial network, GAN), в которой две нейронные сети конкурируют за создание новых данных и, как сообщается, учатся генерировать новые данные с той же статистикой,

что и обучающий набор. Другой аспект проблемы – сложность точного аннотирования данных: лишь несколько крупных компаний могут позволить себе сделать это правильно. Стартапы, разрабатывающие алгоритмы ИИ, сталкиваются с существенными издержками на оплату сторонним организациям за аннотирование данных.

Положение дел в военной авиации США демонстрирует проект «Знаток» (Project Maven), находящийся на острие усилий Пентагона по обеспечению ВС США средствами и системами ИИ. В рамках проекта в 2017 г. вооруженные силы получили подобные средства и системы, позволившие, в частности, автоматизировать процесс просмотра огромного количества видео и фото с самолетов-разведчиков, спутников-шпионов и т. д. Сотрудники разведывательных служб удовлетворены результатами, чего не скажешь о руководстве ВВС. Его представители указывают, что имеющийся в их распоряжении ИИ соответствует уровню развития трехлетнего ребенка, а этого явно недостаточно для нужд военной авиации – и в любом случае выполнение программ должно контролироваться человеком. Правда, ВВС уже полагаются на ИИ для помощи в прогнозном обслуживании авиационного парка и ряде других задач, но это направление хорошо отработано и гражданскими авиакомпаниями. Отмечается, что алгоритмы Maven обучаются и становятся все лучше и лучше.

Как видим, не все ожидания, связанные с развитием технологий ИИ, оправдываются. Идет этап накопления опыта, на основе которого через какое-то время может последовать быстрое, даже взрывообразное развитие – но в разных сферах применения оно будет неравномерным.

*Михаил Макушин,  
главный специалист отдела научно-технического планирования РЭП*



# СПРАВОЧНИК ПРЕДПРИЯТИЙ

РАДИОЭЛЕКТРОННОЙ ПРОМЫШЛЕННОСТИ

[www.spravochnikrep.ru](http://www.spravochnikrep.ru)



**500** предприятий  
РЭП

**55** регионов  
России



## Шаг 1

Купите доступ



## Шаг 2

Войдите в личный кабинет

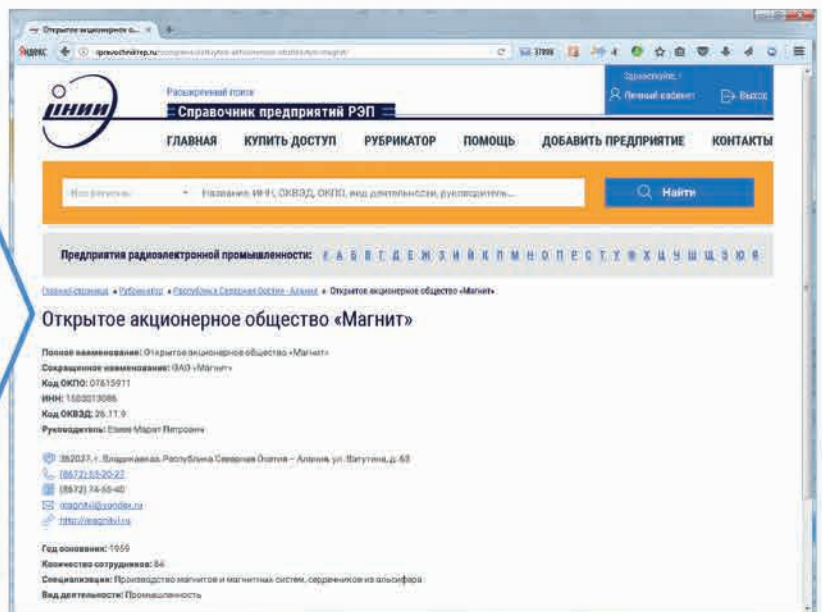


## Шаг 3

Получите актуальные данные

## Страница каждого предприятия содержит:

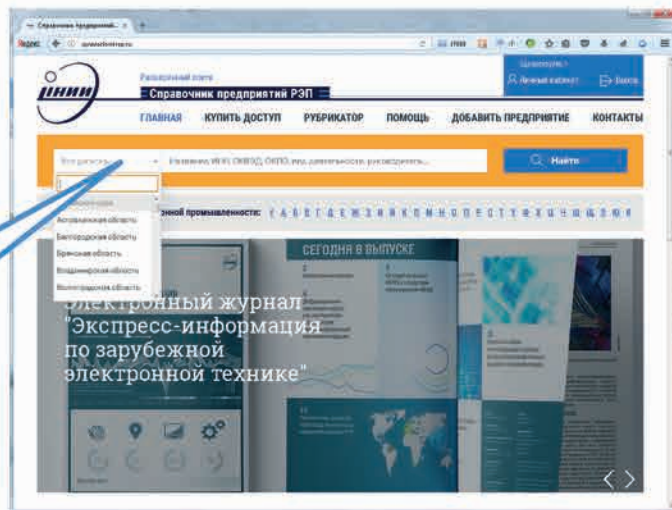
- полное и сокращенное наименование организаций;
- ИНН, ОКВЭД, ОКПО;
- ФИО руководителя;
- юридический адрес;
- телефон;
- e-mail;
- адрес сайта;
- наименование головной организации;
- год основания;
- количество сотрудников;
- специализацию;
- вид деятельности;
- состав входящих организаций;
- технологический уровень.



# Возможности поиска по сайту

1

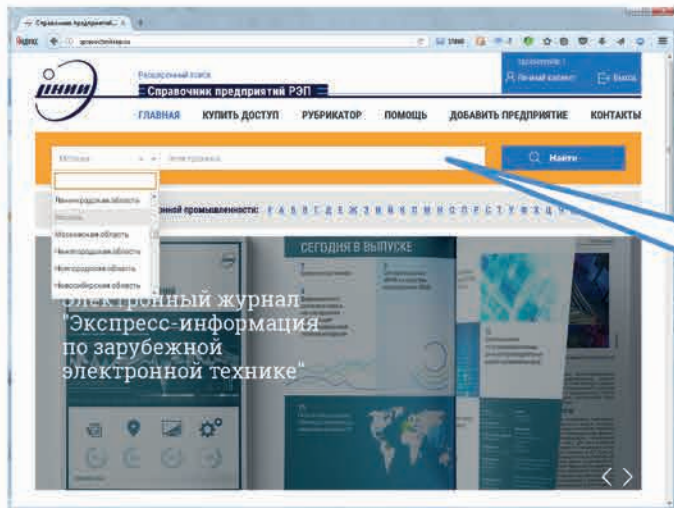
Поиск по региону расположения



Электронный журнал  
"Экспресс-информация  
по зарубежной  
электронной технике"

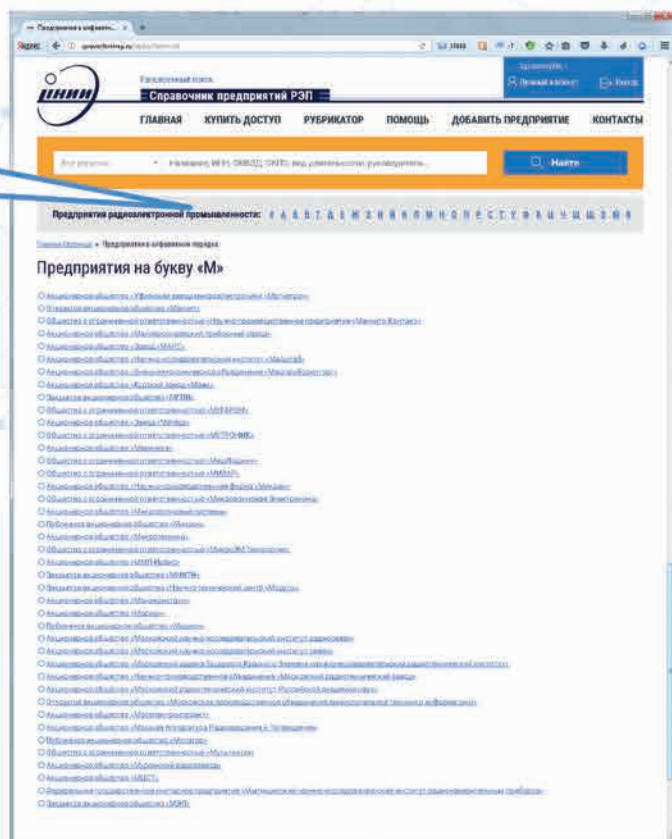
2

Поиск по всем регионам или по одному из регионов по одному из следующих параметров: полному или сокращенному наименованию, ИНН, ОКВЭД, ОКПО, ФИО руководителя, виду деятельности



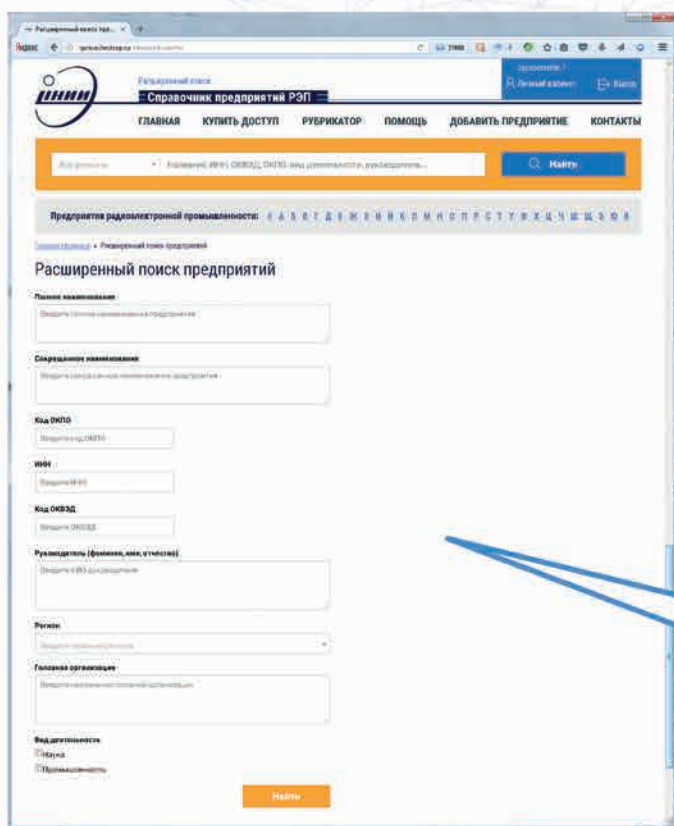
3

Поиск по первой букве наименования предприятия



4

Поиск по одному или нескольким параметрам: полному наименованию, сокращенному наименованию, ИНН, ОКВЭД, ОКПО, ФИО руководителя, региону расположения, виду деятельности, головной организации





# Итоги выставки AutoSens-2019

*Ключевые слова: автономные транспортные средства, безопасность, датчики, лидары, радары.*

*На недавно прошедшей в Брюсселе выставке AutoSens 2019 выяснилось, что в области средств автомобильной сенсорной техники нет недостатка в инновационных решениях. Разработчики автомобильных технологий, поставщики первого уровня и поставщики комплектного оборудования (OEM) охотятся за средствами «надежного восприятия», которые могут работать в любых дорожных условиях, включая ночь, туман, дождь, снег, наледь, нефтяную пленку и т. д. Единственного решения данной проблемы не существует, однако многие компании активно разрабатывают свои новые технологии восприятия и концепции соответствующих средств.*

Основное внимание на выставке уделялось в большей степени перспективным системам помощи водителю (ADAS), а не собственно автономным транспортным средствам (AV). Очевидно, что сообщество разработчиков в целом признает существование разрыва между сегодняшними возможностями и перспективами запуска коммерческих автономных транспортных средств, управляемых искусственным интеллектом без участия людей-водителей.

Речь не идет о том, что самоуправляемые автомобили невозможны. Тем не менее предсказывается, что четвертый уровень<sup>1</sup> автономных транспортных средств будет развернут в очень ограниченной области проектирования систем на уровне операций (operational design domain, ODD) при тщательном учете требований безопасности. Под ODD имеются в виду конкретные дорога, полоса движения, часы работы, погодные условия, время суток, точки посадки и высадки и т. д. На вопрос

о том, достигнет ли автомобиль, управляемый ИИ, интуитивности, присущей людям – то есть понимания контекста управления и того, что он действительно управляет транспортным средством, – отраслевые специалисты отвечают, что это произойдет как минимум лет через 10, а скорее всего – в пределах 20–30 лет.

Главная на данный момент задача, занимающая разработчиков ADAS и высокоавтоматизированных автомобилей, заключается в выборе оптимального оснащения автомобилей средствами восприятия окружающей обстановки (компьютерное зрение, радары и т. д.). Восприятие, т. е. «знание» того, где находятся и куда перемещаются объекты в окружающей среде, – основа каждого высокоавтоматизированного транспортного средства. Там, где автономные транспортные средства слабы по сравнению с водителем-человеком, важна возможность оценить ситуацию и предсказать, куда воспринимаемый объект будет перемещаться дальше.



## ИНТЕЛЛЕКТУАЛЬНОСТЬ ВЫХОДИТ НА ПЕРВЫЙ ПЛАН

На выставке-конференции AutoSens проявилась новая тенденция – наращивание интеллектуальности непосредственно первичных средств сбора данных. Многие поставщики добиваются этого за счет слияния разных датчиков и сенсорных данных. Среди подобных слияний и сочетаний наиболее популярны сегодня следующие:

- RGB-камеры<sup>2</sup> + датчики ближней ИК-области спектра (RGB+NIR);
- RGB-камеры + датчики коротковолновой ИК-области спектра (RGB+SWIR);
- RGB-камеры + лидары;
- RGB-камеры + радары.

Подходы основных игроков отличаются друг от друга. Одни, как было сказано выше, предпочитают строить комбинации датчиков «на переднем рубеже» – непосредственно на уровне сбора данных. Другие, такие как корпорация Waymo (г. Маунтин-Вью, шт. Калифорния, США), отдают приоритет централизованному

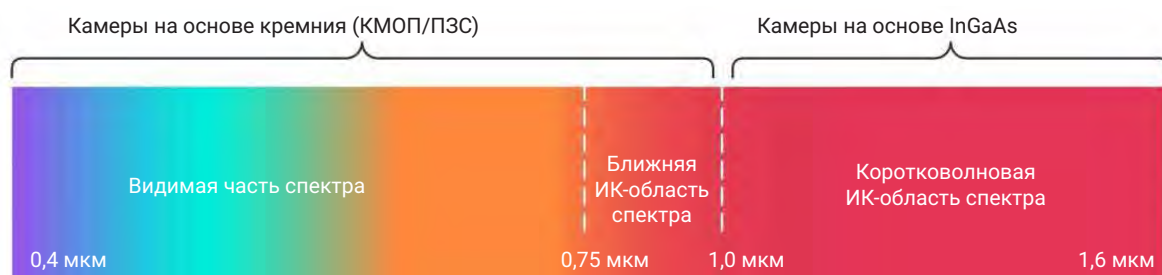
слиянию необработанных данных датчиков непосредственно в центральном процессоре.

Разработанная фирмой Seeing Machines (г. Файшвик, Австралия) система мониторинга водителей (Driver Monitoring System, DMS) была принята в качестве основного стандарта безопасности к 2020 г. в соответствии с требованиями EuroNCAP<sup>3</sup>. Однако помимо нее на выставке AutoSens было продемонстрировано много других новых систем мониторинга, в том числе контролирующих не только водителей, но и пассажиров и другие объекты внутри транспортного средства. Пример – новый датчик изображения RGB-IR, разработанный корпорацией On Semiconductor (г. Феникс, шт. Аризона, США) и сочетающий функции RGB- и ИК-датчиков. В нем используется усовершенствованная технология обработки RGB-IR-видеосигналов фирмы Ambarella (г. Санта-Клара, шт. Калифорния, США) и ПО ИИ фирмы Eyeqis (г. Пало-Альто, шт. Калифорния, США), обеспечивающее понимание ситуации в автомобиле.

## NIR И SWIR: СОПОСТАВЛЕНИЕ

Использование ИК-области спектра обусловлено необходимостью видеть в темноте – как внутри, так и снаружи транспортного средства. В то время как в полупроводниковом RGB-ИК-датчике формирования сиг-

налов изображения используется технология NIR (near infrared, ближняя ИК-область спектра), корпорация Trieye Technologies (г. Тель-Авив, Израиль) представила на выставке камеру, работающую в коротковол-



Источник: Trieye

Рисунок 1. Коротковолновая и ближняя ИК-область спектра, а также видимое излучение

новой ИК-области спектра (SWIR). Различия между двумя этими технологиями показаны на рис. 1.

К преимуществам SWIR относится возможность различать объекты заранее при любых погодных условиях и освещении. Что еще более важно, SWIR может обнаруживать опасности на дороге, такие как наледь (гололедица), в силу своей способности выявлять уникальные спектральные характеристики, определяемые химическими и физическими параметрами каждого материала.

До сих пор использование SWIR-камер ограничивалось военными, научными и аэрокосмическими приложениями из-за чрезвычайно высокой стоимости арсенида индия-галлия (InGaAs), используемого для их создания. Однако специалисты корпорации Trieye утверждают, что нашли способ создавать SWIR-приборы на основе стандартного КМОП-процесса (рис. 2), что позволило значительно снизить цены – если InGaAs-датчик стоит более 8,0 тыс. долл., то КМОП-камера будет предлагаться по цене в несколько десятков долларов.

## НЕХВАТКА АННОТИРОВАННЫХ ДАННЫХ

Одна из самых больших проблем ИИ – нехватка обучающих данных, конкретнее – аннотированных данных. Модель формирования логического вывода приемлема, данные и способ их сбора – тоже, но отмечается необходимость пометки обучающих данных метаданными, что занимает много времени. Для решения проблемы предпринимаются попытки автоматизации процесса. Например, модель Drive.ai для повышения автоматизации аннотирования данных и, соответственно, ускорения утомительного процесса их маркировки использует глубокое обучение. На выставке-конференции AutoSens-2019 состоялась оживленная дискуссия о модели генеративно-сопоставительной сети<sup>4</sup> (generative adversarial network, GAN). В ней две нейронные сети конкурируют за создание

новых данных. Как сообщается, GAN учится генерировать новые данные с той же статистикой, что и у обучающего набора.

Другой аспект проблемы – сложность точного аннотирования данных. Многие данные остаются немаркированными, потому что лишь несколько крупных компаний могут позволить себе сделать это правильно. Стартапы, занимающиеся разработкой алгоритмов ИИ, сталкиваются с существенными издержками на оплату сторонним организациям за аннотирование данных.

Подчеркивается, что GAN – лишь один из подходов к проблеме. Например, фирма Edge Case Research (г. Питтсбург, шт. Пенсильвания, США) предложила другой способ ускорить разработку более безопасного ПО для



Источник: Trieye

Рисунок 2. Структура SWIR-камеры корпорации Trieye





восприятия данных без маркировки. Недавно она анонсировала инструмент под названием Hologram, который предлагает систему стресс-теста восприятия ИИ и анализа рисков. Специалисты фирмы уже дважды запустили без маркировки набор данных емкостью около петабайта. Теперь инструментальное средство Hologram заранее оповещает пользователя о возможных трудностях, выделяя области, где ему лучше вернуться назад и перепроверить данные, собрать больше данных или добавить один или несколько этапов обучения.

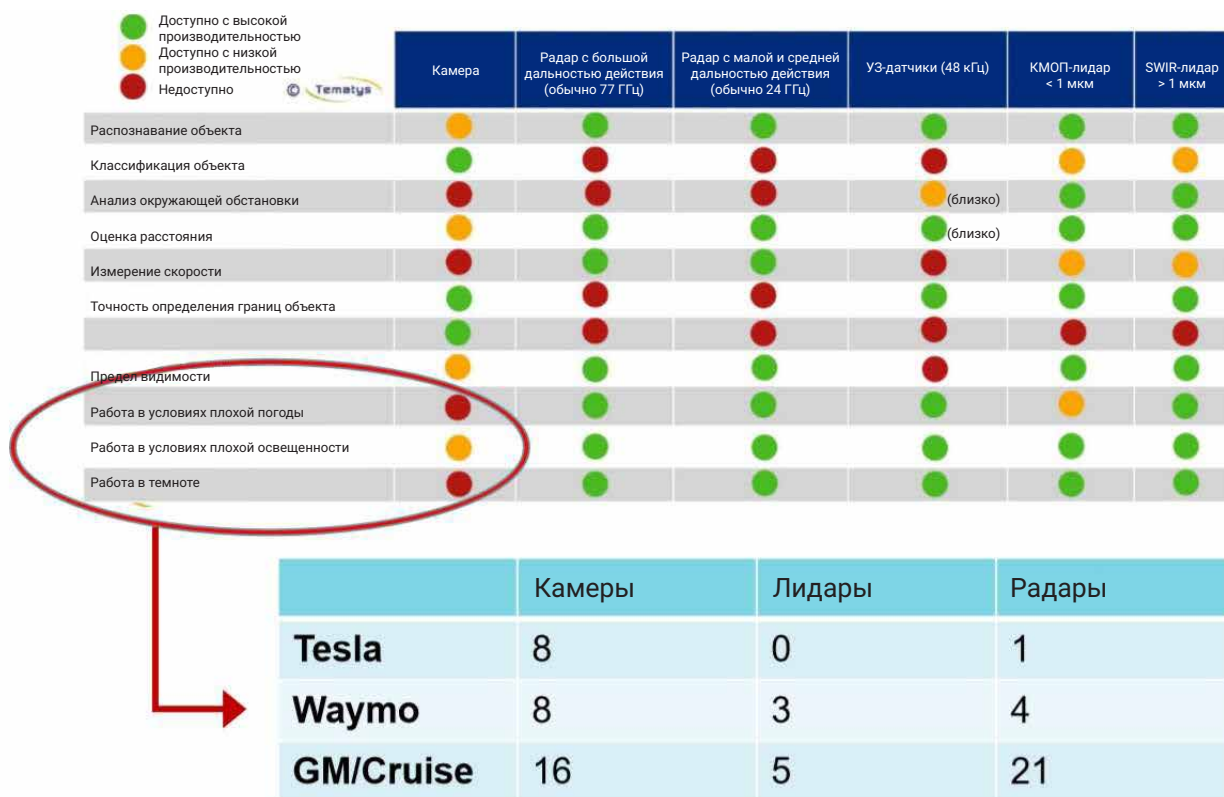
В ходе обсуждений на конференции была отмечена еще одна проблема, касающаяся работы с визуальными данными. Специалисты автомобильной промышленности, работающие над ADAS и автономными транспортными средствами, обеспокоены двумя вещами:

- надежным восприятием окружающей обстановки при любых условиях;

- точными и масштабируемыми визуальными моделями.

Типичные системы камер, устанавливаемые в настоящее время в ADAS или автономном транспорте, отличаются большой вариабельностью (рис. 3). В зависимости от объективов (различные объективы обеспечивают различные поля зрения), датчиков и способов обработки сигнала изображения различаются и все параметры. Любая высокотехнологичная компания выбирает конкретную систему камер, собирает большой набор данных, аннотирует его и обучает, чтобы построить точную модель нейронной сети, настроенную на систему.

Но что происходит, если OEM заменит камеру, первоначально использовавшуюся для обучения данных? Такое изменение может повлиять на точность восприятия, поскольку модель нейронной сети, настроенная на ори-



Источник: Algolux

Рисунок 3. Число камер, лидаров и радаров, используемых в автономных транспортных средствах Tesla, Waymo, GM/Cruise, и их характеристики

гинальную камеру, теперь вынуждена иметь дело с новым набором необработанных данных. Должен ли OEM в связи с этим снова обучать свой набор данных?

Специалисты фирмы VSI Labs (г. Сент-Луис-Парк, шт. Миннесота, США), обсуждая возможность замены формировавателей сигналов изображения, отметили, что при этом необходимо исходить из совпадения (полного или очень близкого) заменяемого и заменяющего приборов. В другом случае подобная замена не будет иметь смысла. Недавно они обучили собственную нейронную сеть для работы с тепловой камерой бортовой ИК-системы переднего обзора (FLIR). Учебные изображения были подобраны под характеристики камеры, на которой впоследствии была развернута нейрон-

ная сеть. Благодаря этому произошедшая замена учебного датчика на рабочий не привела к изменению характеристик системы.

Фирма Algolux (г. Монреаль, Канада), в свою очередь, представила набор средств оптимизации Atlas Camera Optimization Suite, позволяющий изменять ранее созданные наборы данных в соответствии с требованиями новых камер и формировавателей сигналов изображения «в течение нескольких дней». Это позволяет «демократизировать» выбор камеры для OEM-производителей. Однако и здесь есть свои ограничения – характеристики камер, под которые можно оптимизировать существующие наборы данных, должны быть заранее известны. Эти характеристики (камеры и датчика) закладываются в слои обнаружения объектов.

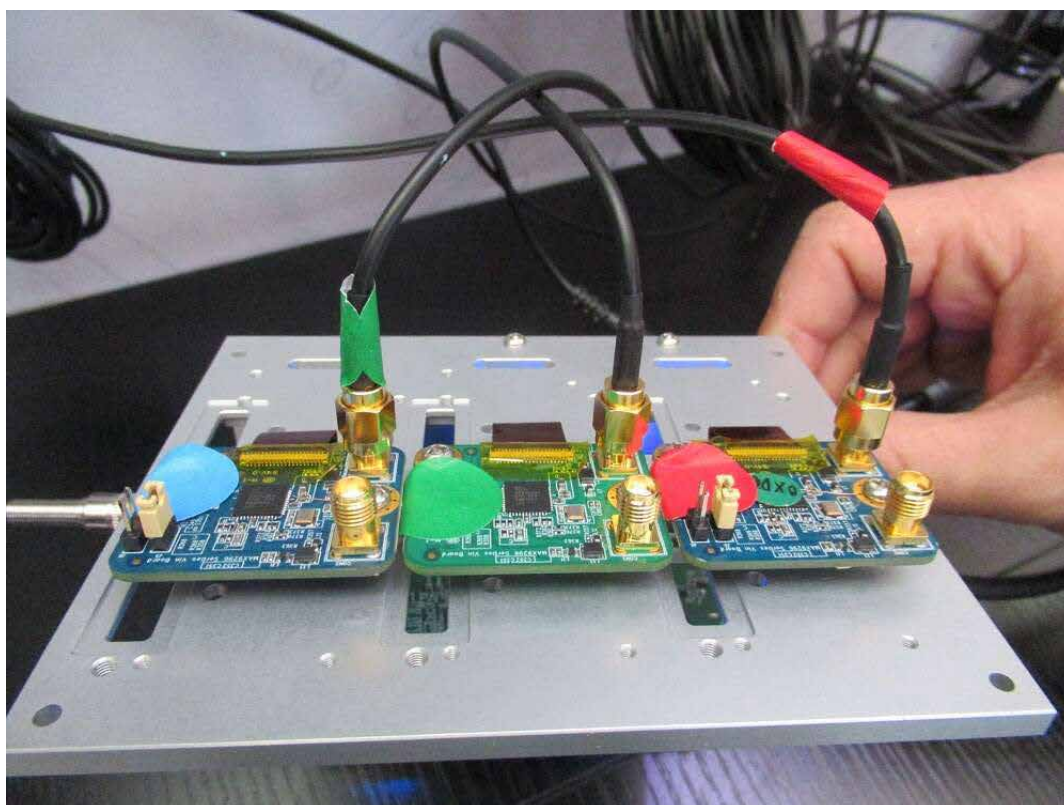
## АППАРАТНОЕ ОБЕСПЕЧЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

За последние несколько лет появилось множество новых стартапов, специализирующихся на процессорах ИИ, что позволило некоторым отраслевым обозревателям заговорить о наступлении «ренессанса» аппаратного обеспечения. Многие ИИ-стартапы рассматривают ADAS и автономные транспортные средства в качестве своих целевых рынков. Так, ориентируясь на формирующийся рынок ИИ-ускорителей, корпорация Seva (г. Маунтин-Вью, шт. Калифорния, США), представила на конференции AutoSens новое ядро ИИ и «стимулирующий интерфейс прикладного программирования» (Invite API).

Любопытно, но появление нового поколения многофункциональных автомобилей еще не привело к выпуску на рынок свежих ИС ИИ – помимо уже разработанных корпорациями Nvidia (г. Санта-Клара, шт. Калифорния, США) и Intel/Mobileye (г. Санта-Клара, шт. Калифорния, США; г. Иерусалим, Израиль), а также ИС «компьютеров полностью самоуправляющихся машин (fullself-driving (FSD) computer),

разработанных корпорацией Tesla (г. Пало-Альто, шт. Калифорния, США) для внутреннего использования.

С другой стороны, демонстрация RGB+IR-камеры на AutoSens показала, что команда корпораций On Semi и Eyeris выбрала «систему-на-кристалле» (SoC) фирмы Ambarella в качестве процессора ИИ для задач мониторинга в автомобиле. Сама система состоит из трех плат (рис. 4). Фирма Ambarella до сих пор рассматривалась как поставщик, традиционно ориентирующийся на средства сжатия видео и компьютерное зрение, ее появление в сфере ИС ИИ, в частности ускорителей ИИ, оказалось неожиданностью. Продемонстрированная ею «система-на-кристалле» (SoC) CV2AQ может поддерживать 10 нейронных сетей при потребляемой мощности менее 5 Вт. Частота смены кадров, контролируемых этой SoC-камерой, составляет 30 кадров в секунду, при этом в автомобиле Eyeris может быть установлено до шести камер, использующих ИИ-алгоритмы мониторинга. Предполагается,



Источник: EE Times

*Рисунок 4. Новая салонная система мониторинга с использованием трех RGB-IR-камер, созданная фирмами On Semi, Ambarella и Eyeris*

что ПО ИИ Ambarella к Зимней выставке бытовой электроники в Лас-Вегасе (Consumer Electronics Show, январь 2020 г.) будет перенесено еще на три платформы.

Представители корпорации On Semi подчеркивают, что приложения для мониторинга водителей и пассажиров требуют возможности «захвата изображений при переменном освещении от прямого солнечного света до полной темноты». Утверждается, что тех-

нология RGB-IR-КМОП-формирователей сигналов изображения обеспечивает выход сигнала полной высокой четкости формата 1080p<sup>5</sup> с использованием задней 3,0-мкм подсветки (BSI) и трехэкспозиционного расширенного динамического диапазона<sup>6</sup>. Датчики, чувствительные как к RGB, так и к ИК-свету, могут захватывать цветные изображения при дневном свете и монохромные ИК-изображения с подсветкой в ближней ИК-области спектра.

## УХОД ЗА ПРЕДЕЛЫ СИСТЕМ МОНИТОРИНГА ВОДИТЕЛЕЙ

Помимо мониторинга водителя ПО ИИ корпорации Eyeris может выполнять сложную аналитику положений тела и выражений лица, мониторинг активности пассажиров и обнаружение объектов. Просматривается все внутреннее пространство автомобиля,

включая поверхности сидений и руль. Иными словами, данное ПО ИИ уже вышло за рамки DMS, разработанной фирмой Seeing Machines.

Представители Seeing Machines, в свою очередь, отметили, что выход других разработчи-

ков за рамки их DMS-системы – естественная эволюция. Компания и сама продолжает совершенствовать свою систему. Преимущество Seeing Machines перед стартапами заключается в опыте использования ИИ в средствах компьютерного зрения, накопленном за последние 20 лет. В настоящее время DMS-система фирмы Seeing Machines принята на вооруже-

ние шестью автопроизводителями и используется в девяти различных программах.

Кроме того, Seeing Machines разработала собственное аппаратное обеспечение – ИС мониторинга состояния водителя Fovio. Предполагается, что СФ-блоки этой ИС будут применяться в конфигурируемых аппаратных платформах.

## ИЗБЫТОЧНОСТЬ И РЕЗЕРВИРОВАНИЕ

Совмещение дополнительных датчиков, работающих в различных режимах, и установка их в транспортном средстве необходимы не только для улучшения восприятия, но и для обеспечения избыточности (резервирования возможностей), крайне важной с точки зрения безопасности.

Стартап Outsight представил на выставке-конференции AutoSens новый высокоинтегрированный модуль, состоящий из нескольких датчиков. Этот модуль был разработан, чтобы обеспечивать восприятие всей окружающей среды (включая снег, лед и нефть на дороге) одновременно с определением местоположения, а использование активного гиперспектрального зондирования позволяет даже классифицировать дорожное покрытие. Специалисты Outsight не разглашают информацию о том, датчики каких фирм интегрированы в их модуль, сославшись на продолжающуюся настройку спецификаций и приложений. Высказывалось предположение, что в модуль будет интегрирована SWIR-камера корпорации Trieye, но сделка между двумя компаниями пока не заключена. Опытные образцы данного модуля, созданного по принципу слияния датчиков, будут предложены поставщикам первого уровня и OEM в I кв. 2020 г. в качестве дополнительной автономной системы, предлагающей «некоррелированные данные» для обеспечения безопасности и «истинной избыточности».

Корпорация AEye (г. Плезантон, шт. Калифорния, США) представила свою новую разработку – iDAR AE110, твердотельный MEMS-

лидар, объединенный с камерой высокой четкости и предназначенный для рынка ADAS и автономных транспортных средств (см. таблицу). Система, интегрирующая два датчика и функции ИИ, работающая в реальном масштабе времени, может использоваться, в частности, в ситуациях, возникающих при превышении каких-либо предельно допустимых параметров (например, выход из строя электронного компонента при превышении допустимого напряжения).

Система iDAR объединяет 2D-камеру («пиксели», RGB) и данные 3D-лидара («воксели»<sup>7</sup>, XYZ) с целью формирования нового типа данных, поступающих с датчиков в реальном масштабе времени. Данные этого типа обеспечивают более точную и интеллектуальную информацию, которая относится к большему, чем у других систем, расстоянию и намного быстрее поступает в систему планирования траектории автономных транспортных средств.

На презентации представители корпорации AEye заявили, что изучались различные варианты использования данной системы – около 300 сценариев. Из них было выбрано 56 применимых случаев, число которых потом сократили до 20 сценариев, где слияние камеры, лидара и ИИ имеет смысл. Был продемонстрирован ролик, в котором маленький ребенок внезапно выбегает за мячом на проезжую часть улицы – прямо перед автомобилем. Модуль, объединяющий камеру и лидар, а также обрабатывающий данные без их отсылки на центральный процессор («на переднем ру-



## ТАБЛИЦА СВОЙСТВА СИСТЕМЫ АЕ110 КОРПОРАЦИИ АЕУЕ ПО СРАВНЕНИЮ С ПРОМЫШЛЕННЫМИ КРИТЕРИЯМИ И ВОЗМОЖНОСТЯМИ

Спецификации лидара	АЕ110	Современные производственные возможности
Частота смены кадров	До 100 Гц	10–20 Гц
Дальность действия	230 м при коэффициенте отражения 10%	100–150 м
Растровая эмуляция	До 400 вертикальных каналов	16–64
Помехи	Менее 0,0000001%	3–11%
Уникальные возможности iDAR	АЕ110	Современные производственные возможности
Шифрование данных датчиков	Интегрированный антиспуфинг*	–
Частота повторной достижимости точки	В 3000 раз быстрее	–
Время смены кадра изучаемой области	10–30 мс (900 снимков)	–
Программно определяемые кадры	Фовеальный рендеринг**, окупаемость, эмуляция, синхронизация, случайность	–
Программная конфигурируемость	Четыре цепи обратной связи	–
UDP***-выход лидара	Оси X, Y, Z, интенсивность, цвета R, G, B, типы точек (фиксированные/плавающие) и т. д.	–

Источник: АЕУе

\* Спуфинг (spoofing) – перехват зашифрованного сигнала с его передачей в измененном виде незаметно для получателя.

\*\* Фовеальный рендеринг (foveated rendering) – техника графического рендеринга, основанная на динамическом отслеживании внимания пользователя к областям изображения.

\*\*\* UDP (user datagram protocol) – протокол пользовательских дейтаграмм.

беже») работает гораздо быстрее, уменьшая время реакции автомобиля. Отмечалось, что платформа iDAR может очень быстро обеспечить расчет снижения (повышения) скорости и необходимого маневра.

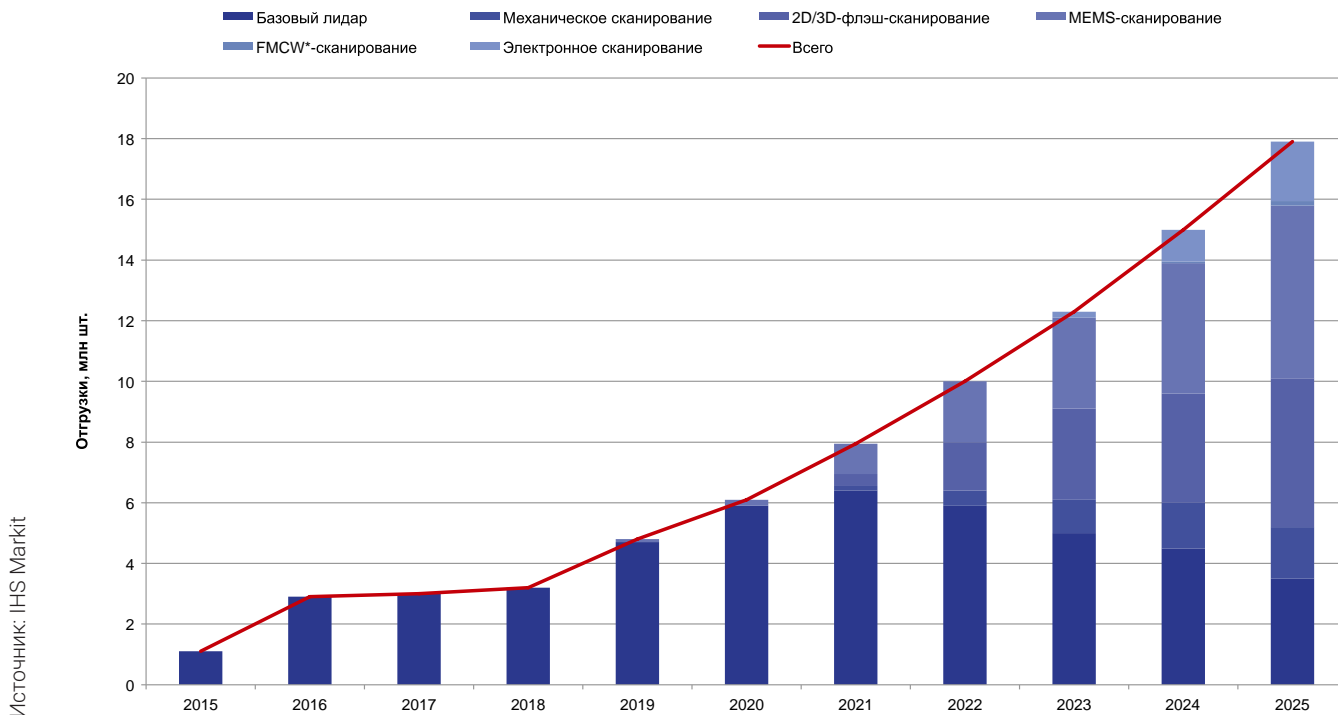
В рамках дискуссии представитель Waymo усомнился в преимуществах обработки данных в первичных модулях по сравнению с обработкой в центральном процессоре, указав что разница в миллисекундах реального значения иметь не будет.

АЕУе при разработке iDAR тесно сотрудничала с корпорациями Hella (г. Липпштадт, Германия) и LG (г. Сеул, Южная Корея), благодаря чему удалось существенно снизить стоимость

устройства – теперь 3D-лидар предлагается по ценам ADAS. Комбинированная система RGB+лидар автомобильного класса со встроенным ИИ появится на рынке в ближайшие три-шесть месяцев по цене менее 1,0 тыс. долл.

На рис. 5 приводятся фактические и прогнозные данные исследовательской корпорации IHS Markit (г. Лондон, Великобритания) по отгрузкам автомобильных лидарных систем в период 2015–2025 гг.

Специалисты IHS Markit на конференции отмечали, что поставщики лидаров демонстрируют «чрезмерно маркетинговый подход, обещая слишком много». Техническое



Источник: IHS Markit

Рисунок 5. Фактические и прогнозные отгрузки автомобильных лидарных систем в 2015–2025 гг. (2019 г. – оценка, 2020–2025 гг. – прогноз)

\* FMCW (frequency modulated continuous wave) – непрерывная частотно-модулированная незатухающая волна. FMCW-радар работает на сверхвысокой частоте (~24 ГГц), которая линейно нарастает на 2 ГГц в течение примерно 20 мс во время цикла измерения (качение частоты).

совершенство лидаров разных типов – вещь важная, но их успешный выход на рынок будет зависеть от стратегии коммерциализации (своевременность выхода на рынок, ценовая политика, инфраструктура поддержки и т. д.).

Соответственно, возникает существенная потребность в стандартизации, формировании альянсов и партнерских отношений (в том числе по проблемам ИИ), управление цепочками поставок и т. п.



Yoshida Junko. 6 Trends on 'Perception' for ADAS/AV. EE Times, September 23, 2019: [https://www.eetimes.com/document.asp?doc\\_id=1335127](https://www.eetimes.com/document.asp?doc_id=1335127)



# Пьезоэлектрические MEMS-микрофоны корпорации Vesper Technologies

*Ключевые слова: аудиозахват, пьезоэлектрические MEMS-микрофоны, распознавание речи, тонкопленочная технология, энергопотребление.*

*Сегодня микрофоны есть практически везде, и область их применения расширяется с удивительной скоростью – благодаря растущему спросу на смартфоны, приборы Интернета вещей, носимую электронику, слуховые аппараты, гарнитуры виртуальной реальности и другую потребительскую электронику. Корпорация Vesper Technologies (г. Бостон, шт. Массачусетс, США), поставщик пьезоэлектрических MEMS-микрофонов, решила использовать эту возможность для увеличения продаж.*

Корпорация Vesper Technologies впервые представила свою технологию распознавания речи с «нулевой» потребляемой мощностью – Zero Power Listening (ZPL) – в 2017 г. Технология основана на пьезоэлектрическом эффекте (впервые обнаруженном французскими физиками Полем-Жаком и Пьером Кюри) – благодаря ему акустический преобразователь работает в качестве акустического переключателя. При попадании звуковой волны на пьезоэлектрический кантилевер последний приходит в движение, которое за счет пьезоэлектриче-

ского эффекта создает разность потенциалов (электрическое напряжение). Напряжение воспринимается компаратором с очень малой потребляемой мощностью, посылающим сигнал возбуждения на остальные части системы.

Два года спустя технология ZPL была освоена крупными клиентами, такими как корпорации Samsung, Amazon и Bose. Ее популярность возросла, а корпорация Vesper Technologies достигла рубежей, которых изначально и не планировала достичь. Все это стало результатом сочетания нескольких факторов.

## РЫНОК НА ПОДЪЕМЕ

В смартфоне iPhone корпорации Apple используется четыре микрофона. В смарт-колонке Echo корпорации Amazon – семь микрофонов. Неудивительно, что современный рынок микрофонов устойчиво развивается. По данным исследовательской фирмы

Yole Développement (г. Лион, Франция), общий рынок MEMS-микрофонов (потребительская, автомобильная, промышленная и военная электроника) составил около 1,1 млрд долл. в 2018 г. и, как ожидается, достигнет 1,5 млрд долл. в 2024-м. При этом среднегодовой рост



продаж в сложных процентах (CAGR) за указанный период оставит 5%. По мнению специалистов Yole Développement, пьезоэлектрические технологии представляют собой одну из тенденций дальнейшего развития. В общей сложности продажи тонкопленочных пьезоэлектрических приборов в 2018 г. превысили 2,6 млрд долл., а в 2024 г. этот показатель вырастет до 6 млрд долл. Прогноз охватывает все типы пьезоэлектрических MEMS-приборов (см. таблицу). Пьезоэлектрические MEMS-микрофоны отличаются от традиционных емкостных микрофонов водонепроницаемостью, пыленепроницаемостью, ультранизкой потребляемой мощностью.

В целом пьезоэлектрическая технология набирает популярность и начинает омолаживать рынок MEMS, распространяясь на такие приборы, как микроакустические системы, пьезоэлектрические ультразвуковые преобразователи, изготовленные методом микрообработки (PMUT)<sup>8</sup>, средства автофокусировки и т. д.

На мировом рынке MEMS-микрофонов лидируют корпорации Knowles и Goertek, ожесточенно конкурирующие друг с другом за долю рынка. При этом корпорация Vesper Technologies, ставшая пионером в области пьезоэлектрических MEMS-микрофонов, до сих пор остается их единственным поставщиком.

## НА КОНУ – ДОЛГОВЕЧНОСТЬ И УСТОЙЧИВОСТЬ

По прогнозам IHS Markit, глобальный рынок умных домов в период до 2023 г. расширится почти в пять раз и достигнет 192 млрд долл. С проникновением в этот сектор приборов, постоянно распознающих речь, возникает риск роста энергопотребления и неблагоприятного воздействия с точки зрения углеродного

следа<sup>9</sup>. Потребляемая мощность стандартной смарт-колонки в режиме ожидания – 2,9 Вт, что близко к показателю в активном режиме (3 Вт). В умном доме с десятком приборов (пульта дистанционного управления, динамики и колонки, домашние помощники и телевизоры) потребление электроэнергии увеличивается на 262 кВт/ч

### ТАБЛИЦА ВРЕМЯ ВЫХОДА НА РЫНОК ПЬЕЗО-MEMS

Тип изделий	Начальный момент доступности тонкопленочной технологии для коммерческой продукции, годы
Печатающие головки струйных принтеров	2007
MEMS-гироскопы	2008
Фильтры на объемных акустических волнах	2011
Микрофоны	2016
Микродинамики	2018
PMUT для съемки отпечатков пальцев	2019
PMUT для распознавания жестов	2019
Средства автофокусировки	2021
PMUT для УЗ-зондирования	2022
Микронасосы	2026

Источник: Yole Développement





в год, что составляет 7,5% среднемирового потребления энергии домохозяйствами.

Пьезоэлектрические MEMS-микрофоны корпорации Vesper Technologies позволяют приборам с батарейным питанием оставаться в режиме «пробуждение-по-звуку» и хорошо подходят для потребительских приложений с малой потребляемой мощностью, постоянно готовых к распознаванию речи. Время автономной работы в таких приложениях имеет первостепенное значение, а в случае пьезоэлектрических MEMS-микрофонов оно может

быть значительно увеличено. Например, при использовании традиционной микрофонной технологии активируемые голосом телевизионные пульты дистанционного управления работают без подзарядки или смены источников питания около четырех недель. Технология ZPL позволяет растянуть этот срок более чем до полугода и даже до года – иначе говоря, по сравнению с другими системами распознавания речи технология корпорации Vesper Technologies может продлить срок службы батареи микрофона в 5–20 раз.

## МАСШТАБ ПРОИЗВОДСТВА

Представители корпорации Vesper Technologies отмечают, что даже перспективной технологии требуются «захватчики рынка»<sup>10</sup>. Так, например, случилось с фирмой Knowles в 2003 г. – она интегрировала MEMS-микрофоны в сотовые телефоны Razr корпорации Motorola, что позволило улучшить функциональность, уменьшив толщину и размер микрофона, и резко поднять продажи данной модели. Примерно это же происходит и с корпорацией Vesper Technologies – в 2018 г. их продажи составили менее 1 млн шт., а в 2019-м, по оценкам, превысят 10 млн шт. Фактически 2019 г. станет первым годом массового производства ZPL-микрофонов. Заказы на них уже сделали такие крупные клиенты, как Samsung, Amazon и Bose. Чтобы обеспечить их выполнение, Vesper Technologies заключила контракты с производителями первого уровня, крупнейшими кремниевыми заводами GlobalFoundries и TSMC, а также поставщиком услуг сборки и тестирования корпорацией Unisem. Vesper Technologies активно продолжает рекламировать преимущества ZPL-технологии – в 2018 г. была продемонстрирована возможность поставлять реализованные с ее использованием приборы в больших объемах (при этом налаживание массового производства обычных MEMS всегда связано со значительными трудностями).

В июле 2019 г. корпорация представила свой первый цифровой пьезоэлектрический MEMS-микрофон VM 3000. Этот прибор потенциально может использоваться в больших матрицах для 3D-аудиозахвата (оцифровки аналогового сигнала). Учитывая, что голосовое взаимодействие становится все более популярным, Vesper Technologies может выйти со своим новым микрофоном на рынки смарт-телевизоров, пультов дистанционного управления и смарт-динамиков. Типичное отношение «сигнал–шум» прибора VM 3000 достигает 63 Дб на частоте 1 кГц, величина амплитуды акустического входного сигнала, при которой выходной сигнал системы изменяется на 3 дБ относительно линейного уровня звукового давления (acoustic overload point, AOP), составляет 122 Дб. В зрелой емкостной технологии для предотвращения снижения показателя «сигнал–шум» из-за капель воды или пыли на 3–5 Дб или более используется защитная сетка, при этом параметры защиты зависят от толщины сетки. Соответственно, в жестких условиях окружающей среды, где необходима робастность, VM 3000 на данный момент представляет собой оптимальный выбор.

До конца 2019 г. корпорация Vesper Technologies намерена представить еще два прибора на основе технологии ZPL.

## ДОЛГОСРОЧНЫЙ ПРОГНОЗ И ПЛАНЫ РАЗВИТИЯ

Перспективные планы Vesper Technologies основаны на трех пунктах. Во-первых, компания стремится стать ведущим поставщиком датчиков для микрофонов. Эта цель может быть достигнута только за счет использования базовых технологий MEMS, улучшения отношения «сигнал–шум» и уменьшения размеров изделий.

Во-вторых, Vesper Technologies планирует производить другие типы датчиков на основе того же производственного процесса, объединять микрофоны с акселерометрами и датчиками температуры. Цель Vesper Technologies – быстро превратиться из разработчика и поставщика микрофонов в разработчика и поставщика однокристалльных решений, содержащих различные датчики.

В-третьих, Vesper Technologies хочет повысить степень интеллектуальности датчиков. Планируется на основе технологии Zero Power расширить возможности обработки сигналов. Например, добиться идентификации конкретных ключевых слов, активирующих систему, при игнорировании других звуков. Современные пьезоэлектрические MEMS-микрофоны реагируют только на звуки в диапазоне от 300 Гц до 6 кГц, включающем в себя голосовой диапазон человека. Так как они не требуют напряжения смещения, их активация происходит примерно через 50 мкс и они не пропускают ключевое слово. Для активации емкостных MEMS-микрофонов необходимо почти в 1000 раз больше времени – т. к.

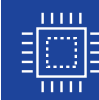
зарядка MEMS до высокого напряжения смещения происходит не сразу.

Специалисты Vesper Technologies считают, что в будущем им удастся создать датчики, обладающие некоторым уровнем искусственного интеллекта. Они смогут применять полученные данные, например о движении и температуре, для улучшения осведомленности об окружающей среде, подобно тому как люди и животные используют свои чувства – зрение, слух, вкус, обоняние и осязание. Перспективные планы корпорации заключаются в использовании устройствами нескольких типов датчиков, комбинирующихся и самоорганизующихся по законам биосистем, с целью большего понимания своей среды и наилучшего реагирования на нее и ее изменения.

Для поддержки своего развития корпорация Vesper Technologies расширяет группы разработки и сбыта. Сейчас они насчитывают 40 человек. В настоящее время офисы корпорации расположены в КНР, Сингапуре и Южной Корее, в ближайшие месяцы планируется открыть представительство на Тайване, в 2020 г. – расширить присутствие в Европе, Южной Корее и Японии. Теперь, когда крупные компании прошли через этап принятия новой технологии Vesper Technologies, пришло время роста. Тем более что конечные потребители – люди – начинают понимать преимущества архитектуры пьезоэлектрических MEMS-микрофонов, их новизну и комфортность использования.



*Pelé Anne-Françoise. MEMS Microphone Market Grows; Vesper Too. EE Times, September 23, 2019: [https://www.eetimes.com/document.asp?doc\\_id=1335128](https://www.eetimes.com/document.asp?doc_id=1335128)*



# Защищенная загрузка с поддержкой FPGA в доверенных вычислительных архитектурах

*Ключевые слова: FPGA, атака по сторонним каналам, корень доверия, надежные вычислительные архитектуры, обратный инжиниринг.*

*Вентильные матрицы, программируемые пользователем (FPGA), могут стать защитой от обратного инжиниринга и предоставлять в некоторых случаях такие возможности обеспечения безопасности, как хранение т. н. черных ключей (black keys – средства защиты от копирования) или криптографические средства защиты от атак по сторонним (побочным) каналам. Разработчики встраиваемых вычислительных систем могут установить улучшенную надежную защиту при загрузке с помощью корня доверия (RoT)<sup>11</sup> на основе FPGA.*

Корень доверия на основе FPGA не только позволяет защититься от обратного инжиниринга, хранит черные ключи или средства криптографии для защиты от атак по побочным каналам. Пользователи также получают возможность настраивать FPGA для добавления других средств защиты системы и удовлетворения конкретных потребностей программы. Эти усиленные средства защиты обеспечивают необходимую аппаратную инфраструктуру, позволяющую RoT взаимодействовать с датчиками и процессорами безопасности, поддерживая при этом безопасность системы на протяжении всего процесса загрузки. Более того, эти усовершенствованные методы доверенной (надежной) загрузки предоставляют механизмы, обеспечивающие проверку подлинности любого нового кода перед его сохранением в энергонезависимой памяти, а также дополнительные проверки

и меры снижения риска доверенных вычислений в процессе загрузки.

Одна из важных концепций надежных вычислений – целостный подход (касающийся не только оборудования), направленный на внедрение технологий и методик безопасности во все аспекты решения – от проектирования и тестирования до цепочки поставок и производства. Другими словами, обеспечение безопасности не ограничивается каким-либо конкретным этапом. Этот комплексный, сквозной подход, часто называемый глубоководной защитой, создает сеть из нескольких уровней, обеспечивающую надежность решения.

На уровне модулей объединение максимально возможного количества доступных методов безопасности, таких как интеграция уникальной технологии доверенной загрузки на процессоре с уникальной технологией до-

веренной загрузки, предоставляемой FPGA, позволяет разработчикам системы безопасности реализовать мультипликативный эффект. Так, в сентябре 2019 г. корпорация Curtiss-Wright представила мощный ЦОС-процессор CHAMP-XD1S (рис. 1). Он оснащен 12-ядерным процессором Intel Xeon D, аппаратной платформой, сочетающей «систему-на-кристалле» (SoC) Zynq Ultra Scale корпорации Xilinx и многопроцессорную SoC (MPSoC) на основе FPGA, а также FPGA интеллектуального контроллера управления платформой (intelligent platform management controller, IPMC) на основе флэш-памяти Smart Fusion 2 корпорации Microsemi для обеспечения безопасности процессорной платы, предназначенной для высокопроизводительных встроенных вычислений (HPEC) и работающей в жестких условиях окружающей среды.

Для защиты от злонамеренных атак и обратного инжиниринга на плате реализована как кибербезопасность, так и защита данных физического уровня. Встроенные расширенные функции безопасности включают расширенные возможности доверенной загрузки, такие как аутентифицированный загрузочный код на основе FPGA. Плата поддерживает технологию безопасной загрузки Intel TXT, а также может поддерживать безопасную загрузку UEFI<sup>12</sup> через операционную систему. Этот модуль имеет дополнительную защиту, использующую PUF<sup>13</sup>, размещается на плате MPSoC FPGA для аутентификации загрузочного кода.

PUF, доступный только в устройствах Xilinx Zynq Ultra Scale+, представляет собой надежный идентификатор, связанный только с одной ИС. На основе вариаций кристаллов ИС, характерных для устройств типа Zynq Ultra Scale+, PUF генерирует криптографически стойкий ключ шифрования, уникальный для каждого конкретного прибора.

Полученный ключ не может быть прочитан кем-либо, включая пользователя, и может использоваться в сочетании с криптографическим ядром встроенного расширенного стандарта шифрования (AES) FPGA. PUF, в дополнение к генерации ключа шифрования, также генерирует помощника, который позволяет повторно генерировать ключ шифрования позже, чтобы обеспечить повышенный уровень его безопасности.

Использование PUF делает невозможными для злоумышленника подделку, клонирование или изменение FPGA, поскольку система не сможет распознать устройство с измененным значением PUF. Подпись уникального идентификатора может быть начальным этапом шифрования и аутентификации загрузочного образа и загрузочного кода для FPGA. Более того, аутентификацию возможно расширить для защиты других частей системы, включая другие артефакты загрузки, кроме самой FPGA.

Таким образом, создается парадигма комбинации FPGA и необходимого аппаратного и программного обеспечения (рис. 2).



Источник: Curtiss-Wright

Рисунок 1. Электронный модуль корпорации Curtiss-Wright с корнем доверия на основе FPGA



Рисунок 2. Парадигма сочетания FPGA и необходимого аппаратного и программного обеспечения

## ДВЕ FPGA ЛУЧШЕ, ЧЕМ ОДНА

В дополнение к MPSoC FPGA-модуля на плате также имеется FPGA Smart Fusion 2, обеспечивающая не только исправность и управление, но и интеграцию дополнительных функций безопасности. Smart Fusion 2 – это FPGA корпорации Microsemi, созданная на основе флэш-памяти, а не СОЗУ, как MPSoC корпорации Xilinx. Она может быть зашифрована, а также имеет собственный набор внутренних средств защиты. Таким образом, пользователю предоставляется два разных типа FPGA.

Новая плата также оснащена микросхемой безопасности модуля доверенной платформы (trusted platform module, TPM) версии 2.0, использующей криптографические методы обеспечения целостности платформы на протяжении всего процесса загрузки вплоть до запуска приложения. TPM часто служит основой для поддержки TXT корпорации Intel, но в более общем смысле она генерирует ключи и управляет ими. TPM 2.0, по сравнению с более ранними версиями, имеет обновленные и дополненные криптографические алгоритмы, предоставляющие разработчикам надежных вычислений большую гибкость. Она также поддерживает не один, а несколько разных криптографических ключей. Помимо этого пользователи могут использовать функции безопасности TPM после загрузки.

Из-за деликатного характера проектирования доверенных компьютеров невозможно публично обсудить все возможности и функции безопасности, встроенные в CHAMP-XD1S. Тем не менее важно отметить, что основным требованием при разработке архитектуры безопасности была гибкость. Плата поставляется с инструментарием FPGA, который дает возможность клиентам добавлять свои собственные функции безопасности или дополнительные расширенные возможности безопасности, предоставляемые корпорацией Curtiss-Wright или даже другими фирмами. Например, разрабатываются дополнительные СФ-блоки, которые можно интегрировать в FPGA для дальнейшего улучшения безопасной загрузки и работы с доверенными вычислениями по сравнению с тем, что доступно у поставщиков.

Хотя разработчикам средств безопасности важно понимать и реализовывать каждый из доступных индивидуальных подходов, пригодных для их аппаратного обеспечения, необходимо также учитывать то, как реализация и взаимное увязывание нескольких подходов могут обеспечить мультипликативный эффект. Конечно, все указания по архитектуре аппаратного обеспечения должны соблюдаться, однако если все сделано правильно, целое действительно становится больше, чем сумма его частей.



## В ЦЕНТРЕ ВНИМАНИЯ: CURTISS-WRIGHT

**Curtiss-Wright Corporation** – американский многоотраслевой производитель.

**Дата основания:** 1929 г. (в результате объединения 12 фирм).

**Штаб-квартира:** г. Дэвидсон, шт. Северная Каролина, США.

**Доход:** 2,41 млрд долл. (2018 г.).

**Операционная прибыль:** 373,6 млн долл. (2018 г.).

**Сферы производства:** авиационно-космическая, оборонная, атомная энергетика, другие отрасли промышленности.

**Количество сотрудников:** 9,0 тыс. человек (2019 г.).

Curtiss-Wright активно осваивает область радиоэлектроники, сделав ее основным направлением перспективного развития. На это ясно указывают осуществленные в последние годы сделки слияния и поглощения:

- Hybricon (2010 г., 19 млн долл.) – поставщик электронных модулей аэрокосмического, военного и гражданского назначения, интеграция электронных подсистем;
- AcraControl (2011 г., 61 млн долл.) – поставщик систем и сетей сбора данных, регистраторов данных и наземных станций телеметрии военного и гражданского аэрокосмического назначения;
- Exlar Corporation (2013 г., 85 млн долл.) – разработчик и производитель высокотехнологичных электроприводов, используемых в решениях по управлению движением на промышленных и военных рынках;
- Parvus (подразделение Eurotech S.p.A., 2013 г., 38 млн долл.) – разработчик и производитель надежных компьютеров малого форм-фактора и подсистем связи аэрокосмического, военного и промышленного назначения, подрядчик Министерства внутренней безопасности.



*Smetana Denis. FPGA-Enabled Trusted Boot Is Part of Building Security into Every Aspect of Trusted Computing Architectures. Military & Aerospace Electronics journal, September 25, 2019: <https://www.militaryaerospace.com/trusted-computing/article/14040672/trusted-computing-embedded-computing-realworld>*



# Тайваньский стартап бросает вызов Google в области технологии распознавания жестов

*Ключевые слова: 60-ГГц монолитные СВЧ ИС, датчики, распознавание жестов, смартфоны, ускорители искусственного интеллекта.*

*Похоже, что распознавание жестов скоро начнет применяться в смартфонах. Тайваньский стартап KaiKuTek, занимающийся проектированием ИС, собирается стать одним из крупнейших бенефициаров в этой новой категории технологий человеко-машинного интерфейса. Новые системы распознавания жестов используют 60-ГГц радары. При этом, если большинство поставщиков 60-ГГц радарных ИС производят свои приборы с использованием относительно дорогого SiGe-процесса, KaiKuTek намерена задействовать стандартный КМОП-процесс.*

## ОБЩАЯ СИТУАЦИЯ НА РЫНКАХ ИС РАСПОЗНАВАНИЯ ЛИЦ, ДВИЖЕНИЯ И ЖЕСТОВ

По данным фирмы Markets and Markets Research, опубликованным в недавнем исследовании «Рынок распознавания лиц по компонентам (программное обеспечение, инструменты и услуги), области применения (распознавание эмоций, отслеживание и мониторинг посещаемости, контроль доступа, правоприменение), вертикально-организованным рынкам и регионам – мировой прогноз до 2024 г.» (Facial Recognition Market by Component (Software, Tools, and Services), Application Area (Emotion Recognition, Attendance Tracking and Monitoring, Access Control, Law Enforcement), Vertical, and Region – Global Forecast to 2024), объем мирового рынка продаж ИС распознава-

ния лиц вырастет с 3,2 млрд долл. в 2019 г. до 7,0 млрд к 2024-му при совокупном среднегодовом темпе прироста в сложных процентах (CAGR) за этот период в 16,6%. Основные факторы роста рынка – увеличение количества пользователей и инициатив по обеспечению безопасности данных со стороны органов государственной власти, широкое использование мобильных устройств и растущий спрос на надежные системы обнаружения и предотвращения мошенничества [1].

По оценкам той же фирмы, опубликованным в исследовании «Рынок датчиков движения по технологиям распознавания движения (инфракрасные, ультразвуковые, микроволновые,

двойные и томографические), приложениям (потребительская электроника, автомобильная, аэрокосмическая и оборонная промышленность, здравоохранение и производство) и географическим регионам – глобальный прогноз до 2025 г.» (Motion Sensor Market by Motion Technology (IR, Ultrasonic, Microwave, Dual Technology, & Tomographic), Application (Consumer Electronics, Automotive, Aerospace & Defense, Healthcare, & Industrial), and Geography – Global Forecast to 2025), объем мирового рынка продаж датчиков движения (включая датчики рас-

познавания жестов) вырастет с 5,7 млрд долл. в 2019 г. до 9,3 млрд в 2025-м при CAGR = 8,3%. Рост рынка датчиков движения обусловлен такими факторами, как высокий спрос на потребительскую электронику, выгодные возможности в развивающихся странах и увеличение расходов на оборону для обновления сопутствующих товаров. Широкое распространение носимой электроники и растущая потребность в коммерциализации Интернета вещей, как ожидается, предоставят богатые возможности роста игрокам на этом рынке [2].

## НОВЫЕ ФУНКЦИИ ЧЕЛОВЕКО-МАШИННОГО ИНТЕРФЕЙСА В СМАРТФОНАХ

Представители корпорации Google в конце июля 2019 г. заявили, что будут поддерживать в своем следующем смартфоне Pixel 4 две новые функции человеко-машинного интерфейса (HMI) – распознавание лиц и распознавание движения. Отмечается, что новые функции в Pixel 4 – результат реализации проекта Project Soli группой специалистов фирмы Advanced Technology and Projects (ATAP), которая впервые начала рекламировать свою технологию обнаружения движения в 2015 г. Функция управления жестами (Motion Sense) для Pixel 4 позволяет пользователю переходить от одного приложения к другому с помощью жестов рук, даже не касаясь телефона. Подчеркивается, что это только начало. По мере совершенствования линейки Pixel функция Motion Sense также будет развиваться. Разработки велись с мая 2015 до второй половины 2019 г. Теперь новые возможности будут добавлены в HMI и на рынок выйдут ИС, обеспечивающие эти функции.

Корпорация Google не одинока в подобных работах. Созданная в январе 2017 г. тайваньская фирма KaiKuTek (г. Тайбэй, также известна как Cool Tech), разработала решение для распознавания жестов 3D, основан-

ное на радиолокационной технологии миллиметрового диапазона (60 ГГц). В отличие от продукции некоторых производителей, изготавливающих радары миллиметрового диапазона 60 ГГц с использованием дорогостоящего SiGe-процесса, решение KaiKuTek для распознавания жестов основано на более зрелом и доступном КМОП-процессе.

Однокристалльное решение («система-на-кристалле», SoC) фирмы объединяет антенны, состоящие из одного транзистора и трех резисторов (1T3R), и монолитные СВЧ ИС (МММС). В него также встроен фирменный (проприетарный) ускоритель ИИ. Кристалл смонтирован в усовершенствованный модуль AiP<sup>14</sup> («антенна-в-модуле»).

Утверждается, что прибор способен с высокой точностью распознавать жесты в пределах 30 см, причем его ускоритель ИИ потребляет менее 1 мВт. Схема (см. рисунок) будет официально запущена в серийное производство в следующем году. Одним из ее производителей станет крупнейший в мире кремниевый завод TSMC.

В настоящее время около 30 сотрудников KaiKuTek работают в Инкубационном центре проектирования ИС компании NanKang (NKIC, г. Тайбэй), который был создан промышлен-





ным бюро Министерства экономики Тайваня и управляется специалистами Научно-исследовательского института промышленных технологий Тайваня (ITRI)<sup>15</sup>. Отмечается, что, поскольку Google оснащает Pixel 4 функцией управления жестами, крупным производителям мобильных телефонов также придется добавить подобные функции в следующее поколение своей продукции, чтобы оставаться конкурентоспособными. Соответственно, решение KaiKuTek будет привлекать все большее внимание.

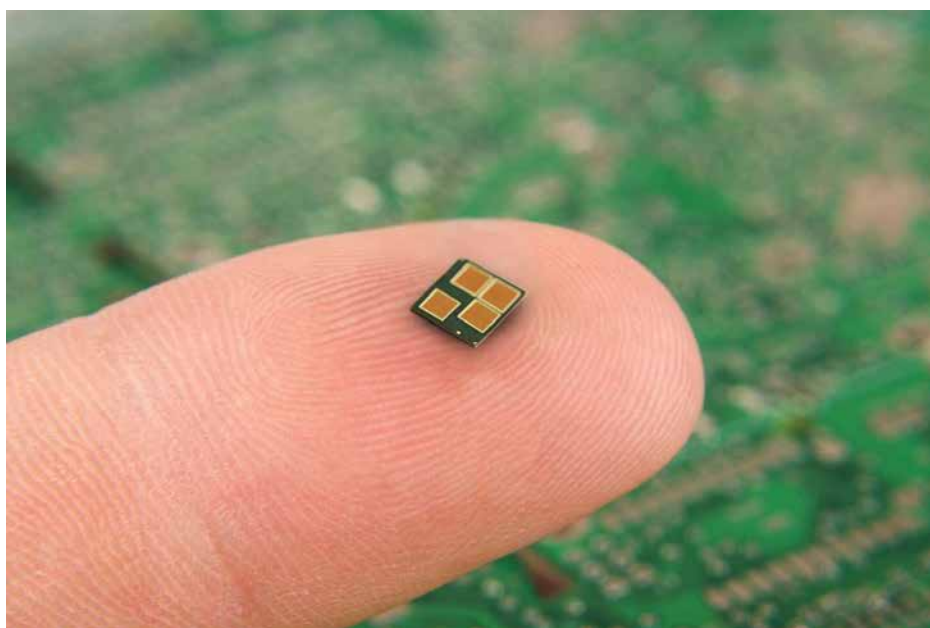
Специалисты KaiKuTek утверждают, что за два года им удалось разработать технологию распознавания жестов, которая по крайней мере соответствует по своим возможностям решению корпорации Google, если не превосходит его. Отмечается, что последняя

версия Google для мобильной операционной системы Android Q (бета-версия<sup>16</sup> доступна для загрузки) также включает поддержку функций управления жестами, которые, вероятно, помогут ускорить внедрение технологии распознавания жестов, что приведет к еще большему спросу на подобные функции. Вероятно, мобильный телефон станет для потребителей лучшим инструментом для ознакомления с этим новым HMI. Люди, обладающие опытом использования сенсорных интерфейсов благодаря играм, таким как Angry Birds, окажутся наиболее подготовленными к использованию нового HMI. Когда потребители привыкнут использовать жесты на мобильных телефонах, они смогут расширить применение этого HMI на другие приложения, включая автомобили, игровые приставки, умные дома и т. д.

## ЗАЧЕМ НУЖНА ТЕХНОЛОГИЯ РАСПОЗНАВАНИЯ ЖЕСТОВ?

Возникает вопрос: насколько высока реальная потребность в распознавании жестов в качестве HMI?

На данный момент сенсорный (касательный) интерфейс практически заменил все механические кнопки, а голосовое управление



*Радиолокационное решение миллиметрового диапазона 60 ГГц от KaiKuTek*

используется для различных функций, включая ответ на входящие вызовы, переключение света, воспроизведение музыки и поиск информации в Интернете. Есть ли явное преимущество у технологии управления жестами? Отметим, что ее нельзя назвать полной заменой сенсорного управления. Использование сенсорного интерфейса для открытия приложений и ответа на вызовы на мобильном телефоне – это интуитивно понятный способ управления этими приложениями. Однако во время игры с использованием сенсорного интерфейса тень от пальцев может мешать видеть происходящее на экране. Кроме того, экран влияет на плавность работы, а ограничивать размер экрана при вводе текста в программе обмена мгновенными сообщениями неудобно.

Если же взять умные часы и другие носимые устройства, у которых экраны значительно меньше, чем экраны мобильного телефона, то ограничения сенсорной технологии становятся еще заметнее. Именно там, где сенсорные интерфейсы не могут быть использованы в полной мере, управление жестами имеет преимущество.

Что касается голосового управления, то, хотя оно уже обеспечивает удобство громкой связи, его реальное использование все еще не лишено недостатков. Независимо

от того, где находятся пользователи, могут возникать помехи от шума окружающей среды, влияющие на точность. Конфиденциальность также может представлять большую проблему – не только когда речь идет о публичных выступлениях, но и в случаях, когда команды должны передаваться в «облако» для обработки.

Отличительная черта 60-ГГц миллиметрового диапазона – относительно малая дальность распространения сигнала. Разработчики KaiKuTek превратили этот недостаток в преимущество. Благодаря малой дальности и использованию направленной антенны не возникает взаимных помех с другими приборами, находящимися поблизости.

На реальном дисплее решение KaiKuTek может распознавать тонкие движения запястья, а также движения пальцев. В плане чувствительности задержка практически отсутствует, поскольку процессы распознавания не выполняются на главном процессоре мобильного телефона – это область процессора ИИ, благодаря чему разработка KaiKuTek позволяет значительно сэкономить заряд мобильного телефона. Решение KaiKuTek – это не только периферийные вычисления, но и вычисления на датчике. Специалисты фирмы полагают, что все рабочие функции можно перевести на управление жестами.

## СТРАТЕГИЯ ДИВЕРСИФИКАЦИИ РЫНКА

Учитывая различные потребности приложений в управлении жестами, KaiKuTek планирует предоставлять индивидуальные решения, которые будут разрабатываться совместно с клиентами. В ближайшем будущем компания намерена начать предлагать обучение распознавания жестов как услугу. Например, разработчики игр могут быть заинтересованы в том, чтобы система распознавала жесты, характерные для их игр, а разработчик программного обеспечения может даже захотеть поддержать способность своих клиентов настраивать жесты.

В ходе подготовки к появлению следующего поколения смартфонов KaiKuTek также рассматривает возможность выпуска аппаратного ключа<sup>17</sup>, позволяющего мобильным телефонам, ноутбукам и другим устройствам, не имеющим встроенного радиолокатора миллиметрового диапазона, поддерживать распознавание жестов, а разработчикам ПО – формировать собственные наборы инструментальных средств приложений распознавания жестов.

Специалисты KaiKuTek отмечают, что разработка распознавания жестов – непростое



дело, требующее опыта. Соответственно, другие фирмы не смогут в ближайшее время легко скопировать их решение. Кроме

того, они уверены в перспективности применения технологии 60-ГГц миллиметровых волн [3].



*Facial Recognition Market by Component (Software, Tools, and Services), Application Area (Emotion Recognition, Attendance Tracking and Monitoring, Access Control, Law Enforcement), Vertical, and Region – Global Forecast to 2024. Markets and Markets Research Private Ltd.: [https://www.marketsandmarkets.com/Market-Reports/facial-recognition-market-995.html?gclid=EAlaIqobChMlvvKKIbf95AIVEamaCh0h6w15EAAAYASAAEgKEaPD\\_BwE](https://www.marketsandmarkets.com/Market-Reports/facial-recognition-market-995.html?gclid=EAlaIqobChMlvvKKIbf95AIVEamaCh0h6w15EAAAYASAAEgKEaPD_BwE)*

*Motion Sensor Market by Motion Technology (IR, Ultrasonic, Microwave, Dual Technology, & Tomographic), Application (Consumer Electronics, Automotive, Aerospace & Defense, Healthcare, & Industrial), and Geography – Global Forecast to 2025. Markets and Markets Research Private Ltd.: <https://www.marketsandmarkets.com/Market-Reports/Motion-Sensor-Market-614.html>*

*Cheng Judith. Taiwan Startup Challenges Google in Gesture Recognition. EE Times magazine, September 22, 2019: [https://www.eetimes.com/document.asp?doc\\_id=1335123](https://www.eetimes.com/document.asp?doc_id=1335123)*



## **ЦНИИ «ЭЛЕКТРОНИКА»**

ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЙ ЦЕНТР  
РОССИЙСКОЙ РАДИОЭЛЕКТРОННОЙ ПРОМЫШЛЕННОСТИ

### **СТРАТЕГИЧЕСКОЕ УПРАВЛЕНИЕ**

- Консультационные услуги в области государственного управления
- Разработка корпоративной стратегии развития
- Разработка и внедрение организационно-управленческой модели
- Разработка маркетинговой стратегии

### **ПРОЕКТНОЕ УПРАВЛЕНИЕ**

- Разработка бизнес-плана
- Внедрение ИТ-инструментов управления проектами
- Подбор источников финансирования
- Комплексное сопровождение проекта

### **СЕРТИФИКАЦИЯ СИСТЕМ МЕНЕДЖМЕНТА КАЧЕСТВА**

- ГОСТ Р ИСО 9001–2015
- ГОСТ РВ 0015–002–2012
- ЭС РД 009–2014
- ЭС РД 010–2015

+7 (495) 940-65-00  
[www.instel.ru](http://www.instel.ru)



# Новейшие исследования в области перспективных материалов

*Ключевые слова: квантовые компьютеры и материалы, сверхструктуры, тонкие пленки, топологические изоляторы и материалы, фотоника.*

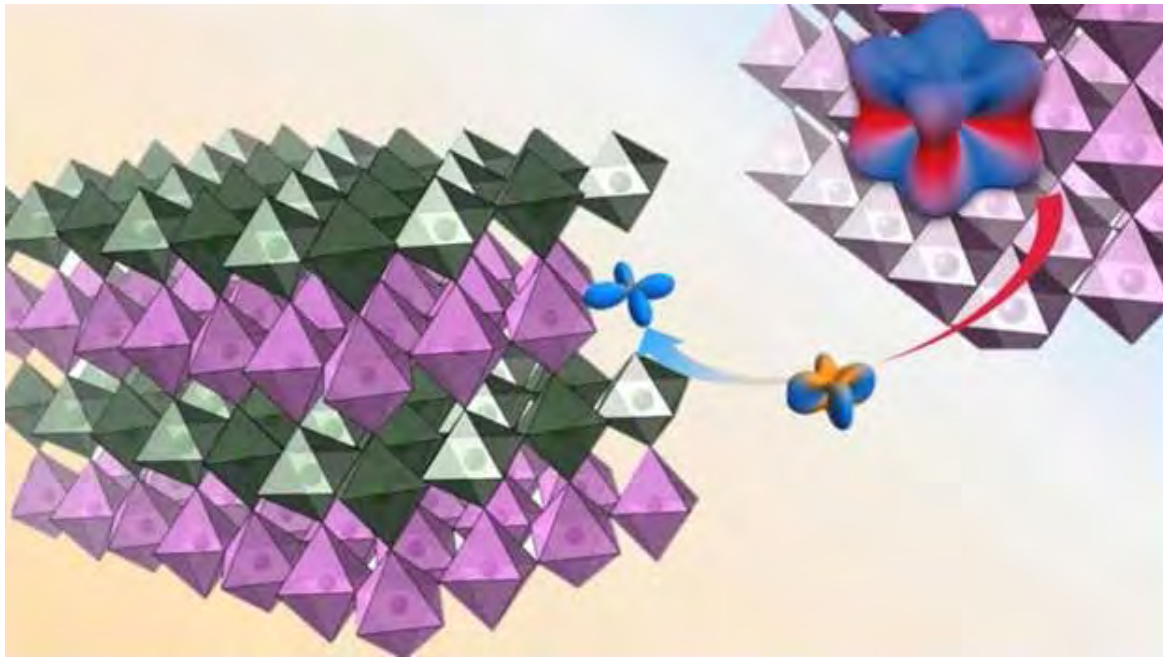
*Работы в области перспективных материалов необходимы для обеспечения дальнейшего прогресса микроэлектроники. При этом исследователям приходится сталкиваться не только с новыми материалами, но и новыми явлениями в уже достаточно хорошо изученных материалах. Важное направление – расширение сферы применения перспективных материалов: примерами могут служить работы ученых Ратгерского университета, Университета штата Мэриленд и Национального института стандартов и технологий США (NIST), Института нелинейной оптики и короткоимпульсной спектроскопии им. Макса Борна и Университета штата Пенсильвания.*

## ВЗАИМОДЕЙСТВИЕ ПЛЕНОК ИРИДИЯ И НИКЕЛЯ

Недавно ученые Ратгерского университета (г. Нью-Брансуик, шт. Нью-Джерси, США) опубликовали в журнале «Труды Национальной академии наук США» (Proceedings of the National Academy of Sciences of the United States of America) отчет об опытах по взаимодействию тонких пленок иридия и слоев на основе никеля. Как отмечается в статье, иридий, переходный металл платиновой группы, «теряет свою идентичность» – т. е. его электроны в ультратонкой пленке «странно» ведут себя при взаимодействии со слоями на основе никеля, которые оказывают неожиданно сильное воздействие на ионы иридия.

Было обнаружено, что на границе раздела между слоем, содержащим никель, и слоем на основе иридия возникает необычная форма магнетизма, которая сильно влияет на поведение вращения и орбитального движения

электронов (см. рисунок). Данное открытие важно потому, что квантовые материалы с очень большим спин-орбитальным взаимодействием являются популярными кандидатами в новые топологические материалы и материалы со сверхпроводимостью. Результаты опытов специалистов Ратгерского университета помогут улучшить понимание квантовых состояний, расширить возможности работы с квантовыми материалами и сферу их применения в электронных приборах и системах новых типов. Кроме того, вероятно, в ближайшее время физикам и материаловедам придется переоценить ранее осуществленные работы и переосмыслить эксперименты по физике спин-орбитальных взаимодействий и магнетизму, особенно когда речь идет о границах разделов или поверхностях материалов с атомами металлов платиновой группы [1].



*Сверхтонкие искусственные сверхструктуры иридия и никеля: воздействие никелевых сверхструктур на ионы иридия*

## ДИТЕЛЛУРИД УРАНА

Подобные необычные свойства – не единственный случай в практике исследователей полупроводниковых материалов. Так, ранее обнаруженные свойства дителлурида урана ( $UTe_2$ ) показывают, что это химическое соединение может оказаться пригодным для решения одной из проблем развития квантовых компьютеров – трудности с переключением памяти при помощи кубитов<sup>18</sup>. Такие операции зачастую оказываются достаточно длинными, чтобы можно было завершить вычисление до потери тонких физических отношений, позволяющих им действовать как группе. Эти отношения, называемые квантовой когерентностью, трудно поддерживать из-за помех в окружающей среде.

Специалисты Национального института стандартов и технологий США (NIST)<sup>19</sup> начали изучать  $UTe_2$  с применением специализированных инструментальных средств как в Центре нейтронных исследований NIST (NIST

Center for Neutron Research, NCNR), так и в Университете штата Мэриленд (г. Колледж-Парк). Было обнаружено, что  $UTe_2$  обладает сверхпроводимостью при низких температурах (ниже  $-271,5$  °C). Его свойства напоминали свойства редких сверхпроводников, которые также одновременно являются ферромагнетиками – действуя как низкотемпературные постоянные магниты. Что любопытно, сам по себе  $UTe_2$  не является ферромагнетиком.

Необычное и сильное сопротивление данного соединения магнитным полям делает его редкостью среди сверхпроводящих материалов и предлагает явные преимущества для проектирования кубитов. Преимущества заключаются, главным образом, в устойчивости кубитов к ошибкам, легко проникающим в квантовые вычисления. Исследователи считают, что  $UTe_2$  может стать крайне перспективным материалом для зарождающейся индустрии квантовых компьютеров [2].



## ТОПОЛОГИЧЕСКИЕ ИЗОЛЯТОРЫ

Еще одно перспективное направление исследований в области материалов – топологические изоляторы<sup>20</sup>. Это квантовые материалы, которые из-за своей необычной электронной структуры на поверхностях и краях проводят электрический ток как металлы, в то же время выступая в качестве изолятора в объемной части. Ученые из Института нелинейной оптики и короткоимпульсной спектроскопии им. Макса Борна (МВ, г. Берлин, Германия) впервые продемонстрировали, как отличать топологические материалы от их обычных аналогов в пределах одной 1 фс ( $10^{-15}$  с), исследуя их ультрабыстрыми лазерными импульсами. Их метод может открыть путь для использования таких материалов в качестве логических элементов в управляемой светом электронике, способной обрабатывать информацию в десятки тысяч раз быстрее, чем это возможно в настоящее время. Результаты исследования опубликованы в журнале *Nature Photonics*.

Наиболее распространенная иллюстрация топологической концепции – эластичный крендель, который можно растягивать, сгибать или скручивать любым способом. Независимо от деформации, невозможно сделать из кренделя рога или добавить в него отверстия, не разрывая его на части. Число отверстий, таким образом, является инвариантным и дает топологическую информацию о форме кренделя. В твердом материале квантово-механические законы ограничивают возможные энергии электронов, что приводит к образованию полос с разрешенной или запрещенной энергетической зоной. Используя концепцию топологии, физики могут описывать сложные формы разрешенных энергетических зон и назначать им конкретное топологическое число. Особая топология зонной структуры в материальной системе проявляется в экзотических свойствах, которые можно наблюдать, – таких как поверхностная проводимость в топологических изоляторах.

Специалисты Института нелинейной оптики и короткоимпульсной спектроскопии им. Макса Борна считают самым замечательным аспектом топологии ее надежность. Примеси и другие помехи, которые обычно нарушают способность материала проводить электричество, не влияют на высокую подвижность электронов на поверхности топологических изоляторов. Эта невосприимчивость к примесям – причина, по которой топологические материалы столь привлекательны для электронной промышленности.

### Как заставить электроны «говорить» о топологии

Хотя топология системы тесно связана с поведением электронов, до сих пор не было обнаружено влияния топологических свойств на динамику электронов в реальном масштабе времени, составляющем фемтосекунду. Используя численное моделирование и теоретический анализ, группа ученых из Института нелинейной оптики и короткоимпульсной спектроскопии им. Макса Борна доказала, что информация о топологии системы действительно закодирована в динамике электронов и может быть получена путем просмотра светового излучения, испускаемого электронами при возбуждении лазерными импульсами. Представим, что электроны в твердом теле движутся в пределах энергетических полос, как бегуны на гоночном треке. Новый метод позволяет выяснить топологию этого «гоночного трека», просто измеряя ускорение «бегунов». Сверхкороткие лазерные импульсы возбуждают электроны системы, заставляя их переходить из одной энергетической зоны в другую, более высокую, придавая им ускорение «на новой дорожке». Ускоренные электроны затем излучают свет и быстро возвращаются в нижнее положение. Процесс длится бесконечно малую долю секунды, однако этого достаточно для того, чтобы электрон «почувствовал» тонкую разницу между энер-

гетическими структурами тривиальных и топологических изоляторов и «закодировал» ее в излучаемом свете.

### **На пути к сверхбыстрой световой электронике**

Текущая работа показывает, как различать тривиальные и топологические изоляторы – иными словами, «считывать» топологическую информацию системы с помощью лазерной спектроскопии. На следующем этапе исследователи из Института нелинейной оптики и короткоимпульсной спектроскопии им. Макса Борна планируют использовать эти знания для преобразования тривиального изолятора в топологический и наоборот с лазерным излучением, то есть для «записи» топологической информации в материал с одинаковой скоростью. Теоретическое доказательство этого эффекта может привести к внедрению топологических материалов в электронику с оптическим управлением, где предел скорости обработки информации определяется только скоростью электронного отклика на импульс светового (лазерного) излучения [3].

### **Топологические изоляторы в фотонике**

Исследователи Университета штата Пенсильвания (г. Филадельфия), где в 2005 г. были впервые обнаружены топологические изоляторы, продемонстрировали возможность их использования в фотонике. Они впервые показали, как топологический изолятор может использовать всю свою площадь. Фотонные ИС, использующие вместо электронов фотоны, обладают потенциалом еще более высоких скоростей и плотностей передачи данных. Однако компоненты, необходимые для их построения, остаются пока значительно крупнее электронных аналогов – из-за отсутствия эффективной архитектуры маршрутизации данных.

Решить проблему габаритов фотонных ИС могло бы переопределение «на лету» краев топологических изоляторов. Возможность прокладывать «трассы» прохождения фотонов друг вокруг друга по мере необходимости оз-

начает, что для эффективного построения каналов передачи данных может использоваться весь внутренний объем. Исследователи Университета штата Пенсильвания совместно с учеными из Миланского технического университета впервые создали и протестировали такое устройство, опубликовав свои выводы в журнале Science.

Данное открытие может оказать большое влияние на приложения с большой информационной емкостью, такие как средства связи 5G или даже 6G в сотовых сетях. Исследователи также заявляют, что это первый случай практического применения топологических изоляторов.

Центры обработки данных (ЦОД), образующие основу сетей связи, направляют звонки, текстовые сообщения, вложения электронной почты и потоковые фильмы между миллионами сотовых устройств. По мере увеличения объема данных, проходящих через ЦОДы, растет и потребность в маршрутизации данных с высокой пропускной способностью, которая может удовлетворить спрос. Переход с электронов на фотоны ускорил бы этот процесс в преддверии предстоящего информационного взрыва, но специалистам придется сначала разработать целую новую библиотеку устройств для передачи фотонов с входа на выход без смешения и потери в рабочем процессе.

Достижения в области увеличения скорости обработки данных в электронике основаны на постоянном масштабировании основных компонентов. Но в области фотоники необходимо использовать другой подход. Ученые из Университета штата Пенсильвания намерены максимизировать сложность фотонных волноводов – предписанных путей, по которым отдельные фотоны идут от входа к выходу в фотонных ИС. Прототип фотонной ИС площадью около 250 мкм, созданный исследователями, имеет мозаичную решетку из овальных колец. «Накачка» микросхемы внешним лазером с целью изменения фотонных свойств отдельных колец дает возмож-





ность изменять их положение в качестве границ волновода. В результате получается реконфигурируемый топологический изолятор. При изменении схем накачки фотоны, движущиеся в разных направлениях, могут «обходить» друг друга, что позволяет фотонам из нескольких пакетов данных проходить через микросхему одновременно. Таким образом, формируется нечто похожее на сложную транспортную развязку. Можно определить края так, чтобы фотоны шли от любого входного порта к любому выходному порту или даже к нескольким выходам одновременно. Это означает по крайней мере на два порядка большее отношение портов к занимаемой площади, чем у современных фотонных марш-

рутизаторов и коммутаторов. Повышение эффективности и скорости – не единственное преимущество нового подхода. Система также устойчива к неожиданным дефектам. Если одно из колец повреждено, например, частицей пыли, то это повреждение создает новый набор краев, по которым можно отправлять фотоны.

Поскольку для переопределения формы волноводов опытной системе требуется внешний лазерный источник, ее габариты пока недостаточно малы, чтобы ее можно было использовать в ЦОДах или других коммерческих применениях. На следующих этапах работ планируется создать схемы быстрой перенастройки в интегрированной форме [4].



*Davis Shannon. Iridium 'Loses Its Identity' When Interfaced With Nickel. Semiconductor Daily, September 25, 2019: <https://www.semiconductor-digest.com/2019/09/25/iridium-loses-its-identity-when-interfaced-with-nickel/>*

*Davis Shannon. Newfound Superconductor Material Could Be the 'Silicon of Quantum Computers'. Semiconductor Daily, August 15, 2019: <https://www.semiconductor-digest.com/2019/08/15/newfound-superconductor-material-could-be-the-silicon-of-quantum-computers/>*

*Davis Shannon. Spying on Topology. Semiconductor Daily, October 2, 2019: <https://www.semiconductor-digest.com/2019/10/02/spying-on-topology/>*

*Davis Shannon. Penn Engineers' New Topological Insulator Reroutes Photonic 'Traffic' On the Fly. Semiconductor Daily, September 13, 2019: <https://www.semiconductor-digest.com/2019/09/13/penn-engineers-new-topological-insulator-reroutes-photonic-traffic-on-the-fly/>*

# Аккумулятор, который можно сгибать, растягивать и скручивать

*Ключевые слова: эластичный аккумулятор, батарея, гибкая электроника, электролит, новый тип батареи.*

*Используемые в коммерческих устройствах батареи на литий-ионной основе слишком жесткие и тяжелые для применения в гибкой электронике или текстильных изделиях. Новый аккумулятор имеет слоистую структуру и выполнен из эластичных материалов, что значительно расширяет сферу его применения.*

Команда исследователей из Швейцарской высшей технической школы Цюриха (ETH Zürich) использовала растяжимые материалы для разработки аккумулятора, который можно сгибать, растягивать и скручивать. Данный тип батареи как нельзя лучше подходит для применения в гибких электронных устройствах.

Современная электронная промышленность все больше внимания уделяет компьютерам или смартфонам с экранами, которые можно сложить или свернуть. Умные предметы одежды используют носимые микроустройства или датчики, например для мониторинга

функций организма. Все подобные устройства нуждаются в источнике энергии. Обычно это литий-ионный аккумулятор – но такие аккумуляторы, к сожалению, слишком тяжелые и жесткие, что делает их принципиально непригодными для применения в гибкой электронике или умных предметах одежды.

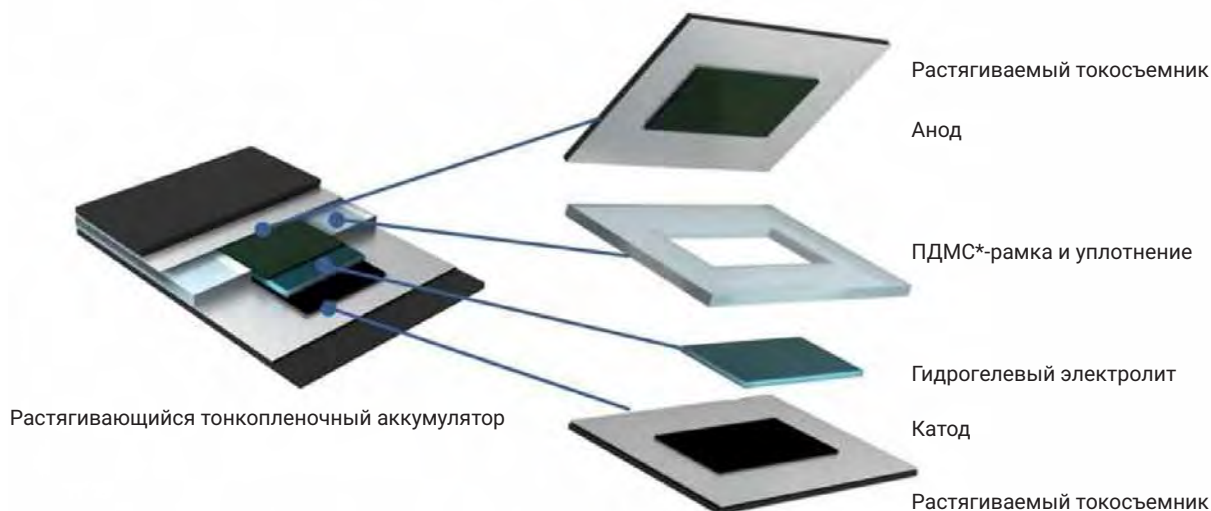
Исследователи ETH Zürich разработали прототип гибкой тонкопленочной батареи (рис. 1), которую можно сгибать, растягивать и даже скручивать, не прерывая подачу энергии. Особые свойства батареи придает использованный в ней электролит.

## ГИБКИЕ КОМПОНЕНТЫ

Так же, как и присутствующие на рынке аккумуляторы, новая батарея имеет слоистую конструкцию. Новаторством стало использование гибких компонентов, благодаря которым всю батарею можно сгибать и растягивать.

В конструкцию батареи входят два токопроводящих компонента для анода и катода из гибкого полимерного композита, содержащего электропро-

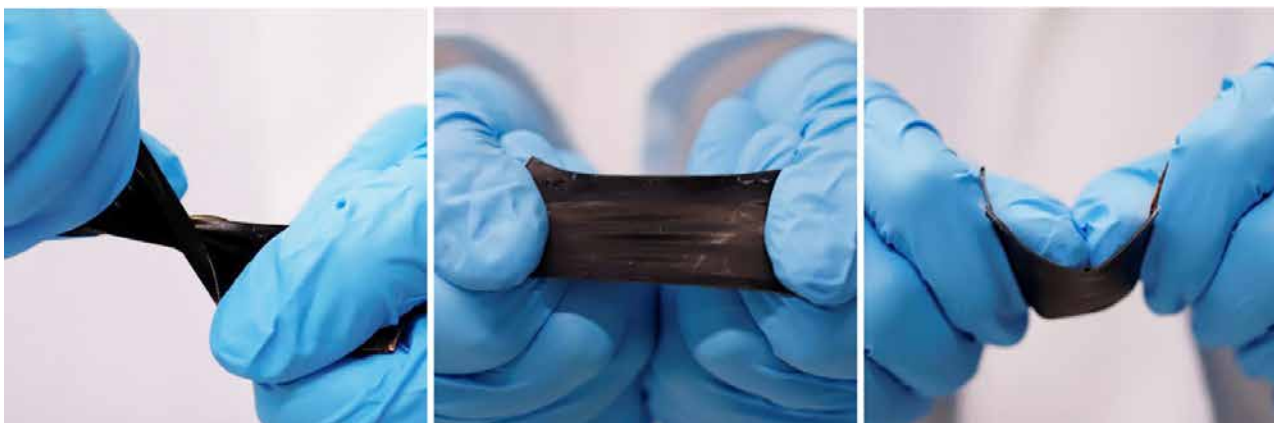
водящий углерод и служащего также внешней оболочкой. На внутреннюю поверхность композита исследователи нанесли тонкий слой микронизированных серебряных чешуек. Благодаря тому, что чешуйки заходят одна на другую, они не теряют контакт друг с другом даже при значительном растяжении эластичного токопроводящего компонента, что гарантирует проводимость (рис. 2). Кроме того, если даже серебряные



Источник: ETH Zürich

Рисунок 1. Прототип гибкой батареи, разработанный учеными из ETH Zürich

\* PDMS (polydimethylsiloxane) – полидиметилсилоксан (ПДМС), линейный полимер диметилсилоксана.



Источник: ETH Zürich

Рисунок 2. Эластичный материал токосъемника выдерживает значительное растяжение и скручивание

чешуйки действительно теряют контакт друг с другом, электрический ток все еще может

протекать через углеродсодержащий композит, хоть и слабее.

## ГЕЛЕВЫЙ ЭЛЕКТРОЛИТ НА ВОДНОЙ ОСНОВЕ

На последнем этапе разработки ученые разместили два токосъемника с наложенными электродами друг на друге и разделили их барьерным слоем, заполнив зазор в барьерной рамке электролитным гелем.

Подчеркивается, что этот гель экологически более безопасен, чем коммерческие электролиты. Жидкий электролит в современных батареях огнеопасен и токсичен. Гелевый электролит, напротив, содержит воду



## В ЦЕНТРЕ ВНИМАНИЯ: ETH ZÜRICH

**ETH Zürich** – Швейцарская высшая техническая школа в Цюрихе, осуществляет обучение в области инженерных и технических наук.

**Дата основания:** 16 октября 1855 г.

**Месторасположение:** г. Цюрих, Швейцария.

**Бюджет:** 1,885 млрд швейцарских франков (2017 г.).

**Численность студентов:** 20,6 тыс. человек.

**Численность преподавателей:** 6,5 тыс. человек (2017 г.).

**Численность административного персонала:** 2,7 тыс. человек (2017 г.).

Швейцарская высшая техническая школа в Цюрихе – один из ведущих технических университетов мира. В ETH Zürich обучались, преподавали и проводили исследования 32 лауреата Нобелевской премии, в т. ч. Альберт Эйнштейн, Леопольд Ружичка, Вольфганг Паули, Владимир Прелог, Рихард Эрнст и Курт Вютрих.

Лаборатория ионно-лучевой физики (LIB) в ETH Zürich специализируется на использовании

ускорительной масс-спектрометрии (УМС) – одного из наиболее современных, сверхчувствительных методов изотопного анализа вещества – и методов на основе фокусируемых ионных лучей, которые применяются в археологии, науках о Земле, биологии, материаловедении и фундаментальной физике. В настоящее время LIB разрабатывает установки УМС следующего поколения.



с высокой концентрацией соли лития, которая не только облегчает поток ионов лития между катодом и анодом во время зарядки или разрядки батареи, но также удерживает воду от электрохимического разложения. В ходе эксперимента исследователи соеди-

нили различные части своего прототипа при помощи клея, однако отметили, что для создания коммерческого аккумулятора необходимо найти другой способ поддерживать герметичность устройства в течение длительного времени.

## ПОТЕНЦИАЛ ПРИМЕНЕНИЯ

С каждым днем область применения для такой батареи расширяется. Производители мобильных телефонов соперничают друг с другом в разработке устройств со складными экранами.

Другие возможности использования включают в себя складные дисплеи для компьютеров, умных часов и планшетов или функциональные ткани, содержащие гибкую электронику.



*A Battery That Can Be Bent, Stretched and Twisted. Printed Electronics World, September 26, 2019: <https://www.printedelectronicsworld.com/articles/18284/a-battery-that-can-be-bent-stretched-and-twisted>*

# Главное авиационное командование ВВС США – об искусственном интеллекте

*Ключевые слова: авиация, ВВС, искусственный интеллект, машинное обучение.*

*Недавно генерал Майк Холмс, руководитель Главного авиационного командования ВВС США, дал интервью корреспондентам, специализирующимся на вопросах обороны и национальной безопасности и входящим в The Defense Writers Group. Основной посыл генерала – в настоящее время средства ИИ еще недостаточно хорошо развиты для того, чтобы быть принятыми на вооружение ВВС США. Чем он аргументировал свою позицию?*

Начальник Главного авиационного командования ВВС США<sup>21</sup> генерал Майк Холмс во время недавнего интервью журналистам The Defense Writers Group заявил, что пока не готов полагаться на информацию, получаемую средствами, созданными в рамках реализации программы развития систем ИИ, известной как Project Maven (maven – «знаток», «эксперт»). Проект Maven был инициирован корпорацией Google (которая впоследствии отказалась от него) для совместной реализации с другими фирмами и должен был стать лидером в усилиях Пентагона по обеспечению вооруженных сил США средствами и системами ИИ. В рамках проекта в течение шести месяцев 2017 г. вооруженные силы получили подобные средства и системы. С наибольшим энтузиазмом к Maven в его нынешнем виде отнеслись сотрудники разведки, получившие возможность автоматизировать однообразный процесс просмотра огромного количества фото и видео с самолетов-разведчиков, спутников-шпионов и т. д. Отмечается, что задействованные для этого средства и системы действуют предсказуемо

и быстро. Однако руководство ВВС далеко не в восторге.

Во время интервью Холмс отметил, что военно-воздушные силы сейчас полагаются на ИИ для помощи в прогнозном обслуживании авиационного парка и ряде других задач, но это направление уже было хорошо отработано гражданскими авиакомпаниями. По словам представителей руководства ВВС США, имеющийся в его распоряжении ИИ соответствует по уровню развития трехлетнему ребенку, что явно недостаточно для нужд военной авиации. При таком уровне развития в любом случае необходим контроль выполнения программ со стороны человека. Правда, Холмс с осторожностью отметил, что алгоритмы Maven обучаются и становятся все лучше и лучше. Именно это и должно делать машинное обучение – подпитывать систему все большим количеством данных, позволяя ей совершенствоваться.

В свою очередь, журналисты указали, что подобный скептицизм долгое время был одним из главных препятствий на пути эффективного использования ИИ вооруженными силами, которые, несмотря на огромные инве-



## МНЕНИЕ ЭКСПЕРТА

Под термином «искусственный интеллект» (ИИ) в статье подразумеваются различные автоматизированные и автоматические системы – нейронные сети, которые автоматизируют просмотр изображений, прогнозное обслуживание техники и помогают специалистам в различной рутинной работе. Ученые при оценке «интеллектуальности» компьютерных систем выделяют «слабый» и «сильный» ИИ. При этом нейронные сети, условно сравниваемые в статье с ребенком, являются рефлексным уровнем и в принципе не способны создать «взрослый» и/или «сильный» ИИ.

Вместе с тем мы все должны понимать, что использование «сильного» ИИ в вооруженных силах для выполнения боевых задач – автономных боевых робототехнических комплексов – создаст угрозу уничтожения человечества. Принятие всеми развитыми странами Национальных программ по развитию ИИ и дискуссии в ООН о запрете создания автономных боевых робототехнических комплексов однозначно свидетельствуют, что создание такого оружия – вопрос обозримого будущего.

Современные достижения в области ИИ, например, миварные технологии с обработкой более 5 млн правил «если-то» за доли секунд и на обычном одноядерном компьютере, сняли фундаментальные научные ограничения на создание «сильного» ИИ, способного превзойти все человечество по разуму и скорости принятия адекватных решений. Таким образом, дорога



к созданию сильного боевого автономного ИИ открыта.

Для России вопрос создания «сильного» ИИ является вопросом жизни или уничтожения. Следовательно, надо переставать копировать западные технологии, прежде всего нейросетевые подходы по созданию «слабого» ИИ, и переходить к созданию отечественных систем «сильного» ИИ на основе отечественной физико-математической школы.

*Олег Варламов, доктор технических наук,  
президент МИВАР*

стиции в НИОКР, демонстрируют устойчивый консерватизм, когда речь идет о передаче ответственности за человеческие жизни новым технологиям. При этом, когда появляется дей-

ствительно эффективное новое оружие, помешать военным широко использовать его без достаточного тестирования крайне трудно, если вообще возможно.



*Clark Colin. Air Combat Commander Doesn't Trust Project Maven's Artificial Intelligence – Yet. Breaking Defense magazine, August 21, 2019: <https://breakingdefense.com/2019/08/air-combat-commander-doesnt-trust-project-mavens-artificial-intelligence-yet/>*

Международный  
научно-практический форум

28/11/2019  
Главное здание  
Российского  
университета  
дружбы народов

**Промышленность.  
Наука.  
Компетенции.  
Интеграция.**



Россия, г. Москва  
ул. Миклухо-Маклая 6

### Секции форума

Управление конкурентоспособностью как основа устойчивого и опережающего развития

Экономика промышленности: теория, стратегия, практика

Цифровая экономика и менеджмент: прорывной опыт, устойчивое развитие, новые проекты

Искусственный интеллект как основа системы управления устойчивым развитием

Центры глобального технологического превосходства - драйверы инновационного развития и устойчивого развития корпорации

Будущее энергетики: в поисках инновационной и устойчивой модели развития

Комплаенс и антикоррупция в современном мире



Подробнее на [www.rudn-forum.ru](http://www.rudn-forum.ru)





# Безнагревная технология для производства гибкой электроники

*Ключевые слова: безнагревные технологии, гибкая электроника, носимая электроника, межсоединения.*

*Учеными разработан метод изготовления металлических межсоединений для электронных устройств без применения тепла. Это создает новые возможности в использовании материалов, а также новые сценарии научных и коммерческих применений.*

Для создания металлических деталей в электронных устройствах традиционно использовалось тепло – для придания требуе-

мой формы металл следовало расплавить. Ученые из Университета штата Айова (США) разработали способ, не предусматривающий



Источник: Университет штата Айова

*Исследователи из Университета штата Айова продемонстрировали способ печати гибкой электроники, не требующий нагрева. На фото – электронные структуры, напечатанные на желатине в рамках этого исследования*





использование тепла при создании электронных межсоединений, что облегчает проектирование гибкой и носимой электроники.

Изначально проект был запущен три года назад на базе технического стартапа в качестве упражнения для аспирантов вуза, однако результат вышел за рамки учебного проекта. По новой технологии металл (в данном случае – сплав висмута, индия и олова) нагревается заранее и сохраняется в жидком виде, что дает возможность создавать межсоединения без повреждения подложки, при комнатной температуре и без плавления.

В процессе производства жидкий металл с температурой ниже точки плавления заключается в полированные оксидные оболочки, образуя частицы размером около 10 мкм. При

разрушении оболочек при помощи механического давления или химического растворения металл растекается и затвердевает. Происходит так называемый процесс холодной сварки, что дает возможность печатать проводящие металлические линии и структуры на различных материалах. Теперь исследователи могут использовать более широкий, чем раньше, спектр подложек для металлических межсоединений – поскольку им не нужно беспокоиться о тепловом повреждении.

Помимо создания межсоединений для гибкой электроники безнагревную технологию можно использовать при изготовлении датчиков измерения структурной целостности здания или в разработке электрических контактов для солнечных элементов.



*Montalbano Elizabeth. Heat-Free Technology Developed for Fabrication of Flexible Electronics. Design News. Materials & Assembly, September 27, 2019: <https://www.designnews.com/materials-assembly/heat-free-technology-developed-fabrication-flexible-electronics/183178586561565>*



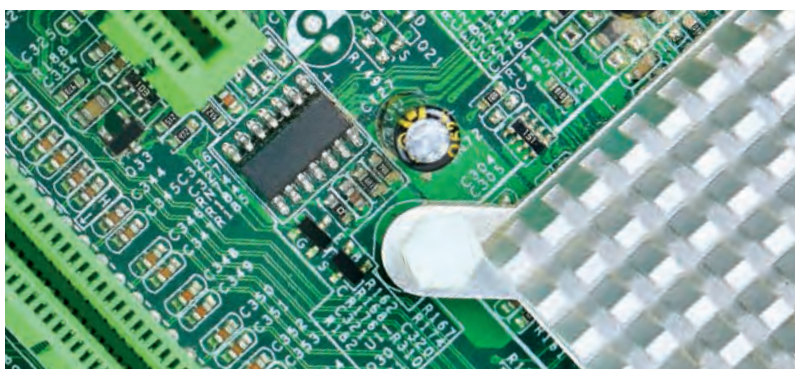
**E·X·P·O**  
**ELECTRONICA**



Самая крупная в России  
выставка электронных  
компонентов, модулей  
и комплектующих

**14-16 апреля 2020**

Москва, МВЦ «Крокус Экспо»



**Специальная экспозиция**  
**Компоненты**  
**для встроенных**  
**систем безопасности**

Представьте свои разработки  
для встраиваемых систем безопасности  
в специальной экспозиции:

- Микроконтроллеры / процессоры со встроенными функциями безопасности
- Токены аутентификации
- Биометрические датчики
- Модули безопасности

**Ваш**  
**КОМПОНЕНТ**  
**успеха!**

[expoelectronica.ru](http://expoelectronica.ru)



Организатор  
Группа компаний ITE  
+7 (499) 750-08-28  
[electron@ite-expo.ru](mailto:electron@ite-expo.ru)

Совместно с выставками





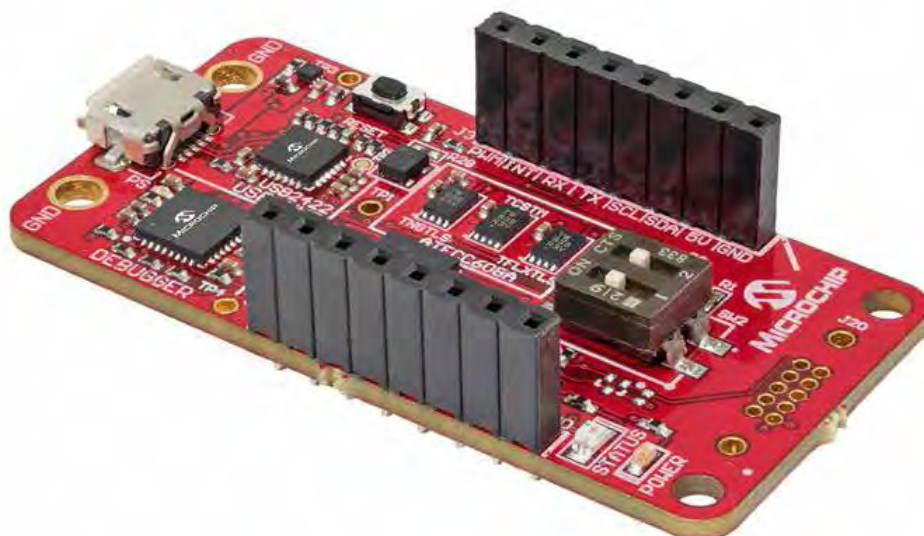
# Платформа Microchip Trust призвана упростить аппаратную безопасность Интернета вещей

*Ключевые слова: Интернет вещей, безопасная аутентификация, аппаратная защита, защитные элементы.*

*Компания Microchip Technology представила первое всесторонне проработанное решение, которое обеспечивает безопасное хранение ключей для устройств с низкой, средней и большой вместимостью, используя защитный элемент ATECC608A.*

Платформа Microchip Trust Platform (MTP), разработанная фирмой Microchip Technology, входящей в группу компаний Crypto Authentication, призвана помочь компаниям любого масштаба внедрить безопасную аутентификацию с целью минимизации или устранения проблем, связанных с уязвимостью систем

Интернета вещей. Аппаратная защита – единственный способ уберечь секретные ключи от физических атак и дистанционного извлечения, но для настройки и подготовки каждого устройства требуются обширные знания в области безопасности, время на разработку и определенные затраты. Производи-



Источник: Microchip Technology Inc.



## МНЕНИЕ ЭКСПЕРТА

Инфраструктура Интернета вещей, как правило, подразумевает наличие большого количества связанных между собой устройств, разнесенных друг от друга на значительные расстояния. И зачастую полностью ограничить физический доступ к ним потенциальных злоумышленников практически невозможно. Поэтому на объектах критической инфраструктуры особенно остро встает вопрос надежной защиты устройств от несанкционированного перехвата и подмены информации, а также физического взлома. Традиционно для этого используются криптографические алгоритмы и протоколы. При этом ключи, с помощью которых осуществляется шифрование и проверка целостности передаваемых данных, должны безопасно храниться и использоваться на устройствах.

Аппаратная защита действительно является единственным надежным способом защиты от физического взлома. Она позволяет защититься от таких видов физических атак, как вычитывание памяти устройства, анализ паразитных сигналов, атаки с помощью лазера и прочие атаки, от которых невозможно защититься только программными средствами.

АО «НИИМЭ» ведет активные работы в этом же направлении и готовится в ближайшее время вывести на рынок аналогичное решение для Интернета вещей – программно-аппаратный комплекс «Звезда», который использует российские криптографические алгоритмы. В рамках



проекта разрабатывается элемент безопасности для устройств Интернета вещей в виде компактной микросхемы, сертифицированной как СКЗИ класса КСЗ, и поставляемой в удобных форм-факторах SIM-карты или в корпусе SOIC-8. В рамках проекта также разрабатывается серверное приложение, позволяющее взаимодействовать с устройствами с обеспечением криптографической защиты передаваемых данных.

*Владимир Сергеев, заместитель начальника  
отдела разработки средств защиты информации  
АО «НИИМЭ»*

тели, как правило, могут осуществлять техническую поддержку только масштабных заказов, в результате чего малый и средний бизнес получает малоэффективные решения. МТР решает эту проблему благодаря использованию трехуровневой системы, обеспечивающей по умолчанию всесторонне проработанные, сконфигурированные или полностью настраиваемые защитные эле-

менты, которые позволяют разработчикам выбирать платформу, наиболее подходящую для их проекта.

Trust & GO – первый уровень, который предоставляет полностью подготовленные защитные элементы с минимальной упорядочиваемой переменной (MOQ) всего 10 единиц. Учетные данные устройства запрограммированы и встроены в защитный элемент



ATECC608A для автоматической регистрации в «облаке» или аутентификации LoRaWAN. Параллельно соответствующие сертификаты и общедоступные ключи доставляются в файле манифеста<sup>22</sup>, который можно загрузить через электронный магазин компании Microchip и их партнеров. Такая система помогает сэкономить месяцы на разработке и значительно облегчает логистику предоставления услуг. Кроме того, она упрощает защиту и управление периферийными устройствами без дополнительных расходов на сторонние службы обеспечения или центры сертификации для клиентов масс-маркета.

Тем клиентам, которые предпочитают более обширную персонализацию технических решений, платформа предлагает уровни TrustFLEX и TrustCUSTOM.

TrustFLEX – это второй уровень системы. Он позволяет клиентам использовать сертификацию в зависимости от запроса и в то же время получать выгоду от предварительно настроенных вариантов использования. Базовые меры безопасности включают в себя усиленную аутентификацию Transport Layer Security (TLS) для подключения к любой IP-сети с использованием любой цепочки сертификатов, аутентификацию LoRaWAN, безопасную загрузку, обновления по беспроводной сети (OTA), защиту IP, защиту пользовательских данных и чередование ключей. Это сокращает время и уменьшает сложность настройки устройства

без необходимости персонализировать номера деталей. Если потребитель хочет персонализировать свои проекты, он может воспользоваться третьим компонентом платформы под названием TrustCUSTOM, который дает возможность осуществлять уникальную персональную настройку, а также настраивает учетные данные пользователя.

Эксперты Microchip утверждают, что рост числа успешных атак на программные решения для обеспечения безопасности подчеркивает необходимость применения компаниями передовых отраслевых практик, включая изоляцию закрытых ключей в защитных элементах. MTP, решая проблемы, связанные с настройкой и технической поддержкой устройств, делает аппаратную безопасность простой и экономически эффективной для разномасштабных компаний. Компания Microchip сотрудничала с Amazon Web Services (AWS) с целью упростить процесс регистрации продуктов, основанных на технологии Интернета вещей и разработанных со всеми вариантами поддержки MTP. Защитные элементы Microchip обеспечивают безопасное предоставление ключей и гарантируют, что ключи никогда не будут находиться в открытом доступе для третьих лиц как во время предоставления услуг, так и на протяжении всего срока службы устройства. Защитный элемент ATECC608A может быть сопряжен с любым микроконтроллером и микропроцессором.



*Best Amy. Microchip Trust Platform Looks to Simplify Hardware-Based IoT Security. New Electronics, September 30, 2019: <http://www.newelectronics.co.uk/electronics-news/microchip-trust-platform-looks-to-simplify-hardware-based-iot-security/219818/>*

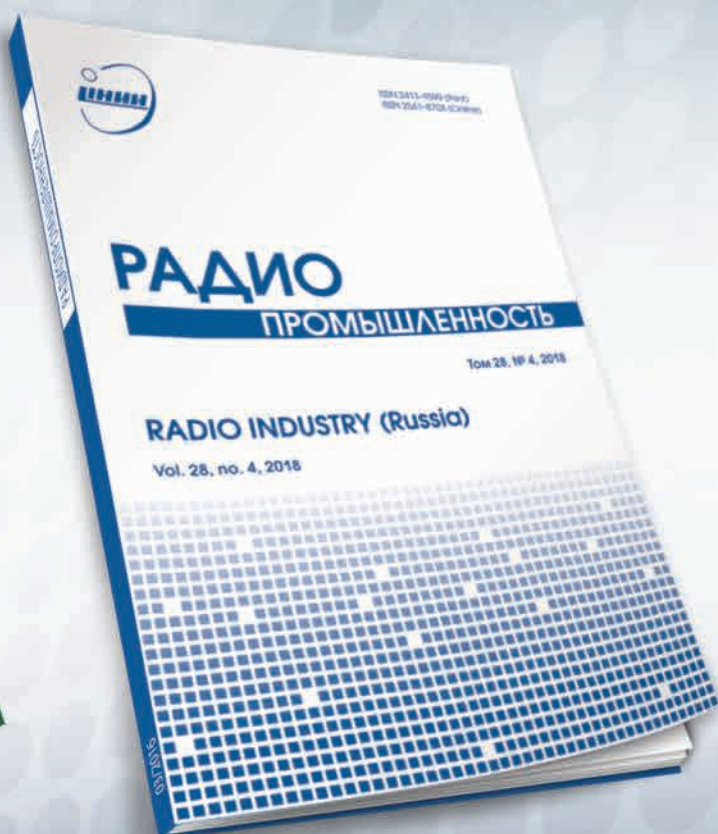


# ПОДПИСКА

на ведущие научные журналы  
радиоэлектронной отрасли



12 номеров в год



4 номера в год

**АКТУАЛЬНЫЕ НАУЧНЫЕ РАЗРАБОТКИ,  
СОВРЕМЕННЫЕ ЭКОНОМИЧЕСКИЕ  
И УПРАВЛЕНЧЕСКИЕ РЕШЕНИЯ**

**Входят в перечень ВАК. Индексируются РИНЦ.**

Подписка в любом почтовом отделении, по тел. +7 (495) 940-65-46,  
e-mail: [publish@instel.ru](mailto:publish@instel.ru), на сайте [www.instel.ru](http://www.instel.ru).



# ГЛОССАРИЙ

- 1 **Четвертый уровень автоматизации автомобиля (Level 4 autonomous driving)** – высокая степень автоматизации: автомобиль может управляться человеком, но необходимости в этом нет; автономное транспортное средство обращается к человеку только в не предусмотренных программным обеспечением случаях.
- 2 **RGB-камера** – цветная цифровая камера, имеющая отдельные выходы для красного, зеленого и синего цветов. Выводит более качественное изображение, чем камеры с композитным цветом.
- 3 **EuroNCAP (European New Car Assessment Programme)** – Европейская программа оценки новых автомобилей, международное некоммерческое объединение, созданное для оценки совершенства автомобилей с точки зрения пассивной безопасности.
- 4 **Генеративно-сопоставительная сеть (generative adversarial network, GAN)** – алгоритм машинного обучения без учителя, построенный на комбинации двух нейронных сетей, одна из которых (сеть G) генерирует образцы, а другая (сеть D) старается отличить правильные («подлинные») образцы от неправильных. Так как сети G и D имеют противоположные цели – создать образцы и отбраковать образцы – между ними возникает антагонистическая игра.
- 5 **1080p** – условное название категории режимов представления видеоизображения. Число 1080 соответствует 1080 линиям вертикальной разрешающей способности, а буква «p» означает «прогрессивная развертка». 1080p рассматривается как один из видеорежимов ТВЧ (термин подразумевает широкоэкранный форматное соотношение 16:9, означающее горизонтальную (дисплейную) разрешающую способность 1920 точек по диагонали и кадровую разрешающую способность 1920´1080, или 2073600 пикселей).
- 6 **Расширенный динамический диапазон (high dynamic range, HDR)** – одна из технологий в рамках телевизионного стандарта 4K.
- 7 **Воксел (voxel – volumetric pixel)** – минимальный адресуемый объемный элемент изображения трехмерного пространства, используемый при быстром рендеринге трехмерных объектов.
- 8 **PMUT (piezoelectric micromachined ultrasonic transducers)** – пьезоэлектрические ультразвуковые преобразователи, изготовленные методом микрообработки. В отличие от объемных пьезоэлектрических преобразователей, использующих движение в толщине пьезоэлектрической керамической пластины, изготовленной из цирконата-титаната свинца (PZT) или монокристаллического магнониобата свинца – титаната свинца (PMN-PT), PMUT основаны на изгибном движении тонкой мембраны, связанной с тонкой пьезоэлектрической пленкой, такой как пленка поливинилиденфторида (PVDF). Преимущества PMUT: увеличенная ширина полосы частот, гибкая геометрия, естественное акустическое полное сопротивление (согласованное по воде), уменьшенные требования к напряжению тока, смешивание различных резонансных частот и потенциал интеграции с поддержкой электронных схем, особенно для миниатюрных высокочастотных устройств.
- 9 **Углеродный след (carbon footprint)** – выброс CO<sub>2</sub> в атмосферу, связанный с деятельностью отдельного человека или организации, например поездки на автомобиле, полета на самолете, производства товаров.
- 10 **Захватчик рынка (killer application, killer apps)** – новаторский продукт, революционная новинка (товар или услуга), с появлением которой устанавливаются новые стандарты требований в конкретной области рынка, вытесняются традиционные продукты или услуги.
- 11 **Корень доверия (root of trust – RoT, также root of security – RoS, root of security trust – RoST)** – набор функций в доверенном вычислительном модуле, которому всегда доверяет операционная система

(ОС) компьютера. Служит отдельным вычислительным механизмом, управляющим криптографическим процессором доверенной вычислительной платформы на ПК или мобильном устройстве, в которое он встроен. Обеспечивает надежность вычислительных функций, включая: шифрование диска «на лету»; обнаружение и сообщение о несанкционированных изменениях в ОС или программах; обнаружение руткитов; предотвращение неправильного чтения или записи программ в память другой программы; аппаратную поддержку управления цифровыми правами (DRM).

- <sup>12</sup> **EFI (extensible firmware interface)** – интерфейс расширяемой прошивки: интерфейс между ОС и микропрограммами, управляющими низкоуровневыми функциями оборудования, предназначенный для корректного инициализирования оборудования при включении системы и передачи управления загрузчику ОС. Первая спецификация EFI была разработана Intel. Позднее от прежнего названия отказались, и последняя версия стандарта носит название Unified Extensible Firmware Interface (UEFI).
- <sup>13</sup> **PUF (physically unclonable function)** – «ДНК» или «отпечаток пальца» кристалла ИС, технология, разработанная специалистами Массачусетского технологического института. Определяет для каждой ИС уникальное цифровое обозначение («подпись» кристалла).
- <sup>14</sup> **Антенна-в-модуле (antenna in package, AiP)** – технология, по которой антенна (антенны) с радио- или радиолокационной головкой или кристаллами встраивается в стандартное устройство поверхностного монтажа. Широко применяется производителями микросхем для 60-ГГц радиостанций и радиолокационного распознавания жестов.
- <sup>15</sup> **Научно-исследовательский институт промышленных технологий Тайваня (Industrial Technology Research Institute, ITRI)** – государственный институт, созданный в начале 1970-х гг. Основная задача – определение перспективных направлений развития науки и техники, фундаментальные исследования и помощь частно-государственным и частным фирмам в освоении их результатов. Значительное число полупроводниковых фирм Тайваня когда-то «отпочковалось» (spin-off) от этого института: UMC (1979 г., первый завод), TSMC (1986 г., первый завод и центр проектирования), Vanguard International Semiconductor Corporation (VIS, декабрь 1994 г., на базе лаборатории субмикронных процессов обработки 200-мм пластин).
- <sup>16</sup> **Бета-версия (beta version)** – предварительная версия аппаратных и программных изделий, предоставляемая избранным пользователям с целью выявления недостатков и возможного усовершенствования.
- <sup>17</sup> **Аппаратный ключ (dongle)** – электронный защитный ключ, подключаемый к параллельному или последовательному порту для предотвращения несанкционированного использования программных продуктов или для обеспечения компьютерной безопасности.
- <sup>18</sup> **Кубит (qubit, q-bit)** – квантовый бит (разряд), отличается от обычного «детерминированного» разряда памяти тем, что может одновременно находиться в двух состояниях, т. е. хранить 0 и 1 одновременно.
- <sup>19</sup> **Национальный институт стандартов и технологий (National Institute of Standards and Technology, NIST)** – нерегулирующий федеральный орган в составе Управления по технологиям Министерства торговли США. Деятельность NIST направлена на продвижение инноваций и обеспечение промышленной конкурентоспособности США за счет развития метрологии, стандартизации и совершенствования технологий с целью обеспечения экономической безопасности и повышения качества жизни населения страны.
- <sup>20</sup> **Топологический изолятор (topology insulator)** – полупроводниковый прибор, объемные свойства которого соответствуют

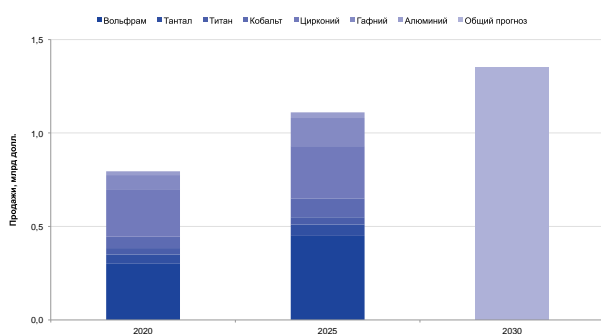




свойствам изолятора, но верхний слой является проводящим. Первые два открытых материала для таких приборов – теллурид висмута ( $\text{Bi}_2\text{Te}_3$ ) и селенид висмута ( $\text{Bi}_2\text{Se}_3$ ). Теоретически материалами для топологических изоляторов могут служить разбавленные магнитные полупроводники типа эпитаксиальных пленок оксида стронция-олова ( $\text{Sr}_3\text{SnO}$ ). Топологические изоляторы могут использоваться в квантовых компьютерах как носители информации.

- <sup>21</sup> **Главное авиационное командование ВВС США (Air Combat Command, ACC)** – одно из шести Главных командований (Major Commands, MAJCOMs) ВВС США. Штаб-квартира расположена в шт. Вирджиния.
- <sup>22</sup> **Файл манифеста (manifest file)** – файл, содержащий список ресурсов, таких как файлы грамматики и базы данных приглашений, которые Speech Server предварительно загружает и кэширует для повышения производительности.

## В СЛЕДУЮЩЕМ ВЫПУСКЕ:



- Технология Ethernet существует достаточно давно и широко используется при автоматизации зданий и промышленных предприятий, создании внутриавтомобильных сетей, в ЦОДах, облачных сервисах и т. д. Скорость передачи данных достигла 400 Гбит/с, а скоро может перешагнуть терагерцевый рубеж.
- По мере освоения полупроводниковой промышленностью все меньших топологических уровней растет популярность таких технологических процессов, как осаждение атомарных слоев и химическое осаждение из паровой фазы, значение тестирования и своевременного обнаружения дефектов (в том числе за счет программного моделирования), а также унифицированной верификации функциональной безопасности с целью сокращения сроков вывода новой продукции на рынок.
- NXP Semiconductors представила новый инструментарий глубокого обучения eIQAuto. Цель – облегчить проектировщикам автономных автомобилей внедрение глубокого обучения в транспортные средства. Компания стремится выделиться среди конкурентов за счет инструментальных средств «автомобильного качества».

# Всё о зарубежной электронной технике

НОВОСТИ



СТАТЬИ



КОММЕНТАРИИ  
ЭКСПЕРТОВ



АНАЛИТИКА

