В течение шести дней мероприятия пятого международного военно-технического форума «Армия-2019» проходили в Конгрессно-выставочном центре «Патриот», на полигоне Алабино и аэродроме Кубинка, а также в 35 городах и населенных пунктах Западного, Южного, Центрального, Восточного военных округов и Северного флота. За время работы форума общее количество гостей и участников превысило 1 млн человек. На полях форума работали представители 120 стран мира. Форум «Армия-2019» совместил наряду со статическими экспозициями и динамическим показом возможностей боевой техники обширную научно-деловую программу и разнообразные культурно-художественные и военно-патриотические мероприятия.

Оборонные инновации
К работе по отбору инновационных разработок и технологий, представляющих интерес для Вооруженных Сил Российской Федерации, на МВТФ «Армия-2019» было привлечено более 350 экспертов от 32 органов военного управления, а также вузов и научно-исследовательских организаций Минобороны России. В результате работы форума военные эксперты отобрали 278 инновационных разработок и проектов.

Одной из перспективных инновационных технологий, впервые представленных на форуме «Армия-2019», является автоматизированная система контроля наличия, движения и расходования горючего (АСК ГСМ). «Сейчас система учета и контроля горючего включает в себя датчики на каждой машине, которые в автоматическом режиме передают данные начальнику службы горючего воинской части, далее в дивизию, затем в армию, в округ и в итоге в Национальный центр управления обороной. Сейчас мы завершаем работу над этой системой и в ближайшее время она поступит в войска», − подчеркнул замминистра обороны Дмитрий Булгаков. Система предназначена для оснащения вооружения − автомобильной и бронетанковой техники, кораблей и судов военно-морского флота, авиации, средств заправки и транспортирования горючего, а также стационарных объектов материально-технического обеспечения по службе горючего. Она позволяет осуществлять в автоматизированном режиме сбор, обработку и передачу данных от топливных баков военной техники до органов военного управления вплоть до Национального центра управления обороной России. Система успешно прошла предварительные испытания и готова к внедрению в Вооруженные Силы. Следует отметить, что система изготовлена полностью на отечественной элементной базе.

Импортозамещение
Отечественная элементная база стала центром внимания нескольких круглых столов и совещаний, которые прошли в рамках научно-деловой программы Форума. В частности, в рамках «Армия-2019» состоялось заседание «Диверсификация предприятий ОПК и формирование гражданских рынков радиоэлектронной продукции. Практика и регулирование», на котором обсуждали готовящееся постановление Правительства по стимулированию использования отечественной элементной базы в естественных монополиях, госкомпаниях, государственных информационных системах и проектах, реализуемых в рамках государственных программ. Сейчас в указанных проектах в большинстве случаев используется иностранная элементная база, и для этого прилагается масса усилий.

Так, по словам заместителя генерального директора и статс-секретаря холдинга «Росэлектроника» госкорпорации «Ростех» Арсения Брыкина традиционно завышаются требования в тендерах, минимизируются сроки поставок, предлагаются невыгодные финансовые условиях контрактов – словом, делается все, чтобы тендеры выигрывали компании, поставляющие иностранное оборудование. В результате из 245 млрд руб., заявленных на различных конкурсах, «Росэлектронике» удалось выиграть поставки только на 6 млрд руб. Хотя системы хранения компании по объему данных занимают 38% всего рынка, но по объему выручки − лишь 8%.

Тема импортозамещения аппаратной элементной базы была поднята и на круглом столе «Перспективы развития технологий беспроводной связи и Интернета вещей для Вооруженных Сил Российской Федерации». Рассматривались в основном технологии 5G и другие технологии связи Интернета вещей для создания российских подключенных устройств, в частности, для целей боевого их использования. На заседании даже прозвучал термин «Интернет боевых вещей» (Internet of Battle Things − IoBT), разработка которых ведется за рубежом, но и наши ОПК планируют разработки таких устройств. Правда, в них уже применяются не стандартные кремниевые полупроводники, а более высокоскоростные арсенид-галлиевые и даже нитрид-галлиевые. Они позволяют работать на более высоких скоростях, но и стоят значительно дороже. В России подобные производства есть, хотя и не для массового рынка. Тем не менее, российские производители вполне могут выпускать интеллектуальные устройства, работающие на высоких частотах до десятков гигагерц с возможностью управления активной фазированной антенной решеткой (АФАР) − технология, которая является основой для сетей 5G.

Конечно, для Вооруженных Сил необходимы технологии связи со встроенной защитой и здесь компания «Микрон» предлагает контроллеры для построения устройств со встроенными российскими алгоритмами шифрования, впрочем, и сама технология АФАР позволяет формировать целенаправленный луч до конкретных клиентов, который практически не дает боковых лепестков для посторонних устройств, − перехватить сообщение 5G будет и так достаточно сложно из-за узкой апертуры направленного луча.

Перспективные вооружения
Очевидно, что на Вооруженные Силы также начинают влиять информационные технологии. Перспективные средства вооружений уже не могут обходиться без ИТ. Министерством обороны принята «дорожная карта» по переходу на электронные форматы обмена в том числе и технической документацией. Поэтому сейчас разрабатываются единые форматы представления 3D-моделей, электронных документов и контроля доступа. В частности, именно эти проблемы обсуждались на заседании «Вопросы создания защищенной информационной среды системы управления жизненным циклом изделия на основе отечественного доверенного программного обеспечения». На нем представители промышленности и производители российского программного обеспечения обменивались опытом по созданию защищенных систем управления полным жизненным циклом изделий.

Методы защиты секретной информации обсуждались и на круглом столе «Системное программирование как ключевое направление противодействия киберугрозам». На нем Дмитрий Шевцов, начальник управления ФСТЭК России, рассказал о новых стандартах, разработанных техническим комитетом №362 «Защита информации». В частности, в этом комитете был разработан стандарт ГОСТ Р 58256-2018 «Защита информации. Управление потоками информации в информационной системе. Формат классификационных меток», который определяет представление меток секретности в информационной системе с мандатным способом разграничения доступа − именно такие используются в Министерстве обороны РФ. Стандарт разработан АО «НПО РусБИТех» (создатель операционной системы AstraLinux). В то же время при сертификации средств защиты на уровень, где требуется мандатный доступ, без реализации формата представления классификационных меток ГОСТ Р 58256-2018 вряд ли она закончится успешно − скорее всего, в этой части потребуется доработка.

Форматы долгосрочного хранения секретных сведений также обусловливают возникновение определенных проблем. Дело в том, что в ближайшей перспективе ожидается появление квантовых компьютеров, которые будут способны взламывать классические алгоритмы шифрования с помощью квантовых методов вычислений. Вполне возможно, что они смогут взломать шифрование за весьма короткое время, что недопустимо для национальной безопасности. Поэтому возникла задача разработки пост-квантовых алгоритмов шифрования для долгосрочного хранения электронных документов. Конечно, квантовое шифрование могло бы решить поставленную задачу, однако сейчас оно используется только для передачи данных, но не для ее хранения. Американский институт NIST уже инициировал конкурс на разработку подобных стандартов шифрования для долгосрочного хранения. Аналогичную работу нужно начинать и в России.

Искусственный интеллект
Наиболее перспективные направления вооружений связаны уже не столько с применением ИТ, сколько с использованием искусственного интеллекта, который может оперативно помогать военным разбираться в боевой обстановке, приоритезировать цели и угрозы, а также оценивать вероятность наступления неблагоприятных событий. Эти вопросы обсуждались на конференции «Технологии искусственного интеллекта в интересах обороны и безопасности государства». В частности, начальник лаборатории ГосНИИАС, д. т. н. Борис Федунов отметил, что методы искусственного интеллекта уже пытались использовать для оснащения летной техникой, и все разработки окончились макетами в 90-х гг. Однако основные принципы использования ИИ в боевых условиях сохранились и сейчас восстанавливаются. Искусственный интеллект можно использовать два решения двух задач: динамического целеполагания, т. е. выбора приоритета целей в условиях боевой обстановки, и оценки состояния боевой машины и возможности ее в дальнейшем выполнить поставленные перед ней задачи. Для быстрого анализа информации, поступающей из различных источников, и оценки как внешней обстановки, так и самого оборудования и можно использовать технологии искусственного интеллекта.

Для решения подобных задач не подходят чисто программные решения, которые требуют объемных вычислений и времени для анализа больших данных. Для них лучше использовать предварительно обученные глубокие нейронные сети, реализовать которые можно с помощью специализированного бортового оборудования. О разработке подобного оборудования рассказал на конференции заместитель генерального директора НТЦ «Модуль» по цифровой обработке сигналов и изображений Виктор Глазов. Его компания разработала уже четвертое поколение векторно-матричных микропроцессоров с оригинальной архитектурой NeuroMatrix, которые хорошо подходят для реализации алгоритмов глубоких сверточных нейронных сетей, которые сейчас и используют для практически всех применений искусственного интеллекта. Компания даже заключила договор с компанией «Нейросети Ашманова» для использования в своих процессорах библиотеки PuzzleLib, которая и позволяет реализовать быстрые алгоритмы решения задач искусственного интеллекта.

Юрий Визильтер, начальник подразделения ФГУП «ГосНИИАС», оценил состояние технологий первого поколения нейронных сетей как «готовы к ОКР» − уже появились российские технологии, которые обеспечивают возможность в режиме реального времени осуществлять распознавание образов и решать другие задачи технического зрения. Второе поколение нейронных сетей, которые позволяли бы выполнять задачи наблюдения за объектам, моделирования его поведения, управления и оптимизации, находятся пока на уровне разработок. Он отметил, что все перечисленные задачи используют механизмы теории графов, в то время как именно в данном понятийном аппарате сформулированы и все решения задач оптимизации. Это позволяет надеяться на создание в недалеком будущем работающих прототипов и второго поколения нейронных сетей. Таким образом, искусственный интеллект может в самое ближайшее время быть интегрирован в перспективные средства вооружений.