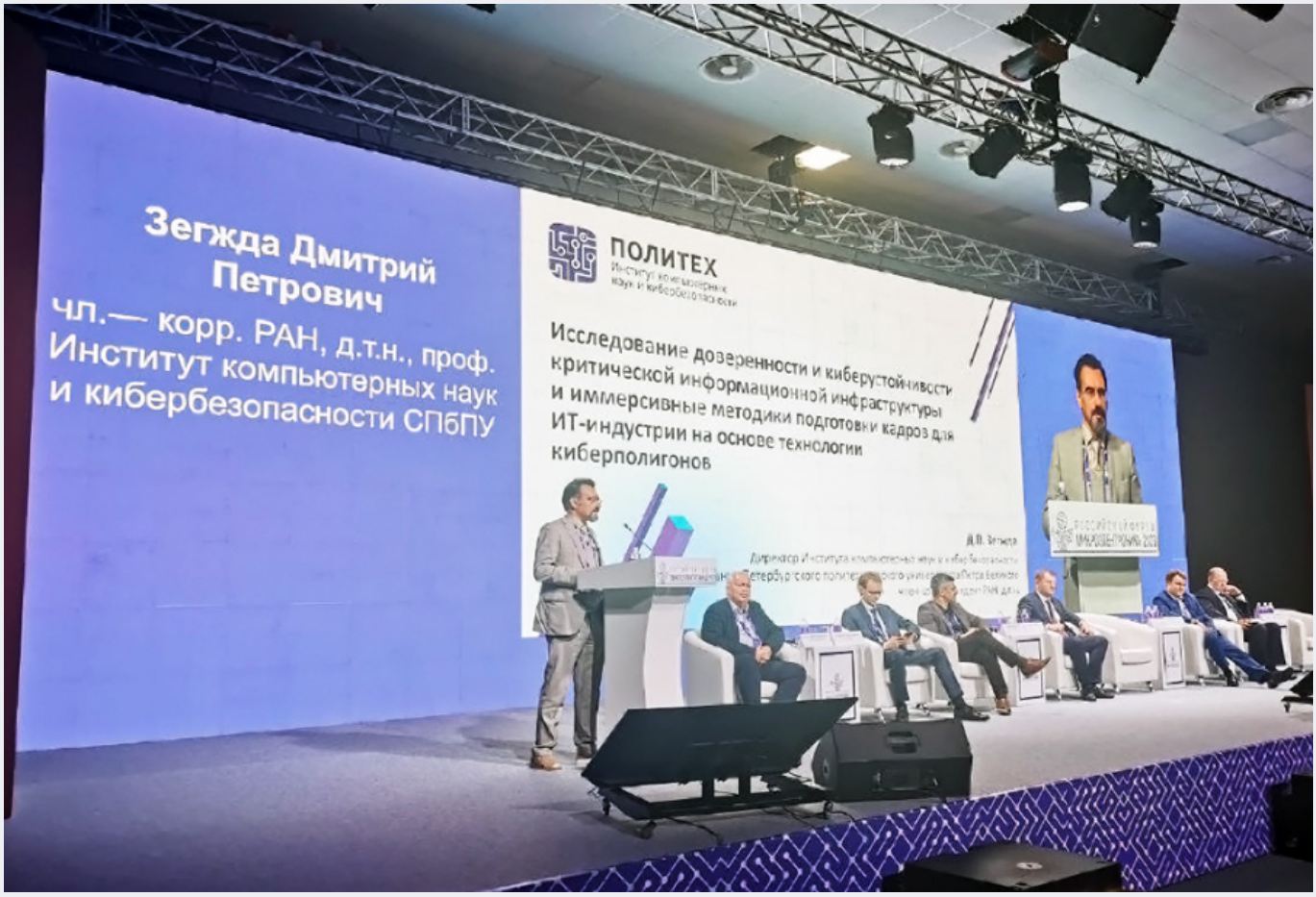
Дмитрий Петрович Зегжда принял участие в работе Всероссийского форума «Микроэлектроника-2023»



Российский форум «Микроэлектроника», ключевое информационное событие года в мире электронных технологий, прошел на федеральной территории Сириус с 9 по 14 октября. В работе форума участвовал Дмитрий Петрович Зегжда, директор Института компьютерных наук и кибербезопасности Санкт-Петербургского политехнического университета Петра Великого, член-корреспондент РАН, д.т.н. Он рассказал об исследованиях киберустойчивости критической информационной инфраструктуры

Участники Форума обсуждали вопросы содействия интеграции российских производителей в проекты по обеспечению ускоренного цифрового развития. Одна из главных задач форума – установление диалога между разработчиками электронной компонентной базы и производителями готовой продукции. «Микроэлектроника» проходит с 2015 года, девятый раз, и собирает ключевых практиков и теоретиков для обсуждения наиболее актуальных вопросов сферы.

В своем обращении к участникам премьер-министр Михаил Мишустин заметил: «…потребности в вычислительных ресурсах продолжают расти, и наши собственные суверенные решения в этой сфере критически необходимы для развития систем искусственного интеллекта, для создания больших нейросетевых моделей. Именно поэтому важно поддерживать отечественную микроэлектронную промышленность».

Дмитрий Петрович Зегжда в своем докладе для пленарного заседания «Доверенные электронные системы и ПАК для критической гражданской инфраструктуры» рассказал об исследованиях доверенности и киберустойчивости критической информационной инфраструктуры. Среди тенденций последнего времени он отметил конвергенцию вычислительных и телекоммуникационных систем и исполнительных устройств во всех сферах жизни, а среди потенциальных проблем – необходимость обеспечения безопасности и надежности цифровизации. Он привел несколько примеров атак на критическую информационную инфраструктуру энергетической и ядерной отраслей – Иран, 2010 год; Южная Корея, 2014; США, 2023, – и дал краткий обзор по кибератакам на отечественные системы.

Дмитрий Петрович, кроме того, поделился опытом внедрения иммерсивных методик в процесс подготовки кадров для ИТ-индустрии – на основе технологии киберполигонов. Киберполигоном называется совокупность аппаратно-программных средств, позволяющих осуществлять воспроизводимые экспериментальные исследования на основе воздействий и наблюдении реакций систем на эти воздействия; аналог – военный испытательный полигон для вооружений и учений. В результате моделирования в том числе высокой нагрузки и кибератак на киберполигоне выявляются условия некорректной работы исследуемых систем – сбои, несоответствия, уязвимости. Киберполигон позволяет осуществлять виртуальные эксперименты, значительно ускоряя и «цикл защиты», и «цикл нападения».