КОЛОНКА ГЛАВНОГО РЕДАКТОРА

Здравствуйте, уважаемые читатели и авторы журнала «Безопасность информационных технологий»!

Вот и подходит к завершению очередной год нашей жизни и годовой цикл издания нашего журнала!

Традиционно начну с краткого (не претендующего на полноту и точность) реферирования основных проектов и новых нормативных документов по проблематике нашего журнала.

Законопроект **о технологической политике России** размещен на портале проектов нормативных актов https://regulation.gov.ru/Regulation/Npa/PublicView?npaID=142132, а его концепция была утверждена Правительством Российской Федерации ранее в мае 2023 г. Законопроект направлен на обеспечение технологического суверенитета страны и создание условий для разработки и внедрения технологических инноваций, определяет цели, задачи и принципы технологической политики, регулирует отношения, возникающие между лицами, осуществляющими деятельность в сфере технологического развития.

В законопроекте введены основные понятия:

– **высокотехнологичная продукция** – космические и летательные аппараты, в том числе беспилотные воздушные судна, средства измерения и оптические приборы, **компьютерное оборудование** и оргтехника, лекарственные средства и медицинские изделия, малотоннажная и среднетоннажная химическая продукция, электрические машины, неэлектрические машины, железнодорожный тяговый подвижной состав, в том числе высокоскоростной, а также с автоматическим управлением, **электроника, в том числе микроэлектроника, и телекоммуникационное оборудование, программное обеспечение в составе высокотехнологичной продукции**, иные товары, работы и услуги, определенные Правительством Российской Федерации;

– **критическая технология** – технология, существенно необходимая для производства важнейших видов высокотехнологичной продукции, имеющая системное значение для функционирования экономики, решения социально-экономических задач, обеспечения обороны и безопасности государства и включенная в перечень критических технологий, утвержденный Правительством Российской Федерации или уполномоченным Правительством Российской Федерации федеральным органом исполнительной власти (ФОИВ);

– **сквозная технология** – перспективная технология межотраслевого назначения (высокотехнологичная область (направление)), обеспечивающая создание высокотехнологичной продукции и/или разработку и внедрение технологических инноваций, оказывающая существенное влияние на развитие экономики, радикально меняя существующие рынки и/или способствуя формированию новых рынков и включенная в перечень сквозных технологий, утвержденный Правительством Российской Федерации;

– **собственная линия разработки** – комплекс мероприятий (проектов, программ) и условий, обеспечивающих создание и устойчивое развитие под национальным контролем конкретных технологий и продуктов на их основе, включая разработку их новых поколений;

– **технологический суверенитет** – суверенитет Российской Федерации, при котором обеспечено наличие под национальным контролем критических технологий, сквозных технологий и собственных линий разработки технологии, жизненного цикла ключевых технических решений, созданы условия для технологического паритета с

иностранными государствами, а также самостоятельного производства высокотехнологичной продукции с применением указанных технологий, что позволяет государству и обществу создавать научно-технологические заделы и достигать технологического лидерства;

– **технология** – совокупность научно и практически обоснованных производственных и технологических операций и процессов, необходимых для производства одного или нескольких видов высокотехнологичной продукции;

– и ряд других понятий.

Принципами технологической политики обозначены:

1) концентрация ресурсов на приоритетных направлениях технологического развития;

2) приоритетное внимание к потребностям покупателей (заказчиков) высокотехнологичной продукции;

3) поощрение частной инициативы в первоочередном порядке, защита частных интересов;

4) поощрение конкуренции в сфере технологического развития, в том числе в области разработки и внедрения конкурирующих технологий, и предоставление мер государственного стимулирования на основе конкурентных процедур;

5) доступность мер государственного стимулирования на всех стадиях разработки и внедрения технологий и технологических инноваций;

6) признание права на риск.

Далее представлены различные инструменты реализации указанных принципов технологической политики.

Законопроект направлен на:

– создание правовой основы для реализации крупнейших проектов технологического суверенитета – больше 10 млрд руб. инвестиций, которые нацелены на создание конкретной продуктовой линейки;

– реализацию проектов сквозных технологий (к таким технологиям относится, например, искусственный интеллект);

– создание правовой базы развития малых технологических компаний;

– создание реестра малых технологических компаний, который, с одной стороны, будет служить витриной для крупных инвесторов, а с другой стороны – обеспечивать концентрацию мер поддержки.

Обращает на себя внимание положение Законопроекта о том, что научные организации и образовательные организации высшего образования вправе создавать исследовательские консорциумы путем учреждения юридического лица либо на основании гражданско-правового договора без образования юридического лица в целях реализации крупномасштабных научных и (или) научно-технических проектов в рамках определенного приоритетного направления технологического развития.

Далее. Во исполнение Указа Президента Российской Федерации от 30 марта 2022 г. № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» принято **Постановление Правительства Российской Федерации от 14 ноября 2023 г. № 1912 «О порядке перехода субъектов критической информационной инфраструктуры Российской Федерации на преимущественное применение доверенных программно-аппаратных комплексов на принадлежащих им значимых объектах критической информационной инфраструктуры»**.

В этом постановлении установлено, что в Российской Федерации:

– переход субъектов критической информационной инфраструктуры (КИИ) на преимущественное применение доверенных программно-аппаратных комплексов (ПАК) на принадлежащих им значимых объектах КИИ осуществляется до 1 января 2030 г. в соответствии с Правилами, утверждёнными данным постановлением;

– с 1 сентября 2024 г. не допускается использование субъектами КИИ на принадлежащих им значимых объектах КИИ ПАК, приобретённых субъектами КИИ с 1 сентября 2024 г. и не являющихся доверенными ПАК, за исключением случаев отсутствия произведённых доверенных аналогов приобретённых ПАК. Подтверждением отсутствия произведённых доверенных аналогов приобретённых ПАК являются заключения Минпромторга России, выданные в соответствии с Правилами, утверждёнными Постановлением Правительства Российской Федерации от 20 сентября 2017 г. № 1135 «Об отнесении продукции к промышленной продукции, не имеющей произведенных в Российской Федерации аналогов, и внесении изменений в некоторые акты Правительства Российской Федерации».

Определён перечень ФОИВ и государственных корпораций, ответственных за организацию перехода субъектов КИИ на преимущественное применение доверенных ПАК на принадлежащих им значимых объектах КИИ в соответствующих сферах (областях) деятельности (далее – уполномоченных органов), в частности:

Министерство науки и высшего образования Российской Федерации – в сфере науки;

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации – в сфере связи;

Министерство промышленности и торговли Российской Федерации – в области оборонной, горнодобывающей, металлургической и химической промышленности;

Государственная корпорация по атомной энергии «Росатом» – в области атомной энергии;

Государственная корпорация по космической деятельности «Роскосмос» – в области ракетно-космической промышленности;

и другие.

Уполномоченным органам до 1 сентября 2024 г. предписано:

– определить должностное лицо в должности не ниже заместителя руководителя уполномоченного органа, ответственное за организацию перехода субъектов КИИ на преимущественное применение доверенных ПАК на принадлежащих им значимых объектах КИИ в соответствующих сферах (областях) деятельности;

– утвердить планы организации перехода субъектов КИИ на преимущественное применение, доверенных ПАК на принадлежащих им значимых объектах КИИ в соответствующих сферах (областях) деятельности.

Утверждены правила перехода субъектов КИИ на преимущественное применение доверенных ПАК на принадлежащих им значимых объектах КИИ.

При этом использованы следующие понятия:

– **программно-аппаратный комплекс** – радиоэлектронная продукция (РЭП), в том числе телекоммуникационное оборудование (ТКО), программное обеспечение (ПО) и технические средства, работающие совместно для выполнения одной или нескольких сходных задач;

– **доверенный ПАК** – ПАК, который соответствует одновременно всем установленным критериям признания ПАК доверенными ПАК;

– **преимущественное применение доверенных ПАК** – применение субъектами КИИ на принадлежащих им значимых объектах КИИ доверенных ПАК, доля которых по состоянию на 31 декабря 2029 г. составляет 100% в общем количестве ПАК, применяемых субъектами КИИ на принадлежащих им значимых объектах КИИ.

Установлены следующие критерии признания ПАК доверенными ПАК:

1) Сведения о ПАК содержатся в едином реестре российской РЭП.

2) ПО, используемое в составе ПАК, соответствует требованиям, утверждённым Постановлением Правительства Российской Федерации от 22 августа 2022 г. № 1478 «Об утверждении требований к программному обеспечению, в том числе в составе программно-аппаратных комплексов, используемому органами государственной власти, заказчиками, осуществляющими закупки в соответствии с Федеральным законом от 18 июля 2011 г. № 223 «О закупках товаров, работ, услуг отдельными видами юридических лиц» (за исключением организаций с муниципальным участием), на принадлежащих им значимых объектах КИИ, Правил согласования закупок иностранного ПО, …, а также закупок услуг, необходимых для использования этого ПО на таких объектах, и Правил перехода на преимущественное использование российского ПО …»

3) Программно-аппаратный комплекс в случае реализации в нем функции защиты информации соответствует требованиям, установленным ФСТЭК и/или ФСБ России в пределах их полномочий, что должно быть подтверждено соответствующим документом (сертификатом).

Уполномоченным органам предписано разработать и утвердить отраслевые планы перехода субъектов КИИ на преимущественное применение доверенных ПАК – отдельно для каждой сферы (области) деятельности.

Уполномоченные органы, начиная с 2026 г., ежегодно должны обеспечивать актуализацию отраслевых планов перехода, указывая в них оценочные, прогнозные и фактические доли доверенных ПАК в общем количестве ПАК, а также соответствующую отчётность о ходе реализации планов. Подробно описан регламент взаимодействия уполномоченных органов с подведомственными субъектами КИИ.

Установлено, что в целях организации перехода субъектов КИИ на преимущественное применение доверенных ПАК на принадлежащих им значимых объектах КИИ уполномоченными органами могут привлекаться отраслевые центры компетенций, в том числе созданные на базе организаций, подведомственных уполномоченным органам, или иные организации в порядке, предусмотренном законодательством Российской Федерации.

В качестве краткого послесловия к вышеизложенному хотел бы обратить внимание читателей на актуальный материал Кривошеина Б.Н. и Покровского И.А. «Понятия и критерии оценки технологической независимости и безопасности объектов критической информационной инфраструктуры», опубликованный в этом номере нашего журнала. Представлен анализ понятий и терминов, использованных в Указе Президента Российской Федерации от 30.03.2022 г. № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации». Определены различия в понятиях технологического суверенитета и безопасности объектов инфраструктуры, а также различия между критериями оценки доверия программно-аппаратных комплексов и критериями российского происхождения.

Далее. Президент Российской Федерации подписал Указ от 8 ноября 2023 г. № 846 «О внесении изменений в Указ Президента Российской Федерации от 16 августа 2004 г.

№ 1085 «Вопросы Федеральной службы по техническому и экспортному контролю» и в Положение, утверждённое этим Указом». Уточнена предельная штатная численность центрального аппарата ведомства.

Положение о ФСТЭК дополняется рядом новых задач.

Теперь служба будет заниматься, в том числе:

– созданием информационной автоматизированной системы для управления деятельностью по технической защите информации и обеспечению безопасности значимых объектов КИИ и функционирования этой системы;

– ведением (в пределах своей компетенции) централизованного учёта информационных систем и иных объектов КИИ по отраслям экономики, а также мониторинга текущего состояния технической защиты информации и обеспечения безопасности значимых объектов КИИ;

– оперативным информированием органов власти, местного самоуправления и организаций об угрозах безопасности информации и уязвимостях информационных систем и иных объектов КИИ, а также о мерах по технической защите от этих угроз и уязвимостей;

– разработкой процессов управления технической защитой информации и обеспечением безопасности значимых объектов КИИ, учитывающие отраслевую специфику данных объектов (за исключением процессов обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы страны) и организовывать внедрение этих процессов;

– организацией взаимодействия органов власти, местного самоуправления и организаций при реализации ими мер по повышению уровня технической защищённости информации и обеспечения безопасности значимых объектов КИИ;

– организацией и проведением оценки эффективности деятельности госорганов по технической защите информации и обеспечению безопасности значимых объектов КИИ.

Из новостей в интернете обратил на себя внимание материал американской компании BitSight (https://www.bitsight.com/blog/bitsight-identifies-nearly-100000-exposed-industrial-control-systems в изложении Echelon Eyes) о том, что в результате анализа в общедоступной сети было обнаружено около 100 000 промышленных систем управления (ICS), которые подвергались риску несанкционированного доступа. Среди таких систем в составе КИИ – электросети, светофорные системы, системы безопасности и водоснабжения, системы управления зданием и автоматические датчики уровня резервуаров, переключатели, исполнительные механизмы,

Компания BitSight утверждает, что ежедневно обрабатывает около 400 млрд событий безопасности и активно отслеживает более 40 млн организаций по всему миру, используя обширную коллекцию наборов данных за несколько лет.

Наибольшее количество промышленных систем управления в сети обнаружено в США, Канаде, Италии, Великобритании, Франции, Нидерландах, Германии, Испании, Польше, Швеции. Утверждается, что не менее 1500 таких систем находится в России.

Проблема чаще всего встречается в сферах образования, технологий, бизнес-услуг, производства, коммунальных услуг, недвижимости, энергетики, гостиничного бизнеса, финансов, а также в правительственных учреждениях.

Данный материал в очередной раз подтверждает необходимость уделять внимание безопасности не только значимых, но и всех объектов критической гражданской инфраструктуры. Успешная кибератака на такие объекты может вызвать катастрофические последствия, которые затронут большое количество людей – например,

массовые сбои в водоснабжении, отключение электроэнергии и многое другое, в зависимости от отрасли, в которых работают уязвимые системы.

Датская компания по кибербезопасности критического оборудования SektorCERT выпустила отчёт (https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-LEAR.pdf в изложении Echelon Eyes) о серии кибератак, которая в мае 2023 г. обрушилась на критическую инфраструктуру страны. За несколько дней были взломаны 22 компании. Некоторым пришлось перейти в режим изоляции, путём отключения интернета и всех несущественных сетевых соединений. Почти во всех случаях злоумышленники воспользовались неисправленными уязвимостями в межсетевых экранах Zyxel, которые широко используются организациями, защищёнными SektorCERT. К большинству инцидентов привели уязвимости, о которых было объявлено в апреле 2023 г. и которые позволяют удалённым злоумышленникам получить полный контроль над межсетевым экраном без аутентификации.

Многие клиенты SektorCERT не загрузили обновления безопасности даже после того, как их предупредили о необходимости это сделать. Первая волна атак началась 11 мая 2023 г. и была нацелена на 16 энергетических организаций, пытавшихся эксплуатировать CVE-2023-28771 (https://nvd.nist.gov/vuln/detail/CVE-2023-28771), и 11 из них хакерам удалось сразу же взломать. SektorCERT полагает, что это был первоначальный этап атаки – разведка, и, скорее всего, злоумышленникам были отправлены только конфигурации и учётные данные брандмауэра.

Через 10 дней другой злоумышленник также попытался атаковать КИИ Дании, но сумел скомпрометировать только одну организацию. В течение следующих нескольких дней 6 других организаций снова были скомпрометированы через межсетевые экраны Zyxel. Эта волна атак началась 24 мая 2023 г., когда SektorCERT получила предупреждение, указывающее на присутствие в одной из организаций хакеров, предположительно связанных с группировкой Sandstorm.

Несколько слов о новостях стандартизации. Большая творческая работа в рассматриваемый период была проведена в рамках ТК 167 в ходе доработки проектов трех новых предварительных национальных стандартов (ПНСТ) по результатам их общественного обсуждения. Терминология и концепция одного из этих ПНСТ – «Инфраструктура критическая информационная. Доверенные интегральные схемы и электронные модули. Общие положения», разработанного рабочей группой «Доверенные Интегральные схемы» ТК 167, будут представлены в статье руководителя рабочей группы Леонида Н. Кессаринского с соавторами в следующем номере журнала.

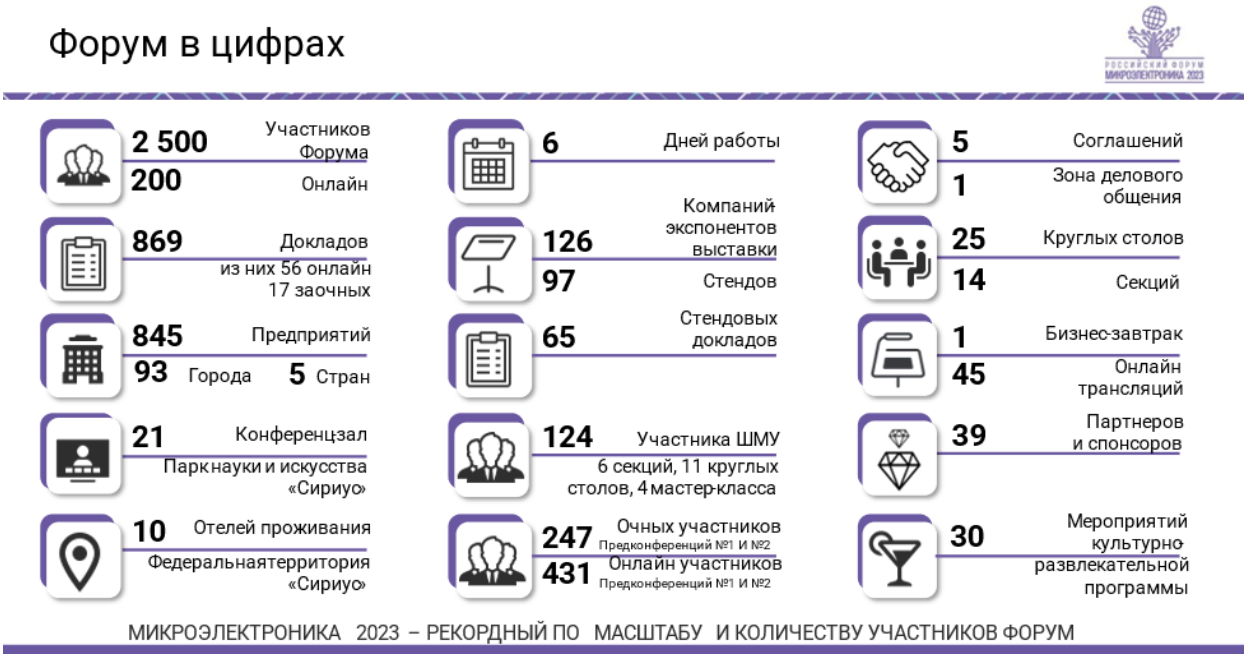
Накануне Всемирного дня стандартизации в г. Сочи с 10 по 13 октября 2023 г., состоялась конференция Госкорпорации Ростех «Содействие развитию систем управления качеством, метрологии и стандартизации организаций промышленности». Своим мнением о проблемах отечественной стандартизации ЭКБ на страницах нашего журнала в материале «Актуальные вопросы стандартизации ЭКБ и несколько ложек приправы в кипящий котел» поделился Роман Г. Левин, генеральный директор РНИИ «Электронстандарт» и руководитель ТК 303.

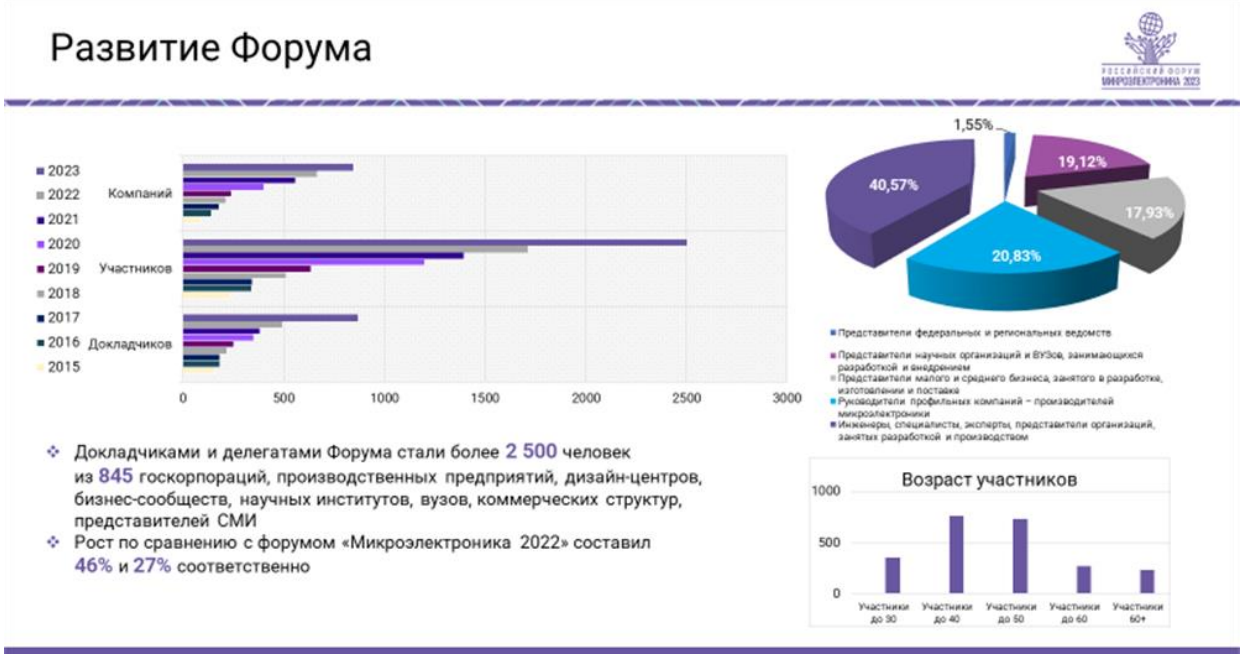
Подробный анализ представленных на конференции докладов выполнен в аналитическом мнении «Под солнцем Сочи в «Зеленой роще» об измерениях, контрафакте и системах менеджмента качества», подготовленном для нашего журнала Еленой Г.

Панарской, экспертом по стандартизации, членом Экспертно-аналитической группы «Доверенные интегральные схемы» ТК 167.

Практически параллельно с конференцией по стандартизации в Парке науки и искусств федеральной территории Сириус состоялся девятый (предъюбилейный) Российский Форум «Микроэлектроника 2023» – главная информационно-коммуникационная площадка радиоэлектронной отрасли и всех отраслей-потребителей электроники. Форум собрал рекордные 2500 участников и на мой взгляд получился фееричным, а наши вопросы доверенной ЭКБ и систем для критичной гражданской инфраструктуры заняли в программе Форума центральное место.

Пленарное заседание Форума «Доверенные электронные системы и ПАК для критической гражданской инфраструктуры» состоялось в первый день работы – 10 октября 2023 г. Выступили Константин А. Смазнов (ГК «Росатом»), Карен Р. Карапетян (Сбер), Артур В. Глейм (ПАО «РЖД»), Дмитрий П. Зегжда (Институт компьютерных наук и кибербезопасности СПбПУ) Иван Г. Анцев (АО «Радар-ММС»), Владимир И. Шевченко (НИЯУ МИФИ), Захар К. Кондрашов (АО «НИИМА «Прогресс»). Также состоялся трек из шести обзорно-дискуссионных заседаний «Доверенные ЭКБ и РЭУ для критической гражданской инфраструктуры». Координатором подготовки и модератором пленарного заседания и трека обзорно-дискуссионных заседаний по доверенности РЭУ и ЭКБ выступил Ваш покорный слуга. Некоторыми статистические данные по итогам Форума с читателями нашего журнала любезно поделилась Юлия В. Морозова – исполнительный директор Агентства деловых коммуникаций «ПрофКонференции» – многолетнего доверенного😊 оператора Форума «Микроэлектроника».





18 – 19 октября в НИЯУ МИФИ проводилась Всероссийская научно-техническая конференция «Кибернетика и информационная безопасность 2023» («КИБ-2023»). В программу конференции было включено 77 докладов, соавторами которых являются 120 ведущих специалистов в этой области от 34 вузов и организаций. Мнением о конференции на страницах журнала поделились ее организаторы Сергей В. Дворянкин, председатель оргкомитета «КИБ-2023» и Игорь М. Ядыкин, ученый секретарь оргкомитета «КИБ-2023».

И, наконец, несколько приятных моментов – поздравления с юбилеями!

От имени редакции, авторов и читателей нашего журнала от души поздравляю Федеральную службу России по экспортному контролю, ее руководителей, специалистов и обеспечивающих сотрудников, с полувековым юбилеем ФСТЭК России! Наше поздравление опубликовано на завершающей странице обложки! Желаем компетентной, эффективной, активной и результативной деятельности на благо процветания и безопасности России!

В декабре 2023 г. отмечаем 60-летие Минского «ИНТЕГРАЛА».

13 декабря 1963 г. был запущен Минский приборостроительный завод имени Ф.Э. Дзержинского, который сразу начал освоение первых диодов. Первые знаменитые электронные часы изготовили в августе 1973 г., а первый образец персонального компьютера ПК-300 – в 1991 г. Орден Ленина увенчал разработку и производство элементной базы для электронных блоков космического комплекса «Буран».

В настоящее время в г. Минске располагается ОАО «ИНТЕГРАЛ» – управляющая компания холдинга «ИНТЕГРАЛ» и здесь же сосредоточены основные производственные площадки и дизайн-центр (НТЦ «Белмикроистемы»), другие заводы холдинга располагаются в городах Брест, Пинск, Гомель и Молодечно. Сегодня предприятия Интеграла выпускают более 3 тысяч типов интегральных микросхем, 500 типов дискретных полупроводниковых приборов, 200 типов жидкокристаллических индикаторов, 150 типов других изделий электронной техники. Более 90% продукции поставляется на экспорт, при этом порядка 80% в Российскую Федерацию.

КОЛОНКА ГЛАВНОГО РЕДАКТОРА

Работу наших белорусских коллег всегда отличали высочайший профессионализм, ответственность и душевность. Кстати, отмечу статью наших белорусских коллег в этом выпуске журнала!

От души поздравляем генерального директора Андрея С. Буйневича, его заместителя по научной работе Анатолия И. Белоуса (члена редколлегии нашего журнала), всех руководителей, специалистов и сотрудников предприятий холдинга с юбилеем и желаем им успехов и процветания!

14 декабря этого года выступаю с докладом «Доверенные интегральные микросхемы: проблемная ситуация, терминология и нормативное регулирование» на юбилейной научной конференции Интеграла «Отечественная микроэлектроника. Современное состояние и направления развития».

15 декабря 2023 г. отмечаем 30-летний юбилей одного из лидеров Российской микроэлектроники – АО «ПКК «Миландр» (г. Зеленоград). С момента основания в 1993 г. бизнес предприятия был направлен на поставки электронных компонентов. Однако новая жизнь Миландра началась в 2003 г. с создания дизайн-центра и первых разработок микросхем с их контрактным производством на зарубежных кремниевых фабриках (они были первыми!) и последующих сборке и тестировании на своей базе. Так были созданы микросхемы памяти СОЗУ 1 Мб, контроллер 1986 ВЕ2 с АРМ М3, 12-ти разрядный АЦП и многое другое – всего более 200 типономиналов микросхем.

Не удивительно, что в современных реалиях именно Миландр подвергся одной из наиболее жестких санкционных атак! Но, нас прессуют – а мы крепчаем! От души поздравляю моих друзей и коллег – основателя и идейного лидера АО ПКК «Миландр» Михаила И. Павлюка, его супругу и верного соратника Светлану, генерального директора Алексея Ю. Новоселова, заместителя генерального директора Сергея С. Шумилина (члена ТК 167, рабочей группы «Доверенные ИС» и автора нашего журнала), всех руководителей, специалистов и сотрудников АО ПКК «Миландр» с юбилеем предприятия! Желаю кораблю Миландра «семь футов под килем», а его команде – максимальных стойкости, прочности, живучести, надежности, долговечности и безотказности! Ваши многочисленные партнеры, соратники, коллеги и друзья, все потребители вашей продукции уверены, что все у вас, а значит и у всех нас, получится и будет отлично!

Этот непростой год заканчивается – а какой из последних лет был для нас простым?

Поздравляю читателей и авторов нашего журнала с наступающим 2024 годом, желаю здоровья, работоспособности, востребованности и оптимизма!
До скорой встречи на страницах журнала БИТ!

Искренне ваш,

Главный редактор Александр Ю. Никифоров
доктор технических наук, профессор
Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, Москва, 115409, Россия

Editor in chief Alexander Yu. Nikiforov
Doctor of Technical Sciences, Professor
National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
Kashirskoe sh., 31, Moscow, 115409, Russia
e–mail: aynik@spels.ru, https://orcid.org/0000-0002-2427-663X