ОТ ГЛАВНОГО РЕДАКТОРА

ОБРАЩЕНИЕ ГЛАВНОГО РЕДАКТОРА К АВТОРАМ И ЧИТАТЕЛЯМ

Editor in Chef Letter to the Authors and Readers

DOI: http://dx.doi.org/10.26583/bit.2022.1.01

Уважаемые коллеги!

Приступив к исполнению обязанностей главного редактора журнала «Безопасность информационных технологий», хочу поделиться с нашими авторами и читателями мыслями и планами по развитию и расширению проблематики издания. Конечно, все привычные для журнала научно-технические и методические вопросы развития системы информационной безопасности, защиты информации и соответствующих технологий, программных и аппаратных средств по-прежнему актуальны и остаются в центре нашего внимания. Вместе с тем, считаю полезным расширить тематику журнала и включить в нее актуальное и перспективное направление развития доверенных систем и радиоэлектронной аппаратуры (РЭА), а также электронной компонентной базы (ЭКБ) для их реализации, включая вопросы задания технических требований, методов и технологий обеспечения и контроля доверенности на всех этапах жизненного цикла изделий – в процессе их разработки, изготовления и эксплуатации в реальных условиях (в том числе при дестабилизирующих воздействиях).

Свойства и понятия доверенности принято относить к информации и средствам ее обработки, но эта категория пока еще не вполне устоялась применительно к доверенным ЭКБ и РЭА, доверенным процессам и технологиям их проектирования (Security by Design) и производства (Security by Process), а также подходам к верификации, тестированию и испытаниям изделий. Важно подчеркнуть, что категорию доверенности ЭКБ и РЭА следует рассматривать в широком смысле относительно всего спектра дестабилизирующих воздействий и угроз как искусственного, так и естественного происхождения. Это далеко выходит за рамки комплектования и обеспечения средств защиты информации (СЗИ), вооружения, военной и специальной техники (ВВСТ), которые составляют относительно небольшой объем от общей потребности в ЭКБ и РЭА, и по сути являются лишь видимой вершиной огромного «электронного айсберга»! Категория доверенности должна охватывать и объективно распространяться практически на всю инфраструктуру и аспекты нашей жизнедеятельности – промышленность, энергетику, торговлю и услуги, навигацию и связь, коммуникацию и транспорт (в т.ч. беспилотный), интернет вещей, коммунальное хозяйство, медицинские и диагностические системы, бытовую технику, системы видеонаблюдения и контроля доступа – перечень практически не ограничен. Даже современные кабели зарядки телефонов и автоматы защиты бытовой электросети в каждой квартире в своем составе содержат электронные компоненты, управляющие их работой и влияющие на доверенность. Таким образом, сегодня все – как традиционные, так и новые сферы нашей жизни – насыщены интеллектуальной электроникой и критически уязвимы для сбоев, отказов и несанкционированного вмешательства.

ЭКБ (РЭА) могут считаться доверенными если они:

– соответствуют требованиям нормативных документов и декларированным свойствам, характеристикам и параметрам в течение заданных сроков, в режимах и условиях эксплуатации у потребителя;

– не имеют недекларированных элементов, возможностей и каналов управления функционированием, считывания и искажения внутренней информации, нарушения работоспособности и других скрытых уязвимостей или каналов утечки информации;

– не имеют признаков контрафактной продукции и недокументированных изменений (коррекций), внесенных в процессе ее разработки и/или производства, и потенциально оказывающих влияние на их способность удовлетворять потребности в соответствии с назначением.

Таким образом, категория доверенности ЭКБ (РЭА) включает в себя совокупность следующих неотъемлемых свойств изделия, которые требуют нормирования и подтверждения:

– качество, как свойство изделия удовлетворять потребности в соответствие с назначением и описанием;

– надежность, как способность сохранять качество в течение всего периода эксплуатации;

– живучесть и стойкость, как способность сохранять качество в реальных условиях эксплуатации;

– верифицированность и тестопригодность (адаптированность для повторной верификации в независимой лаборатории), как гарантированное и документально подтвержденное соответствие декларированным составу и техническим свойствам, параметрам, функциональным и эксплуатационным характеристикам;

– обеспечение безопасности информации, как результат испытаний на отсутствие недекларируемых элементов в составе изделия, скрытых уязвимостей и каналов утечки информации, возможностей несанкционированных внешнего управления, искажения (потери) данных и в целом работоспособности (повреждения) изделия, а также несанкционированного считывания внутренней информации из изделия (в т.ч. по радиоканалу);

– подлинность (аутентичность), как достоверно подтвержденное отсутствие признаков контрафактной продукции;

– отсутствие недокументированных изменений (коррекций), внесенных в процессе ее разработки и/или производства и не верифицированных в установленном порядке (в результате типовых испытаний).

Совокупность перечисленных свойств являются критически необходимой для эффективного использования гражданской ЭКБ в целевых системах, однако в настоящее время она практически не охвачена системой стандартизации и государственного нормативного регулирования.

Отметим, что в стране накоплен значительный положительный опыт создания изделий ЭКБ оборонного назначения, которые по принципам разработки и производства являются заведомо доверенными, что обеспечивается их реализацией в соответствие с комплексом государственных военных стандартов «Климат-8» и общих технических условий на группы однородной продукции, а также специальными проверками. Однако номенклатура оборонной ЭКБ не может являться конкурентоспособной основой для создания широкого спектра гражданской продукции – прежде всего, по многократной избыточности своих технических требований и финансово-экономическим характеристикам. Накопленный опыт обеспечения доверенности при реализации оборонной ЭКБ относится в основном к унифицированным комплектующим изделиям невысокой степени сложности и не ориентирован на аппаратурно-ориентированные системы-на-кристалле и системы-в-корпусе (СнК/СвК) с распределенным циклом создания, что требует значимого переосмысления и радикальной коррекции методов и подходов обеспечения эффективной реализации и конкурентоспособности современных гражданских доверенных изделий.

ОТ ГЛАВНОГО РЕДАКТОРА

Современная доверенная ЭКБ гражданского назначения, создаваемая в рамках реализации Концепции развития электронной отрасли, является перспективной для внутреннего рынка при следующих ее особенностях:

– ЭКБ как правило относится к аппаратурно-ориентированным изделиям (или изделиям частного применения) и предназначена для нужд конкретных групп потребителей (т.е. не является унифицированной);

– значительная часть номенклатуры ЭКБ характеризуется широким разнообразием при относительно невысокой тиражности;

– процесс создания ЭКБ является распределенным: разработка в дизайн-центрах (фаблесс) на основе готовых IP-блоков, изготовление на кремниевых фабриках, верификация, тестирование, испытания и сертификация готовых изделий в испытательных и сертификационных центрах и «тестовых домах»;

– процесс разработки и изготовления, комплектность документов, объем тестирования, сама необходимость испытаний ЭКБ определяются разработчиком/изготовителем/потребителем на основе технико-экономической целесообразности, и практически не регламентированы нормативными документами;

– сертификация ЭКБ проводится в соответствии с отраслевыми добровольными системами качества, как правило, не учитывающими особенности технических требований к электронной продукции;

– конструктивное исполнение ЭКБ в виде СнК/СвК, в том числе в виде 2,5D- и 3D-микромодулей и сборок на чиплетах;

– критически важным свойством гражданской ЭКБ является конкурентоспособность на основе минимизации стоимости и сроков реализации проектов с учетом обеспечения доверенности.

Перечисленные особенности такой гражданской ЭКБ и РЭА на ее основе (не относящейся к СЗИ и ВВСТ) для обеспечения «доверенности» требуют проведения комплекса научно-технических мероприятий и государственного нормативного регулирования на всех этапах жизненного цикла от задания технических требований, разработки, производства, поставки до входного контроля и эксплуатации изделий, особенно, создаваемых в рамках государственных или частно-государственных проектов с привлечением бюджетных средств.

Искренне надеюсь, что наш журнал «Безопасность информационных технологий», станет авторитетной коммуникационно-дискуссионной площадкой для создателей и потребителей доверенной электроники, внесет значимый вклад в развитие и информационное обеспечение этого очень актуального, перспективного и наукоемкого направления, являющегося фундаментом информационно-технологической независимости и безопасности страны, основой для радикального увеличения внутреннего спроса на отечественную электронную продукцию в условиях цифровой трансформации экономики.

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 shosse, 31, Moscow, 115409, Russia
e-mail: aynik@spels.ru, https://orcid.org/0000-0002-2427-663X