Научная статья
УДК 004.052
DOI: 10.26583/bit.2025.2.13

ДОВЕРЕННОСТЬ ИНТЕГРАЛЬНЫХ СХЕМ: ХАРАКТЕРИСТИКИ И ПРИЧИНЫ ИХ НАРУШЕНИЯ

Сергей Г. Мосин[1,2]
[1]*Казанский (Приволжский) федеральный университет, ул. Кремлевская, 18, Казань, 420008, Россия*
[2]*ООО «ЛабСистемс», ул. Федосеева, 5, Владимир, 600000, Россия*
smosin@ieee.org, https://orcid.org/0000-0003-1389-2602

Аннотация. Основные технологии четвертой промышленной революции (Индустрии 4.0) активно внедряют в различные секторы экономики с формированием платформ критической инфраструктуры (КИ). Разработка аппаратного обеспечения объектов КИ требует использования доверенных интегральных схем (ИС). Существенный рост функциональной и структурной сложности современных ИС, а также нарушение цепочек поставок ИС в силу геополитической обстановки и/или недобросовестной конкуренции приводят к проблеме – нарушению доверенности ИС. Систематизация ошибок и причин их появления – основа построения моделей и разработки методов, отвечающих за выбор соответствующих контрмер для обеспечения доверенности ИС на всех этапах жизненного цикла. Объект представленного исследования – интегральные схемы, как основа аппаратного обеспечения критической инфраструктуры. Предмет исследования – ошибки и причины их возникновения на разных этапах стадий проектирования и производства, влияющие на доверенность ИС. Цель предложенной работы – определить возможные причины нарушения доверенности ИС (ДИС), возникающие на этапах проектирования и производства, классифицировать ошибки и степень их влияния на характеристики ДИС. Выполнена декомпозиция характеристик ДИС на ключевые и обеспечивающие. Предложено отображение систематических, случайных и преднамеренных ошибок на характеристики ДИС Определены причины нарушения ключевых характеристик ДИС.

Ключевые слова: *доверенность интегральных схем, устойчивость, надежность, безопасность, защищенность, систематические ошибки, случайные ошибки. преднамеренные ошибки.*

Для цитирования: *Мосин, Сергей Г. Доверенность интегральных схем: характеристики и причины их нарушения. Безопасность информационных технологий, [S.l.], т. 32, № 2, с. 178–191, 2025. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1788. DOI: http://dx.doi.org/10.26583/bit.2025.2.13.*

Scientific article

TRUSTWORTHY OF INTEGRATED CIRCUITS: CHARACTERISTICS AND REASONS FOR THEIR VIOLATION

Sergey G. Mosin[1,2]
[1]*Kazan (Volga region) Federal University, Kremlyovskaya str., 18, Kazan, 420008, Russia*
[2]*LabSystems LLC, Fedoseeva str., 5, Vladimir, 600000, Russia*
smosin@ieee.org, https://orcid.org/0000-0003-1389-2602

Abstract. The main technologies of the fourth industrial revolution (Industry 4.0) are actively implemented in various sectors of the economy with the formation of critical infrastructure (CI) platforms. The development of hardware for CI objects requires the use of trustworthy integrated circuits (IC). A significant increase in the functional and structural complexity of modern IC, as well as the

disruption of IC supply chains due to the geopolitical situation and/or unfair competition lead to a problem – violation of the trustworthiness of the IC. Systematization of faults and the reasons for their occurrence is the basis for development both models and methods responsible for choosing the appropriate countermeasures to ensure the trustworthiness of the IC at all stages of the life cycle. The object of the presented study is integrated circuits as the basis of the CI hardware. The subject of the study is faults and the reasons for their occurrence at different stages of the design and manufacturing phases that affect the trustworthiness of the IC. The scope of the proposed work is to determine the possible causes of violation of the trustworthiness of the IC (TwIC) that occur at the design and production phases, classify faults and the degree of their impact on the characteristics of the TwIC. The decomposition of the TwIC characteristics into key and supporting ones has been performed. A mapping of systematic, random and intentional faults onto the TwIC characteristics has been proposed. The causes of violation of the TwIC key characteristics have been determined.

Keywords: *trustworthy of integrated circuits, resilience, reliability, safety, security, systematic faults, random faults, intentional faults.*

For citation: *Mosin, Sergey G. Trustworthy of integrated circuits: characteristics and reasons for their violation. IT Security (Russia), [S.l.], v. 32, no. 2, p. 178–191, 2025. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1788.*
DOI: http://dx.doi.org/10.26583/bit.2025.2.13.

Введение

Переход к четвертой промышленной революции (Индустрия 4.0) определил активное внедрение в различные отрасли экономики таких современных технологий как Интернет вещей (*IoT – Internet of Things*), анализ больших данных (*Big Data*), искусственный интеллект (*AI – Artificial Intelligence*) и машинное обучение (*ML – Machine Learning*), системы широкополосной связи пятого и последующих поколений (5*G* и *B*5*G* – *Beyond* 5 *Generation*), высокопроизводительные вычисления (*HPC – High-Performance Computing*), системы хранения данных (*Data Centers*) и др., которые выступают основой критической инфраструктуры (КИ). К аппаратным и программным средствам КИ предъявляют высокие требования по надежности и качеству функционирования. Для всестороннего обеспечения совокупности требований введено понятие доверенности и определена совокупность характеристик доверенной системы (табл. 1). В частности, согласно Международной организации по стандартизации (*ISO – International Standard Organization*) *доверенность* – способность объекта удовлетворять ожидания заинтересованных сторон проверяемым способом. Проверяемость включает измеримость и возможность демонстрации посредством объективных доказательств [1].

Особое место в разработке доверенного аппаратного обеспечения занимает проектирование и производство доверенных интегральных схем (ИС). Работы российских и зарубежных авторов демонстрируют результаты проведенных исследований в данной области. Подход к заданию общих требований к доверенной электронной компонентной базе (ЭКБ) представлен в [2]. Защищенность и безопасность доверенных ИС исследованы в [3]. Актуальность и нормативно-правовая база использования доверенной ЭКБ при реализации аппаратных платформ критической информационной инфраструктуры обозначены в [4–6]. Проблемы функциональной безопасности при использовании недоверенной ЭКБ рассмотрены в [7]. Аспекты надежности и оценка доверенности ИС на этапе их корпусирования представлены в [8–10]. Маршрут доверенного проектирования интегральных схем предложен в [11], а отечественная доверенная система автоматизированного проектирования в базисе программируемых логических интегральных схем представлена в [12]. Технологии защиты микросхем от обратного проектирования (*Reverse Engineering*) рассмотрены в [13].

Таблица 1. Характеристики доверенной системы (заслуживающей доверенности)

Название	**Значение**
подотчетность (*accountability*)	свойство, которое гарантирует, что действия объекта могут быть однозначно отождествлены с этим объектом
точность (*accuracy*)	мера близости результатов наблюдений, вычислений или оценок к истинным значениям или значениям, признанным истинными
подлинность (*authenticity*)	свойство объекта быть тем, за кого он себя выдает
доступность (*availability*)	свойство объекта быть доступным и пригодным к использованию по требованию уполномоченного субъекта
управляемость (*controllability*)	свойство системы, позволяющее человеку или внешнему агенту вмешиваться в её функционирование
информационная безопасность (*information security*)	свойство объекта сохранять конфиденциальность, целостность и доступность информации
целостность данных (*data integrity*)	свойство данных, указывающее на то, что они не были изменены несанкционированным образом с момента их создания, передачи или сохранения
целостность системы (*system integrity*)	свойство точности и законченности
конфиденциальность (*privacy*)	свобода от вторжения в частную жизнь или дела личности
качество (*quality*)	степень, в которой характеристики объекта удовлетворяют явные и подразумеваемые требования при использовании в заданных условиях
надежность (*reliability*)	способность объекта выполнять заданные функции без отказов в течение заданного интервала времени при определённых условиях
устойчивость (*resilience*)	способность системы сохранять функции и структуру при внутренних и внешних изменениях, а при необходимости – плавно деградировать
живучесть (*robustness*)	способность системы поддерживать свой уровень производительности при различных обстоятельствах
безопасность (*safety*)	свойство системы при определенных условиях не приводить к состоянию, в котором человеческая жизнь, здоровье, имущество или окружающая среда подвергаются опасности
защищенность (*security*)	устойчивость к преднамеренным несанкционированным действиям, направленным на причинение вреда или ущерба системе
прозрачность (*transparency*)	свойство системы или процесса подразумевать открытость и подотчетность
удобство использования (*usability*)	степень, в которой система может использоваться указанными пользователями для достижения заданных целей с эффективностью, результативностью и удовлетворением в указанном контексте применения

Важно отметить, что жизненный цикл ИС включает множество этапов в рамках стадий проектирования, производства и использования, на каждом из которых существует множество факторов и причин, потенциально влияющих на характеристики доверенности ИС и приводящих к их нарушению. Цель предложенной работы – определить возможные причины нарушения доверенности ИС, возникающие на этапах проектирования и производства, классифицировать ошибки и степень их влияния на характеристики доверенности ИС. Систематизация ошибок и причин их появления – основа построения моделей и разработки методов, отвечающих за выбор соответствующих контрмер для обеспечения доверенности ИС на всех этапах жизненного цикла.

1. Доверенность интегральных схем

При рассмотрении интегральных схем (ИС) в качестве объектов доверенности важно определить соответствующие характеристики и обозначить причины, которые могут приводить к их нарушению. В общем случае можно выделить три класса причин с точки зрения природы их появления и степени влияния на нарушение характеристик доверенной ИС – систематические, случайные и преднамеренные ошибки.

Ошибки могут приводить к нарушению корректного функционирования ИС, т.е. потере ее способности обеспечивать заданный функционал должным образом. Для снижения сложности анализа влияния ошибок на доверенность ИС предложено выделить ключевые (отмечены серым) и обеспечивающие характеристики доверенности (рис. 1).

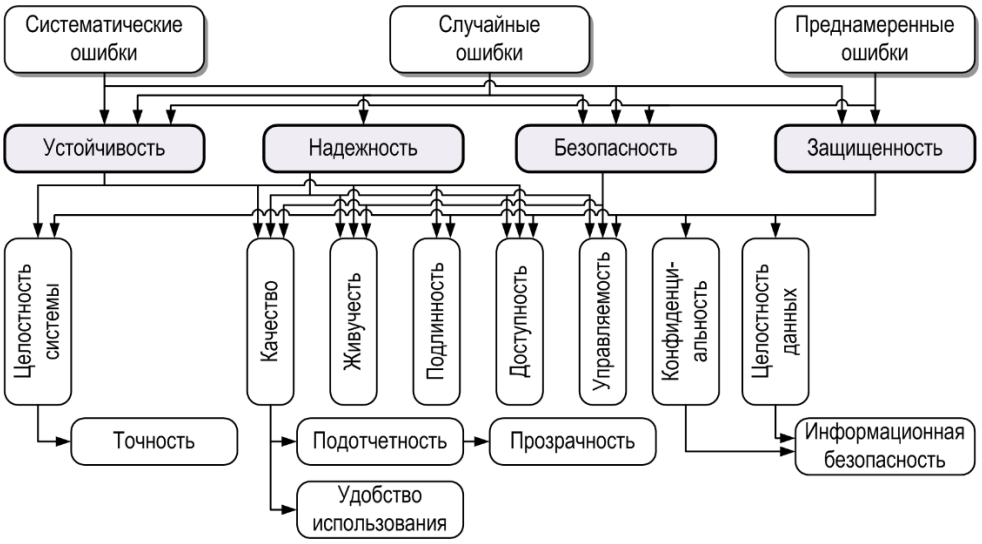


Рис. 1. Отображение ошибок на характеристики доверенности ИС

Систематические ошибки связывают с отклонением от утвержденных и принятых в профессиональном сообществе правил и маршрутов проектирования, что приводит к возникновению в проекте системных несоответствий еще на ранних стадиях разработки. Систематические ошибки носят детерминированный характер и могут влиять на устойчивость через нарушение корректной работы ИС, снижению ее безопасности и защищенности.

Случайные ошибки связывают с возникновением дефектов и неисправностей в структуре и компонентах ИС, которые могут быть спровоцированы многими факторами технологического процесса производства полупроводниковых структур, внутренними электрохимическими процессами и внешними воздействиями, например радиацией, электромагнитными полями, колебаниями температуры, нестабильностью источников электропитания и др. Случайные ошибки обладают стохастической природой и могут влиять на нарушение корректной работы ИС и снижение ее надежности.

Преднамеренные ошибки – результат злонамеренного формирования вредоносных условий появления уязвимостей и осуществления атак, которые приводят к потере защищенности ИС и использующих их электронных систем. Различают два режима воздействия преднамеренных ошибок на ИС – активный, при котором нарушается нормальная работа устройства, и пассивный, при котором сохраняется работоспособность устройства, а ошибка обеспечивает отложенных эффект.

Возникновение систематических и случайных ошибок преимущественно влияет на безопасность ИС, а преднамеренных ошибок – на защищенность.

2. Варианты ошибок и причины их возникновения

Нарушение цепочек поставок ИС в силу влияния глобальной пандемии [14] и санкционных ограничений [15] на фоне возрастающего спроса спровоцировало производителей микроэлектронных систем обращаться к поставщикам и дистрибьютерам второго уровня за требуемой элементной базой. Это в свою очередь активизировало незаконную деятельность по наполнению рынка мошенническими, поддельными и контрафактными ИС. Данное обстоятельство требует от легальных производителей микроэлектронных систем использовать доверенные ИС особенно для приложений критической инфраструктуры, оценивать и обеспечивать надежность каждого этапа разработки ИС.

Укрупненная модель жизненного цикла ИС представлена на рис. 2. В этой модели отображена последовательность этапов без указания локальных и/или глобальных итерационных процессов, что обеспечивает достаточную адекватность анализа ошибок и причин их возникновения на стадиях проектирования и производства. На каждом этапе имеет место совокупность причин, нарушающих доверенность ИС. Рассмотрим варианты ошибок и их влияние на ключевые характеристики доверенности ИС (табл. 2) только для этапов стадий проектирования и производства (номера выделены серым цветом), т.е. до получения ИС как продукта, реализуемого потребителям.

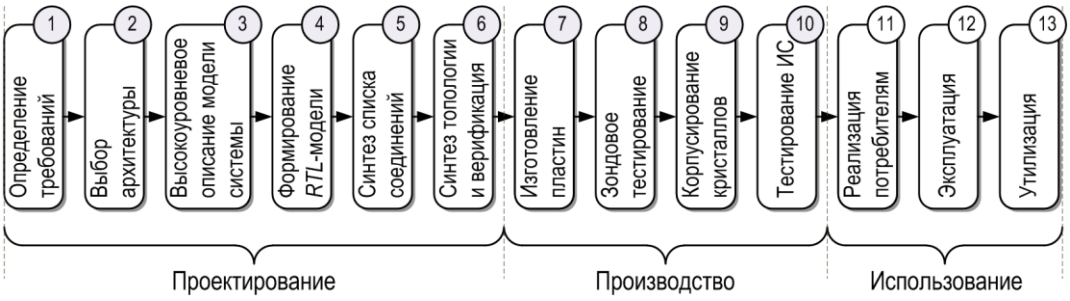


Рис. 2. Этапы жизненного цикла ИС

2.1 Недостатки спецификации

Разработка спецификации на ИС – начальный процесс, обеспечивающий формирование основных требований и ограничений на разрабатываемое устройство с учетом множества внутренних, внешних, входных и выходных параметров. Спецификация основной схемы отражает требования по обеспечению ожидаемой производительности при потребляемой мощности и занимаемой площади кристалла в заданных границах (*PPA – Performance, Power, Area*).

В этом случае цель проектирования представлена оптимизационной задачей вида

$$V_{opt} = V_{i,j,k} = \arg\max_{i} \min_{j,k} \left(F\left(Per_i, Pow_j, Area_k, \mathbf{P}\right)\right) \quad (1)$$

s.t.

$$Per_i \in \mathbf{Per};\ Pow_j \in \mathbf{Pow};\ Area_k \in \mathbf{Area};\ i,j,k \in \mathbb{N},$$

где V_{opt} – оптимальное решение; $\mathbf{Per}$ – множество значений выходных параметров (производительность); $\mathbf{Pow}$ – множество значений мощности, потребляемой ИС; $\mathbf{Area}$ – множество значений занимаемой ИС площади на кристалле; $\mathbf{P}$ – множество значений внутренних, внешних и входных параметров.

Решение задачи (1) для современных приложений требует меньшей занимаемой площади кристалла и меньшего энергопотребления, обеспечивая более высокую производительность схемы. При этом сама оптимизация может влиять на выбор

интегральной технологии, библиотек стандартных ячеек и/или *IP*-ядер, шин и/или межсоединений, элементов памяти и др. Некорректность или неточность такого выбора может иметь отложенный эффект и повлиять на устойчивость произведенного кристалла ИС. Неправильные предположения, указанные в спецификации, о требуемой мощности, производительности и площади могут привести к неадекватной или неисправной функциональности ИС, например, из-за нарушений синхронизации в критических путях, которые проявляются на более поздних этапах физической реализации.

Таблица 2 Причины нарушения ключевых характеристик доверенности ИС

Причина	**№ этапа появления**	**Характеристика**
Систематические		
Недостатки спецификации: – PPA; – концепции тестирования; – концепции безопасности; – концепции защищенности	 1, 2 1, 2 1–3 1, 2	 устойчивость надежность безопасность защищенность
Недостатки архитектуры: – обеспечение *PPA*; – обеспечение тестирования и диагностики неисправностей; – обеспечение безопасности; – обеспечение защищенности	 2, 3 2, 3 2, 3 2, 3	 устойчивость надежность безопасность защищенность
Некачественные *IP*: – контрафакт / непроверенные; – *DFT* несовместимые; – без подтвержденной безопасности; – аппаратные закладки (трояны) и уязвимости	 2–6 2–6 2–6 2–6	 устойчивость надежность безопасность защищенность
Недостоверные средства *CAD*/*CAM*/*CAE*	3–6	устойчивость, надежность
Некачественные *PDK*	5, 6	устойчивость, надежность
Некорректная реализация: – базовой схемы; – тестирующих подсхем; – подсхем контроля безопасности; – подсхем обеспечения защищенности	 3–6 4–6 4–6 4–6	 устойчивость надежность безопасность защищенность
Случайные		
Возникновение дефектов	7–12	устойчивость / надежность / безопасность /
Преднамеренные		
Извлечение конфиденциальной информации	7–10	защищенность
Реверс-инжиниринг	7–10	защищенность
Анализ кристалла на возможные уязвимости	7–9	защищенность
Вмешательство в топологию кристалла: – изменение логики (реконфигурирование); – внедрение дефекта(ов); – внедрение вредоносного кода; – внедрение/подмена части кристалла внутри корпуса	 7–9 7–9 7–10 7, 9	 устойчивость / надежность / безопасность / защищенность

Отсутствие или недостаточная проработка в спецификации концепций тестирования, безопасности и защищенности влияет на точность оценки достаточности и качества предлагаемых решений, которые в свою очередь влияют на выбор и последующую реализацию подсхем тестирования, обеспечения безопасности и защищенности основной схемы, требующих дополнительную площадь кристалла и повышающих потребление мощности, что, в большинстве случаев, негативно сказывается на производительности реализуемой ИС [16]. Причина обозначенной проблемы является внутренней для компании-разработчика ИС и связана с человеческим фактором – невнимательностью и/или недостаточной квалификацией менеджеров проекта и инженеров по требованиям.

2.2 Недостатки архитектуры

Синтез архитектуры осуществляют на основе требований спецификации с применением различных технологий, например система-на-кристалле (*SoC – System-on-Chip*), сеть-на-кристалле (*NoC – Network-on-Chip*), многокристальный модуль (*MCM – Multi-Chip Module*), многокристальная компоновка (*MCP – Multi-Chip Package*), система в корпусе (*System-in-Package*) и др. Современные технологии проектирования и реализации ИС ориентированы на активное использование *IP*-ядер, предварительно разработанных самостоятельно или приобретенных у сторонних компаний-разработчиков. Важно отметить, что такие компании занимают существенную долю глобального рынка микроэлектроники. Ошибки, допущенные и не выявленные на данном этапе, будут иметь крайне негативное значение как в общем аспекте доверенности реализуемой ИС, так и в финансовых потерях проекта, в частности, согласно «правилу десяти». Синтез архитектуры должен носить системных характер и охватывать как обеспечение требований *PPA*, так и обеспечение требуемого уровня тестирования и диагностики неисправностей, безопасности и защищенности разрабатываемой ИС, в том числе за счет использования соответствующих специализированных *IP*-ядер.

Анализ архитектуры позволяет рассматривать и осуществлять выбор оптимального варианта из множества синтезированных архитектур, обнаруживать несоответствие спецификации, структурные и/или функциональные недостатки. Архитектурное исследование важно выполнять также на последующих этапах виртуального прототипирования ИС с целью выявления потенциальных проблем и их скорейшего устранения – до выхода на производство.

2.3 Некачественные *IP*-ядра

Парадигма повторного использования предварительно разработанных компонентов системы и оформленных в виде библиотечных элементов, например *IP*-ядер, – *design reuse* или *IP-reuse* – позволяет существенно сократить время проектирования сложных систем без потери качества в условиях применения доверенных *IP*. В зависимости от этапа проектирования *IP*-ядра представляют на различных уровнях абстракции с различным уровнем защищенности – в виде поведенческих аппаратно-ориентированных *HDL*-описаний (*HDL – Hardware Description Language*) или описаний на уровне регистровых передач (*RTL – Register Transfer Level*), которые представлены мягкими ядрами (*soft IP-core*), на вентильном уровне в виде списка соединений – твердые ядра (*firm IP-core*), на физическом уровне описание топологии или ее части в виде *GDSII*- (*Graphic Database System*) или *CIF*-файла (*Crystallographic Information File*) – жесткие ядра (*hard IP-core*). Наряду с защищаемыми и лицензируемыми *IP*-ядрами на рынке представлены библиотеки элементов с открытым исходным кодом. Надежность *IP*-ядер – принципиально важная характеристика при их использовании и включении в свои проекты.

В случае приобретения *IP*-ядер у сторонних компаний-разработчиков или поставщиков возникают внешние угрозы, связанные с подделкой, нарушением функциональности или недокументированными возможностями библиотечных элементов. Поддельные *IP*-ядра – результат пиратской деятельности злонамеренных субъектов в цепочке поставок как *IP*, так и *ИС*, когда клонируют их описание и/или конструкцию. Включение поддельных *IP*-ядер в проект прямо или косвенно влияет на доверенность разрабатываемой ИС, поскольку поддельные *IP* могут обладать систематическими и случайными ошибками, а также включать вредоносные модификации, отключающие или нарушающие работу подсхем тестирования и контроля безопасности, содержать уязвимости и аппаратные закладки, что может привести к скомпрометированной устойчивости, нарушению надежности и защищенности.

Тенденция последних лет – включение компаниями-разработчиками *IP*-ядер механизмов защиты своих авторских прав, которые делают невозможным для пользователя доступ к фактическому описанию компонента, превращая его в «черный ящик». Одним из вариантов такой защиты выступает принятый стандарт *IEEE* 1735-2023 [17], который обеспечивает унифицированную схему шифрования и дешифрования используемых описаний *IP*-блоков, которая разрешает синтез и функциональную верификацию проекта средствами авторизованных средств САПР без отображения описания компонентов, используемых в виде «черных ящиков». В этом случае невозможно использовать методы комплексной проверки доверенности таких *IP*-ядер, а следовательно, при злонамеренных действиях вероятно включение уязвимостей, аппаратных троянов, недокументированных возможностей, которые влияют не только на защищенность, но и устойчивость, надежность и безопасность проектируемой ИС.

Негативные воздействия от использования поддельных *IP*-ядер, а также *IP*-ядер с сомнительным качеством и потенциальными функциональными недостатками возможно устранить исключительно через перепроектирование ИС и физического исключения вредоносного элемента из проекта.

2.4 Недостоверные средства *CAD*/*CAM*/*CAE*

Средства автоматизации сквозного проектирования ИС – сложные наукоемкие продукты, которые требуют привлечения высококвалифицированных специалистов и существенных затрат времени и финансовых средств на разработку, внедрение, развитие и сопровождение, что непосредственно сказывается на высокой стоимости конечной лицензии [12, 18]. В этих реалиях основной прямой вариант злонамеренных действий со стороны разработчиков САПР микроэлектроники видится в ограничении возможностей или отказе в доступе к своим средствам проектирования ИС по собственной инициативе или в силу санкционной государственной политики, например [15].

Последствия подобных ограничений приводят к использованию при проектировании ИС нелицензионных и/или недостаточно функциональных САПР, которые могут нарушить целостность маршрута проектирования со всем комплексом верификации промежуточных решений, негативно сказаться на устойчивости и надежности ИС через систематические ошибки, а также не позволить обнаружить влияние преднамеренных ошибок, что сказывается на безопасности и защищенности таких ИС.

2.5 Некачественные *PDK*

Комплект для проектирования технологического процесса (*PDK – Process Design Kit*) представляет собой набор файлов, правил, требований и документации, предоставляемых производителем полупроводников, который позволяет проектировать и проверять корректность топологии ИС для конкретного производственного процесса. Типовой *PDK* содержит технологические файлы, библиотеки стандартных и параметрических ячеек, файлы правил проектирования и проверки – *DRC* (*Design Rule*

Checking), *LVS* (*Layout Versus Schematic*), *ERC* (*Electrical Rule Checking*), экстракции паразитных параметров (*xRC*), *ESD* (*Electrostatic Discharge*) и др.

Использование неполного или поврежденного *PDK* приводит к нарушениям в топологии ИС на этапе проектирования и проявляется в нарушении ее устойчивости и надежности на стадии производства.

2.6 Некорректная реализация

Данная проблема является внутренней для компании, проектирующей ИС, и зачастую связана с человеческим фактором – невнимательность сотрудников, их недостаточная квалификация, отсутствие перекрестных и/или многоступенчатых проверок и др. Варианты злонамеренного допущения ошибок при проектировании не будем рассматривать, но и исключать их не стоит.

Ошибки проектирования могут привести к полному или частичному нарушению функциональности основной схемы, что будет влиять на устойчивость ИС, если допущенные ошибки не устранить до стадии производства. Неправильная реализация или отсутствие тестирующей подсхемы также будут влиять на устойчивость ИС особенно в условиях ее эксплуатации, когда схемы встроенного самотестирования (*BIST – Built-In Self-Test*) не смогут обнаруживать неисправности и дефекты, связанные со старением полупроводниковых структур [19]. Кроме того, ошибки тестопригодного проектирования не позволят обнаруживать неисправности и дефекты на этапах производства ИС, что влияет на ее надежность, а также на оценку количества годных производственной линии и гарантированное качество партии ИС (*QA – Quality Assurance*). При этом избыточная тестопригодность, выраженная максимальными управляемостью и наблюдаемостью, может стать причиной нарушения защищенности, за счет получения доступа через тестовые шины и сканирующие пути к внутренней, в т.ч. конфиденциальной информации ИС, и безопасности, при злонамеренном реконфигурировании или переводе ИС в выделенный (*offline*) режим тестирования с нарушением *online*-функционирования. К настоящему времени разработаны многочисленные стандарты сканирующих путей и тестовых шин для различных типов ИС, которые активно используют на практике: архитектура граничного сканирования цифровых ИС [20], метод тестопригодности встраиваемых систем-на-кристалле [21], граничное сканирование современных цифровых сетей (дифференциальных цепей) [22], смешанная тестовая шина [23], тестовый доступ для трехмерных интегральных схем (3*DIC*) [24]. Ошибки реализации подсхем обеспечения безопасности и защищенности негативно сказываются на соответствующих характеристиках доверенности ИС.

Влияние ошибок проектирования на ИС носит постоянный характер. Исключить их проявления возможно только при перепроектировании устройства.

2.7 Возникновение дефектов

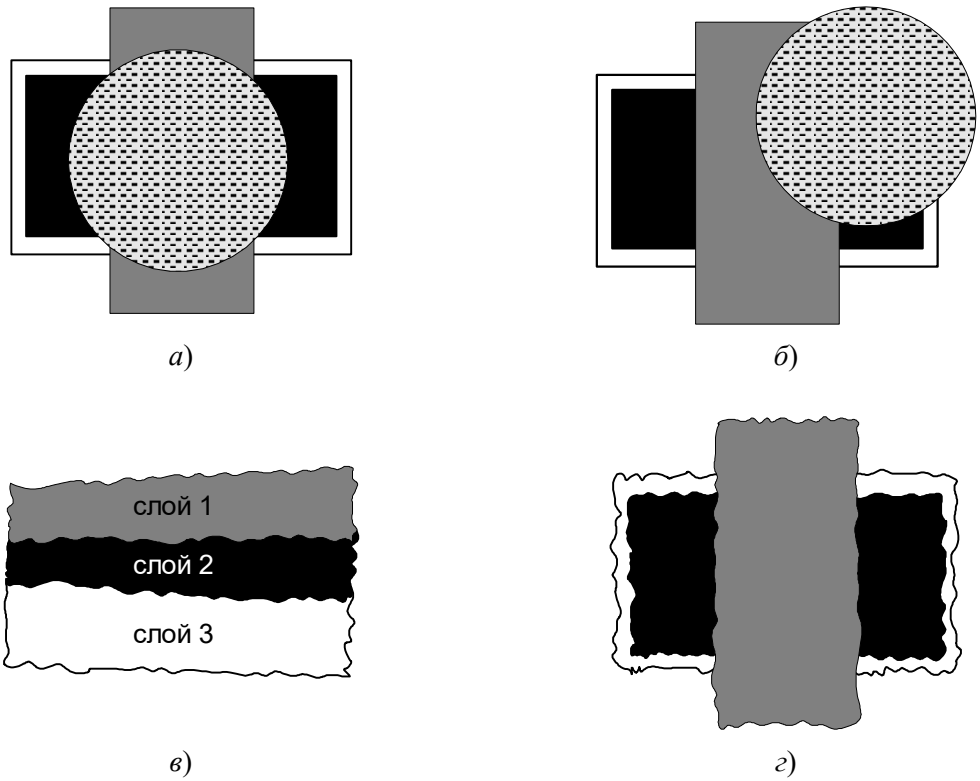
Нарушение работы ИС в первую очередь связывают с возникновением физических дефектов, которые могут проявиться на уровне кристалла в одном или нескольких слоях топологии. Появление дефектов в ИС вызвано возникновением или исчезновением участка материала в топологии кристалла, что существенным образом изменяет его электрические свойства. Подобные эффекты, как правило, обусловлены нарушениями технологических процессов производства ИС или старением материалов.

Причинами физических дефектов могут служить случайные флуктуации внешних условий производства, например турбулентный характер подачи газов при выполнении операций диффузии и окисления; неточности в управлении; отклонения в физических и химических параметрах используемых материалов, например плотности и вязкости фоторезиста, загрязнение воды и газа; человеческий фактор.

Дефекты, возникающие в процессе производства ИС – производственные дефекты – можно разделить на две группы (рис. 4) [25]. К первой относят дефекты

конструкционных материалов, вызванные, например, оседанием микрочастиц пыли или появлением окисла на поверхности кремниевой пластины во время процесса ее обработки. Дефекты конструкционных материалов могут быть двух видов – катастрофические и параметрические. Катастрофические дефекты являются причиной возникновения короткого замыкания или разрыва цепи, что приводит к полному нарушению работы электронных компонентов (рис. 5).

Рис. 4. Классификация производственных дефектов ИС



а) *б*)

в) *г*)

Рис. 5. Виды производственных дефектов: а) катастрофический; б) параметрический; в) глобальный; г) локальный

2.8 Извлечение конфиденциальной информации

На этапах производства ИС появляются возможности злонамеренного доступа к внутренним ресурсам кристалла для извлечения конфиденциальной информации из ПЗУ, например симметричных или закрытых ключей. При изготовлении пластины информацию можно получить как из фотошаблонов, так и, собственно, из топологии кристалла. На остальных производственных этапах – только из топологии с использованием методов неразрушающего контроля, например атомно-силового зондового сканирования.

2.9 Реверс-инжиниринг

Комплексный анализ топологии проприетарного кристалла ИС в процессе ее производства открывает путь для сбора информации о внутренней структуре, основных элементах и соединениях между ними, а также функциональных возможностях и др., которая может быть использована для несанкционированного воспроизведения, тиражирования и подмены на рынке оригинального изделия. При этом в ходе реверс-инжиниринга возможно нарушение устойчивости, надежности и безопасности клонированной ИС, а также внедрение в нее вредоносных подсхем, влияющих на защищенность. Для потребителей такие ИС неотличимы без специализированной проверки от оригинальных устройств, но выступают источником множества рисков, опасности и уязвимости конечной продукции, где они используются.

2.10 Анализ кристалла на уязвимости

На ранних производственных этапах кристалл ИС является открытым, т.е. в нем не активированы защитные механизмы (*SE – Security Engine*). Доступ к логике и системам «открытого» кристалла не представляет прямой угрозы защищенности. Однако, злонамеренный анализ такого кристалла позволяет понять принцип функционирования *SE* и обнаружить уязвимости, которые в дальнейшем могут быть использованы для несанкционированного манипулирования ИС для снижения или обхода ее защищенности.

2.11 Вмешательство в топологию кристалла

Одна из вероятных угроз в ходе производственных этапов – злонамеренная модификация топологии кристалла ИС, которая может приводить к изменению логики устройства с отклонением функциональности относительно используемой спецификации или с включением дополнительных недокументированных возможностей, открывающих путь к преднамеренным вредоносным воздействиям. Такое реконфигурирование может приводить к нарушению как устойчивости ИС, так и ее надежности в силу провоцирования внутренних дефектов в структуре кристалла. Модификация может затрагивать микропрограммное обеспечение в ПЗУ ИС, что чревато внедрением аппаратных закладок и непосредственным влиянием на нарушение безопасности такой ИС. На этапе производства пластины открываются специфические угрозы по подмене части кристалла реализуемой ИС через злонамеренную модификацию фотошаблонов, но стоит отметить крайне низкую вероятность такой угрозы в силу исключительно высоких затрат на исполнение и потенциально легкое обнаружение изменений на этапах контроля и тестирования. В свою очередь угроза внедрения дополнительных вредоносных кристаллов на этапе корпусирования многокристальных ИС (рис. 6) обладает высокой вероятностью и может приводить к случайным и преднамеренным ошибкам.

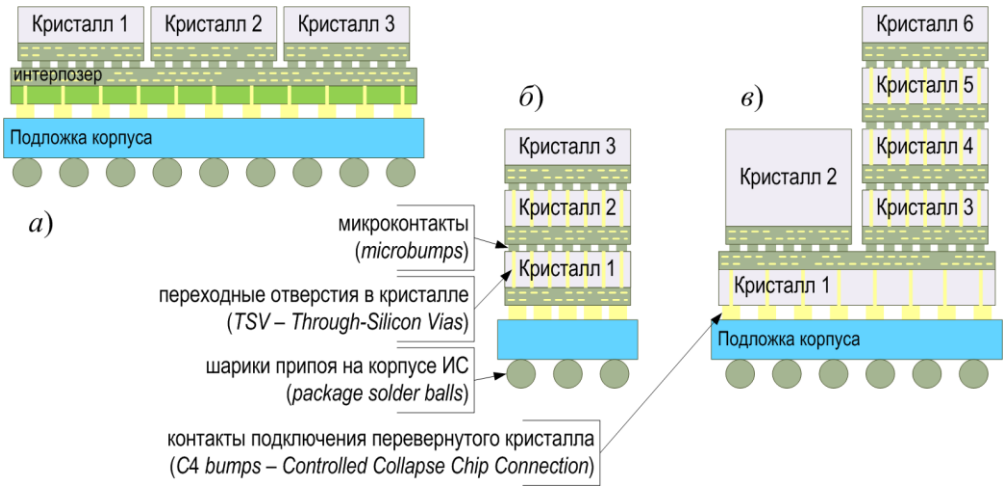


Рис. 6. Виды многокристальных ИС: а) 2.5D; б) 3D; в) 5.5D

Заключение

В данной работе проведен анализ жизненного цикла ИС с целью определения возможных причин нарушения ДИС. Особое внимание уделено этапам проектирования и производства, на выходе которых получаем ИС как продукт для дальнейшего использования, в том числе при реализации аппаратного обеспечения платформ критической инфраструктуры. Представлена классификация ошибок с точки зрения природы их возникновения и степени влияния на характеристики ДИС. Предложено отображение систематических, случайных и преднамеренных ошибок на характеристики ДИС Определены и описаны потенциальные причины нарушения ключевых характеристик ДИС. Полученные результаты выступают основой для построения моделей и методов выбора контрмер, обеспечивающих ДИС в условиях возникновения потенциальных ошибок на различных этапах жизненного цикла интегральных схем.

СПИСОК ЛИТЕРАТУРЫ:

1. ISO/IEC TS 5723:2022, Trustworthiness – Vocabulary. International Organization for Standardization and International Electrotechnical Commission. URL: https://www.iso.org/obp/ui/en/#iso:std:iso-iec:ts:5723:ed-1:v1:en (дата обращение: 07.05.2025).
2. Кессаринский Л.Н., Никифоров А.Ю. Подход к заданию общих требований к доверенной электронной компонентной базе для регулируемого рынка критической информационной инфраструктуры в вопросах и ответах. Безопасность информационных технологий. 2025, т. 32, № 1, с. 8–16. URL: https://bit.spels.ru/index.php/bit/article/view/1761/1457 (дата обращение: 07.05.2025).
3. Rama E. et al. Trustworthy Integrated Circuits: From Safety to Security and Beyond. IEEE Access, v. 12, 2024, p. 69603–69632. DOI: 10.1109/ACCESS.2024.3400685.
4. Кессаринский Л.Н. Доверенная электроника на форуме «Микроэлектроника 2024». Вопросы кибербезопасности. 2024, № 5(63), с. 115–119. DOI: 10.21681/2311-3456-2024-5-115-119.
5. ПНСТ 911-2024 Критическая информационная инфраструктура. Доверенные интегральные микросхемы и электронные модули. Общие положения. URL: https://normadocs.ru/pnst_911-2024 (дата обращения: 07.05.2025).
6. Белоус А., Солодуха В. Доверенная ЭКБ для доверенных аппаратно-программных платформ: проблемы и пути решения. Часть 2. Электроника: НТБ. 2021, № 4, с. 72–77. DOI: 10.22184/1992-4178.2021.205.4.72.76. – EDN: BKANKK.
7. Смирнов, Дмитрий О. Функциональная безопасность и недоверенная электронная компонентная база. Безопасность информационных технологий, [S.l.], т. 29, № 2, с. 128–143, 2022. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2022.2.10.
8. Lu R., Chuang Y.-C., Wu J.-L., and He J. Reliability challenges from 2.5D to 3DIC in advanced package development. IEEE International Reliability Physics Symposium (IRPS), p. 1–4, 2023. DOI: 10.1109/IRPS48203.2023.10117647.
9. Chen M. -F., Chen F. -C., Chiou W. -C. and Yu D. C. H. System on Integrated Chips (SoIC™) for 3D Heterogeneous Integration, in Proc. IEEE 69th Electronic Components and Technology Conference (ECTC), Las Vegas, NV, USA, 2019, p. 594–599. DOI: 10.1109/ECTC.2019.00095.
10. Итальянцев А. Новые проблемы перспективных методик корпусирования. Зарубежная электронная техника. 2018, вып. 7(6656), с. 6–9. URL: https://www.niime.ru/upload/iblock/a02/a02ff7ec20742fcee50d67ca1d7825e8.pdf (дата обращения: 07.05.2025).
11. Певцов, Е.Ф, Деменкова, Т.А. Доверенное проектирование интегральных схем. Наноиндустрия. 2021, т. 14, № S7(107), с. 856–859. DOI: 10.22184/1993-8578.2021.14.7s.856.859. – EDN: QVAIUI.
12. Гаврилов С.В., Железников Д.А., Заплетина М.А., Тиунов И.В., Хватов В.М., Чочаев Р.Ж., Шокарев Д.Б. Разработка доверенных средств проектирования ИС в базисе гетерогенных ПЛИС. Труды ИСП РАН. 2023, т. 35, вып. 5, с. 107–126. DOI: 10.15514/ISPRAS–2023–35(5)–8.
13. Федорец В.Н., Белов Е.Н., Балыбин С.В. Технологии защиты микросхем от обратного проектирования в контексте информационной безопасности: научно-популярное издание. Техносфера. Мир электроники, 2019. – 216 с. – EDN: LJHRGC.
14. Mosin S., Kislyakov M. An In-Pandemic View on the Global Trends in Microelectronic Design and Market. Proc. IEEE East-West Design & Test Symposium (EWDTS). Batumi, Georgia, 2021, p. 273–276. DOI: 10.1109/EWDTS.2018.8524618.

15. Amberg P., Turrado L., Sancho G., McGrath R. and Mann S. EU Issues 12th Sanctions Package Targeting Russia. Baker McKenzie. URL: https://sanctionsnews.bakermckenzie.com/eu-issues-12th-sanctions-package-targeting-russia/ (дата обращения: 30.04.2025).
16. Mosin S. A Model for Univariant and Multivariant Simulating the Battery Lifetime of UE NB-IoT. In Proc. International Russian Automation Conference (RusAutoCon). Sochi, Russian Federation. 2024, p. 13–18, paper ID 10694326. DOI: 10.1109/RusAutoCon61949.2024.
17. IEEE Recommended Practice for Encryption and Management of Electronic Design Intellectual Property (IP). IEEE Std 1735-2023, 6 Nov. 2023, p. 1–237. URL: https://ieeexplore.ieee.org/document/10505231 (дата обращения: 30.04.2025).
18. Bykov S.O., Mosin S.G. An automated technique for design of custom network-on-chip topologies. Proc. of IEEE East-West Design and Test Symposium (EWDTS'2015). Batumi, Georgia, 2015, p. 192–194. DOI: 10.1109/EWDTS.2015.7493139.
19. Mosin S.G. Design-for-testability automation of mixed-signal integrated circuits. In Proc IEEE 26th International SOC Conference (SOCC 2013). Erlangen, Germany, 2013, p. 244–249. DOI: 10.1109/SOCC.2013.6749695.
20. IEEE Standard for Test Access Port and Boundary-Scan Architecture. IEEE Std 1149.1-2013 (Revision of IEEE Std 1149.1-2001), p. 1–444, 13 May 2013. DOI: 10.1109/IEEESTD.2013.6515989.
21. IEEE Standard Testability Method for Embedded Core-based Integrated Circuits – Redline. IEEE Std 1500-2022 (Revision of IEEE Std 1500-2005) – Redline, p. 1–168, 12 Oct. 2022. DOI: 10.1109/IEEESTD.2022.9916221.
22. IEEE Standard for Boundary-Scan Testing of Advanced Digital Networks. IEEE Std 1149.6-2015 (Revision of IEEE Std 1149.6-2003), p. 1–230, 18 March 2016. DOI: 10.1109/IEEESTD.2016.7436703.
23. IEEE Standard for a Mixed-Signal Test Bus. IEEE Std 1149.4-2024 (Revision of IEEE Std 1149.4-2010), p. 1–116, 6 Dec. 2024. DOI: 10.1109/IEEESTD.2024.10776765.
24. IEEE Standard for Test Access Architecture for Three-Dimensional Stacked Integrated Circuits. IEEE Std 1838-2019, p. 1–73, 13 March 2020. DOI: 10.1109/IEEESTD.2020.9036129.
25. Ланцов, В.Н., Мосин С.Г. Современные подходы к проектированию и тестированию интегральных микросхем [Текст]: монография. Владимир: Изд-во Владим. гос. ун-та, 2010. – 285 с. – ISBN 978-5-9984-0120-6.

REFERENCES:

[1] ISO/IEC TS 5723:2022, Trustworthiness – Vocabulary. International Organization for Standardization and International Electrotechnical Commission. URL: https://www.iso.org/obp/ui/en/#iso:std:iso-iec:ts:5723:ed-1:v1:en (accessed: 07.05.2025).
[2] Kessarinskiy L.N., Nikiforov A.Yu. AN Approach to setting general requirements for a trusted electronic component a base for a regulated market of critical information infrastructure in questions and answers. IT Security (Russia). 2025, v. 32, no. 1, p. 8–16. URL: https://bit.spels.ru/index.php/bit/article/view/1761/1457 (accessed: 07.05.2025) (in Russian).
[3] Rama E. et al. Trustworthy Integrated Circuits: From Safety to Security and Beyond. IEEE Access, v. 12, 2024, p. 69603–69632. DOI: 10.1109/ACCESS.2024.3400685.
[4] Kessarinskiy L. N. Doverennaya elektronika na forume "Mikroelektronika 2024". Voprosy kiberbezopasnosti. 2024, no. 5(63), p. 115–119. DOI: 10.21681/2311-3456-2024-5-115-119 (in Russian).
[5] PNST 911-2024 Kriticheskaya informatsionnaya infrastruktura. Doverennye integralnye vikroshemy i elektrolnye moduli. Obschie polozheniya. URL: https://normadocs.ru/pnst_911-2024 (accessed: 07.05.2025) (in Russian).
[6] Belous A., Solodukha V. Trusted electronic components for trusted hardware and software platforms: problems and solutions part 2. Electronics: STB, 2021, no. 4, p. 72–77. DOI: 10.22184/1992-4178.2021.205.4.72.76. – EDN: BKANKK.
[7] Smirnov, Dmitry O. Functional Security and an Untrusted Electronic Component Base. IT Security (Russia), [S.l.], v. 29, no. 2, p. 128–143, 2022. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2022.2.10 (in Russian).
[8] Lu R., Chuang Y.-C., Wu J.-L., and He J. Reliability challenges from 2.5D to 3DIC in advanced package development. IEEE International Reliability Physics Symposium (IRPS), p. 1–4, 2023. DOI: 10.1109/IRPS48203.2023.10117647.
[9] Chen M. -F., Chen F. -C., Chiou W. -C. and Yu D. C. H. System on Integrated Chips (SoICTM) for 3D Heterogeneous Integration, in Proc. IEEE 69th Electronic Components and Technology Conference (ECTC), Las Vegas, NV, USA, 2019, p. 594–599. DOI: 10.1109/ECTC.2019.00095.

[10] Italyantsev A. Novye problemy perspektivnykh metodik korpusirovaniya. Zarubezhnaya electronnaya tekhnika. 2018, v. 7(6656), p. 6–9 URL: https://www.niime.ru/upload/iblock/a02/a02ff7ec20742fcee50d67ca1d7825e8.pdf (дата обращения: 07.05.2025) (in Russian).
[11] Pevtsov E.P., Demenkova T.A. Trusted VLSI design. Nanoindustry. 2021, v. 14, no. S7(107), p. 856–859. DOI: 10.22184/1993-8578.2021.14.7s.856.859. – EDN: QVAIUI (in Russian).
[12] Gavrilov S.V., Zheleznikov D.A., Zapletina M.A., Tiunov I.V., Khvatov V.M., Chochaev R.Z., Shokarev D.B. Development of the Trusted Tools for IC Design on Heterogeneous FPGAs. Trudy ISP RAN/Proc. ISP RAS. 2023. v. 35, issue 5, p. 107–126 URL: https://www.ispras.ru/proceedings/docs/2023/35/5/isp_35_2023_5_107.pdf (accessed: 07.05.2025) (in Russian).
[13] Fedorets V.N., Belov E.N., Balybin S.V. Tekhnologii zaschity mikroskhem ot obratnogo proektirovaniya v kontekste informatsionnoy bezopasnosti: nauchno-populyarnoe izdanie. Technosfera. Mir elektroniki, 2019. 216 p. – EDN: LJHRGC (in Russian).
[14] Mosin S., Kislyakov M. An In-Pandemic View on the Global Trends in Microelectronic Design and Market. Proc. IEEE East-West Design & Test Symposium (EWDTS). Batumi, Georgia, 2021, p. 273–276. DOI: 10.1109/EWDTS.2018.8524618.
[15] Amberg P., Turrado L., Sancho G., McGrath R. and Mann S. EU Issues 12th Sanctions Package Targeting Russia. Baker McKenzie.URL: https://sanctionsnews.bakermckenzie.com/eu-issues-12th-sanctions-package-targeting-russia/ (accessed: 30.04.2025).
[16] Mosin S. A Model for Univariant and Multivariant Simulating the Battery Lifetime of UE NB-IoT. In Proc. International Russian Automation Conference (RusAutoCon). Sochi, Russian Federation. 2024, p. 13–18, Paper ID 10694326. DOI: 10.1109/RusAutoCon61949.2024.
[17] IEEE Recommended Practice for Encryption and Management of Electronic Design Intellectual Property (IP). IEEE Std 1735-2023, 6 Nov. 2023, p. 1-237. URL: https://ieeexplore.ieee.org/document/10505231 (accessed: 30.04.2025).
[18] Bykov S.O., Mosin S.G. An automated technique for design of custom network-on-chip topologies. Proc. of IEEE East-West Design and Test Symposium (EWDTS'2015). Batumi, Georgia, 2015, p. 192–194. DOI: 10.1109/EWDTS.2015.7493139.
[19] Mosin S.G. Design-for-testability automation of mixed-signal integrated circuits. In Proc IEEE 26th International SOC Conference (SOCC 2013). Erlangen, Germany, 2013, p. 244–249. DOI: 10.1109/SOCC.2013.6749695.
[20] IEEE Standard for Test Access Port and Boundary-Scan Architecture, in IEEE Std 1149.1-2013 (Revision of IEEE Std 1149.1-2001), pp. 1-444, 13 May 2013. DOI: 10.1109/IEEESTD.2013.6515989.
[21] IEEE Standard Testability Method for Embedded Core-based Integrated Circuits - Redline, in IEEE Std 1500-2022 (Revision of IEEE Std 1500-2005) – Redline, p. 1–168, 12 Oct. 2022. DOI: 10.1109/IEEESTD.2022.9916221.
[22] IEEE Standard for Boundary-Scan Testing of Advanced Digital Networks. IEEE Std 1149.6-2015 (Revision of IEEE Std 1149.6-2003), p. 1–230, 18 March 2016. DOI: 10.1109/IEEESTD.2016.7436703.
[23] IEEE Standard for a Mixed-Signal Test Bus. IEEE Std 1149.4-2024 (Revision of IEEE Std 1149.4-2010), p. 1–116, 6 Dec. 2024. DOI: 10.1109/IEEESTD.2024.10776765.
[24] IEEE Standard for Test Access Architecture for Three-Dimensional Stacked Integrated Circuits. IEEE Std 1838-2019, p. 1–73, 13 March 2020. DOI: 10.1109/IEEESTD.2020.9036129.
[25] Lancov, V.N., Mosin S.G. Sovremennye podkhody k proektirovaniyu i testirovaniyu integralnykh mikroskhem [Tekst]: monografiya. Vladimir: Izd-vo Vladim. gos. un-ta, 2010. – 285 s. – ISBN 978-5-9984-0120-6 (in Russian).

Статья поступила в редакцию 23.04.2025; одобрена после рецензирования 29.05.2025;
принята к публикации 30.05.2025
The article was submitted 23.04.2025; approved after reviewing 29.05.2025;
accepted for publication 30.05.2025