Научная статья/Scientific article
УДК 004.052
http://dx.doi.org/10.26583/bit.2026.1.01
https://elibrary.ru/dgrcgu

ПОДХОДЫ К ПРОТИВОДЕЙСТВИЮ КОНТРАФАКТНОМУ ПРОИЗВОДСТВУ АНАЛОГОВЫХ ИНТЕГРАЛЬНЫХ СХЕМ

Сергей Г. Мосин[1]✉, Виталий А. Телец[2]
[1]Казанский (Приволжский) федеральный университет, ул. Кремлевская, 18, Казань, 420008, Россия
[1]ООО «ЛабСистемс», ул. Федосеева, 5, Владимир, 600000, Россия
[2]Национальный исследовательский ядерный университет «МИФИ», Каширское ш., 31, Москва, 115409, Россия
✉*smosin@ieee.org*

Аннотация. Интенсивное развитие и внедрение технологий Индустрии 4.0 в разные секторы промышленности и поступательная информатизация общества влияют на рост потребления микросхем и электронной компонентной базы широкой номенклатуры. Существующие производственные мощности кремниевых фабрик не всегда способны обеспечить фактический уровень потребления микросхем, определяя рост дефицита и формирование негативных условий для появления контрафактных производств. Проектирование и производство аналоговых интегральных схем (АИС), которые становятся все более востребованными в приложениях беспроводной связи, Интернета-вещей и датчиков, остаются крайне сложными задачами, влияя на стоимость устройства и привлекательность к фальсификации со стороны злоумышленников. Объектом проведенного исследования выступают аналоговые интегральные схемы. Проблема – рост контрафактного производства АИС и усиление угроз доверенности электронных систем критической инфраструктуры. Предмет – методы устранения преднамеренных ошибок, негативно влияющих на характеристики доверенности АИС, и подходы к противодействию контрафактному производству АИС. Цель предложенной работы – систематизация решений противодействия контрафактному производству АИС и формирование стратегий обеспечения интересов защищающейся от контрафактного производства стороны. Приведена классификация контрафактных микросхем. Рассмотрены подходы к противодействию контрафактному производству АИС. Показано, что подобные подходы требуют дополнительных расходов на проектирование и производство, увеличивают используемую площадь кристалла, повышают теоретическую вероятность возникновения дефектов на кристалле и, следовательно, снижают показатель выхода годных микросхем, но это осознанный выбор разработчиков и производителей микросхем для противодействия злоумышленникам. Предложены стратегии выбора схем обфускации, основанные на многокритериальной оптимизации, применимые при автоматизации проектирования для обеспечения доверенности (*Design-for-Trust*).

Ключевые слова: *доверенные интегральные схемы, аналоговые интегральные схемы, цепочки поставок, контрафакт, преднамеренные ошибки, противодействие контрафактному производству, схемы обфускации, стратегии выбора*

Для цитирования: Мосин, С., Телец, В. (2026). Подходы к противодействию контрафактному производству аналоговых интегральных схем. *Безопасность информационных технологий,* 33(1), 1-15. doi: http://dx.doi.org/10.26583/bit.2026.1.01

APPROACHES TO COUNTERING COUNTERFEIT PRODUCTION OF ANALOG INTEGRATED CIRCUITS

Sergey G. Mosin[1]✉, Vitaly A. Telets[2]
[1]Kazan (Volga region) Federal University, Kremlyovskaya St., 18, Kazan, 420008, Russia
[1]LabSystems LLC, Fedoseeva St., 5, Vladimir, 600000, Russia
[2]National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Kashirskoe sh., 31, Moscow, 115409, Russia
✉*smosin@ieee.org*

Abstract. The intensive development and adoption of Industry 4.0 technologies across various industrial sectors, coupled with the progressive digitalization of society, are driving increased consumption of a wide range of integrated circuits (ICs) and electronic components. Existing silicon fabrication facilities cannot always meet the actual consumption level of ICs, leading to growing shortages and creating favorable conditions for the emergence of counterfeit production. The design and manufacturing of analog integrated circuits (AICs), which are increasingly in demand for applications in wireless communications, the Internet of Things (IoT), sensors, and transducers, remain highly complex tasks. This complexity impacts device cost and makes them attractive targets for malicious counterfeiting. The object of this study is analog integrated circuits. The problem addressed is the growth of counterfeit AIC production and the escalating threats to the trustworthiness of electronic systems in critical infrastructure. The subject is methods for eliminating intentional flaws that negatively affect the trustworthiness attributes of AICs, and approaches to combat counterfeit AIC production. The aim of this work is to systematize solutions for combating counterfeit AIC production and to formulate strategies for protecting the interests of the party defending against counterfeiting. A classification of counterfeit ICs is provided. Approaches to countering counterfeit AIC production are reviewed. It is shown that such approaches necessitate additional design and manufacturing costs, increase die area, raise the theoretical probability of on-chip defects, and consequently reduce the yield of functional ICs. However, this is a conscious choice made by IC designers and manufacturers to counter malicious actors. Obfuscation strategy selection schemes based on multi-criteria optimization are proposed, applicable to design automation for trust (Design-for-Trust, DfTr).

Keywords: *trustworthy integrated circuits, analog integrated circuits, supply chains, counterfeiting, intentional faults, counteraction to counterfeit production, obfuscation schemes, selection strategies*

For citation: Mosin, S., Telets, V. (2026). Approaches to countering counterfeit production of analog integrated circuits. *IT Security (Russia),* 33(1), 1-15. doi: http://dx.doi.org/10.26583/bit.2026.1.01

Введение

Глубокая информатизация общества и переход к цифровой экономике в контексте четвертой промышленной революции (Индустрия 4.0) стимулируют возрастание объемов мирового рынка микроэлектроники, что в свою очередь определяет ежегодный рост потребления электронной компонентной базы в целом и интегральных схем в частности [1]. Экстенсивный рост производства компаниями-производителями интегрированных устройств (*IDM – Integrated Device Manufacturer*) не позволяет в полной мере обеспечить возрастающие потребности рынка [2], что проявляется в изменении структуры рынка производителей интегральных схем (ИС) и электронных компонентов (ЭК), а также в поступательном увеличении контрафактных ИС и ЭК в цепочках поставок.

Наряду с классическими *IDM*-компаниями, реализующими вертикальные бизнес-процессы замкнутого цикла с ориентацией на собственные проектные и производственные ресурсы, активно развиваются компании с функциональным профилированием, деятельность которых встраивается в горизонтальные бизнес-процессы проектирования и производства востребованных ИС за счет множественной кооперации. Вторая модель позволила перераспределить процессы проектирования и производства ИС между различными дизайн центрами и компаниями, которые не обладают собственными производственными мощностями (*fabless*), и кремниевыми фабриками (*mini-fab*, *foundry*) [3], повышая эффективность и снижая финансовые издержки на строительство, обслуживание и обновление производственных линий. Такое взаимодействие способствует успешному выходу на рынок полупроводников небольших компаний – с меньшей капитализацией по сравнению с классическими *IDM*. Развитие новых архитектур ИС, таких как 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., стимулирует появление новых *fabless*-компаний со своей спецификой бизнес-моделей: разработчики

IP-ядер (*IP – Intellectual Property*), интеграторы *IP*-ядер в *SoC*/*NoC*, вендоры собственных и/или сторонних *IP*-ядер и т.д.[1]

Переход от вертикальной к горизонтальной модели производства ИС расширяет спектр участников цепочки поставок и повышает вероятность внешних угроз, связанных с внедрением аппаратных троянов, организацией атак по сторонним каналам (*Side-Channel Attacks*), в том числе с использованием неисправностей – активные атаки, выполнением недобросовестного обратного инжиниринга (*Reverse Engineering*) и развертыванием контрафактного производства. Структура цепочки поставок от проектирования до утилизации ИС с определением основных инструментов и объектов доверенности для каждого звена и вовлеченных игроков представлена на рис. 1.

Каждое звено цепочки поставок потенциально подвержено разнообразным угрозам с различной степенью сложности их реализации, а также соответствующими временными и стоимостными расходами. Например, интеграция трояна в ИС на этапе проектирования потенциально более простая и менее затратная задача, по сравнению с аналогичной интеграцией на этапе производства. Подготовка и реализация атак по сторонним каналам при поставке и эксплуатации ИС проще и безопаснее для потенциального злоумышленника, чем на этапе производства. Недобросовестный обратный инжиниринг направлен на извлечение конфиденциальной информации, необходимой для создания поддельной ИС. Под контрафактной ИС понимают:[2, 3] 1) неавторизованную копию, 2) не соответствующую проекту, модели и/или спецификации действительного изготовителя компонента (изделия) (*OCM – Original Component Manufacturer*), 3) производимую не *OCM* или неавторизованным сторонним подрядчиком, 4) не соответствующую спецификации, дефектный или бывший в употреблении продукт *OCM*, продаваемый как новый или рабочий, 5) имеющую неверную или ложную маркировку и/или документацию.

Исторически сложилось, что цифровые ИС выступали основными целями контрафактного производства. Однако в последнее десятилетие в число «лидеров» по контрафакту вошли аналоговые и радиочастотные ИС (*RF IC*) [4, 5] (рис. 2).

Данное обстоятельство обусловлено возрастанием спроса на аналоговые ИС (АИС) и *RF IC*, в том числе благодаря активному развитию современных систем связи, приложений Интернета-вещей (*IoT – Internet of Things*) и промышленного *IoT* (*IIoT – Industrial IoT*) [6]. Для цифровых ИС разработаны и активно используются эффективные методы противодействия контрафактному производству, которые в большинстве случаев не применимы для АИС. Актуальным направлением в области автоматизации микроэлектронного проектирования выступает проектирование для обеспечения доверенности (*DfTr – Design-for-Trust*), которое наряду с тестопригодным проектированием (*DFT – Design-for-Test*), проектированием для обеспечения высокого показателя выхода годных (*DFY – Design-for-Yield*), проектирования под особенности производственной линии (*DFM – Design-for-Manufacturing*) и др. становится необходимым и обязательным инструментом средств автоматизированного проектирования как цифровых, так и аналоговых, и смешанных ИС (*EDA – Electronic Design Automation*).

[1]Semiconductor IP Cores Market. Verified Market Reports, Feb. 2025. 210 p. Report ID. 308108. URL: https://www.verifiedmarketreports.com/product/semiconductor-ip-cores-market/ (дата обращения: 22.10.25).
[2]ГОСТ Р 57880-2017. Национальный стандарт Российской Федерации. Система защиты от фальсификаций и контрафакта. Изделия электронные. Предотвращение получения, методы обнаружения, сокращение рисков применения и решения по использованию фальсифицированной и контрафактной продукции.
[3]U.S. Department of Commerce. Defense industrial base assessment: Counterfeit electronics. Jan. 2010.

Звено	Проектирование	Производство	Поставка	Эксплуатация	Утилизация
Объект доверенности	• САПР / *EDA* • *Soft IP* • *Hard IP* • *PDK* (*Process Design Kit*)	• Топология • *3D* п/п структуры • Корпусы • Программы испытаний	• Партия ИС • Сопроводительная документация • ТУ • Регламенты*	• Спецификация • Маркировка • Отчеты о входном контроле • ТУ • Технические характеристики	• ЭКБ / электронное оборудование • ТУ • Нормативные документы**
Игроки	• Вендоры • Разработчики *IP* • Интеграторы *IP* • Разработчики *PDK* (*mini-fab / foundry*)	• *mini-fab / foundry* • Интеграторы *SoC*, *NoC*, *MCM*, *MCP*, *SiP* • Разработчики / поставщики корпусов • Центры корпусирования • Испытательные центры	• Производители оригинальных ИС и ЭК (*OCM*) • Вендоры / поставщики ИС и ЭК • Потребители	• Сертификационные центры • Вендоры / поставщики ИС и ЭК • Технический контроль (ОТК) • Испытательные центры	• Центры утилизации • Центры накопления и сортировки • Надзорные органы
Преднамеренные ошибки	Внедрение аппаратных троянов				
		Атаки по сторонним каналам			
		Обратный инжиниринг			
			Контрафакт		

* ГОСТ Р 71914-2024.
** Федеральный закон от 24.06.1998 № 89-ФЗ;
Приказ Минпромторга РФ от 04.04.2023 г. № 173;
ГОСТ Р 70146-2022.

Рис. 1. Отображение преднамеренных ошибок на цепочку поставок

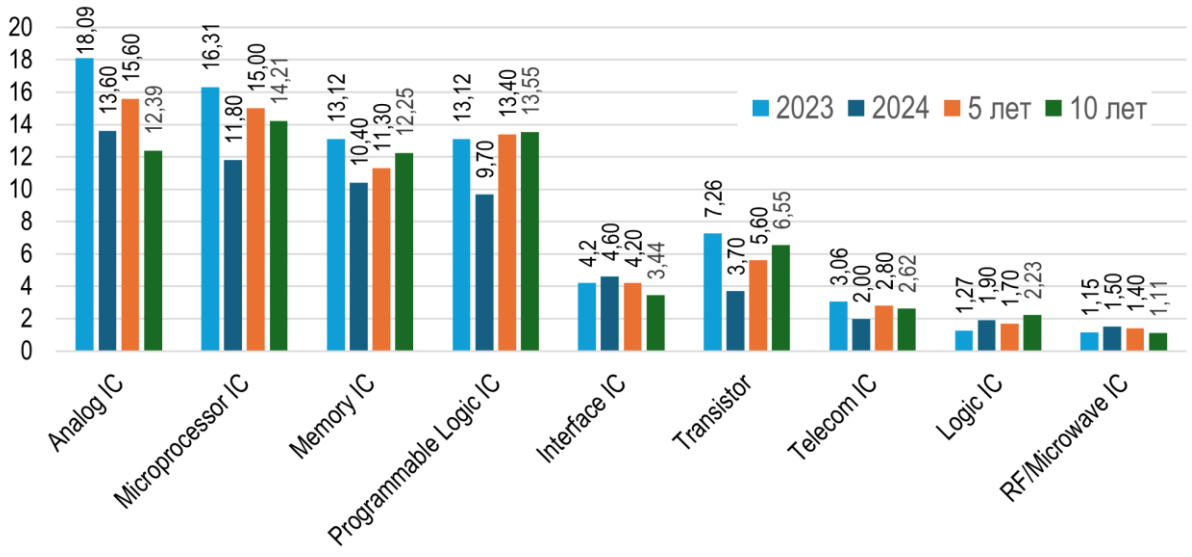


Рис. 2. Доля контрафактной продукции по категориям ИС и ЭК (%)

Объектом проведенного исследования выступают АИС. *Проблема* – рост контрафактного производства АИС и усиление угроз доверенности электронных систем критической инфраструктуры. *Предмет* – методы устранения преднамеренных ошибок, негативно влияющих на характеристики доверенности АИС, и подходы к противодействию контрафактному производству АИС. Цель работы – систематизация решений противодействия контрафактному производству АИС и формирование стратегий

обеспечения интересов защищающейся от контрафактного производства стороны. Применение рациональных методов устранения преднамеренных ошибок при проектировании и производстве АИС оказывает влияние на устойчивость к воздействию внешних факторов (ВВФ), надежность, безопасность и защищенность как самих ИС, так и электронных систем, в которых они используются, а обеспечиваемое при этом противодействие контрафактному производству минимизирует негативное влияние на экономические потери и риски микроэлектронной промышленности на национальном и глобальном уровне.

1. Особенности АИС и возможные преднамеренные ошибки

Активное развитие микропроцессорной техники и цифровой электроники в целом переместило аналоговые интегральные схемы на второй план глобального рынка полупроводников. Однако с появлением и интенсивным внедрением современных телекоммуникационных систем и технологий (беспроводная связь, сенсорные сети, *IoT* и *IIoT* и т.п.) потребность в АИС стремительно возросла, а существующие производственные мощности не всегда успевают обеспечивать потребность рынка.

Аналоговые ИС – это микросхемы, предназначенные для преобразования и (или) обработки сигналов, изменяющихся по закону непрерывной или прерывистой функции[4]. АИС используют физические процессы движения носителей электрического заряда в полупроводниковых структурах для выполнения различных функций, к которым относят усиление, фильтрацию, модуляцию/демодуляцию, сравнение, базовые арифметические операции, выборку и хранение, сложные функциональные преобразования (например, сравнение сигнала(ов), преобразование частоты сигнала в напряжение и др.), коммутацию и переключение, стабилизацию источников питания, а также съем сигналов от объектов через преобразователи физических величин и датчики, и др. Справедливо в этой связи указать и на ИС аналого-цифровых и цифро-аналоговых преобразователей (АЦП и ЦАП).

Достижения в области полупроводниковых технологий и методов проектирования продолжают стимулировать инновации в области АИС, открывая путь к повышению производительности, эффективности и расширению возможностей интеграции. Ключевые тенденции, определяющие будущее аналоговых ИС:

Интегральные схемы смешанных сигналов: интеграция аналоговых и цифровых функций на одном кристалле, в том числе с использованием АЦП и ЦАП, будет расширяться, предлагая компактные решения с повышенной степенью интеграции, с улучшенной производительностью, чувствительностью, защищенностью от наводок, многоканальностью, устойчивостью к ВВФ, со сниженным энергопотреблением и более низкими производственными затратами. Такая интеграция жизненно важна для приложений, требующих как аналоговой и аналого-цифровой (и обратной) обработки сигналов, так и цифрового управления.

Высокочастотные приложения и устройства с высоким уровнем мощности: достижения в области материалов, таких как карбид кремния (*SiC*) и нитрид галлия (*GaN*), позволяют разрабатывать АИС, функционирующие на более высоких частотах (*high-frequency*) и с более высокими уровнями мощности (*high-power*). Эти ИС незаменимы для приложений в телекоммуникациях, силовой электронике, электромобилях и системах возобновляемой энергетики, космической аппаратуре и аппаратуре энергетических комплексов.

Миниатюризация и маломощные приложения: спрос на более компактные и энергоэффективные АИС стимулирует инновации в области миниатюризации и реализации маломощных (*low-power*) схем.

Улучшенные возможности датчиков и обработки сигналов реального времени: АИС с усовершенствованными технологиями сенсорики, улучшенными алгоритмами обработки

[4]ГОСТ Р 57435–2017. Национальный стандарт Российской Федерации. Микросхемы интегральные. Термины и определения.

сигналов и интегрированными интерфейсами между элементами и каналами съема и обработки информации открывают новые возможности для приложений *IoT*/*IIoT*, носимых устройств, интеллектуальных датчиков в промышленности, медицине и здравоохранении, авионике, космическом и автомобилестроении и др. Такие АИС используют в разработке интеллектуальных систем (информационно-измерительных, измерительно-информационных, сбора, обработки и управления данными), способных собирать и анализировать данные в режиме реального времени.

Несмотря на технологическое развитие в области микроэлектроники, проектирование и производство АИС остаются крайне сложными задачами, которые обусловлены многочисленными причинами [7]:

- высокая трудоемкость проектирования, требующая опыта и высокой квалификации инженеров-проектировщиков, конструкторов, технологов и других специалистов;
- недостаточное обеспечение всех этапов и стадий проектирования средствами *EDA*, необходимыми моделями и вычислительными методами, что обуславливает существенную долю ручного труда;
- высокая чувствительность входных и выходных характеристик к отклонениям в параметрах внутренних компонентов и внешним условиям, неотъемлемое присутствие допусков и шумов (тепловые, фликкер, джиттер), смещения рабочих точек и отклонения от рабочих режимов и др.;
- предрасположенность к «изящным сбоям», когда при совокупности внешних и/или внутренних факторов выходные характеристики АИС выходят за допустимые границы с сохранением в целом характера функционального преобразования;
- итерационное многошаговое перепроектирование и повторное производство кристалла до получения АИС, удовлетворяющей требованиям спецификации;
- проблематичность, но необходимость поддержания на этапе проектирования методологий *DFT*, *DFY* и *DFM*.

Получение работоспособной АИС требует существенных временных и финансовых затрат со стороны производителя (*OCM*), что определяет ценность интеллектуальной собственности и потребность в ее защиты. Пиратское и контрафактное производство в целом наносит прямые и косвенные убытки *OCM*, нарушает доверенность таких интегральных схем и электронных систем, в которых они используются [8].

Преднамеренные ошибки вызывают угрозы интеллектуальной собственности для АИС, которые можно разделить на четыре группы в зависимости от доступа злоумышленника к звену цепочки поставок [9].

Внедрение аппаратных троянов – злонамеренная вредоносная модификация проекта, которая может использоваться для получения несанкционированного доступа к конфиденциальной информации или оказания деструктивного влияния на функционирование АИС с целью нарушения нормальной работы электронной системы.

Атаки по сторонним каналам и с использованием неисправностей нацелены на данные, обрабатываемые и хранимые ИС, при этом не затрагивая напрямую конфиденциальную информацию, необходимую для разработки самой ИС. Сторонние каналы могут представлять данные об энергопотреблении, электромагнитном излучении, временных характеристиках и т.д., по которым можно восстановить особенности выполняемых преобразований и характеристики обрабатываемых сигналов. Атаки на сторонние каналы – пассивные атаки, осуществляющие неинвазивный сбор сведений. Атаки с использованием неисправностей – активные атаки, направленные на нарушение функционирования АИС.

Обратный инжиниринг подразумевает извлечение конфиденциальной информации об *IP*-ядрах или топологии АИС, представленной в зависимости от уровня абстракции архитектурой, списком соединений, топологией, технологическими правилами и т.п. и необходимой для создания идентичных или похожих *IP*/ИС или извлечения секретной информации, например конфигураций или ключей шифрования.

Контрафакт – это фальсифицированная АИС, которая получена в результате множества потенциальных нарушений безопасности в цепочке поставок, нелегально поступившая на открытый рынок полупроводников с нарушением исключительных прав правообладателей и претендующая на подлинность.

Различают следующие категории контрафактных ИС, включая АИС (рис. 3) [10].

- *Восстановленные*: ИС извлекают из использованной системы, переупаковывают и перемаркировывают, а затем продают на рынке как новые. По факту такие ИС могут быть как полностью неисправными, так и с отклонениями от номинальных характеристик, когда предыдущее использование нанесло значительный ущерб сроку их службы или производительности.
- *Перемаркированные*: фальсификаторы удаляют старую маркировку с корпуса (или даже из кристалла) и наносят новую, используя недостоверную информацию. Перемаркировка может применяться также для необоснованного указания на улучшенные технические характеристики ИС, например, вместо исходного коммерческого (*commercial*) класса на индустриальный (*industrial*), военный (*military*) или космический (*space*).

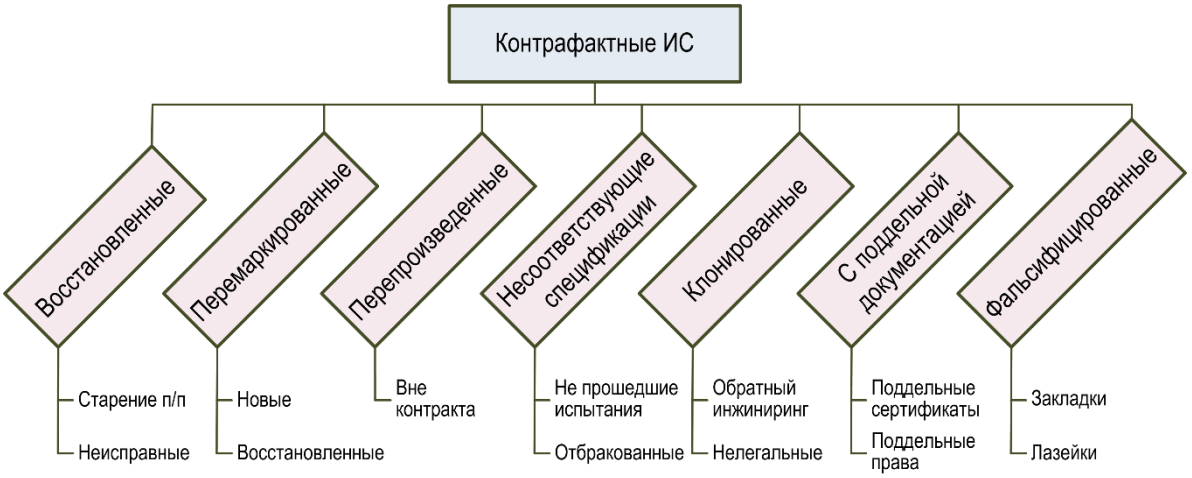


Рис. 3. Классификация контрафактных ИС

- *Перепроизведенные*: неучтенные излишки ИС, изготовленные вне контракта с *ОСМ*, которые незаконно поступают на открытый рынок. В некоторых случаях фиксируется производство изделий на технологических линиях с ведома правообладателя, в так называемую, «третью смену», но тогда это можно квалифицировать как мошенничество при получении неучтенной прибыли, т.е. как экономическое преступление.
- *Несоответствующие спецификации/дефектные*: ИС, не прошедшие испытания выходного контроля на производстве, но незаконно попавшие в цепочку поставок. Выявление неисправностей в таких ИС представляет сложную задачу (например, при перемежающихся отказах), а их использование – серьезная угроза надежности аппаратуры и систем, в которых они применяются.
- *Клонированные*: ИС, несанкционированно произведенные без легальных прав на интеллектуальную собственность, – точные копии оригиналов. Клонирование может осуществляться путем обратного инжиниринга или незаконного получения прав интеллектуальной собственности.
- *С поддельной документацией*: ИС, сопровождаемые поддельной документацией – сертификаты, спецификация (технические условия на поставку), идентификация партии и дата производства, и т.п.
- *Фальсифицированные*: ИС с внесенными на любом этапе жизненного цикла несанкционированными изменениями, например включение в схему аппаратных троянов (закладок). Такие ИС действуют либо как «кремниевая бомба замедленного действия», когда при определенных внешних воздействиях провоцируется нарушение работоспособности

устройства, либо как лазейка (*backdoor*), через которую используемая или обрабатываемая конфиденциальная информация может быть передана злоумышленнику.

Выход контрафактной продукции на рынок имеет последствия, варьирующиеся от потерь доходов *ОСМ* и налогов на уровне государства до рисков для безопасности при использовании низкокачественных ИС в составе электронной аппаратуры. Борьба с фальсификацией и противодействие контрафактному производству – серьезный вызов для правительств, промышленности и общества.

2. Подходы к противодействию контрафактному производству АИС

Защита интеллектуальной собственности на АИС через государственную и/или международную регистрацию патентов и ноу-хау не позволяет *ОСМ* в полной мере защитить себя от угрозы подделки и контрафактного производства злоумышленниками. В этой связи разработчики и производители АИС вынуждены прибегать к специальным решениям, которые связаны с внедрением в свои схемы дополнительных подсхем, противодействующих и/или усложняющих процесс сбора и использования конфиденциальной технологической информации для выпуска контрафактной продукции [11]. Подобные подходы требуют дополнительных расходов на проектирование и производство, увеличивают используемую площадь кристалла, повышают теоретическую вероятность возникновения дефектов на кристалле и, следовательно, снижают показатель выхода годных микросхем, но это осознанный выбор *ОСМ* для противодействия злоумышленникам.

К числу наиболее распространенных и эффективных подходов можно отнести:

- блокировку подсхем;
- распределенное производство;
- защиту от восстановленных ИС;
- обфускацию.

Используемые подходы позволяют *ОСМ* бороться с большинством угроз внутри цепочки поставок.

2.1. Блокировка подсхем

Блокировка (*Locking*) привлекает разработчиков цифровых и АИС, поскольку позволяет организовать защиту от злоумышленников в любом звене цепочки поставок. Микросхемы с внедренными подсхемами блокировки потенциально доступны злоумышленникам, но без секретных ключей противодействуют ведению контрафактного производства и/или усложняют его. Реверс инжиниринг с блокировкой не позволит получить функционально полный проект оригинальной АИС и контрафактные ИС (клонированные, перепроизведенные) не будут соответствовать спецификации и функциональным требованиям. Активация заблокированной АИС происходит при доверенной загрузке секретных ключей в защищенную от несанкционированного доступа память микросхемы (*TPM – Tamper-Proof Memory*). Наиболее распространенными на практике выступают методы блокировки цепей смещения и модулей калибровки АИС.

Блокировка цепи смещения. Работа аналоговых схем очень чувствительна к выбору положения рабочих точек активных элементов, то есть действующих постоянных токов и напряжений. При проектировании АИС выполняют синтез функциональной схемы и проектирование цепей смещения. На первом этапе проектируется схема для выполнения заданной функции, а в ходе параметрического синтеза цепи смещения формируются условия для поддержания желаемых рабочих точек транзисторов на определенном уровне для достижения целевых характеристик выходных параметров АИС, что критически важно для ее функционирования и надежности.

Блокировка смещения заключается в перепроектировании цепи смещения таким образом, чтобы секретный ключ мог использоваться для управления ее параметрами и, следовательно, ее выходными сигналами. Применение некорректного ключа приводит к значительным колебаниям в режимах работы транзисторов, при которых в схеме

наблюдается нарушение характеристик одного или нескольких выходных параметров. Использование корректного секретного ключа заставляет схему вести себя ожидаемым образом. Методы блокировки цепи смещения ориентированы на использование секретных ключей достаточно большой длины, чтобы предотвращать атаки полным перебором (*brute-force*), а также должны гарантировать, что никакие комбинации некорректных ключей не смогут привести аналоговую схему в состояние ее нормальной работы или близкое к нему. Например, в [12] представлен патент, описывающий подход к блокировке смещений АИС за счет изменения ширины транзисторов с использованием секретного ключа.

Блокировка модулей калибровки воздействует на регулировочные элементы аналоговой схемы, которые компенсируют производственные вариации и неидеальности. Использование некорректных ключей будет приводить к отклонениям от нормальной работы схем компенсации, что провоцирует нарушение характеристик выходных параметров всей АИС. Например, в [13] предложен калибровочный контур, использующий АЦП и цифровую схему оптимизатора, которые обрабатывают выходной сигнал АИС и через цепь обратной связи повышают стабильность выходных характеристик. Блокировка применяется к схеме цифрового оптимизатора на основе метода логической блокировки *SFLL* (*Stripped Functionality Logic Locking*). В [14] описано решение, в котором механизм блокировки управляет диапазоном программируемости аналогов транзисторов с плавающим затвором (*AFGT – Analog Floating Gate Transistor*). Полный диапазон настройки блокируется, если сначала не запрограммировать *AFGT* в определенном порядке и с определенными напряжениями, которые составляют секретный аналоговый ключ.

Методы блокировки подсхем существенно усложняют процесс контрафактного производства АИС, но не гарантируют полного противодействия.

2.2. Распределенное производство

Данный подход был предложен для снижения рисков на производстве за счет использования в цепочке поставок частичной информации обо всем проекте [15]. На этапе проектирования обеспечивается функциональная декомпозиция топологии схемы для раздельного производства на разных кремниевых фабриках с последующей сборкой итоговой АИС, ее тестированием и корпусированием на доверенном производстве (рис. 4).

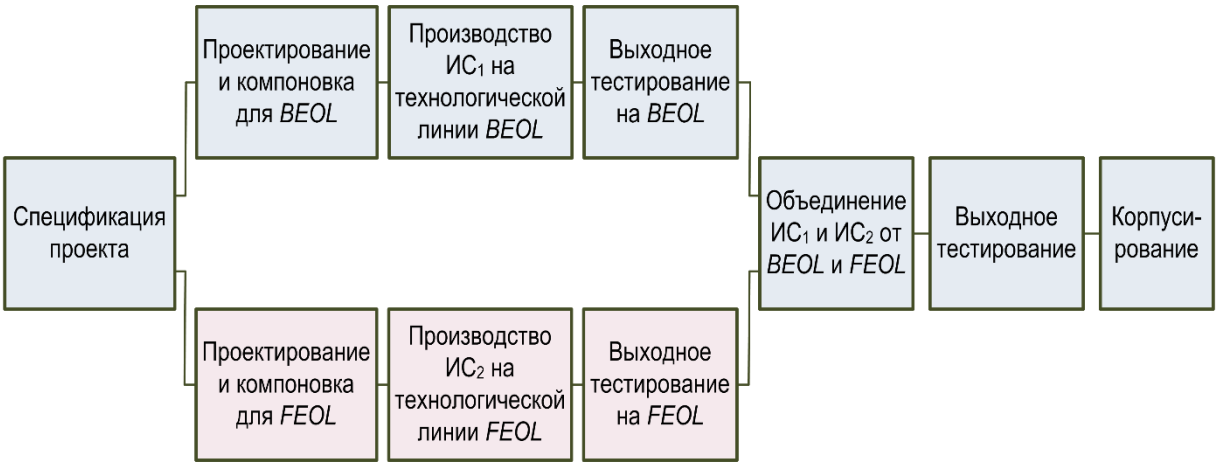


Рис. 4. Диаграмма организации распределенного производства АИС

Распределение топологии для производства происходит между двумя линиями: с низким уровнем доверия, производящей нижние слои ИС, включая транзисторы (*FEOL – Front-End-Of-Line*), и доверенной, производящей верхние слои ИС – слои металлизации и межсоединений (*BEOL – Back-End-Of-Line*). В результате *FEOL*-линия получает редуцированную топологию, по которой невозможно однозначно определить структуру и функциональные возможности устройства, т.е. она лишена необходимой информации для

пиратского копирования или реверс-инжиниринга проекта. Годные кристаллы с двух линий поступают на окончательную сборку на доверенном производстве, где обеспечивается интеграция реализаций от *FEOL* и *BEOL* в единый кристалл с контролем его работоспособности и дальнейшим корпусированием.

Для *RF IC* такой подход позволяет не распространять информацию о структуре и параметрах планарных конденсаторов и индуктивностей, которые принято реализовывать в верхних слоях металлизации.

2.3. Защита от восстановления ИС

Методы данной группы, которые могут быть внешними и внутрисхемными, направлены преимущественно на анализ структуры ИС с целью определения отклонений контролируемых параметров из-за старения и/или деградации материалов. Внешние методы представлены физическим и электрическим контролем, которые требуют специализированного оборудования и длительного времени на проведение испытаний, что ограничивает их применение для больших партий ИС. Внутрисхемные методы основаны на интеграции в топологию АИС специализированной подсхемы, контролирующей чувствительные к старению и/или износу материала характеристики и формирующие соответствующий признак, доступный на специализированном внешнем выводе корпуса микросхемы.

Методы второй группы являются перспективными решениями для выявления восстановленных ИС. На практике распространены реализации на основе мониторинга задержек распространения сигналов на внутренних линиях [16], кольцевых генераторах [17] и специализированных сенсорах [18, 19].

Активно развивающимся направлением выступают инициативы разработчиков *EDA* по внедрению инструментов управления жизненным циклом полупроводниковых изделий (*SLM – Silicon Lifecycle Management*) в цепочки поставок [20, 21]. *SLM* также предполагает интеграцию в топологию ИС специальных датчиков и использование средств интеллектуального сбора и хранения данных мониторинга на протяжении всего жизненного цикла системы, что предназначено для повышения эффективности проектирования и улучшение качества ИС и электронных систем, прогнозирования деградации или отказа чипов в полевых условиях – формирует цифровой портрет изделия и существенно усложняет неконтролируемое восстановление ИС на этапе утилизации.

2.4. Обфускация

Аппаратное запутывание или аппаратная обфускация (*obfuscation*) предусматривает применение методов преднамеренного сокрытия фактической структуры, топологии и функциональности микросхемы или специальное включение в структуру и топологию дополнительных объектов, которые усложняют или делают невозможным несанкционированное получение технических сведений об ИС для успешного контрафактного производства [22].

Аппаратная обфускация АИС может использовать методы блокировки, когда применение корректного секретного ключа обеспечивает номинальное конфигурирование элементов схемы для формирования электрических характеристик согласно спецификации проекта [23]. Применение некорректного секретного ключа приводит к отклонениям в конфигурации внутренних элементов схемы с нарушением или критическим несоответствием выходных характеристик АИС спецификации. Например, внутрисхемная реализация транзистора в виде матричной структуры (на рис. 5, *а*) позволяет при помощи прикладываемого ключа конфигурировать его фактическую структуру, задавая ширину (W) и длину (L) затвора, а также важное для электрических характеристик эффективное соотношение $(W/L)_{eff}$. Параллельное соединение транзисторов в матричной конфигурации позволяет увеличить фактическую ширину канала эквивалентного транзистора, а следовательно

$$\left(\frac{W}{L}\right)_{eff} = \frac{W_1}{L} + \frac{W_2}{L} + \cdots + \frac{W_n}{L} = \frac{1}{L}\sum_{i=1}^{n} W_i ,$$

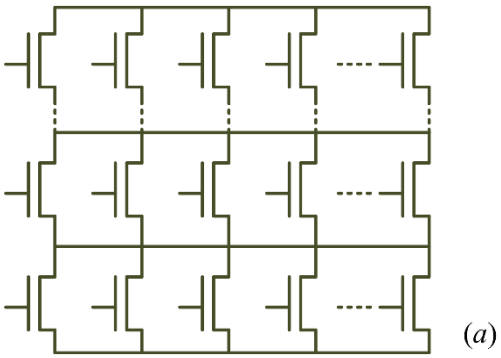
где W_i – ширина i-го транзистора в выбранной строке конфигурации.

Последовательное соединение транзисторов будет также влиять на увеличение длины затвора эквивалентного транзистора. Например, для двух последовательно включенных транзисторов в конфигурации получаем

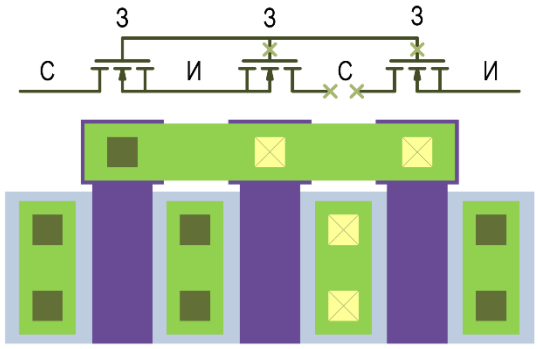
$$\left(\frac{W}{L}\right)_{eff} = \frac{\frac{W_1}{L_1}\ \frac{W_2}{L_2}}{\frac{W_1}{L_1} + \frac{W_2}{L_2}},$$

где W_1/L_1 – соотношение для транзистора в цепи истока, а W_2/L_2 – соотношение для транзистора в цепи стока.

Другим направлением обфускации выступает *камуфлирование*, связанное с внесением скрытых изменений в оригинальный проект как на уровне структуры отдельно взятых элементов схемы, так и цепей межсоединений без негативного влияния на его работоспособность и характеристики [24]. Такие изменения вводят злоумышленника в заблуждение при клонировании или обратном инжиниринге АИС, маскируя список соединений и топологию оригинальной микросхемы фиктивными элементами. Например, при обратном инжиниринге реализованные в топологии фиктивные транзисторы с отсутствующими электрическими соединениями воспринимаются как действующие и подключенные (рис. 5, *б*), что приводит к неточностям и грубым ошибкам в восстанавливаемом списке соединений, режимах работы и электрических характеристиках.



(*а*)



(*б*)

Рис. 5. Примеры аппаратной обфускации: (а) матричная конфигурация транзисторов [13]; электрически не подключенные фиктивные транзисторы [25]

3. Стратегии выбора схем обфускации

Для сравнения различных вариантов реализации схем обфускации и количественной оценки эффективности разных вариантов предложено использовать набор метрик [24].

Пессимистическая для защищающегося оценка пространства поиска

$$\lambda_1 = \prod_{i=1}^{|\mathbf{S}|} \lceil \alpha_{max}\, N_i \rceil ,$$

$$\alpha_i = N_i^{obf} / N_i \ , \alpha_{max} = \max_i \alpha_i ,$$

где $\mathbf{S}$ – множество компонентов схемы, потенциально участвующих в обфускации, $|\mathbf{S}|$ – мощность $\mathbf{S}$, N_i – количество вариантов обфускации для i-го компонента множества $\mathbf{S}$, N_i^{obf} – количество неактивных вариантов из N_i при обфускации i-го компонента.

Общее время моделирования для исчерпывающего поиска в пространстве поиска λ_1

$$\lambda_2 = \lambda_1 T,$$

где T – общее время моделирования характеристик схемы на совокупности тестовых наборов.

Коэффициент несоответствия характеристик обфусцированной схемы спецификации оригинальной схемы

$$\lambda_3 = 100/n \sum_{j=1}^{n} I(j),$$

$$I(j) = \begin{cases} 0, & \text{при соответствии спецификации;} \\ 1, & \text{при несоответствии спецификации,} \end{cases}$$

где n – количество выполненных моделирований схемы ($n \leq \lambda_1$).

Среднее отклонение неисправных схем от спецификации (%)

$$\lambda_4 = 100/n \sum_{j=1}^{n} \sqrt{\sum_{k=1}^{l} \left(1 - \hat{p}_{jk}\right)^2},$$

$$\hat{p}_{jk} = \begin{cases} 1, & \text{при соответствии схемы } j \text{ спецификации } k; \\ p_{jk}/s_k, & \text{при несоответствии схемы } j \text{ спецификации } k, \end{cases}$$

где p_{jk} – значение k-го параметра неисправной схемы j, s_k – значение k-го параметра из спецификации.

Отклонение «лучшей» неисправной схемы, характеристики которой максимально близки граничным значениям спецификации (%)

$$\lambda_5 = 100 \min_j \sqrt{\sum_{k=1}^{l} \left(1 - \hat{p}_{jk}\right)^2}.$$

На основе метрик $\lambda_1 - \lambda_5$ предложены стратегии обеспечения интересов защищающейся от контрафактного производства стороны, которые можно представить в виде многокритериальной оптимизации, отражающей:

- *только функциональные требования*

$$\arg \max_j(\lambda_4) \Big| \min_j(\lambda_3) \to 0, \quad (1)$$

s.t. $n \leq \lambda_1$,

т.е. выбор варианта обфускации (j), при котором ошибочная активация злоумышленником фиктивных элементов приводит к максимальному отклонению от параметров спецификации оригинальной схемы при минимальном отклонении параметров номинальной обфусцированной схемы от аналогичных параметров спецификации оригинальной схемы;

- *функциональные требования с ресурсными ограничениями*

$$arg \min_{u,v}(A) \max_j(\lambda_4) \Big| \min_j(\lambda_3) \to 0, \quad (2)$$

s.t.

$$n \leq \lambda_1 ; A = F\left(\mathbf{S}_u, N_{i_u}^v\right); i_u = 1..|\mathbf{S}_u|; \mathbf{S}_u \in \mathbf{S}; v = 1..N_{max},$$

т.е. выбор варианта обфускации с соблюдением требований (1) и с минимальными накладными расходами по площади кристалла на его реализацию;

- *функциональные требования с временными ограничениями*

$$arg \max_{u,v,w}(\lambda_2) \max_j(\lambda_4) \Big| \min_j(\lambda_3) \to 0, \quad (3)$$

s.t.

$$n \leq \lambda_1 ; N_i = N_{i_u}^v; N_i^{obf} = N_{i_u}^{obf,w}; i_u = 1..|\mathbf{S}_u|; \mathbf{S}_u \in \mathbf{S}; v = 1..N_{max}; w = 1..N_{max}^{obf},$$

т.е. выбор варианта обфускации с соблюдением требований (1) и с максимальными расходами времени на его исчерпывающее моделирование злоумышленником.

Возможны и более сложные стратегии, учитывающие одновременно условия (2) и (3), а также дополнительные требования к проекту обфускации, в том числе с использованием λ_5. В силу конфликтов между обозначенными выше критериями поиск оптимального варианта не всегда возможен. Поэтому решение многокритериальных задач (1)–(3), а также сформулированных на их основе, зачастую представляют множеством допустимых решений с приоритетным доминированием критерия $\min_j(\lambda_3) \to 0$.

Заключение

В работе проведен анализ влияния перехода от вертикальной к горизонтальной модели производства ИС на цепочки поставок и риски внешних угроз для *OCM*. В качестве объекта исследования выделены АИС и рост их контрафактного производства – как проблема. Приведена классификация контрафактных микросхем. Рассмотрены методы устранения преднамеренных ошибок, негативно влияющих на характеристики доверенности АИС, и подходы к противодействию контрафактному производству АИС. Предложены стратегии выбора схем обфускации, основанные на многокритериальной оптимизации. Полученные результаты вносят вклад в развитие методов автоматизации проектирования для обеспечения доверенности (*DfTr – Design-for-Trust*) в рамках противодействия контрафактному производству.

СПИСОК ЛИТЕРАТУРЫ/REFERENCES:

1. Цветников, Михаил Ю; Францышин, Давид В. Анализ рынка доверенной электронной компонентной базы для объектов критической информационной инфраструктуры. Безопасность информационных технологий, [S.l.], т. 32, № 3, с. 180-197, 2025. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583//bit.2025.3.16.
   Tsvetnikov, Mikhail Yu.; Frantsyshin, David V. Trusted electronic component database market analysis for critical information infrastructure facilities. IT Security (Russia), [S.l.], v. 32, no. 3, pp. 180-197, 2025. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583//bit.2025.3.16 (in Russian).
2. Chiang, H., Zeng G. Worldwide Semiconductor Integrated Device Manufacturing Market: Top 10 Vendor Ranking and Insights, 1Q24. IDC, Aug. 2024. Doc # US51693624. URL: https://my.idc.com/research/viewtoc.jsp?containerId=US51693624 (accessed: 22.10.2025).
3. Хисамов, А., Назаренко А. Минифабы в микроэлектронике: история и возможности. Электроника: Наука, Технология, Бизнес. 2024, т. 232, № 1, с. 64-69. DOI: http://dx.doi.org/10.22184/1992-4178.2024.232.1.64.69.
   Khisamov A., Nazarenko A. Minifabs in microelectronics: history and opportunities. Electronics: Science, Technology, Business. 2024, v. 232. no. 1. pp. 64-69. DOI: http://dx.doi.org/10.22184/1992-4178.2024.232.1.64.69 (in Russian).
4. Akhoundov D. 2023 Annual Report. ERAI, Inc. URL: https://www.erai.com/erai_blog/3183/2023_annual_report (accessed: 22.10.2025).
5. Akhoundov D. 2024 Annual Report. ERAI, Inc. URL: https://www.erai.com/erai_blog/3187/_2024_annual_report (accessed: 22.10.2025).
6. 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, pp. 273-276. DOI: http://dx.doi.org/10.1109/EWDTS.2018.8524618.
7. Ланцов, В.Н., Мосин С.Г. Современные подходы к проектированию и тестированию интегральных микросхем: монография. Владимир: Изд-во Владим. гос. ун-та, 2010. – 285 с. – ISBN 978-5-9984-0120-6.
   Lancov, V.N., Mosin S.G. Sovremennye podkhody k proektirovaniyu i testirovaniyu integralnykh mikroskhem: monografiya. Vladimir: Izd-vo Vladim. gos. un-ta, 2010. 285 s. ISBN 978-5-9984-0120-6 (in Russian).
8. Никифоров, А., Телец В., Кессаринский Л., Левин Р., Бойченко Д. Концепция доверенной ЭКБ микроэлектроники – новой категории изделий электронной компонентной базы для регулируемых рынков критической информационной инфраструктуры. Электроника: Наука, Технология, Бизнес. 2025, № 7(248), с. 56-74. DOI: http://dx.doi.org/10.22184/1992-4178.2025.249.7.56.74.
   Nikiforov, A., Telets V., Kessarinsky L., Levin R., Boychenko D. The concept of trusted electronic component base as a new category of electronic component base products for regulated markets of critical information

infrastructure. Electronics: Science, Technology, Business. 2025, no. 7(248), pp. 56-74. DOI: http://dx.doi.org/10.22184/1992-4178.2025.249.7.56.74 (in Russian).
9. 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. DOI: http://dx.doi.org/10.26583/bit.2025.2.13.
Mosin, Sergey G. Trustworthy of integrated circuits: characteristics and reasons for their violation. IT Security (Russia), [S.l.], v. 32, no. 2, pp. 178-191, 2025. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2025.2.13 74 (in Russian).
10. Guin U., DiMase D., Tehranipoor M. Counterfeit Integrated Circuits: Detection, Avoidance, and the Challenges Ahead. J. Electron. Test. 2014, v. 30, pp. 9-23. DOI: http://dx.doi.org/10.1007/s10836-013-5430-8.
11. Московская, Юлия М.; Денисов, Андрей Н.; Никифоров, Александр Ю. Система обеспечения качества доверенного микроэлектронного производства. Безопасность информационных технологий, [S.l.], т. 31, № 1, с. 42-53, 2024. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2024.1.01.
Moskovskaia, Iuliia M.; Denisov, Andrey N.; Nikiforov, Alexander Yu. The quality assurance system of the trusted Microelectronic production. IT Security (Russia), [S.l.], v. 31, no. 1, pp. 42-53, 2024. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2024.1.01 (in Russian).
12. Rao V.V., Savidis I. Transistor sizing for parameter obfuscation of analog circuits. U.S. Patent 11157674 B2. Oct. 26, 2021.
13. Jayasankaran N. G., Borbon A. S., Sanchez-Sinencio E., Hu J., and Rajendran J. Towards provably-secure analog and mixed-signal locking against overproduction. 2018 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), San Diego, CA, USA. 2018, pp. 1-8. DOI: http://dx.doi.org/10.1109/TETC.2020.3025561.
14. Rao Nimmalapudi S. G., Volanis G., Lu Y., Antonopoulos A., Marshall A., Makris Y. Range-Controlled Floating-Gate Transistors: A Unified Solution for Unlocking and Calibrating Analog ICs. 2020 Design, Automation & Test in Europe Conference & Exhibition (DATE), Grenoble, France. 2020, pp. 286-289. DOI: http://dx.doi.org/10.23919/DATE48585.2020.9116251.
15. Jarvis R. and McIntyre M. G. Split manufacturing method for advanced semiconductor circuits. U.S. Patent 2004.0102019 A1. May 27, 2004.
16. Zhang X., Xiao K. and Tehranipoor M. Path-delay fingerprinting for identification of recovered ICs. 2012 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), Austin, TX, USA. 2012, pp. 13-18. DOI: http://dx.doi.org/10.1109/DFT.2012.6378192.
17. Sahoo S. R., Sudeendra K., Mahapatra A., Swain A. K., Mahapatra K. K. On-chip RO-Sensor for Recycled IC Detection. IEEE International Symposium on Nanoelectronic and Information Systems (iNIS), Bhopal, India. 2017, pp. 252-256. DOI: http://dx.doi.org/10.1109/iNIS.2017.60.
18. Alnuayri T., Khursheed S., Martínez A. L. H. and Rossi D. Differential Aging Sensor Using Subthreshold Leakage Current to Detect Recycled ICs. IEEE Transactions on Very Large Scale Integration (VLSI) Systems. 2021, v. 29, no. 12, pp. 2064-2075. DOI: http://dx.doi.org/10.1109/TVLSI.2021.3115247.
19. Dimopoulos A., Sima M., Neville S. W. A Small Tamper-Resistant Anti-Recycling IC Sensor With a Reused I/O Interface and DC Signalling. IEEE Open Journal of Circuits and Systems. 2024, v. 5, pp. 34-348. DOI: http://dx.doi.org/10.1109/OJCAS.2024.3487072.
20. Tahoori M., Zorian Y. Special Issue on Silicon Lifecycle Management. IEEE Design & Test. 2024, v. 41, no. 4, pp. 5-6. DOI: http://dx.doi.org/10.1109/MDAT.2024.3392620.
21. Zhang Z. et al. Addressing the Combined Effect of Transistor and Interconnect Aging in SRAM towards Silicon Lifecycle Management. IEEE 42nd VLSI Test Symposium (VTS), Tempe, AZ, USA. 2024, pp. 1-5, DOI: http://dx.doi.org/10.1109/VTS60656.2024.10538862.
22. Иванов, Михаил А. и др. Обфускация логических схем генераторов псевдослучайных чисел на регистрах сдвига с линейными и нелинейными обратными связями. Безопасность информационных технологий, [S.l.]. 2021, т. 28, № 1, с. 74-83. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2021.1.06.
Ivanov, Michael A. et al. Obfuscation of logic schemes of pseudo-random number generators based on linear and non-linear feedback shift registers. IT Security (Russia), [S.l.]. 2021, v. 28, no. 1, pp. 74-83. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2021.1.06 (in Russian).
23. Chaudhuri J., Bhattacharya M., Chakrabarty K. Enhancing Analog IC Security Using Randomized Obfuscation Circuits. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. 2025, v. 44, no. 3, pp. 867-881. DOI: http://dx.doi.org/10.1109/TCAD.2024.3466810.
24. Leonhard, J., Sayed A., Louërat M. -M., Aboushady H., Stratigopoulos H. -G. Analog and Mixed-Signal IC Security via Sizing Camouflaging. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. 2021, v. 40, no. 5, pp. 822-835. DOI: http://dx.doi.org/10.1109/TCAD.2020.3011662.

Конфликт интересов. *Авторы заявляют об отсутствии конфликта интересов.*
Conflict of interest. *The authors declare no conflict of interest.*

ИНФОРМАЦИЯ ОБ АВТОРАХ:

Сергей Геннадьевич Мосин, *д.т.н., доцент; профессор, Казанский (Приволжский) федеральный университет, заместитель генерального директора, ООО «ЛабСистемс».*
e-mail: smosin@ieee.org,
https://orcid.org/0000-0003-1389-2602,
Scopus Author ID: 8370098000.

Виталий Арсеньевич Телец, *д.т.н., профессор; директор Центра экстремальной прикладной электроники, Национальный исследовательский ядерный университет «МИФИ».*
e-mail: 1355t@mail.ru,
https://orcid.org/0000-0003-4944-676X,
Scopus Author ID: 6506571314.

INFORMATION ABOUT THE AUTHORS:

Sergey Gennadievich Mosin, *Doctor of Technical Sciences, Associate Professor; Professor, Kazan (Volga Region) Federal University, Deputy General Director, LabSystems LLC.*
e-mail: smosin@ieee.org,
https://orcid.org/0000-0003-1389-2602,
Scopus Author ID: 8370098000.

Vitaly Arsenyevich Telets, *Doctor of Technical Sciences, Professor; Director of the Center for Extreme Applied Electronics, National Research Nuclear University MEPhI (Moscow Engineering Physics Institute).*
e-mail: 1355t@mail.ru,
https://orcid.org/0000-0003-4944-676X,
Scopus Author ID: 6506571314.

Статья поступила в редакцию 01.12.2025; одобрена после рецензирования 12.01.2026; принята к публикации 20.01.2026
The article was submitted 01.12.2025; approved after reviewing 12.01.2026; accepted for publication 20.01.2026