Леонид Н. Кессаринский¹, Алексей О. Ширин², Кирилл А. Коваль³,
Фарид Ф. Тайибов⁴, Анна С. Каменева⁵

^{1, 2, 3}Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, г. Москва, 115409, Россия

^{4, 5}АО «ЭНПО СПЭЛС»,

Каширское ш., 31, г. Москва, 115409, Россия

¹e-mail: LNKessarinskiy@mephi.ru, <https://orcid.org/0000-0001-7756-6166>

²e-mail: Aoshir@spels.ru, <https://orcid.org/0000-0001-9121-0529>

³e-mail: Kirilloid53@yandex.ru, <https://orcid.org/0000-0003-3296-0340>

⁴e-mail: Fftai@spels.ru, <https://orcid.org/0000-0002-0370-4180>

⁵e-mail: ASPih@spels.ru, <https://orcid.org/0000-0002-0735-937X>

ВЫЯВЛЕНИЕ ПРИЗНАКОВ КОНТРАФАКТА В ИЗДЕЛИЯХ ЭЛЕКТРОННОЙ КОМПОНЕНТНОЙ БАЗЫ В АСПЕКТЕ ОБЕСПЕЧЕНИЯ ПРОМЫШЛЕННОЙ КИБЕРБЕЗОПАСНОСТИ

DOI: <http://dx.doi.org/10.26583/bit.2019.2.09>

Аннотация. В программе цифровизации экономик развитых стран выделяется относительно новое направление развития так называемых киберфизических систем управления, в частности, промышленными технологическими процессами, что мотивирует постановку нетрадиционных задач по обеспечению безопасности критически важных объектов информационной инфраструктуры. Очевидной угрозой потери устойчивости технологических процессов является использование контрафактной элементной базы в условиях наблюдаемого общего увеличения доли контрафактной продукции, в том числе и в изделиях электронной компонентной базы. Поэтому появляется объективный запрос на системное решение проблемы выявления контрафакта не только с позиций охраны объектов интеллектуальной собственности, но и в аспекте обеспечения промышленной безопасности в ходе сертификации соответствующих технических решений. Учитывая, что для испытательных центров и лабораторий такая постановка связана с организацией достаточно нового вида деятельности в условиях недостаточности соответствующей нормативной базы. В работе проведен обзор зарубежных нормативных документов, определяющих методы и средства выявления контрафакта в радиоизделиях, который может быть использован в качестве начальной основы для формирования отечественной нормативной базы.

Ключевые слова: идентификация, контрафакт, элементная компонентная база, микроэлектроника.

Для цитирования: КЕССАРИНСКИЙ, Леонид Н. et al. ВЫЯВЛЕНИЕ ПРИЗНАКОВ КОНТРАФАКТА В ИЗДЕЛИЯХ ЭЛЕКТРОННОЙ КОМПОНЕНТНОЙ БАЗЫ В АСПЕКТЕ ОБЕСПЕЧЕНИЯ ПРОМЫШЛЕННОЙ КИБЕРБЕЗОПАСНОСТИ. Безопасность информационных технологий, [S.l.], v. 26, n. 2, p. 117-128, 2019. ISSN 2074-7136. Доступно на: <<https://bit.mephi.ru/index.php/bit/article/view/1204>>. Дата доступа: 03 june 2019. doi:<http://dx.doi.org/10.26583/bit.2019.2.09>.

Leonid N. Kessarinskiy¹, Alexey O. Shirin², Kirill A. Koval³,
Farid F. Taiibov⁴, Anna S. Kameneva⁵,

^{1, 2, 3}National Research Nuclear University MEPHI
115409, Moscow, Kashirskoye shosse, 31

^{4, 5}JSC ENPO SPELS,

115409, Moscow, Kashirskoye shosse, 31

¹e-mail: LNKessarinskiy@mephi.ru, <https://orcid.org/0000-0001-7756-6166>

²e-mail: Aoshir@spels.ru, <https://orcid.org/0000-0001-9121-0529>

³e-mail: Kirilloid53@yandex.ru, <https://orcid.org/0000-0003-3296-0340>

⁴e-mail: Fftai@spels.ru, <https://orcid.org/0000-0002-0370-4180>

⁵e-mail: ASPih@spels.ru, <https://orcid.org/0000-0002-0735-937X>

**Counterfeit electronic components identifying methods in terms
of industrial cyber security**

DOI: <http://dx.doi.org/10.26583/bit.2019.2.09>

Abstract. The program of digitalization of the economies of developed countries highlights a relatively new direction of development of the so-called cyberphysical control systems, in particular, industrial technological processes, which motivates the formulation of non-traditional tasks to ensure the security of critical information infrastructure. The obvious threat of loss of stability of technological processes is the use of counterfeit components in a view of the observed overall increase in a volume of counterfeit products, including electronic components. Therefore, there is a clear request for a systematic solution to the problem of detecting counterfeit not only from the standpoint of the protection of intellectual property, but also in the aspect of industrial safety during the certification of appropriate technical solutions. Considering that for testing centers and laboratories this statement implies the organization of rather new type of activity under conditions of insufficiency of the corresponding regulatory base. The paper reviews the foreign normative documents defining the methods and means of detecting counterfeit in radio electronics, which can be used as the initial basis for the formation of the domestic regulatory framework.

Keywords: authentication, counterfeit, electronics components, microelectronics.

For citation: KESSARINSKIY, Leonid N. et al. Counterfeit electronic components identifying methods in terms of industrial cyber security. *IT Security (Russia)*, [S.l.], v. 26, n. 2, p. 117-128, 2019. ISSN 2074-7136. Available at: <<https://bit.mephi.ru/index.php/bit/article/view/1204>>. Date accessed: 03 june 2019. doi:<http://dx.doi.org/10.26583/bit.2019.2.09>.

Введение

Ежегодный рост доли контрафактных образцов элементной компонентной базы (ЭКБ), приходящих в испытательные лаборатории сформировался в устойчивый тренд, который может быть причиной снижения достоверности и эффективности работы поставщиков и сертификационных центров при отсутствии системного подхода к парированию проблемы [1-9]. При этом общее сокращение сроков испытаний ЭКБ приводит к тому, что подозрительные на контрафакт образцы и неоднородные выборки поступают даже в центры испытаний на стойкость к воздействию специальных факторов, что было редкостью еще пять лет назад. Одним из важнейших первых шагов системного подхода для противодействия контрафакту является анализ существующей отечественной и иностранной нормативной базы по методам и средствам выявления подозрительных образцов ЭКБ. К сожалению, в настоящее время в России недостаток национальных государственных стандартов, содержащих требования к испытательным лабораториям и определяющие методы и средства выявления контрафактных ЭКБ (отсутствуют за исключением [10–12], которые являются переводом стандартов SAE, описываемых ниже).

В то же время существует ряд международных стандартов, разработанных для борьбы с контрафактной продукцией в ЭКБ, появившихся как следствие переноса производственных мощностей микроэлектроники из стран Европы и США в Юго-Восточную Азию. Промышленность, особенно военный и аэрокосмический сегменты, была вынуждена создавать методы выявления контрафактных изделий. Но, поскольку контрафакция очень выгодна, фальсификаторы хорошо мотивированы изобретать все новые способы подделки. Это требует совершенствования методов выявления контрафактной микроэлектронной продукции, объединения усилий в их внедрении. В данной статье представлена попытка обзора системного подхода к выявлению контрафакта на основе международных стандартов (AS6171, AS5553 и др.) Общества инженеров автомобилестроителей (SAE), разработанных по заказу и успешно применяемых в аэрокосмической отрасли США.

1. Состояние дел с контрафактом в мире

Мировой объем торговли контрафактной и пиратской продукцией в мире, по данным Организации экономического сотрудничества и развития, в 2013 году составил 461 млрд долларов, а в 2017 году уже свыше 553 млрд долларов [13]. Исследование, проведенное «Business Week», показало, что поддельный продукт составляет не менее 7% от внешней мировой торговли [14]. В России, согласно данным Росстата, оборот контрафактной продукции в 2017 году приблизился к трем трлн рублей [15]. Контрафактная экспансия сказалась и на рынке электронных изделий.

Начало массовому появлению контрафактных изделий ЭКБ положил перенос производства микроэлектронных изделий и устройств из США и Европы в Юго-Восточную Азию. Сделано это было с целью удешевления производства (за счет дешевой рабочей силы). Но азиатские фабрики небольшие по масштабу, не имеют достаточных сил и средств для реализации всей технологической цепочки производства микроэлектронных изделий в рамках одного предприятия, поэтому отдельные этапы технологического передела осуществляются разными компаниями. Такое многообразие и разрозненность производителей изделий ЭКБ провоцируют появление контрафактных изделий.

Изготовление и сбыт контрафактных микроэлектронных изделий приносят высокий доход организаторам. В США в течение последних 10 лет в среднем более 1,4 млн экземпляров компонентов попадают под подозрение в контрафактном происхождении [16]. Такая активность привела к тому, что, как показано в другом исследовании, проведенном Министерством торговли США с 2005 по 2008 год, 50% производителей компонентов и 55% дистрибьюторов сталкивались с контрафактными компонентами [17]. Вместе с тем мировым трендом как в странах Запада, так и в России, является снижение стоимости электронных устройств военного применения, в том числе за счет использования микроэлектронных устройств широкого применения вместо специальных микроэлектронных устройств в военной технике. Но существовавшие неэффективные методы контроля аутентичности позволили контрафактным изделиям проникнуть и в эту сферу применения: эксперты оценили, что среди всех закупок Министерства обороны США запасных и сменных компонентов до 15% являются контрафактной продукцией [17].

2. Типы контрафактных изделий ЭКБ

Изделие ЭКБ, имеющее контрафактное происхождение, представляет собой несанкционированную копию подлинного изделия: не соответствует стандартам проектирования и качества функционирования авторизованного изготовителя, изготовлено неавторизованным производителем без согласия проектанта, не отвечает техническим условиям, является дефектным или бывшим в употреблении, которое поставляется под видом нового, имеет некорректную (поддельную) документацию или маркировку.

По признакам фальсификации контрафактную продукцию можно условно разделить на 7 категорий:

- бывшие в употреблении (повторно используемые);
- перемаркированные;
- бракованные;
- незаконно произведенные (в том числе выпущенные сверх контрактного объема и невостребованные заказчиком);
- клонированные;

- незаконно измененные (восстановленные);
- имеющие поддельную документацию.

К бывшим в употреблении (повторно используемым) и перемаркированным изделиям ЭКБ относятся демонтированные с печатных плат изделия с перекрашенными корпусами, удаленной и нанесенной заново маркировкой. В некоторых случаях кристаллы могут быть перенесены из одних корпусов в другие, с другой маркировкой. Эти изделия, проданные под видом новых, в лучшем случае не обеспечивают необходимых ресурса и производительности, а худшем – приводят к неработоспособности электронного устройства. Перемаркированные изделия могут быть как той же марки, что и исходное изделие, так и выдаваемыми за изделия более высокой категории, а значит, более дорогими.

К незаконно произведенным относятся в первую очередь изделия выпущенные производителем, получившим доступ к интеллектуальной собственности компании-разработчика, но не имеющего договорных отношений с дизайн-центром. Часто эти изделия не проходят испытаний в условиях, определенных разработчиком, и не достигают функциональных характеристик прежде всего по надежности и долговечности работы. Второй разновидностью незаконно произведенных изделий являются изделия, имеющие дефекты и подлежащие отбраковке, но попавшие на рынок.

К незаконно произведенным относятся и изделия, которые могут содержать аппаратные незадекларированные возможности (так называемые закладки).

Клонированные изделия выпущены производителем, не обладающим законными правами на использование чужой интеллектуальной собственности. Клонирование осуществляется методом обратного проектирования или путем нарушения авторских прав.

Самый простой, а потому распространенный способ фальсификации – подделка документации, при котором изменяется спецификация на изделие. Выявить кристаллы с поддельной спецификацией можно при испытаниях, но при отсутствии методики испытания, созданной авторизованным производителем, способ становится высокочувствительным.

В настоящее время распространены два типа контрафактных изделий ЭКБ – перемаркированные бывшие в употреблении изделия, проданные под видом новых (примерно 80% всех подделок) и незаконно произведенные, не соответствующие техническим требованиям производителя.

3. Обзор методов выявления контрафактных изделий

Используемые в настоящее время методы обнаружения контрафактных изделий, использованные при появлении первых фальшивых партий, актуальны и в наше время, поскольку позволяют выявить большую часть подделок. Каждый тип фальсификации оставляет характерные отметки, которые методики проверки и испытаний призваны обнаружить.

Все методы выявления контрафактных изделий можно условно разделить на «традиционные» и «сравнительные». К традиционным можно отнести методы, которые служили другим целям, но с появлением фальсификата были адаптированы для его обнаружения. В большинстве случаев они могут вполне эффективно применяться даже при отсутствии подлинного образца для сравнения. Сейчас они стали общепринятыми.

К сравнительным методам можно отнести специально разработанные методы выявления контрафактных изделий. Но практически все эти методы хорошо работают,

если имеется достоверная подлинная база для сравнения, поскольку они фокусируются на тонких различиях между подлинным и поддельным изделиями.

Конечно, такое разделение методов весьма условно, и каждая испытательная лаборатория сама выбирает тот набор методов, который наиболее подходит для нее. Ограничениями здесь служат бюджет, выделяемый на испытания, и время проведения испытаний.

Традиционные методы выявления контрафактных изделий

– *Предварительная проверка документации*

Этап проверки, который трудно переоценить. На данном этапе проверяется не только подлинность сопровождающих документов, но и их легитимность: существует ли такой производитель, как напечатан документ, насколько производитель легитимен, выпускал ли он в указанное время указанный тип изделия и т.д.

– *Визуальный внешний осмотр, проверка на перемаркировку и шлифовку*

Самый недорогой и быстрый метод обнаружения дефектов контрафактного происхождения. Из оборудования требуется только оптический микроскоп. Очень важен также опыт испытателя, так как признаки подделки часто едва заметны.

К визуально-оптическому методу примыкают методы обнаружения перемаркировки / шлифовки изделий. Применение таких видов фальсификации относится в основном к микросхемам в пластиковых корпусах: химически или механически у корпуса микросхемы снимается верхняя часть для уничтожения оригинальной маркировки, затем верхняя плоскость шлифуется или заменяется на новый слой («блэктоппинг») и на ней выполняется новая маркировка. Для выявления перемаркировки проводится испытание на устойчивость к растворителям, для выявления блэктоппинга применяется тест на ацетон.

Если перемаркировка осуществляется лазером, то глубина новой маркировки отличается от аутентичной, и на корпусе могут остаться следы прожогов, что также должно быть выявлено испытателем.

Очень часто использование визуально-оптического метода совмещено с контролем массы образцов ЭКБ, выявлением таким методом неоднородностей выборок для испытаний.

– *Электрические испытания*

К этому виду испытаний относятся функциональный и параметрический анализы параметров изделия ЭКБ, выполняемые на испытательных стендах. Важным аспектом является выделение критичных параметров - критериев годности (ПКГ) изделий, существенно определяющих функционал и трудность подделки образцов. Идеальным является проведение контроля всех параметров ЭКБ в объеме технических условий или «datasheet» в диапазоне рабочих температур. Опыт работы испытателя с различными классами ЭКБ, знание стандартов по измерению ПКГ и функциональному контролю является важным фактором при составлении программы испытаний.

Смежным с электрическими испытаниями является метод измерения радиочастотных характеристик, предложенный и запатентованный коллегами «18 ЦНИИ» МО РФ [18–21]. Для повышения достоверности распознавания клонированных изделий микроэлектроники в параметрический анализ включен метод сравнения по s-параметрам. Оценивается импульсный отклик «четырёхполосника», который связан с АЧХ. Причем доказано, что отклики, связанные с контрафактным происхождением, находятся за пределами статистических отклонений откликов, вызванных технологическими вариациями процесса изготовления.

– Рентгеновский контроль

Рентгеновский контроль изделия ЭКБ позволяет максимально просто увидеть внутренние структуры. Рентгеновская проверка становится еще более эффективной, когда сомнительные изделия можно сравнить с известным подлинным изделием.

– Физический анализ и декапсуляция

Эти методы испытаний относятся к разрушающим и выполняются на отобранных из партии образцах. Оптимальным путем проведения идентификации изделий является применение разрушающих методов на образцах, уже прошедших испытания на стойкость к внешним воздействующим факторам. Декапсуляция может быть осуществлена путем механического или химического удаления крышки или верхних слоев корпуса компонента, чтобы обеспечить доступ к кристаллу (микросхема, транзистор и т.д.) и/или внутренним структурам компонента (модуль, микросборка и т.д.). Декапсулированные изделия проверяются на соответствие номеров партий, даты изготовления, заводских меток. Кроме того, оценивается внешний вид и расположение кристалла.

– Сканирование электронным микроскопом

Позволяет более полно и детально исследовать микроскопические внутренние структуры изделий ЭКБ. В сочетании с энергодисперсионной рентгеновской спектроскопией метод позволяет сравнивать микроскопические области изделия по химическому составу.

– Рентгенофлуоресцентный анализ

Этот метод используется, как и энергодисперсная рентгеновская спектроскопия (ЭДС) для идентификации элементарных компонентов изделий ЭКБ. Но размер пятна измерения у рентгенофлуоресцентного спектрографа намного больше, чем у энергодисперсного, что делает его не таким эффективным при исследовании внутренних структур тем не менее его намного проще использовать, чем энергодисперсную спектрографию, и оборудование стоит гораздо дешевле. Это делает рентгенофлуоресцентный анализ очень удобным методом.

Сравнительные методы выявления контрафактных изделий

– Проверка качества маркировки

Проверка выполняется аналогично ранее описанным методам, но с использованием новых химических соединений, увеличенного времени воздействия (до нескольких часов) и воздействия при нагревании, в том числе – окунанием.

– Инфракрасная спектроскопия с Фурье-преобразованием

Инфракрасная спектроскопия с Фурье-преобразованием – метод, используемый для идентификации органических соединений. Полимеры, которые составляют корпус микросхемы и материал для блоттинга («вставок»), используемый для сокрытия признаков подделки, являются органическими материалами, а также для обнаружения органических загрязнителей на контрафактном изделии.

– Ионная хроматография

Этот метод используется для обнаружения ионного загрязнения, которое обычно присутствует в форме солей или органических кислот и может откладываться на изделии при обработке или применении химикатов во время процесса фальсификации.

– Акустическая микроскопия

Акустическая микроскопия позволяет фокусировать звуковые волны на разных глубинах внутри образца и обнаружить потенциальные неровности и пустоты. Также можно выявить вновь нанесенное покрытие после удаления маркировки (блэктоппинг), растрескивание и расслоение в корпусе изделия.

– Дифференциальная сканирующая калориметрия

Дифференциальная сканирующая калориметрия измеряет химические реакции как функцию температуры. Реакции, такие как температура плавления, температура стеклования, кристалличность и теплоемкость, являются свойствами, присущими определенным полимерам, которые можно измерить. Если фальсификатор изменил корпус микросхемы, добавив другой полимер, дифференциальная сканирующая калориметрия может обнаружить это изменение.

– Термогравиметрический анализ

Термогравиметрический анализ измеряет потерю веса образца в зависимости от температуры. Этот метод полезен тем, что разные полимеры разлагаются (теряют вес) при разных температурах. Опять же при сравнении корпуса сомнительного изделия с подлинным изделием, если корпус изделия был изменен, метод может сделать эти различия очевидными.

– Термомеханический анализ

Термомеханический анализ измеряет изменение размеров в зависимости от температуры. Двумя важными свойствами, которые могут быть показательными, являются температура размягчения и коэффициент теплового расширения полимера. Различные полимеры или даже один и тот же полимер с разными количествами наполнителей будут давать разные температуры размягчения и теплового расширения.

4. Обоснование выбора методов, входящих в комплекс испытаний для выявления контрафактных изделий ЭКБ

Важной задачей испытательной лаборатории является выбор методологии испытаний изделий электронной компонентной базы на наличие признаков контрафактного происхождения. Речь идет о комплексном исследовании изделий ЭКБ, так как ни один метод выявления, каким бы мощным он ни был с точки зрения аппаратного оснащения, не является достаточным. Признаки контрафактного происхождения могут проявляться совершенно по-разному, поэтому необходимо применение именно комплексных проверок и испытаний.

Важными факторами при выборе методов испытаний являются время испытаний, которое должно быть приемлемым для заказчиков, связанных сроками производства, а также стоимость испытаний, так как заказчики ограничены бюджетом.

При выборе методов испытаний для формирования оптимального комплекса применена концепция приемлемого уровня риска при выявлении изделий контрафактного происхождения в партии однородных изделий, разработанная Юджволом Гуином и др. [22]. Концепция легла в основу технического меморандума SAE AS6171:2016 [23] и рекомендована к применению в аэрокосмической промышленности. Согласно этой концепции для большинства изделий ЭКБ выбирается средний уровень риска при выявлении контрафактного изделия. Из технического меморандума SAE AS6171:2016tm следует, что средний уровень риска предполагает, что изделия ЭКБ поступают от авторизованного или франчайзингового дилера, имеющего внутреннюю систему качества, не упомянутого в отчетах о недобросовестных поставщиках и публикациях в технических изданиях, из промышленно развитого региона, в том числе и из Юго-Восточной Азии (кроме провинции Гаунджоу, КНР), применяются для электронных устройств общего назначения, потеря работоспособности которых не может привести к катастрофическим последствиям.

Среднему уровню риска соответствует следующий комплекс методов испытаний:

Документальный контроль. Контролю подлежат не только документация, но и элементы фирменного стиля производителя, качество печати и штампов, правдоподобность номеров и дата изготовления партий изделий.

Визуально-оптический контроль. Визуальному контролю подвергаются не только изделия, но и, если есть возможность, фирменная упаковка.

Определение перемаркировки или шлифовки корпусов изделий микроэлектроники, в том числе – химические испытания на стойкость маркировки и отсутствие блэктоппинга.

Измерение геометрических размеров и точное взвешивание. Как показывает опыт применения этих методов, разброс размеров и веса изделий ЭКБ, вызванный технологической нестабильностью, значительно меньше отклонений этих параметров, вызванных доработкой при восстановлении или клонированием [24, 25].

2D Рентгеноскопия. Позволяет исследовать внутреннюю структуру изделия, в том числе расположение кристалла. Помимо неправильного соединения проводников, неправильного расположения элементов и неоднородности материала, наличия пустот в материале, прикрепляемом к матрице, или герметизации этот метод позволяет выявить наличие внедренных посторонних элементов.

Функциональный и параметрический контроль. Исследуются не только электрические характеристики изделий при различных температурах, но и временной «дрейф» параметров.

Декапсуляция для получения доступа непосредственно к кристаллу, изучение его идентификационной маркировки, геометрического размещения.

Аналогичный по составу комплекс испытаний определен ГОСТ 57880 -2017, приложение Е.1. Эти же виды испытаний считаются базовыми при условии отсутствия достоверного образца для сравнения, т.е. образцов изделий, представленных подлинным изготовителем [26, 27].

Как показано в работе [28], выбранный комплекс испытаний позволяет выявлять контрафактные изделия с приемлемым уровнем риска 73–75%. Усиление методов визуально-оптического контроля применением точного взвешивания и измерений геометрических размеров позволяет повысить уровень риска при выявлении контрафактных изделий до 80%.

Обозначенный выше комплекс методов проверок и испытаний может быть определен как базовый. В случае возникновения подозрения в сомнительности изделия, или если заказчик определил более высокий уровень риска, базовый комплекс дополняется более мощными методами:

- если в результате визуально-оптического осмотра были обнаружены признаки использования запрещенных материалов, особенно в материале выводов, в свинцовой отделке, таких как появление «усов», вызванных присутствием олова, подмена дорогих материалов выводов (золото, палладий) дешевыми (алюминий) с соответствующим изменением вида выводов, то может быть принято решение об испытаниях на рентгеновском флуоресцентном оборудовании;

- если в результате исследований рентгеноскопией выявлена сомнительная топология изделия или присутствие посторонних элементов, то может быть применен метод испытаний на радиологической отклик.

На уровень риска при выявлении контрафактных изделий существенно влияет репрезентативный объем выборки от партии изделий для проведения испытаний.

Мы придерживаемся методологии осуществления выборки образцов изделий в части репрезентативного объема, изложенной в [29, 30], где для партий изделий более 200 штук применяется выборка в 119 штук на неразрушающие методы контроля, 45 штук

– на электрические и параметрические испытания и 3 штуки – на разрушающие методы контроля. Такой объем выборки позволяет обеспечить 90% достоверность того, что процент контрафактных изделий в партии не превысит 2%. При меньших объемах партий выборки пропорционально уменьшаются так, чтобы с 90% достоверностью обеспечить процент контрафактных изделий не более 5%.

Как показывают некоторые источники, вероятность появления контрафактных изделий можно оценить в 15% [17]. При указанном объеме выборки для ожидаемого значения отклонения от нормального качества в 15%, уровень допустимого разброса в 2% является вполне достижимым [17], а значит выборка репрезентативна.

Заключение

Проведен обзор основных российских и иностранных нормативных документов, определяющих методы и средства выявления признаков контрафакта в изделиях ЭКБ. Международным лидером в составлении нормативной документации является международное Общество инженеров автомобилестроителей (SAE), чьими услугами по разработке стандартов прибегают другие отрасли промышленности, в т.ч. аэрокосмические предприятия США.

Обзор литературных данных доказывает, что существует устойчивый рост числа контрафактных радиоизделий, поступающих в испытательные и сертификационные центры. В тоже время анализ состояния отечественной нормативной базы выявил недостаточность документов уровня национального стандарта (ГОСТ), определяющих методы и средства выявления контрафактной элементной базы. Большинство испытательных лабораторий выпускают собственные методики и стандарты предприятий, ориентируясь на документы SAE.

Таким образом, показана объективная необходимость разработки национального стандарта по методам и средствам выявления контрафактной продукции ЭКБ с учетом эффективности существующих и используемых на практике методик.

СПИСОК ЛИТЕРАТУРЫ:

1. Лактионов А.В., Левин Р.Г., Емельянова И.В., Ершов Л.А., Малютенкова С.Э. Опыт выявления электронных компонентов с признаками контрафактного происхождения в ИЦ АО «РНИИ «Электронстандарт». Петербургский журнал электроники № 1 (90) 2018. С. 27–46.
2. Венедиктов К.А., Голубев А.А., Емельянова И.В., Малютенкова С.Э., Лактионов А.В., Звягина М.И., Ямщиков Ю.А. Выявление контрафактных электронных компонентов методами физикотехнического анализа. Доклад на международной научно-технической конференции «Пути решения задач обеспечения современной радиоэлектронной аппаратуры надежной электронной компонентной базой» «СЕРТИФИКАЦИЯ ЭКБ-2017». «РНИИ «Электронстандарт», Санкт-Петербург, 2017 г.
3. Ершов Л., Левин Р., Батулин А., Коломенская Н., Емельянова И., Кононов В. Что такое контрафакт и как с ним бороться. Нормативная основа и практика выявления контрафактных электронных компонентов. Электроника: наука, технология, бизнес. № 6 (156) 2016. Техносфера, Москва, С. 88–93.
4. Малинин В.Г. Методы выявления контрафактной электронной компонентной базы иностранного и отечественного производства при поставках для комплектации аппаратуры особо надежных объектов. Тезисы докладов IV Всероссийской научно-технической конференции секции ЭКБ «Импортозамещение. Обеспечение предприятий промышленности электронной компонентной базой отечественного производства», «Тестприбор», Москва, 2015 г. С. 63–68.
5. Балыбин С.В., Белов Е.Н., Федорев В.Н. Проблемы информационной безопасности военной техники, использующей интегральные схемы иностранного производства. Военная мысль. № 12 2011. С. 11–21.
6. Белов Е.Н., Пономарев А.А., Семенов А.В., Федорев В.Н. Угрозы информационной безопасности вооружения и военной специальной техники, укомплектованных электронной компонентной базой иностранного производства. Военная мысль. № 12 2013. С. 35–43.

7. Перспективные технологии защиты микросхем от обратного проектирования в контексте информационной безопасности [Текст] / Е.Н. Белов, С.В. Балыбин, А.А. Пономарев [и др.]; под ред. В.Н. Федорца. – М.: Техносфера, 2017. 215 с.
8. Кессаринский, Леонид Н. et al. Идентификация элементной компонентной базы киберфизических систем. Безопасность информационных технологий, [S.l.], v. 25, n. 3, p. 67-78, 2018. ISSN 2074-7136. URL: <<https://bit.mephi.ru/index.php/bit/article/view/1141>> (дата обращения: 12.02.2019). doi:<http://dx.doi.org/10.26583/bit.2018.3.07>.
9. Дураковский А.П., Кессаринский Л.Н., Ширин А.О., Артамонов А.С., Бойченко Д.В., Тайилов Ф.Ф. Идентификация элементной компонентной базы с целью исключения контрафакта и анализа результатов радиационных испытаний. Актуальные направления развития систем охраны, специальной связи и информации для нужд органов государственной власти Российской Федерации: XI Всероссийская межведомственная научная конференция: материалы и доклады (Орёл, 5–6 февраля 2019 года). В 10 ч. Ч. 5 / под общ. ред. П. Л. Малышева. – Орёл: Академия ФСО России, 2019. С. 65–67.
10. ГОСТ Р 57880-2017 Система защиты от фальсификаций и контрафакта. Электронные изделия. Предотвращение получения, методы обнаружения, сокращение рисков применения и решения по использованию фальсифицированной и контрафактной продукции.
11. ГОСТ Р 57881-2017 Система защиты от фальсификаций и контрафакта. Термины и определения.
12. ГОСТ Р 57882-2017 Система защиты от фальсификации и контрафакта. Изделия электронные. Критерии верификации для оценки соответствия практики и методов организаций требованиям по противодействию обороту фальсифицированной и контрафактной продукции.
13. Материалы VI Международного форума «Антиконтрафакт – 2018». Итоговые документы. Москва. С. 155.
14. Урличич Ю., Данилин Н., Чернов Д., Белослудцев С. Контрафактная продукция на рынке электронных компонентов. Современная электроника № 5/2006. С. 7.
15. Материалы VI Международного форума «Антиконтрафакт – 2018». Итоговые документы. Москва. С. 33.
16. Рыков И. Как выявить контрафактные электронные компоненты? Технологии в электронной промышленности. № 4/2013. С. 75.
17. Boby A. Detection and Avoidance Measures of IC Counterfeits: A Survey. Australian Journal of Basic and Applied Sciences, 8 (18) December 2014. P. 37–42.
18. Семенов А.В., Федорцов В.Н. Выявление контрафакта внутри однородной партии микросхем при измерении s-параметров. «Проблемы разработки перспективных микро – и нанoeлектронных систем. (МЭС)» №3/2014, С. 21–24.
19. Семенов А.В., Федорцов В.Н., Старцев В.Н. Контроль однородности партии типовых микросхем при измерении радиочастотных характеристик. «Проблемы разработки перспективных микро- и нанoeлектронных систем. (МЭС)» № 3/2016. С. 49–56.
20. Семенов А.В., Старцев В.Н., Степанов Е.Н. Технометрическая идентификация микросхем для контроля жизненного цикла и поиска контрафакта. «Проблемы разработки перспективных микро – и нанoeлектронных систем. (МЭС)» №4/2018. С. 143–148.
21. Семенов А.В., Балыбин С.В., Потапов А.Ю., Федорцов В.Н. Способ контроля идентичности изделий в партии однотипных микросхем. Патент № RU 179137 U1.
22. Ujjwal Guin, Daniel DiMase, Mohammad Tehranipoor. “A Comprehensive Framework for Counterfeit Defect Coverage Analysis and Detection Assessment”. Journal of Electronic Testing. February 2014. DOI 10.1007/s10836-013-5428-2.
23. Руководящий материал. AS6171:2016. Табл.6, 7. Test Methods Standard; General Requirements, Suspect/Counterfeit, Electrical, Electronic, and Electromechanical Parts. SAE International.
24. Фролова А. «Основные методы определения контрафактной продукции. Из практики испытательной лаборатории ООО «ПетроИнТрейд». Вестник электроники № 3 /2011. С. 44–46.
25. Поддельные микросхемы ST TDA7293. Вскрытие показало. Радиодетали и электронные компоненты. Обзор. 12 мая 2018 г. www.Akinava.ru.
26. John M. Radman and Daniel D. Phillips. Новые подходы к обнаружению контрафактных электронных компонентов. Журнал «IN COMPLIANCE», OCTOBER 2010.
27. Даниэль Оливье. «5 методов, используемых для обнаружения контрафактных электронных компонентов». Бюллетень «JJS manufacturing»: URL: <https://www.jjsmanufacturing.com> (дата обращения: 15. 03. 2018 г.)
28. Zhang X., Xiao K., Tehranipoor M. Path-delay fingerprinting for identification of recovered ICs // Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), 2012 IEEE International Symposium. 3-5 Oct. 2012. P. 13–18. doi: 10.1109/DFT.2012.6378192.)
29. Кононов В.К., Ершов Л.А., Левин Р.Г. и др. Новые стандарты в области подтверждения соответствия и предотвращения контрафакта и подделок. Петербургский журнал электроники, 1/2015. С. 30–46.

REFERENCES:

- [1] Laktionov A.V., Levin, R.G., Emelyanova I.V., Ershov, L.A., Malyenkov S. E. Experience in identifying electronic components with signs of counterfeit origin in IC JSC " RNI "Elektronstandart". *Peterburgskiy zhurnal elektroniki* № 1 (90) 2018. P. 27–46. (in Russian).
- [2] Venediktov K.A., Golubev A.A., Yemel'yanova I.V., Malyutenkova S.E., Laktionov A.V., Zvyagina M.I., Yamshchikov YU.A. Identification of counterfeit electronic components by methods of physical and technical analysis. *Doklad na mezhdunarodnoy nauchno-tekhnicheskoy konferentsii «Puti resheniya zadach obespecheniya sovremennoy radioelektronnoy apparatury nadezhnoy elektronnoy komponentnoy bazoy» «SERTIFIKATSIYA EKB-2017»*. «RNII «Elektronstandart», Sankt-Peterburg, 2017. (in Russian).
- [3] Yershov L., Levin R., Baturin A., Kolomenskaya N., Yemel'yanova I., Kononov V. What is counterfeit and how to deal with it. The regulatory framework and the practice of identifying counterfeit electronic components. *Elektronika: nauka, tekhnologiya, biznes*. № 6 (156) 2016. Tekhnosfera, Moskva. P. 88–93. (in Russian).
- [4] Malinin V.G. Methods for identifying counterfeit electronic component base of foreign and domestic production in deliveries to complete the equipment of especially reliable objects. *Tezisy dokladov IV vserossiyskoy nauchno-tekhnicheskoy konferentsii sektsii EKB «Importozameshcheniye. Obespecheniyepredpriyatiy promyshlennosti elektronnoy komponentnoy bazoy otechestvennogo proizvodstva»*, «Testpribor», Moskva, 2015 g. P. 63–68. (in Russian).
- [5] Balybin S.V., Belov E.N., Fedorets V.N. Problems of information security of military equipment using integrated circuits of foreign manufacture. *Voyennaya mysl'*. №12 2011. P. 11–21. (in Russian).
- [6] Belov E.N., Ponomarev A.A., Semenov A.V., Fedorets V.N. Threats to the information security of weapons and military special equipment, equipped with a foreign-made electronic component base. *Voyennaya mysl'*. № 12 2013. P. 35–43. (in Russian).
- [7] Advanced technologies for protecting circuits from reverse engineering in the context of information security. Ye. N. Belov, S.V. Balybin, A.A. Ponomarev [i dr.]; pod red. V.N. Fedortsa. – Moskva: Tekhnosfera, 2017. 215 p. (in Russian).
- [8] Kessarinskiy, Leonid N. et al. Authentication of electronics components for cyber-physical systems. *IT Security (Russia)*, [S.l.], v. 25, n. 3, p. 67-78, 2018. ISSN 2074-7136. URL: <<https://bit.mephi.ru/index.php/bit/article/view/1141>> (accessed: 12.02.2019). doi:<http://dx.doi.org/10.26583/bit.2018.3.07>. (in Russian).
- [9] Durakovskiy A. P., Kessarinskiy L. N., Shirin A. O., Artamonov A. S., Boychenko D. V., Tayibov F. F. Identification of the element component base in order to eliminate counterfeit and analyze the results of radiation tests. *Aktual'nyye napravleniya razvitiya sistem okhrany, spetsial'noy svyazi i informatsii dlya nuzhd organov gosudarstvennoy vlasti Rossiyskoy Federatsii: XI Vserossiyskaya mezhvedomstvennaya nauchnaya konferentsiya: materialy i doklady (Orol, 5–6 fevralya 2019 goda)*. V 10 ch. CH. 5 pod obshch. red. P. L. Malysheva. – Orol: Akademiya FSO Rossii, 2019. P. 65–67. (in Russian).
- [10] GOST R 57880-2017 System of protection against fraud and counterfeit. *Elektronnyye izdeliya. Predotvrashcheniye polucheniya, metody obnaruzheniya, sokrashcheniye riskov primeneniya i resheniya po ispol'zovaniyu fal'sifitsirovannoy i kontrafaktnoy produktsii*. (in Russian).
- [11] GOST R 57880-2017 System of protection against fraud and counterfeit. *Terminy i opredeleniya*. (in Russian).
- [12] GOST R 57880-2017 System of protection against fraud and counterfeit. *Izdeliya elektronnyye. Kriterii verifikatsii dlya otsenki sootvetstviya praktiki i metodov organizatsiy trebovaniyam po protivodeystviyu oborotu fal'sifitsirovannoy i kontrafaktnoy produktsii*. (in Russian).
- [13] Materialy VI Mezhdunarodnogo foruma «Antikontrafakt – 2018». *Itogovyye dokumenty*. Moskva. P. 155. (in Russian).
- [14] Urlichich YU., Danilin N., Chernov D., Belosludtsev S. Counterfeit products in the market of electronic components. *Sovremennaya elektronika* № 5/2006. P. 7. (in Russian).
- [15] Materialy VI Mezhdunarodnogo foruma «Antikontrafakt – 2018». *Itogovyye dokumenty*. Moskva. P. 33. (in Russian).
- [16] I. Rykov. How to identify counterfeit electronic components? *Tekhnologii v elektronnoy promyshlennosti*. № 4/2013. P. 75. (in Russian).
- [17] Boby A. Detection and Avoidance Measures of IC Counterfeits: A Survey. *Australian Journal of Basic and Applied Sciences*, 8 (18) December 2014. P. 37–42.
- [18] Semenov A.V., Fedorets V.N. Detection of counterfeit within a homogeneous batch of chips in the measurement of s - parameters. «Problemy razrabotki perspektivnykh mikro – i nanoelektronnykh sistem. (MES)» №3/2014. P. 21–24. (in Russian).

- [19] Semenov A.V., Fedorets V.N., Startsev V.N. Control of uniformity of a batch of typical microcircuits when measuring radio frequency characteristics. Problemy razrabotki perspektivnykh mikro – i nanoelektronnykh sistem. (MES)» №3/2016, P. 49–56. (in Russian).
- [20] Semenov A.V., Startsev V.N., Stepanov Ye.N. Technometric identification of microcircuits for life cycle monitoring and searching for counterfeit. «Problemy razrabotki perspektivnykh mikro – i nanoelektronnykh sistem. (MES)» № 4/2018. P. 143–148. (in Russian).
- [21] Semenov A.V., Balybin S.V., Potapov A. YU., Fedorets V. N. The method of controlling the identity of products in the batch of the same type of chips. Patent № RU 179137 U1. (in Russian).
- [22] Ujjwal Guin, Daniel DiMase, Mohammad Tehranipoor. “A Comprehensive Framework for Counterfeit Defect Coverage Analysis and Detection Assessment”. Journal of Electronic Testing. February 2014. DOI 10.1007/s10836-013-5428-2.
- [23] SAE Standart AS6171:2016. Test Methods Standard; General Requirements, Suspect/Counterfeit, Electrical, Electronic, and Electromechanical Parts. SAE International.
- [24] A. Frolova. «Osnovnyye metody opredeleniya kontrafaktnoy produktsii. Iz praktiki ispytatel'noy laboratorii OOO «PetroInTreyd». Vestnik elektroniki № 3 2011g. P. 44–46. (in Russian).
- [25] Poddel'nyye mikroskhemy ST TDA7293. Vskrytiye pokazalo. Radiodetali i elektronnyye komponenty. Obzor. 12 maya 2018 g. www.Akinava.ru. (in Russian).
- [26] John M. Radman and Daniel D. Phillips. Novyye podkhody k obnaruzheniyu kontrafaktnykh elektronnykh komponentov. Zhurnal «IN COMPLIANCE», OCTOBER 2010.
- [27] Danielle Olivier. «5 techniques used to detect counterfeit electronic components». Byulleten' «JJS manufacturing»: <https://www.jjsmanufacturing.com> (accessed:15.03.2018).
- [28] Zhang X., Xiao K., Tehranipoor M. Path-delay fingerprinting for identification of recovered ICs. Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), 2012 IEEE International Symposium. 3-5 Oct. 2012. P. 13–18. doi: 10.1109/DFT.2012.6378192.)
- [29] Kononov V.K., Yershov L.A., Levin R.G. i dr. New standards in the field of conformity assessment and prevention of counterfeit and fakes. Peterburzhskiy zhurnal elektroniki, 1/2015. P. 30–46. (in Russian).

*Поступила в редакцию – 27 мая 2019 г. Окончательный вариант – 31 мая 2019 г.
Received – May 27, 2019. The final version – May 31, 2019.*