Анатолий П. Дураковский[1], Леонид Н. Кессаринский[2], Алексей О. Ширин[3]
[1,2,3]Национальный исследовательский ядерный университет «МИФИ», Каширское ш., 31, Москва, 115409, Россия
[1]e-mail: APDurakovskiy@mephi.ru, https://orcid.org/0000-0002-8311-7735
[2]e-mail: LNKessarinskiy@mephi.ru, https://orcid.org/0000-0001-7756-6166
[3]e-mail: Aoshir@spels.ru, https://orcid.org/0000-0001-9121-0529

РАЗВИТИЕ ТЕРМИНОЛОГИИ НОРМАТИВНОЙ БАЗЫ ИСПЫТАНИЙ НА ВЫЯВЛЕНИЕ ПРИЗНАКОВ КОНТРАФАКТА В ИЗДЕЛИЯХ ЭЛЕКТРОННОЙ КОМПОНЕНТНОЙ БАЗЫ АППАРАТУРЫ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

DOI: http://dx.doi.org/10.26583/bit.2020.1.02

Аннотация. Целью статьи является разработка предложений по формированию нормативного поля систем защиты от фальсификаций и контрафактной продукции, однозначно понимаемого набора терминов, сокращений и определений на основе гармонизированных отечественных и зарубежных стандартов в этой области. 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 (ЭКБ). Предлагается подход системного решения 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 задачи 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 ЭКБ, который может быть использован в качестве начальной основы для формирования отечественной нормативной базы.

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

Для цитирования: ДУРАКОВСКИЙ, Анатолий П.; КЕССАРИНСКИЙ, Леонид Н.; ШИРИН, Алексей О. РАЗВИТИЕ ТЕРМИНОЛОГИИ НОРМАТИВНОЙ БАЗЫ ИСПЫТАНИЙ НА ВЫЯВЛЕНИЕ ПРИЗНАКОВ КОНТРАФАКТА В ИЗДЕЛИЯХ ЭЛЕКТРОННОЙ КОМПОНЕНТНОЙ БАЗЫ АППАРАТУРЫ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ. Безопасность информационных технологий, [S.l.], v. 27, n. 1, p. 19-27, 2020. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1249>. Дата доступа: 10 feb. 2020. DOI:http://dx.doi.org/10.26583/bit.2020.1.02.

Anatoly P. Durakovskiy[1], Leonid N. Kessarinskiy[2], Alexey O. Shirin[3]
[1,2,3]National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Kashirskoye shosse, 31, Moscow, 115409, Russia
[1]e-mail: APDurakovskiy@mephi.ru, https://orcid.org/0000-0002-8311-7735
[2]e-mail: LNKessarinskiy@mephi.ru, https://orcid.org/0000-0001-7756-6166
[3]e-mail: Aoshir@spels.ru, https://orcid.org/0000-0001-9121-0529

Terms and definitions base development for counterfeit electronics test for critical information infrastructure objects

DOI: http://dx.doi.org/10.26583/bit.2020.1.02

Abstract. The paper suggests a number of proposals for formation of the regulatory field of protection systems against fraud and counterfeit products, as well as for a uniquely understood set of terms, abbreviations and definitions based on the most harmonized domestic and foreign standards in this area. The program of digitalization of the economies of developed countries highlights a relatively new direction of development of the so-called cyberphysical control systems for industrial technological processes, in particular. This motivates a formulation the new non-traditional tasks to ensure the security of critical information infrastructure. The obvious threat of stability losses of technological processes is the use of counterfeit components in view of an overall observed increase of volume of counterfeit products, including the electronic components. Therefore, there is a clear request to find a systematic solution to the problem of counterfeit detection not only from the standpoint of intellectual property protection, but also having in mind the important aspects of industrial safety during the certification of appropriate technical solutions. It is rather new type of activity for testing centers and laboratories 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 a starting point for formation of the domestic regulatory framework.

Keywords: authentication, counterfeit, electronics components, microelectronics.
For citation: DURAKOVSKIY, Anatoly P.; KESSARINSKIY, Leonid N.; SHIRIN, Alexey O. Terms and definitions base development for counterfeit electronics test for critical information infrastructure objects. IT Security (Russia), [S.l.], v. 27, n. 1, p. 19-27, 2020. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1249>. Date accessed: 10 feb. 2020. DOI:http://dx.doi.org/10.26583/bit.2020.1.02.

Введение

В настоящее время в России только формируется нормативное поле систем защиты от фальсификаций и контрафактной продукции, происходит гармонизация отечественных и зарубежных стандартов в этой области. Поэтому важно сформировать однозначно понимаемый набор терминов, сокращений и определений.

Основные термины и определения были введены в октябре 2017 г. в ГОСТ Р 57881-2017 «Система защиты от фальсификаций и контрафакта. Термины и определения»[1] по терминам в контрафакте (КФ), но он не охватывает практические вопросы выявления контрафактных изделий. Указанный стандарт дополняет ГОСТ Р 57880-2017 «Система защиты от фальсификаций и контрафакта. Изделия электронные. Предотвращение получения, методы обнаружения, сокращения рисков применения и решения по использованию фальсифицированной и контрафактной продукции» (российский аналог международного стандарта AS5553A) по обеспечению недопущения поставок контрафактных изделий, но он в основном определяет организационные вопросы обеспечения поставок и проверок изделий электронной компонентной базы (ЭКБ). На данный момент нет отечественного национального стандарта, который бы содержал технические требования к методам выявления признаков контрафакта в ЭКБ и их реализующим испытательным установкам, а также алгоритм оценки достоверности результатов испытаний комплексом методов.

В зарубежной практике стандарт AS5553A дополняет стандарт AS6171A, который формирует технические требования к методам выявления признаков контрафакта в ЭКБ, определяет регламент задания входных данных для такого рода испытаний и алгоритм оценки достоверности полученных результатов. В его основу положена так называемая таксонометрическая модель Гуина – Димейса. Модель разработана в 2013 году, совершенствовалась авторами из «Сообщества автомобильных инженеров» (SAE), что

[1]ГОСТ Р 57881-2017 Система защиты от фальсификаций и контрафакта. Термины и определения.

привело к обновлению в 2018 г. некоторых понятий и терминов – соответственно, обновился и стандарт с AS6171 до AS6171A[2] [1, 2].

Для формирования отечественной нормативно-методологической базы по выбору оптимальных методик выявления контрафактных и фальсифицированных изделий ЭКБ необходимо дополнить существующую систему терминов (ГОСТ Р 57881[1], ГОСТ 16504[3]) определениями, которые предлагаются в данной статье.

1. Анализ существующих терминов и определений

Прежде всего, следует привести термины из ГОСТ Р 57881, которые будут использованы ниже в статье.

«Аутентичная продукция» – «продукция, отвечающая требованиям утвержденной для данной продукции нормативной и технической документации, нормативных правовых документов в области оборота данной продукции, изготовленная физическим лицом или организацией, наделенными соответствующими правами, проходящая в течение жизненного цикла техническое обслуживание, ремонт и/или модификации в соответствии с требованиями разработчика, государства-изготовителя либо государства-регистратора изделия соответственно и допущенная к дальнейшему применению либо эксплуатации уполномоченными лицом или организацией» [3, 4].

«Аутентичность» – «свойство объекта, свидетельствующее о его подлинности» [3, 4]. Аутентичность – синоним понятия подлинность, а процесс аутентификации – проверка подлинности.

На основе определения, существует несколько вариантов нарушения аутентичности изделия:

а) изделие изготовлено правообладателем, но оно не соответствует утвержденной документации (например, в результате брака, изменения конструкции с нарушением технических условий и/или регламента производства, существенных с точки зрения документации повреждений при транспортировке, хранении и т.д.);

б) изделие соответствует технической документации (обладает необходимым функционалом, электрические параметры находятся в пределах установленных норм), но изготовлено с нарушением прав правообладателя (например, в результате незаконного клонирования, выпуска дополнительной «ночной» партии микросхем без уведомления правообладателя или незаконного присвоения и перепродажи изделий, забракованных службой контроля качества предприятия);

в) комбинация описанных выше случаев.

Таким образом, «контрафактное изделие» («контрафакт») – «изделие, при изготовлении, продаже, обмене, распространении, импорте или ином введении в оборот которого, и при внесении изменений в которое, были нарушены исключительные права на результаты интеллектуальной деятельности или средства индивидуализации». Данное определение из ГОСТ Р 57881 дает более широкое толкование термина, по сравнению с Гражданским кодексом РФ (п.1 ст. 1515: «Товары, этикетки, упаковки товаров, на которых незаконно размещены товарный знак или сходное с ним до степени смешения обозначение, являются контрафактными»), поскольку включает также критерий внесения изменений в изделие.

[2]Руководящий материал. AS6171A:2018. Test Methods Standard; General Requirements, Suspect/Counterfeit, Electrical, Electronic, and Electromechanical Parts. SAE International.

[3]ГОСТ 16504-81 Система государственных испытаний продукции. Испытания и контроль качества продукции. Основные термины и определения (с Изменением № 1).

Основная задача – проведение проверок аутентичности изделий ЭКБ, выявление или подтверждение отсутствия признаков контрафакта [5]. «Демаскирующие признаки контрафакта (или признаки контрафакта)» – «свойства и качества изделия, по которым можно обнаружить его контрафактное происхождение». Процедура выявления наличия или подтверждения отсутствия «демаскирующих признаков» опирается на проверку сопроводительной документации, свойств и параметров изделий ЭКБ в ходе испытаний с применением различных разрушающих и неразрушающих методов [6–9]. Как правило, несколько методов испытаний применяются в комплексе (не поодиночке) для достижения максимально достоверного результата.

2. Термины, связанные с проведением испытаний ЭКБ

Несмотря на «Достоверность (испытаний или исследований)» – вероятность повторяемости полученных результатов испытаний ЭКБ независимо от выбора испытательной лаборатории при выбранных экспериментальных условиях». Обеспечивать максимальную достоверность – одна из основных задач при проведении испытаний на наличие или отсутствие признаков контрафакта изделий ЭКБ. Для этого методы выявления применяют комплексно на основе анализа особенностей различных способов фальсификаций ЭКБ, объединенные в типы контрафакта [6, 8, 10–12].

«Типы контрафакта ЭКБ» – способ фальсификации изделий ЭКБ, характеризуемый совокупностью признаков контрафактного происхождения (демаскирующих признаков контрафакта). Принято выделять семь основных типов контрафакта:

1. «Повторное использование» – это ЭКБ, демонтированная из выведенной из эксплуатации (бракованной, неработоспособной, устаревшей, утилизированной, запасной и т.д.) аппаратуры и предлагаемые для использования под видом новых изделий.
2. «Перемаркировка» – нанесение на изделие ЭКБ отличной от аутентичной маркировки, как правило, не заводским способом.
3. «Перепроизводство» (т.н. «3-я смена», «ночная смена») – ЭКБ, изготовленные на заводском оборудовании без контроля правообладателя, в том числе выпущенные сверх контрактного объема и невостребованные заказчиком. Характерно для ЭКБ, непосредственное изготовление которого организовано в странах юго-восточной Азии.
4. «Брак» – изделия, несоответствующие заявленным в официальной документации техническим или функциональным характеристикам в т.ч. забракованные службой контроля качества предприятия, но незаконно присвоенные и перепроданные под видом годной продукции.
5. «Клонирование» – незаконное воспроизведение изделия на основе результатов обратного проектирования (реинжиниринга), т.е. восстановление топологии и схемотехники изделия путем послойного травления и фотографирования кристалла.
6. «Несоответствие документации» – ситуация, при которой вместе с изделиями ЭКБ прилагается документация на другой типономинал.
7. «Недекларированные возможности» – функциональные возможности изделия ЭКБ, не описанные или не соответствующие описанным в документации, при использовании которых возможно получить несанкционированный доступ к обрабатываемой информации, произвести саботаж, нарушить запланированную работу аппаратуры. Согласно стандарту AS6171A, этот вариант модификации ЭКБ относится к типам контрафакта [5, 6, 13, 14].

Существующая практика предусматривает проведение испытаний на выявление (подтверждение отсутствия) признаков контрафакта, результатом которых является вывод об отсутствии (или наличии) таких признаков. Но для потребителей ЭКБ гораздо важнее

получить результат о подтвержденной аутентичности изделий (или контрафакте) с определенным уровнем достоверности [15–20].

Таким образом, существует необходимость в систематизации задания требований, составления комплекса методов для заданного уровня и с оценкой достоверности результатов испытаний. Для решения этой задачи необходимо прежде всего определить ключевые метрики.

Прежде всего нужно ввести градацию по требованиям к проведению испытаний на основе критичности аппаратуры назначения – уровни доверия, которые будут определять в том числе экономическую эффективности при формировании программы испытаний.

«Уровень доверия (УД) ЭКБ» – специальный показатель, характеризующий степень уверенности в том, что изделие ЭКБ аутентичное (т.е. «подлинное»):

УД1 – максимальная уверенность – ЭКБ для наиболее критической аппаратуры,

УД6 – минимальная уверенность – ЭКБ для менее критической аппаратуры.

«Целевая достоверность аутентичности (ЦД)» – требуемая достоверность подтверждения аутентичности изделия в ходе испытаний на отсутствие демаскирующих признаков контрафакта; измеряется в процентах и определяется требуемым уровнем доверия. Пример возможной градации уровней доверия и соответствующей целевой достоверности приведен в табл. 1.

Таким образом, задаются требования для проведения испытаний на подтверждение аутентичности (выявление признаков контрафакта) ЭКБ, которые необходимо будет обеспечить применением комплекса методов. Или другими словами – достичь заданной достоверности испытаний.

Для проведения оценки достоверности испытаний, необходимо ввести еще ряд метрик.

«Уровень выявления признаков контрафакта (УВПКФ)» – достоверность выявления выбранного набора признаков контрафакта комплексом методов испытаний; измеряется в процентах. Важно отметить, что набор признаков контрафакта выбирается на основе анализа типа контрафакта.

«Уровень выявления испытательной лабораторией (центром) признаков контрафакта» – достоверность выявления всех известных признаков контрафакта комплексом из всех, доступных лаборатории (центру), методов испытаний – является интегральным показателем оснащенности лаборатории (центра) и определяет предельный (как правило, недостижимый на практике) уровень достоверности результатов испытаний.

«Уровень выявления признаков контрафакта разного типа» – достоверность выявления всех признаков контрафакта, характерных для выбранного типа контрафакта, комплексом методов испытаний; измеряется в процентах. Частный случай УВПКФ, который нужен для дифференцированной оценки достоверности результатов испытаний по разным типам контрафакта.

В соответствии с заданной целевой достоверностью и доступными лаборатории методами испытаний, часть демаскирующих признаков контрафакта будут уверенно выявляться (достоверность выявления будет больше или равна целевому значению), часть признаков не будет выявляться совсем, а достоверность выявления третьей части признаков будет меньше целевой, но выше нуля. Соответственно, классификация демаскирующих признаков по результатам испытаний будет важной справочной информацией и для потребителя ЭКБ, и для самого испытательного центра, и для регулирующего органа.

«Выявляемый демаскирующий признак контрафакта» – признак контрафакта, достоверность выявления которого данным комплексом методов выше или равна целевой.

«Частично выявляемый демаскирующий признак контрафакта» – признак контрафакта, достоверность выявления которого данным комплексом методов ниже целевой, но выше нуля.

Таблица 1. Пример возможной градации уровней доверия и соответствующей целевой достоверности

Уровень доверия	Описание аппаратуры назначения ЭКБ	Целевая достоверность результатов испытаний
УД1	• Наиболее критичная аппаратура, • аппаратура обработки информации «ОВ», • аппаратно-программные комплексы уровня доверия по требованиям ФСТЭК России[4]	>95%
УД2	• Критичная аппаратура, • аппаратура обработки информации «СС», • аппаратно-программные комплексы уровня доверия 2 по требованиям ФСТЭК России[4]	90%-95%
УД3	• Критичная аппаратура, • аппаратура обработки информации «С», • аппаратно-программные комплексы уровня доверия 3 по требованиям ФСТЭК России[4]	80%-90%
УД4	• Критичная аппаратура, • аппаратура обработки информации «ДСП», сведениях о здоровье граждан, генетическая информация, • аппаратно-программные комплексы уровня доверия 4 по требованиям ФСТЭК России[4], • аппаратура значимых объектов КИИ 1 категории[5]	70%-80%
УД5	• Менее критичная аппаратура, • аппаратура обработки «персональных данных», сведений, составляющих банковскую, налоговую тайну и др. • аппаратно-программные комплексы уровня доверия 5 по требованиям ФСТЭК России[4], • аппаратура значимых объектов КИИ 2 категории[5]	60%-70%
УД6	• Менее критичная аппаратура, • аппаратура обработки сведений, составляющих коммерческую тайну, • аппаратно-программные комплексы уровня доверия 6 по требованиям ФСТЭК России[4], • аппаратура значимых объектов КИИ 3 категории[5]	50%-60%

«Невыявляемый демаскирующий признак контрафакта» – признак контрафакта, который не выявляется данным комплексом методов испытаний т.е. достоверность выявления которого равна нулю.

[4]«Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» утверждены приказом ФСТЭК России от 30 июля 2018 г. № 131, приказ зарегистрирован Минюстом России 14 ноября 2018 г. № 52686, вступил в силу с 1 августа 2018 г., применяется при проведении сертификационных испытаний с 1 мая 2019 г.

[5]Постановление Правительства Российской Федерации № 127 от 08.02.2018 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» (с изменениями от 13 апреля 2019 г.) [3].

«Результирующий уровень выявления признака комплексом выбранных методов» – достоверность выявить определенный признак с помощью комплекса выбранных (в т.ч. всех доступных лаборатории) методов.

Предварительно прогнозируется, и по результатам проведения испытаний проводится оценка достоверности результатов испытаний – рассчитывается наиболее важная метрика: «подтвержденная достоверность аутентичности» – достоверность подтверждения аутентичности изделия ЭКБ, по результатам проведенных испытаний на выявление (отсутствие) признаков контрафакта с применением комплекса методов.

Таким образом, результаты испытаний на подтверждение подлинности изделий ЭКБ должны представлять собой набор следующих сведений:

- наличие или отсутствие признаков контрафакта в изделиях ЭКБ;
- подтвержденную достоверность аутентичности изделий (если признаков контрафакта не выявлено) – это значение должно быть выше требуемого целевого для соответствия заданному уровню доверия;
- уровень выявления разных типов контрафакта;
- группировка демаскирующих признаков на «выявляемые», «частично выявляемые» и «невыявляемые».

Заключение

Проведен обзор основных российских и иностранных нормативных документов, определяющих основные термины и определения процессов выявления признаков контрафакта в изделиях ЭКБ. Международным лидером в области формирования нормативных документов испытаний на выявление признаков контрафакта и подтверждения аутентичности изделий ЭКБ является международное Общество инженеров автомобилестроителей (SAE).

Анализ литературных данных определяет необходимость добавления ряда важных терминов в отечественные нормативные документы для формирования законченной единой системы понятий и метрик процесса испытаний ЭКБ для подтверждения аутентичности. Предложения по терминам представлены в данной статье.

СПИСОК ЛИТЕРАТУРЫ:

1. Белов Е.Н., Пономарев А.А., Семенов А.В., Федорец В.Н. Угрозы информационной безопасности вооружения и военной специальной техники, укомплектованных электронной компонентной базой иностранного производства. Военная мысль. № 12, 2013. С. 35–43.
2. 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.
3. Постановление Правительства Российской Федерации № 127 от 08.02.2018 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации».
4. 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.
5. Дураковский А.П., Кессаринский Л.Н, Ширин А.О., Артамонов А.С., Бойченко Д.В., Тайибов 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.
6. Кессаринский, Леонид Н. и др. Идентификация элементной компонентной базы киберфизических систем. Безопасность информационных технологий, [S.l.], № 3. С. 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.

7. 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 физико-технического 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.
8. 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.
9. 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.
10. 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.
11. Семенов А.В., Старцев В.Н., Степанов Е.Н. Технометрическая идентификация микросхем для контроля жизненного цикла и поиска контрафакта. «Проблемы разработки перспективных микро- и наноэлектронных систем. (МЭС)» №4/2018. С. 143–148.
12. 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.
13. Кессаринский, Леонид Н. и др. Выявление признаков контрафакта в изделиях электронной компонентной базы в аспекте обеспечения промышленной кибербезопасности. Безопасность информационных технологий, [S.2.], № 2. С. 117–128, 2019. ISSN 2074-7136. URL: <https://bit.mephi.ru/index.php/bit/article/view/1204> (дата обращения: 01.11.2019).
14. Ершов Л., Левин Р., Батурин 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.
15. Фролова А. «Основные методы определения контрафактной продукции. Из практики испытательной лаборатории ООО «ПетроИнТрейд». Вестник электроники № 3 /2011. С. 44–46.
16. Поддельные микросхемы ST TDA7293. Вскрытие показало. Радиодетали и электронные компоненты. Обзор. 12 мая 2018 г. www.Akinava.ru. URL:https://mysku.ru/blog/aliexpress/62915.html.
17. John M. Radman and Daniel D. Phillips.Новые подходы к обнаружению контрафактных электронных компонентов. Журнал «IN COMPLIANCE», OCTOBER 2010.
18. Даниэль Оливье. «5 методов, используемых для обнаружения контрафактных электронных компонентов». Бюллетень «JJS manufacturing». URL: https://www.jjsmanufacturing.com (дата обращения: 15. 03. 2018 г.)
19. 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.
20. 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] 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).
[2] GOST R 57882-2017 System of protection against fraud and counterfeiting. Electronic parts. Verification criteria for conformity assessment of practice and methods of organizations to the protection against fraud and counterfeiting requirements (in Russian).
[3] Postanovlenie Pravitel'stva Rossijskoj Federacii № 127 ot 08.02.2018 «Ob utverzhdenii Pravil kategorirovaniya ob"ektov kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii» (in Russian).
[4] 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». Peterburgskij zhurnal elektroniki № 1 (90) 2018. P. 27–46 (in Russian).
[5] 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 (Orel, February 5–6, 2019). V 10 ch. Ch. 5 pod obshch. red. P.L. Malysheva. – Orel: Akademiya FSO Rossii, 2019. P. 65–67 (in Russian).

[6] Kessarinskiy, Leonid N. et al. Authentication of electronics components for cyber-physical systems. IT Security (Russia), [S.l.], 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).

[7] 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).

[8] 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).

[9] GOST R 57880-2017 System of protection against fraud and counterfeiting. Electronic parts. Avoidance, detection, mitigation and disposition of fraudulent/counterfeit parts (in Russian).

[10] 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.

[11] 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).

[12] Ujjwal Guin, Daniel DiMase, Mohammad Tehranipoor. «A Comprehensive Framework for Counterfeit Defect Coverage Analysis and Detection Assessment». Journal of Electronic Testing. Febluary 2014. DOI 10.1007/s10836-013-5428-2.

[13] Kessarinskiy, Leonid N. et al. Counterfeit electronic components identifying methods in terms of industrial cyber security IT Security (Russia), [S.2.], n. 2. P. 117–128, 2018. ISSN 2074-7136. URL: <https://bit.mephi.ru/index.php/bit/article/view/1204> (accessed: 01.11.2019).

[14] 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).

[15] A. Frolova. «Osnovnyye metody opredeleniya kontrafaktnoy produktsii. Iz praktiki ispytatel'noy laboratorii OOO «PetroInTreyd». Vestnik elektroniki № 3 2011g. P. 44–46. (in Russian).

[16] Poddel'nyye mikroskhemy ST TDA7293. Vskrytiye pokazalo. Radiodetali i elektronnyye komponenty. Obzor. May 12, 2018. www.Akinava.ru. URL: https://mysku.ru/blog/aliexpress/62915.html (in Russian).

[17] John M. Radman and Daniel D. Phillips. Novyye podkhody k obnaruzheniyu kontrafaktnykh elektronnykh komponentov. Zhurnal «IN COMPLIANCE», October 2010.

[18] Danielle Olivier. «5 techniques used to detect counterfeit electronic components». Byulleten' «JJS manufacturing»: https://www.jjsmanufacturing.com (accessed:15.03.2018).

[19] 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.)

[20] 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 – 2 декабря 2019 г. Окончательный вариант – 6 февраля 2020 г.
Received – December 02, 2019. The final version – February 06, 2020.