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

МАРКИРОВКА И ПРОВЕРКА ПОДЛИННОСТИ ИЗДЕЛИЙ МИКРОЭЛЕКТРОНИКИ НА ОСНОВЕ НЕКЛОНИРУЕМОСТИ РАДИАЦИОННОГО ПОВЕДЕНИЯ

DOI: http://dx.doi.org/10.26583/bit.2020.3.02

Аннотация. Статья посвящена проблеме подделки электронных устройств. Постоянно растущие требования к характеристикам и функциональным возможностям изделий электронной компонентной базы (ЭКБ), применяющимся в ответственной аппаратуре (космических аппаратах, технике двойного и специального назначения, транспорте и т.д.), приводят к применению продукции коммерческой категории качества иностранного производства. Таким образом, возникает риск применения ЭКБ контрафактного происхождения, что определяет необходимость проводить испытания и исследования, подтверждающие аутентичность изделий. Но даже применение всего арсенала методов исследований не гарантирует 100% достоверности результата, подтверждающего аутентичность изделия. Кроме того, глобальная тенденция заключается в том, что количество поддельных микросхем (и не только микросхем) увеличивается, но эффективность методов обнаружения падает. Одним из методов борьбы с контрафакцией является маркировка подлинных компонентов. И самый безопасный для маркировки метод, основанный на физически неклонируемых функциях (ФНФ) т.е. таких свойств изделия, которые невозможно воспроизвести в следствие естественного разброса характеристик паразитных структур, неопределенности результатов случайных процессов технологии производства. Распределение амплитуд ионизационных откликов и радиационная деградация параметров по мере накопления поглощенной дозы является одной из таких ФНФ т.к. обладает нужными свойствами: невозможностью воспроизведения с одной стороны, и однородностью результатов в рамках одной партии микросхем или транзисторов с другой стороны. Поэтому предлагается использовать различные признаки ухудшения радиационного поведения в качестве ФНФ. Несколько примеров такого использования представлены в статье.

Ключевые слова: электроника, подделка, контрафакт, радиация, чипы, физически неклонируемая функция.

Для цитирования: ДУРАКОВСКИЙ, Анатолий П.; КЕССАРИНСКИЙ, Леонид Н.; ШИРИН, Алексей О. МАРКИРОВКА И ПРОВЕРКА ПОДЛИННОСТИ ИЗДЕЛИЙ МИКРОЭЛЕКТРОНИКИ НА ОСНОВЕ НЕКЛОНИРУЕМОСТИ РАДИАЦИОННОГО ПОВЕДЕНИЯ. Безопасность информационных технологий, [S.l.], v. 27, n. 3, p. 18–25, 2020. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1289>. Дата доступа: 08 sep. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.3.02.

Anatoly P. Durakovskiy[1], Leonid N. Kessarinskiy[2], Alexey O. Shirin[3]
[1,2]National Research Nuclear University MEPhI
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

The use of microelectronics radiation behavior as physical uncloned function to find counterfeit

DOI: http://dx.doi.org/10.26583/bit.2020.3.02

Abstract. The study is devoted to the problem of counterfeiting electronic devices. The constantly increasing requirements for the characteristics and functionality of electronic components for critical equipment (spacecraft, dual-purpose and special-purpose equipment, transport, etc.) lead to the use of foreign-made commercial products. Thus, there is a risk of using counterfeit electronic components, which determines the need to provide tests to the authenticity confirmation. But even the use of the entire arsenal of research methods does not guarantee 100% authenticity of the product. In addition, the global trend is that the number of counterfeit microcircuits (and not only ICs) is increasing, but the effectiveness of detection methods is falling. One of the methods used to combat counterfeiting is the marking of genuine components. And the safest method for marking is based on physical unclonable functions (PUF) i.e. such properties of the product that cannot be reproduced due to the natural spread of the characteristics of parasitic structures, and the uncertainty of the results of random processes of production technology. The distribution of the amplitudes of ionization responses and the radiation degradation of parameters with the accumulation of the absorbed dose is one of such PUFs because possesses the necessary properties: the impossibility of reproduction on the one hand, and uniformity of results within one batch of microcircuits or transistors on the other hand. Therefore, it is proposed to use various signatures of deterioration of radiation behavior as PUF. Several examples of this use are presented in the paper.
Keywords: electronics, counterfeit, radiation, chips, physical uncloned function.
For citation: DURAKOVSKIY, Anatoly P.; KESSARINSKIY, Leonid N.; SHIRIN, Alexey O. The use of microelectronics radiation behavior asphysical uncloned function to find counterfeit. IT Security (Russia), [S.l.], v. 27, n. 3, p. 18-25, 2020. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1289>. Date accessed: 08 sep. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.3.02.

Введение

Как известно, вся микроэлектроника делится на 4 основных класса: коммерческая, промышленная, военная и космическая. В соответствии с назначением, большинство техники ответственного применения традиционно комплектуется изделиями соответствующего класса. Однако общая тенденция к усложнению аппаратуры, расширению функциональных возможностей, рост требований к различным показателям эффективности (энергопотребление и энергосохранение, КПД, плотность мощности и др.) привела к массовому использованию в военной и космической технике ЭКБ промышленного или даже коммерческого класса качества. С другой стороны, географическое разделение центров разработки и производства изделий ЭКБ с переносом производственных и утилизационных мощностей в страны Азии стало дополнительной причиной резкого обострения проблемы контрафакта [1–4].

Рост доли контрафактной микроэлектроники за последние годы стал мировой проблемой. Созданы международные технические комитеты и группы исследователей по разработке общей стратегии по борьбе с контрафактом, воплотившихся в стандарты AS5553, AS6171, AS6081 и др. Стратегия борьбы с контрафактом сводится к доверенным путям поставки ЭКБ и проверке на наличие признаков контрафакта в испытательных лабораториях. Несмотря ни на что доля контрафактных микросхем растет, качество подделок постоянно увеличивается, что усложняет процесс их выявления. Согласно версии AS6171A (2018 г.) вероятность выявления некоторых типов контрафакта (например, клонирования) составляет всего несколько процентов, даже при использовании всех известных методов проверок (более 30) [5–10]. Что делать? Одной из эффективных стратегий решения этой проблемы является маркировать изделия ЭКБ на основе так называемых физически неклонируемых функций.

1. Физически неклонируемые функции

Несмотря на строгость правил технологического процесса изготовления серийной микроэлектроники, естественный разброс параметров, характеристики паразитных

структур, неконтролируемые параметры внешней среды создают уникальные элементы конструкции изделия ЭКБ, которые невозможно подделать. Принцип маркировки ЭКБ для последующей идентификации на основе таких элементов называется принципом аутентификации на основе ФНФ. Существует несколько идей и реализаций процесса аутентификации на основе ФНФ. Все их объединяет выполнение нескольких правил:

1. Реализация элемента с ФНФ не должна влиять на основное функционирование изделия. Лучше всего, если такие элементы будут «сами собой» существовать в любом изделии без приложения дополнительных усилий проектировщиков.
2. Проверяемые характеристики элемента с ФНФ нельзя подделать или воспроизвести. Они должны быть основаны на случайных процессах.
3. Результаты проверки (измерения) характеристик элементов с ФНФ должны иметь свойство воспроизводиться независимо от лаборатории или производителя измерительного оборудования.
4. Результаты проверки (измерения) характеристик элементов с ФНФ должны иметь возможность дать однозначный ответ: подлинное изделие или контрафактное. Не важно на основе сравнения с прогнозируемым результатом, эталонными значениям или результатом сравнения с эталонным образцом.

Одной из таких ФНФ является радиационное поведение изделия ЭКБ. Реализация такой ФНФ внутри микросхем или мощных дискретных приборов не требует создания специальных блоков. Радиационное поведение для современных технологических процессов определяется деградацией характеристик, связанных с паразитными структурами и связанными с ними параметрами ЭКБ [11–12].

2. Радиационное поведение как физически неклонируемая функция

Примеры применения радиационного поведения в качестве характеристик ФНФ приведены ниже. Недостатком использования радиационного поведения в качестве ФНФ для аутентификации является то, что это разрушающее испытаний и придется жертвовать образцом. Однако, примерно половина методов выявления контрафакта, перечисленных в AS6171 также являются разрушающими (например, проверка перемаркировки), что не мешает их комбинировать и проводить на одних и тех же образцах.

Приведем примеры использования радиационного поведения в качестве ФНФ для определения неоднородных образцов в выборке.

Мощные МОП транзисторы (МОПТ) IRFNG50 фирмы International Rectifier. Две партии производства: 0842 Мексика и 1038 США. С точки зрения функционирования и параметры образцов МОПТ соответствуют нормам из datasheet. Реализация ФНФ заключается в измерении деградации порогового напряжения отпирания транзистора в зависимости от накопленной дозы. Графики зависимостей приведены на рис. 1 и 2. Горизонтальной чертой на графике показано предельное значение параметра (не менее 2В), которое допускается документацией, а пересечение ее является критерием параметрического отказа образца [13].

Результаты измерения деградации порогового напряжения от поглощенной дозы в ходе радиационного воздействия позволяет сделать два вывода: для одной партии различий между образцами нет, для любых образцов из разных партий – различия существенные и позволяют однозначно отнести их к нужной партии.

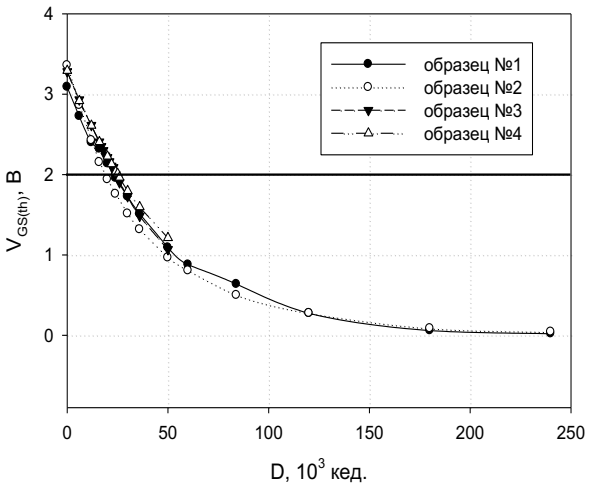


Рис. 1. Зависимость порогового напряжения транзисторов IRFNG50 партии 0842 (Мексика) от уровня поглощенной дозы

Fig. 1. Dependence of threshold voltage of IRFNG50 transistors batch 0842 (Mexico) on the level of absorbed dose

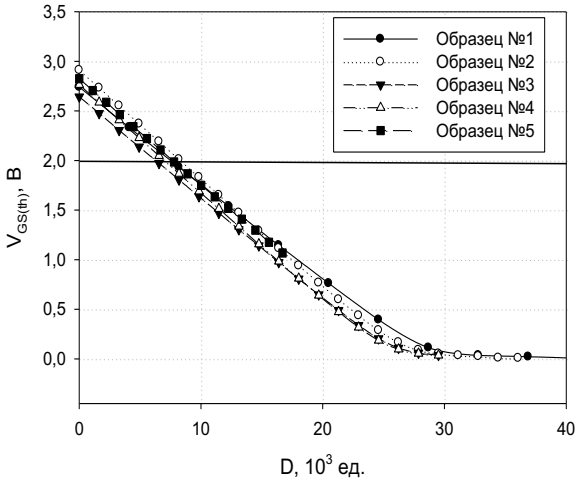
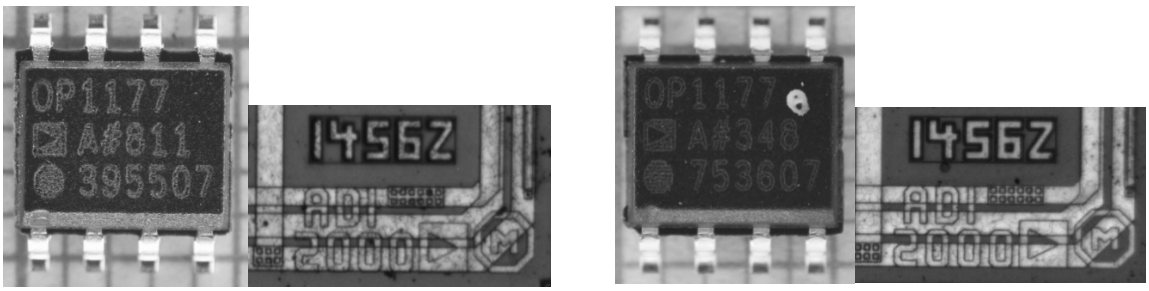


Рис. 2. Зависимость порогового напряжения транзисторов IRFNG50 партии 1038 (США) от уровня поглощенной дозы.

Fig. 2. Dependence of threshold voltage of IRFNG50 transistors batch 1038 (USA) on the level of absorbed dose

Операционный усилитель OP1177ARZ фирмы Analog Devices. Были исследованы 4 партии разных лет производства: 2008, 2010, 2012, 2013. За исключением даты производства, внешне образцы выглядят одинаковыми по внешнему виду, по характеристикам и по меткам на кристаллах [14]. На рис. 3 приведены примеры для двух партий 2008 и 2013 годы.

Реализация ФНФ заключалась в снятии карт ионизационного отклика кристаллов микросхем. Процедура выполняется следующим образом. Сначала выполняется проверка параметров образцов, чтобы убедиться в их годности. Затем часть пластикового корпуса над кристаллом химически стравливается. Открытый кристалл начинает подвергаться сканирующему воздействию сфокусированного (диаметр 10 мкм, длительность 10 пс, длина волны 1,06 мкм) лазерного луча одновременно с фиксацией всплеска тока по цепям питания микросхемы.



п.395507 п.753607

Рис. 3. Внешний вид корпусов и маркировка кристаллов OP1177ARZ

Fig. 3. Appearance of cases and marking of OP1177ARZ crystals

Объединение данных о месте выстрела лазером и амплитудой отклика составляет карту ионизационного отклика, которая фактически показывает взаимосвязь нескольких физических процессов и их характеристик: (а) локальной области кристалла (на которое

происходит воздействие сфокусированного излучения), (б) механизмом и особенностями сбора сгенерированного избыточного заряда (с учетом локального профиля легирования кремния, геометрии и топологии областей, переотражения лазерного излучения от слоев металлизации, первичной рекомбинации и т.д.), (в) движением этого заряд от места генерации до исследуемых выводов микросхемы (с учетом потерь по мере движения, рекомбинацией, перезарядом паразитных реактивностей). С учетом огромного количества непредсказуемых внутренних факторов (в том числе паразитных элементов), влияющих на итоговую форму отклика на выводах микросхемы, карту ионизационного отклика можно считать еще одной реализацией физически неклонируемой функции.

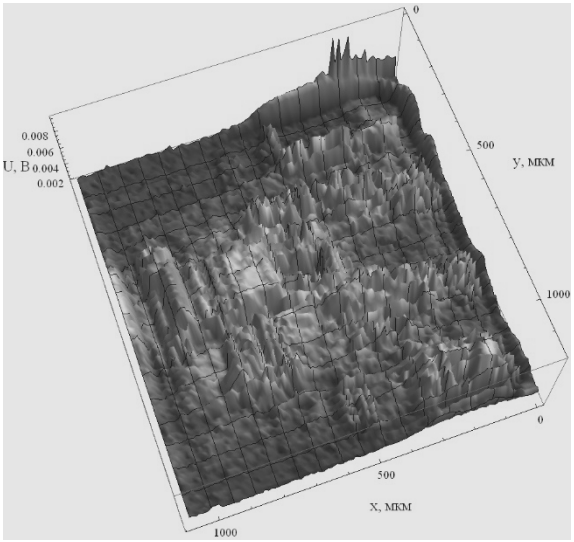


Рис. 4. 3D-карта ионизационного отклика n.395507
Fig. 4. 3D map of the ionization response b. 395507

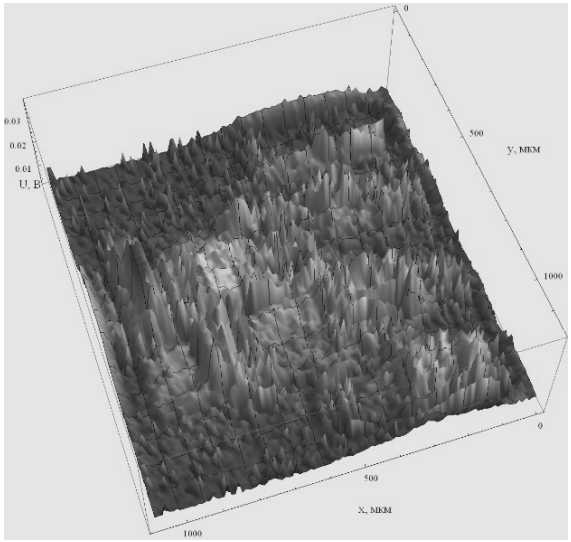


Рис. 5. 3D-карта ионизационного отклика n. 753607
Fig. 5. 3D map of the ionization response b. 753607

На рис. 4 и 5 приведены карты отклика для разных партий микросхем OP1177ARZ. После проведенных исследований не остается сомнений в отличии топологии и технологии изготовления партии 395507 от партии 753607, как на поверхности, так и внутри кристалла (см. рис. 6.). Это в дальнейшем было подтверждено детальным анализом топологии кристаллов в месте наиболее значимого различия карт отклика.

a) b)

Рис. 6. Фотография кристалла OP1177ARZ. a) область 1 партии 395507; b) область 1 партии 753607
Fig. 6. Photo of OP1177ARZ crystal. a) area of 1st batch 395507; b) area of 1st batch 753607

Таким образом, карта ионизационного отклика – вариант реализации ФНФ в ходе полностью автоматического сканирования независимо от функционального назначения изделия. Его преимущество по сравнению с послойным травлением и сравнением металлизации с эталоном в том, что ионизационный отклик формируется одновременно и картой металлизации (определяет долю лазерного излучения, доходящую до кремниевых областей), и топологией самих кремниевых областей кристалла (анализ которых обычно ограничен для визуального сравнения топологии).

Заключение

Испытания изделий микроэлектроники на выявление признаков является одним из составляющих стратегии противостоянию контрафакту. Но, к сожалению, даже применение всех методов выявления не обеспечивает 100% гарантию того, что проверенное изделие является подлинным.

Выходом из такой ситуации служит аутентификация образцов на основе физически неклонируемых функций.

В статье изложены примеры реализации аутентификации образцов ЭКБ на основе ФНФ – радиационного поведения изделий. В качестве примеров приведены данные для мощных полупроводниковых приборов, аналоговых микросхем низкой степени интеграции.

Поскольку радиационные испытания являются одним из обязательных видов испытаний ЭКБ, для проверки соответствия условиям работы аппаратуры в условиях, например, космической радиации – использование полученных данных о радиационном поведении изделий для аутентификации является дополнительным результатом проводимых исследований.

СПИСОК ЛИТЕРАТУРЫ:

1. Jo Vann, Supplier anti-counterfeit requirements, report of IEC TC107 WG3. March 2018. URL:https://www.caa.co.uk/uploadedFiles/CAA/Content/Standard_Content/Commercial_industry/Aircraft/Airworthiness/Seminars/Production_Organisations_28th_March_2018/IECQ%20Anti-Counterfeit%20Standards%20-%20Jo%20Vann.pdf (дата обращения: 15.08.2020).
2. U.S. Dept. of Comm., Defense Industrial Base Assessment: Counterfeit Electronics (2010). P. 179. URL: https://docplayer.net/398759-Defense-industrial-base-assessment-counterfeit-electronics.html (дата обращения: 15.08.2020).
3. Farinaz Koushanfar, Saverio Fazzari, Carl McCants, William Bryson, Matthew Sale, Peilin Song, and Miodrag Potkonjak. 2012. Can EDA combat the rise of electronic counterfeiting? In Proceedings of the 49th Annual Design Automation Conference (DAC '12). Association for Computing Machinery, New York, NY, USA, 133–138. DOI: https://doi.org/10.1145/2228360.2228386
4. Alkabani Y., Koushanfar F., Kiyavash N., Potkonjak M. (2008) Trusted Integrated Circuits: A Nondestructive Hidden Characteristics Extraction Approach. In: Solanki K., Sullivan K., Madhow U. (eds) Information Hiding. IH 2008. Lecture Notes in Computer Science. Vol 5284. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-540-88961-8_8.
5. Gassend, B., Lim, D., Clarke, D., Van Dijk, M., & Devadas, S. (2004). Identification and authentication of integrated circuits. Concurrency Computation Practice and Experience, 16(11), 1077–1098. DOI: https://doi.org/10.1002/cpe.805.
6. S. Pope, "Trusted Integrated Circuit Strategy," in IEEE Transactions on Components and Packaging Technologies. Vol. 31, no. 1. P. 230–234, March 2008. DOI: https://doi.org/10.1109/TCAPT.2008.918319.
7. 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

8. 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: (дата обращения: 12.02.2019). doi:http://dx.doi.org/10.26583/bit.2018.3.07.
9. 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: (дата обращения: 01.11.2019).
10. Дураковский А.П., Кессаринский Л.Н, Ширин А.О. Развитие терминологии нормативной базы испытаний на выявление признаков контрафакта в изделиях электронной компонентной базы аппаратуры объектов критической информационной инфраструктуры. Безопасность информационных технологий, [S.1.], № 1. С. 19–27, 2020. ISSN 2074-7136. URL: (дата обращения: 02.12.2019)
11. A.Y. Nikiforov et al., "Basic trends in electronic components product range development: Radiation hardness aspects," 2017 IEEE 30th International Conference on Microelectronics (MIEL), Nis, 2017. P. 45–48. DOI: https://doi.org/10.1109/MIEL.2017.8190066.
12. A. Borisov, M. Belova, L. Kessarinskiy, D. Boychenko, and A. Nikiforov “Analysis of total dose effects in modern analog ICs”, RAD Conference Proceedings vol. 2015-June. P. 427–431, 2015. URL:http://apps.webofknowledge.com/InboundService.do?product=WOS&Func=Frame&SrcApp=Alerting&SrcAuth=Alerting&secure=false&locale=en_US&SID=D43b5tW6hoBz151lRqN&customersID=Alerting&mode=FullRecord&IsProductCode=Yes&Init=Yes&Alias=WOK5&action=retrieve&UT=WOS%3A000387979700088 (дата обращения: 15.08.2020).
13. N.E. Aristova, A.Y. Borisov, A.S. Tararaksin, L.N. Kessarinskiy and A.V. Yanenko, "Automatic test complex for parametric control of power NMOS and PMOS transistors," 2015 International Siberian Conference on Control and Communications (SIBCON), Omsk, 2015. P. 1–4. DOI: https://doi.org/10.1109/SIBCON.2015.7146984.
14. A. Demidova, A. Pechenkin, A. Borisov, L. Kessarinskiy, D. Boychenko, and A. Yanenko “Identification of IC chips by ionization response comparison on the example of OP1177”, RAD Conference Proceedings vol. 2015-June. P. 409–411, 2015. URL:http://apps.webofknowledge.com/InboundService.do?customersID=Alerting&mode=FullRecord&IsProductCode=Yes&product=WOS&Init=Yes&Func=Frame&DestFail=http%3A%2F%2Fwww.webofknowledge.com&action=retrieve&SrcApp=Alerting&SrcAuth=Alerting&SID=D43b5tW6hoBz151lRqN&UT=WOS%3A000387979700084 (дата обращения: 15.08.2020).

REFERENCES:

[1] Jo Vann, Supplier anti-counterfeit requirements, report of IEC TC107 WG3. March 2018. URL:https://www.caa.co.uk/uploadedFiles/CAA/Content/Standard_Content/Commercial_industry/Aircraft/Airworthiness/Seminars/Production_Organisations_28th_March_2018/IECQ%20Anti-Counterfeit%20Standards%20-%20Jo%20Vann.pdf (accessed: 15.08.2020).
[2] U.S. Dept. of Comm., Defense Industrial Base Assessment: Counterfeit Electronics (2010). P. 179. URL: https://docplayer.net/398759-Defense-industrial-base-assessment-counterfeit-electronics.html (accessed: 15.08.2020).
[3] Farinaz Koushanfar, Saverio Fazzari, Carl McCants, William Bryson, Matthew Sale, Peilin Song, and Miodrag Potkonjak. 2012. Can EDA combat the rise of electronic counterfeiting? In Proceedings of the 49th Annual Design Automation Conference (DAC '12). Association for Computing Machinery, New York, NY, USA, 133–138. DOI: https://doi.org/10.1145/2228360.2228386
[4] Alkabani Y., Koushanfar F., Kiyavash N., Potkonjak M. (2008) Trusted Integrated Circuits: A Nondestructive Hidden Characteristics Extraction Approach. In: Solanki K., Sullivan K., Madhow U. (eds) Information Hiding. IH 2008. Lecture Notes in Computer Science. Vol 5284. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-540-88961-8_8.
[5] Gassend, B., Lim, D., Clarke, D., Van Dijk, M., & Devadas, S. (2004). Identification and authentication of integrated circuits. Concurrency Computation Practice and Experience, 16(11), 1077–1098. DOI: https://doi.org/10.1002/cpe.805.
[6] S. Pope, "Trusted Integrated Circuit Strategy," in IEEE Transactions on Components and Packaging Technologies. Vol. 31, no. 1. P. 230–234, March 2008. DOI: https://doi.org/10.1109/TCAPT.2008.918319.
[7] 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).

[8] 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).

[9] 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).

[10] Durakovskiy A.P., Kessarinskiy L.N, Shirin A.O. Terms and definitions base development for counterfeit electronics test for critical information infrastructure object**sю** IT Security (Russia), [S.1.], n. 1. P. 19-27, 2020. ISSN 2074-7136. URL: <https://bit.mephi.ru/index.php/bit/article/view/1249> (accessed: 02.12.2019).

[11] A.Y. Nikiforov et al., "Basic trends in electronic components product range development: Radiation hardness aspects," 2017 IEEE 30th International Conference on Microelectronics (MIEL), Nis, 2017. P. 45–48. DOI: https://doi.org/10.1109/MIEL.2017.8190066.

[12] A. Borisov, M. Belova, L. Kessarinskiy, D. Boychenko, and A. Nikiforov “Analysis of total dose effects in modern analog ICs”, RAD Conference Proceedings vol. 2015-June. P. 427–431, 2015. URL:http://apps.webofknowledge.com/InboundService.do?product=WOS&Func=Frame&SrcApp=Alerting&SrcAuth=Alerting&secure=false&locale=en_US&SID=D43b5tW6hoBz151lRqN&customersID=Alerting&mode=FullRecord&IsProductCode=Yes&Init=Yes&Alias=WOK5&action=retrieve&UT=WOS%3A000387979700088 (accessed: 15.08.2020).

[13] N.E. Aristova, A.Y. Borisov, A.S. Tararaksin, L.N. Kessarinskiy and A.V. Yanenko, "Automatic test complex for parametric control of power NMOS and PMOS transistors," 2015 International Siberian Conference on Control and Communications (SIBCON), Omsk, 2015. P. 1–4. DOI: https://doi.org/10.1109/SIBCON.2015.7146984.

[14] A. Demidova, A. Pechenkin, A. Borisov, L. Kessarinskiy, D. Boychenko, and A. Yanenko “Identification of IC chips by ionization response comparison on the example of OP1177”, RAD Conference Proceedings vol. 2015-June. P.409–411, 2015. URL:http://apps.webofknowledge.com/InboundService.do?customersID=Alerting&mode=FullRecord&IsProductCode=Yes&product=WOS&Init=Yes&Func=Frame&DestFail=http%3A%2F%2Fwww.webofknowledge.com&action=retrieve&SrcApp=Alerting&SrcAuth=Alerting&SID=D43b5tW6hoBz151lRqN&UT=WOS%3A000387979700084 (accessed: 15.08.2020).

Поступила в редакцию - 9 июля 2020 г. Окончательный вариант - 21 августа 2020 г.
Received - July 09, 2020. The final version - August 21, 2020.