УДК 621.37.037

СПЕЦПРОЕКТНЫЕ РЕИНЖИНИРИНГОВЫЕ ИССЛЕДОВАНИЯ РАДИОЭЛЕКТРОННЫХ ИЗДЕЛИЙ

М.С. Костин[@], к.т.н., доцент
Д.С. Воруничев, ст. преподаватель

Московский технологический университет (МИРЭА), Москва 119454, Россия
[@]Автор для переписки, e-mail: mihailkos@mail.ru

В связи с постоянной динамикой развития инженерных технологий радиоэлектронных изделий, развитием элементной компонентной базы и материально-технической базы современных электронных средств ранее применяемые методы обратного инжиниринга становятся малоэффективными, а, следовательно, знания о них не позволяют сформировать новую стратегию реализации реверсного противодействия. Вместе с тем анализ современных решений и средств прототипирования позволяет разработать комплекс технических мер противодействия спецпроектным исследованиям, обеспечивающих оригинальность и неповторимость отечественных изделий, что является актуальным в целях обеспечения экономической безопасности в сфере ОПК. В работе рассмотрены методы и средства спецпроектного реинжиниринга топологии многослойных печатных плат и интегральных микросхем. Сформулирован концептуальный подход реинжиниринговой модернизации радиоэлектронных изделий. Представлены базисные технологические процессы реинжиниринга схемотехнической конфигурации радиоэлектронных средств, основанные на принципах разрушающего и неразрушающего спецпроектного исследования: механообработка и химическое травление, оптическое сканирование, радиовидение, рентгенографический анализ. Впервые предложен метод тепловизионного электроиндукционного анализа печатных плат. Показано, что реинжиниринг может быть использован не только в целях модификации изделия, но и позволяет воссоздать весь технологический цикл производства по исследуемому образцу.

Ключевые слова: спецпроектный реинжиниринг, прототипирование, техническое противодействие, печатный модуль, интегральная микросхема.

THE SPECIAL PROJECT REVERSE ENGINEERING STUDY OF RADIOELECTRONIC PRODUCTS

M.S. Kostin[@],
D.S. Vorunichev

Moscow Technological University (MIREA), Moscow 119454, Russia
[@]Corresponding author e-mail: mihailkos@mail.ru

With the constant dynamics of the complicated development of the designs of radio electronic products, the development of the ECB, the material and technical and production base of modern radioelectronic facilities, the previously applied reverse engineering methods and technologists become ineffective, and therefore knowledge of them can not fully form the New Implementation Strategy Reverse reaction. While the study and analysis of modern methods and means of prototyping of the Defense industrial complex.

In this work, methods and means of special design reverse engineering of the topology of multi-layer printed circuit boards and case integrated circuits are considered. The concept of reengineering repair of radioelectronic equipment in security and video sur-veillance is formulated. The presented basic technological processes of reverse engineering of the circuit configuration of printed-film radio electronic products based on various physical principles of destructive and non-destructive special design research: machining and chemical etching, optical scanning, radio vision, X-ray analysis. For the first time, a method of thermal imaging (electro-induction) analysis of printed circuit boards with multilayer topology is proposed. It is shown that reverse engineering allows not only to repeat the design in the form of a modification, but also completely to completely recreate the whole technological production cycle for the sample under study.

Keywords: special project reengineering, prototyping, technical counteraction, printing module, integrated microcircuit.

В связи с активным развитием Государственной целевой программы по импортозамещению чрезвычайно важной стратегической задачей становится рациональная модернизация и активный контроль экономической безопасности ключевых секторов отечественной промышленности. В ней особая роль отводится развитию современных радиоэлектронных средств, технологиям их производства и противодействию спецпроектным реинжиниринговым исследованиям оригинальных изделий оборонно-промышленного комплекса (ОПК), в том числе, поставляемых под экспортные заказы либо частично изготовляемых импортным высокотехнологичным производством на базе российской технической документации, в исключительных случаях – по внешнеэкономической кооперации.

В то же время, принимая во внимание объем морально устаревшего радиоэлектронного оборудования и элементной компонентной базы (ЭКБ), находящихся в режиме долгосрочной эксплуатации, и ограниченного перечня импортной ЭКБ, допущенной ОПК, возрастает необходимость активной модернизации и, если потребуется, продления жизненного цикла радиоэлектронной аппаратуры. Это требует подготовки квалифицированных специалистов, умеющих модернизировать существующее радиоэлектронное оборудование, в том числе специального назначения (особенно в тех случаях, когда конструкторская документация утрачена или недоступна), и создания высокотехнологичных реинжиниринговых центров, оснащенных современными лабораториями с высокоточным оборудованием системного анализа, диагностики и прототипирования.

Продление жизненного цикла изделий представляет собой системный порядок действий и инструкций по разработке и внедрению методов и технологий, позволяющих в кратчайшие сроки:

- локализовать неисправность устройства;
- провести функциональное тестирование;
- определить надежность изделия;
- подобрать замены неисправным элементам на современном технологическом уровне;
- устранить отказ изделия;
- создать его усовершенствованный аналог-прототип даже в случае отсутствия рабочей документации;
- разработать и предусмотреть конструкторско-технологические меры на этапе проектирования и производства изделия по противодействию методам и средствам реверсного инжиниринга.

1. Концептуальный подход реинжиниринговой модернизации изделий в аспектах отраслевой экономической безопасности

В настоящее время при модернизации радиоэлектронного производства в условиях ускоренного инновационного развития возникает спрос на реинжиниринговые услуги по оригинальному проектированию и созданию изделий и технологий их производства, а также усовершенствованию производственных линий на базе отечественных и зарубежных технических решений. Технологии высокоточного производства усложняются, приобретая комплексный характер, что, в свою очередь, усиливает спрос на специфическую деятельность, связанную с развитием процесса разработки новых методов экспертного реинжиниринга.

Перспектива полной технологической независимости от зарубежных поставщиков еще трудно реализуема, так как импортные инновационные технологии являются мощным ресурсным объектом закрытой интеллектуальной собственности и защищены проектно-техническими приемами реверсного противодействия, в том числе, исключающего возможность легкодоступного прототипирования: известно, что реинжиниринг способен не только повторить конструкцию изделия, но и даже полностью воссоздать весь технологический цикл производства по исследуемому образцу.

Чтобы усилить конкурентные позиции отечественных производителей, особенно в части ОПК, необходимо обеспечить также внедрение и эффективную защиту оригинальных инженерных решений и технологий, составляющих объект не только интеллектуальной собственности, полагая, что «*know-how*», воплощенное в изделие, можно защитить через спецпроектные концептуальные решения реинжинирингого противодействия. Это обусловливает необходимость разработки научного подхода в области методов и средств реинжиниринговых исследований.

Определение уровня развития радиоэлектронной промышленности в части запатентованных решений может осуществляться посредством изучения документов международных патентных архивов. Однако опыт целого ряда технических решений, по какой-либо причине недоступных или мало изученных, можно свободно позаимствовать за счет применения реверсного инжиниринга образца изделия, приобретенного на абсолютно правовых основаниях. Важно отметить, что с точки зрения защиты интеллектуальной собственности реверсный инжиниринг является спорным предметом правового поля, так

как воссоздание точной копии изделия явным образом нарушает авторское право. Однако безлицензионные реверсинжиниринговые специсследования в части анализа продукции, в том числе импортного производства, с последующим созданием нового модернизированного изделия, не повторяющего в точной копии оригинал исследуемого образца, а лишь учитывающий детали и взаимосвязи в нем, не является нарушением прав интеллектуальной собственности. Напротив, они активно влияют на стимулирование рационализаторских конструкторско-технологических решений, развитие новых методов проектирования и технологий в производстве, в понимании методов спецпроектного анализа. Они позволяют строить собственную отечественную модель противодействия реверсному инжинирингу, тем самым сохраняя недоступным воссоздание функциональных изделий, не говоря уже о технологиях, реализующих их оригинальное исполнение.

Концептуальный подход спецпроектного реинжиниринга начинается с экспертного технического исследования образца готового изделия либо системного процесса и разворачивается обратным ходом в логическом порядке для выявления производственных технологий. Он представляет собой процесс модернизационного прототипирования изделия по функционально-логическим, физическим и объемно-топологическим характеристикам путем многопараметрического исследования, измерения и системно-целевой диагностики конструктивных элементов для разработки технических данных в зависимости от условий эксплуатации и новых требований к прототипному выпуску.

Таким образом, концептуальная стратегия спецпроектных исследований нацелена на создание нового усовершенствованного прототипного изделия, его параметрическое исследование и диагностику, обеспечивающих повышение надежности, развитие новых технических решений и технологий. Она не противоречит нарушению прав патентообладателей и не преследует цель копирования изучаемого образца. В то же время исследования в области реинжиниринга и спецпроектной диагностики играют ключевую роль в обеспечении информационно-технической безопасности радиоэлектронной аппаратуры [1], реализуемой на базе импортной ЭКБ, в том числе военного назначения. Они преследуют цель идентификации элементов и электрических цепей, реализующих программно-аппаратные решения закладных средств радиотехнической разведки (РТР) и внутрисистемной радиоэлектронной борьбы (РЭБ).

2. Реинжиниринг радиоэлектронных изделий с многослойной печатной топологией

Характер, сложность многослойного топологического исполнения изделий печатных плат и необходимость в нем определяются выбором способа обработки сигналов, типоконструкцией и интеграцией ЭКБ, рядом массогабаритных, теплофизических и радиочастотных параметров схемотехнической архитектуры радиоэлектронного устройства.

Хорошо известно, что в радиоэлектронике разделяют три подхода в решении задач обработки сигналов: аналоговая, цифровая и аналого-цифровая обработка. При этом аналоговая обработка является исключительно аппаратным способом, состоящим в применении радиоэлектронных элементов и устройств, использующих различные физические принципы, явления и свойства материалов, в то время как цифровая обработка реализуется посредством универсальной программно-аппаратной алгоритмизации, динамично

осваивающей более высокочастотную область радиочастотного спектра. Такой подход в области активного применения средств цифровой обработки сигналов приводит к миниатюризации и типизации создания ЭКБ на базе ТТЛ- и КМОП-логики: микропроцессоров, контроллеров и ПЛИС. Это, безусловно, положительно влияет на унификацию технологии процессов от серийного до массового производства, с одной стороны, но является негативным фактором в развитии обеспечения технического противодействия реинжиниринговым исследованиям печатных модулей - с другой [2]. Данный фактор мотивируется тем, что экспертный реинжиниринг многослойных печатных плат (МПП) способен не только послойно повторить оригинальность топологии рисунка, но и – с высокой степенью вероятности – полностью воссоздать принципиальную схему радиоэлектронного узла. При этом наличие печатной платы в сборе с электроэлементной базой является не обязательным условием, поскольку типизация посадочных мест ЭКБ с определяемым числом выводов, топологией цепей обвязки по питанию, сигнальных шин, посадочных мест под дискретные элементы позволяют практически безошибочно идентифицировать и констатировать принадлежность печатного узла к конкретному функциональному типу изделия по разводке МПП. Важно отметить, что функциональная идентификация печатных модулей по топологии является ключевым моментом в обеспечении технических мер противодействия при их изготовлении в условиях зарубежного высокотехнологичного производства в любом формате внешнеэкономической кооперации.

Разделяют следующие методы спецпроектного реинжиниринга многослойных печатных модулей: разрушающие и неразрушающие.

К разрушающим методам реинжиниринга МПП относится послойная механообработка образца шлифованием (рис. 1). Технология полного разрушающего реинжиниринга не гарантирует отсутствие повреждений топологии МПП при плотной разводке, потому не является прогрессивной и применяется только в особых случаях, когда исключается эффективность применения методов неразрушающего спецпроектного реинжиниринга, позволяющего восстанавливать топологию с применением косвенных методов экспертного анализа: оптического сканирования, тепловизионный (электроиндукционный), радиоволновый, рентгеновский [3].

Метод оптического сканирования является эффективным методом восстановления топологии печатного рисунка при помощи светового сканера, однако ограничивается применением только на двухсторонние печатные платы и чаще применяется в сочетании с методом механического шлифования для МПП. Восстановленный при помощи ПО Mentor Graphics прототип образца четырехслойной платы (см. рис. 1) представлен на рис. 2.

Тепловизионный метод реинжиниринга МПП отличается простотой реализации и заключается в электроиндукционном нагревании МПП высокочастотным током малой мощности до 30 МГц ближним полем плоского электромагнитного индуктора. По сравнению с индукционным нагревом, применяемым для разогрева электропроводящих материалов (медных проводников) переменным током частотой не более 30 МГц, диэлектрический нагрев проводится обычно с использованием более высоких частот, свыше 100 МГц. Поэтому топология МПП, идентифицируемая графическим тепловизором, имеет четко очерченные контуры печатного рисунка в каждом слое и в явном виде выделяется на фоне диэлектрического основания (рис. 3). Кроме того, в отдельных случаях, в качестве деталь-

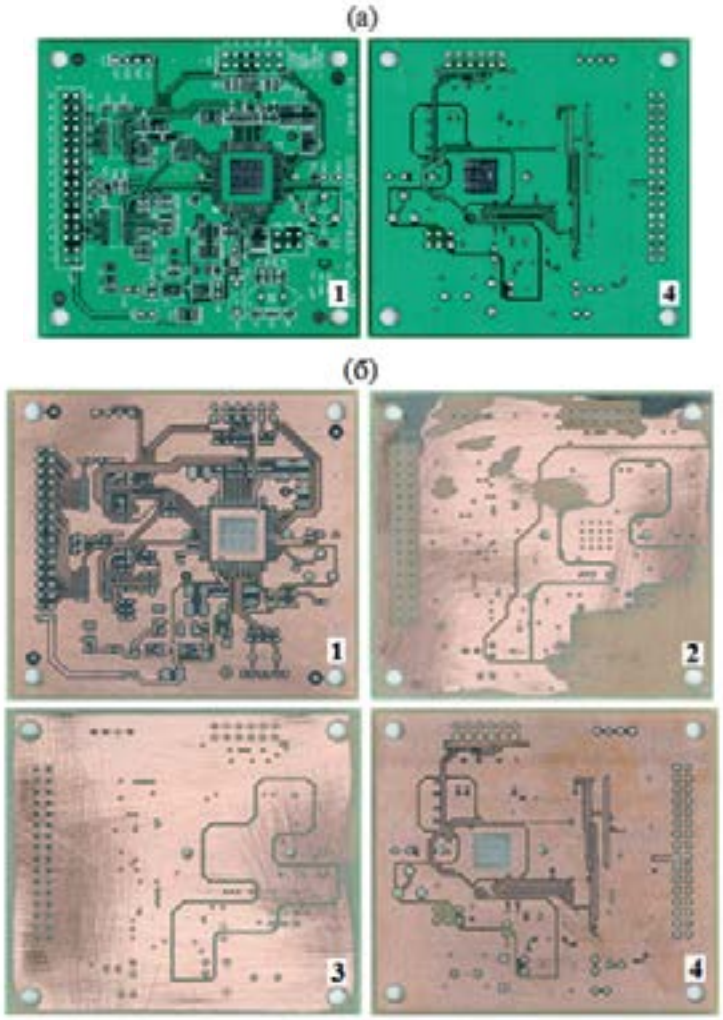

Рис. 1. Реинжиниринг четырехслойной МПП методом послойной механообработки образца печатной платы шлифованием:
а – образец МПП; б – оттиски топологии печатных слоев.

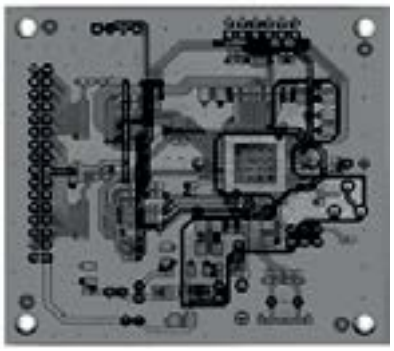

Рис. 2. Послойный прототип топологии образца МПП.

ного рассмотрения фрагментарных элементов топологии может быть использован метод нагревания печатных проводников постоянным током малой мощности.

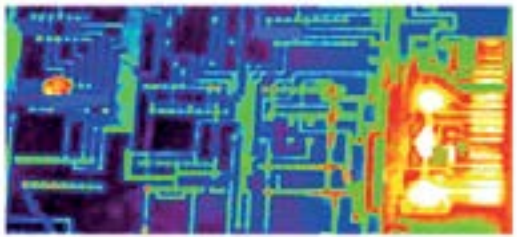

Рис. 3. Тепловизионный портрет печатной топологии образца МПП.

Радиоволновый и рентгеновский методы так же, как и тепловизионный, относят к прогрессивным реинжиниринговым методам неразрушающего прототипирования топологии печатного рисунка МПП. Радиоволновый метод основан на принципах регистрации распределения электромагнитного поля в ближней зоне Френеля при помощи средств графической радиовизуализации (радиовидения) при возбуждении элементов печатной топологии электромагнитным полем сверхвысокочастотного диапазона. Рентгеновский метод является самым точным и обеспечивает послойную регистрацию МПП в двух координатных плоскостях с управляемой глубиной облучения (рис. 4).

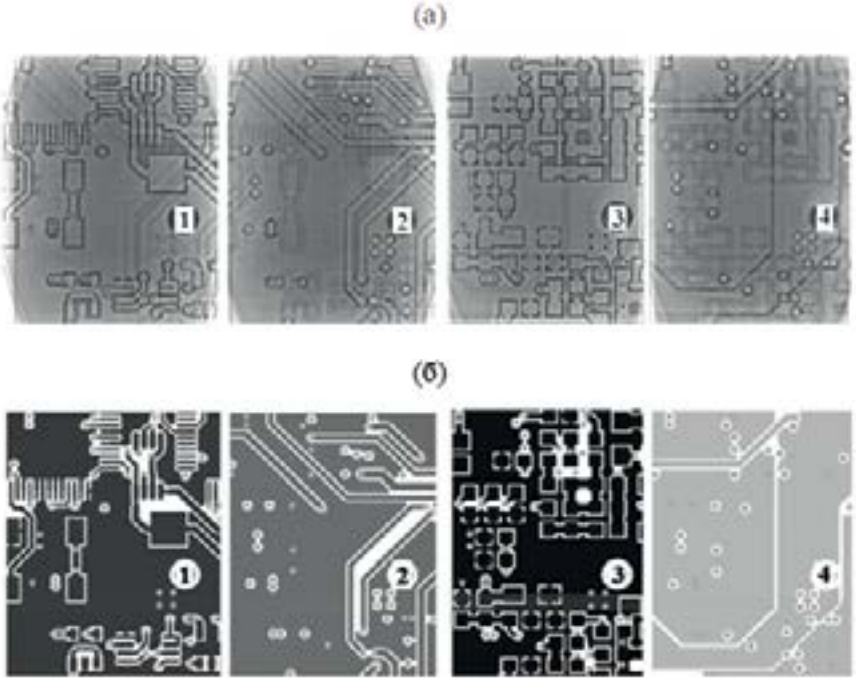

Рис. 4. Рентгенографический анализ фрагментарного образца четырехслойной печатной платы: а – послойные рентгенограммы МПП; б – восстановленная топология в ПО Mentor Graphics.

3. Реинжиниринг корпусных пленочных интегральных микросборок

Реинжиниринг интегральных микросхем (ИМС), как и в случае с реинжинирингом МПП, заключается в воссоздании печатной топологии электрической схемы ИМС. Прототипирование топологии сложной микросхемы ускоряет процесс разработки нового интегрального изделия с улучшенными характеристиками по времени на порядки ввиду уменьшения затрат на создание нового электронного устройства. Так, реинжиниринг

корпусных ИМС с технологией по разрешению не менее 1 мкм и числом эквивалентных вентилей на кристалле до 3000 позволяет менее, чем за полгода полностью воссоздать не только топологию ИМС, но и ее электрическую принципиальную схему. Последняя отличается рядом улучшенных характеристик, например, по мощности и надежности выходных каскадов в более жестком климатическом исполнении и т.д. [4].

Прототипирование принципиальной схемы осуществляется путем исследования и сопоставления кристаллографических изображений с типовыми решениями изготовления элементов на подложке ИМС при последовательном травлении слоев металлизации. В качестве слоя металлизации может выступать, например, алюминий, каждый слой которого разделяется диоксидом кремния. Если топология и структура транзисторов в пленочном исполнении при микровизионном исследовании не очевидна, на кристалле подложки ИМС производится дополнительно поперечный срез.

В отличие от реинжиниринга МПП, где существует возможность применения неразрушающих методов исследования макротопологии, спецпроектный реинжиниринг микротопологии изделий корпусных ИМС осуществляется только при помощи разрушающих методов: механического фрезерования и послойного химического травления, шлифования и послойного химического травления. По существу, выбор метода деконструкции ИМС определяется типом материала, из которого состоит ее корпус: пластиковый (полимерный), керамический (металлокерамический) или металлостеклянный.

Процесс механообработки корпусных ИМС служит в качестве подготовительной операции технологического процесса травления, обеспечивая предварительное истончение активной зоны травления, а для составных шовных корпусов из полимеров является единственным шагом к началу проведения микровизионного исследования топологии.

Технологический процесс послойного химического травления заключается в удалении части материала корпуса при помощи концентрированного раствора серной и азотной кислот при температуре около +100 ºС, потому требует соблюдения всех норм обеспечения техники безопасности. При этом серная кислота участвует в основном процессе травления, а азотная – только подтравливает побочный продукт образования углеродистых масс от реакции материала корпуса ИМС с серной кислотой (рис. 5).

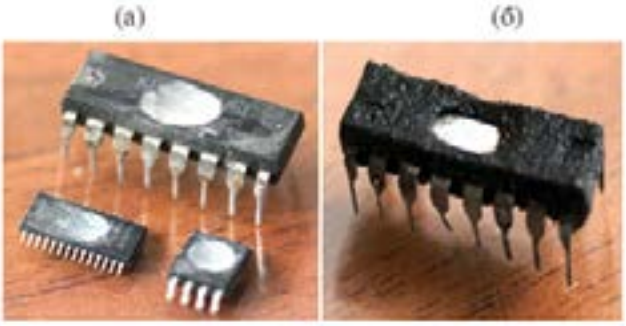

Рис. 5. Реинжиниринг микротопологии изделий корпусных ИМС:
а – механообработка корпуса; б – химическое травление корпуса.

На рис. 6 приведены фотографические материалы микровизионного исследования образцов ИМС методом фрезерования и послойного химического травления. На фотографических снимках можно четко увидеть очерченные контуры типовых решений тонкопленочного формирования эквивалентных вентилей и цепей периферической обвязки на базе КМОП-логики.

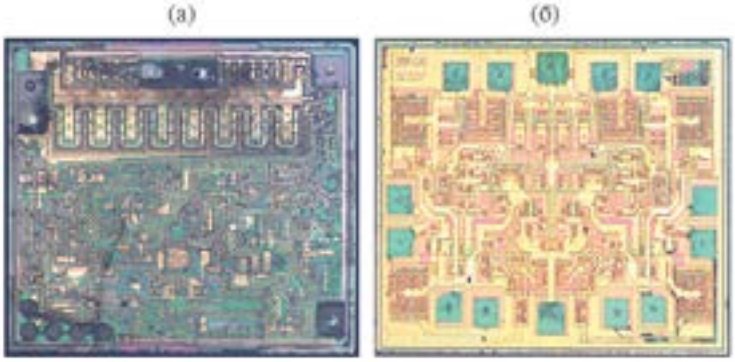

Рис. 6. Микротопологии образцов изделий корпусных ИМС:
а – восьмиразрядный сдвиговый регистр; б – микроконтроллер.

Заключение

Нынешние технологии производства печатных плат и интегральных микросхем усложняются, приобретая комплексную и регулярную микроминиатюризационную направленность, что, в свою очередь, усиливает спрос на специфическую деятельность, связанную с развитием процесса разработки новых способов экспертного реинжиниринга – параметрического прототипирования. Действительно, концептуальная стратегия спецпроектных реинжиниринговых исследований направлена на создание нового усовершенствованного прототипного изделия, а также параметрическое исследование и диагностику с целью повышения его надежности и т.д. Однако проводимые исследования в области реинжиниринга и спецпроектной диагностики играют не менее важную ключевую роль в обеспечении информационно-технической безопасности радиоэлектронной аппаратуры, поскольку без знания способов обратного инжиниринга невозможна эффективная организация его активному противодействию.

Отсюда анализ современных методов и средств спецпроектного прототипирования конструкций радиоэлектронных изделий, рассмотренных в работе, а также идентификация особенностей технологии их производства и номенклатуры ЭКБ позволяют выработать комплекс технических мер противодействия спецпроектным исследованиям, исключая преднамеренное копирование и, тем самым, обеспечивая подлинную оригинальность изделий, выпускаемых радиоэлектронной промышленностью в составе ОПК.

Литература:

1. Магомедов Ш.Г. Оценка степени влияния сопутствующих факторов на показатели информационной безопасности // Российский технологический журнал. 2017. Т. 5. № 2. С. 47–56. [Электронный ресурс]. – URL: https://rtj.mirea.ru/upload/medialibrary/641/rtzh_2_2017_47_56.pdf.

2. Keng Tiong Ng. The art of PCB reverse engineering (standard edition): Unravelling the beauty of the original design. USA: CreateSpace Independent Publishing Platform, 2015. 372 p.

3. Guo Z., Tehranipoor M., Forte D., Di J. Investigation of obfuscation-based anti-reverse engineer-ing for printed circuit boards // Proceed. of the 52nd Annual Design Automation Conf. (DAC). San Francisco, CA, USA. June 8–12, 2015. N.Y.: IEEE, 2015. P. 93–98.

4. Torrance R., James D. The state-of-the-art in IC reverse engineering // Cryptographic Hardware and Embedded Systems (CHES). Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2009. V. 5747. P. 363–381.