АППАРАТНЫЕ ТРОЯНЫ. ЧАСТЬ 1: НОВЫЕ УГРОЗЫ КИБЕРБЕЗОПАСНОСТИ

HARDWARE TROJANS. PART 1: NEW THREATS TO CYBER SECURITY

УДК 621.382, ВАК 05.27.01

Е.Кузнецов, А.Сауров**
E.Kuznetsov, A.Saurov**

В первой части цикла обзорных статей, посвященных аппаратным закладкам в интегральных схемах, – аппаратным троянам – рассмотрены потенциальные угрозы кибербезопасности, которые они несут. Анализируются возможные пути их несанкционированного внедрения. Для выработки методов и стратегий борьбы, предупреждения, выявления и противодействия приведена всесторонняя классификация аппаратных троянов.

In the first part of the cycle of reviews dedicated to hardware Trojans in integrated circuits potential threats to cyber security are considered. The possible ways of their unauthorized insertion are examined. For development of methods and strategies of prevention, detection and counteraction, the comprehensive classification of hardware Trojans is presented.

За последние десятилетия электронные системы от компьютеров до средств автоматизации, управления и контроля прочно вошли в нашу повседневную жизнь, и затрагивают все ее стороны. Построение и функционирование таких систем основано на интегральных микросхемах (ИС). ИС являются элементной базой всех современных электронных систем, обрабатывающих информацию в важнейших отраслях, включая финансовый, промышленный, оборонный и транспортный сектор. Проблема надежности и безопасности выполнения ИС своих функций тесно связана с обеспечением кибербезопасности электронных систем. В последнее время в связи с глобализацией и увеличивающейся сложностью ИС, эта проблема приобретает все большую актуальность. Без ее решения электронные системы могут не только не выполнять те функции, которые заложены в них согласно спецификации, но и выступать проводником внешних злонамеренных атак на систему.

В последние годы появились новые потенциальные угрозы безопасности в рассматриваемой сфере, основанные на аппаратных средствах, – так называемые аппаратные закладки или аппаратные трояны, которые представляют собой намеренную злоумышленную модификацию электрической схемы или ее конструкции, приводящую к некорректному функционированию электронного устройства. Подобно программной закладке (программному трояну), аппаратная закладка представляет собой своего рода черный вход в электронное устройство. При этом аппаратный троян обладает дополнительным преимуществом – он постоянно присутствует на самом низком уровне обработки информации, что ведет к сохранению угроз отказа или отклонения от нормального функционирования ИС на протяжении всего времени использования электронного устройства, причем проблему невозможно предотвратить никакими программными или аппаратными средствами защиты. Несанкционированной модификации может быть подвержен любой тип ИС и, это может быть причиной, как несущественных частичных сбоев, так и полного отказа системы. Аппаратный троян может воздействовать на систему самостоятельно, а может активироваться программным обеспечением, в которое преднамеренно заложена такая возможность. Аппаратная закладка может долгое время оставаться бездействующей и активироваться через заданное время, внешним воздействием или

* НПК "Технологический центр"/ SMC "Technological Centre".

некоторыми определенными активными процессами в работе ИС. Спектр аппаратных закладок – их возможности, размеры, механизмы срабатывания, потребляемая мощность – огромен, что в совокупности с увеличивающейся сложностью ИС, как на физическом, так и на функциональном уровнях, предоставляют широкие возможности злоумышленнику для скрытного размещения аппаратных троянов.

Относительная простота внедрения аппаратных закладок в современную ИС не может не вызывать беспокойство. Модификации могут быть внесены в аппаратную часть ИС как на этапе разработки, так и в процессе производства, включая такие стадии как спецификация, проектирование, верификация и изготовление. Более того, аппаратная закладка может быть внесена в уже изготовленную ИС [1]. Ситуация осложняется тем, что современные тенденции в полупроводниковой промышленности характеризуются разделением разработки и изготовления ИС, причем последнее выполняется несколькими фабриками, разбросанными по всему миру, преимущественно в Азии. Привлечение сторонних соисполнителей характерно не только для изготовления ИС, но и для проектирования: разработчики пользуются сторонним программным обеспечением, широко используют готовые блоки (IP-блоки), спроектированными третьей стороной. IP-блоки часто поставляются в бинарном виде и проектируются сторонними фирмами, специализирующимися на определенных технических проектах. Поэтому аппаратный троян может быть простым изменением параграфа в спецификации, дополнительной строкой в исходном коде, написанном на языке описания аппаратуры (HDL), или же модификацией кремниевого кристалла на производственной фабрике, например, небольшим изменением топологии транзистора. Если изменение выполнено в диффузионном слое, то на чипе оно становится практически "невидимым" [2].

В настоящее время проблема аппаратных закладок всесторонне исследуется в мире. Так, политехническим институтом Нью-Йоркского Университета ежегодно проводятся соревнования между командами по внедрению и поиску специальных устройств [3], что способствует развитию технологий предупреждения внедрения и методов обнаружения аппаратных троянов. Агентство по перспективным оборонным научно-исследовательским разработкам США (DARPA) инициировала в 2007 году специальную программу по обеспечению аутентичности используемых в военных системах США микросхем и проводит НИОКР по развитию методов и технологий обнаружения аппаратных закладок [4]. Большинство других публикуемых исследований проводится университетскими группам и в основном посвящены методам предотвращения внедрения троянов при разработке ИС, а также способам их выявления в ИС после изготовления.

Если аппаратный троян когда-либо был внесен в систему, то он присутствует всегда неза-

Over the past decade, electronic systems from computers to automation, control and monitoring tools have become part of our everyday lives and affecting all sides of it. The structure and operation of such systems are based on integrated circuits (IC). IC is a base for all modern electronic systems that process information in key sectors, including finances, industry, defense and transport. The problem of reliability and safety of operation of IC is closely connected with cyber security of electronic systems. Recently, in connection with globalization and the increasing complexity of IC, this issue is becoming increasingly important. Without its solution the electronic systems can not only perform the functions according to their specification, but also to be a conductor for external malicious attacks on the system.

In recent years, there were new potential security threats in this sphere, based on the so-called hardware Trojans – a malicious modifications of electric connection or design, leading to incorrect operation of the electronic device. Hardware Trojan, like software one, is a kind of back door into the electronic device. But hardware Trojan has an additional feature – he is always presented at the lowest level of information processing, which leads to the conservation threats of failure or deviation from normal functioning of the IC for the entire usage time of the electronic device, and the problem cannot be prevented by any software or hardware protection. Any type of IC may be subject to unauthorized modification, and this may be the cause of both minor and serious failures. A hardware Trojan can influence the system independently, or can be activated by the software, in which such possibility was intentionally provided. A

висимо от того, включена она или выключена. Потенциально он может нарушить работу всей системы, если внесен в любую из составляющих ее ИС. Воздействие аппаратных троянов может варьироваться от простых целевых атак до сложных атак, которые обеспечивают точку опоры программным атакам высокого уровня. К целевым, в частности, относятся следующие атаки:

- изменение бита информации, нарушающего целостность хранимых данных;
- ослабление функциональности криптографических ядер;
- атаки, приводящие к утечке конфиденциальной информации.

Система может быть инфицирована несколькими аппаратными закладкам, которые совместными действиями подрывают ее безопасность.

Для полного понимания воздействия аппаратных троянов на системы и их обнаружения необходимо изучение возможностей изменения информации при внедрении закладок, а также возможных механизмов их активации. Поэтому исследования возможных угроз, которые несут трояны, разработка конструкции и методов их внедрения, механизмов активации являются необходимой частью работы в поиске способов предупреждения внедрения, выявления и противодействия аппаратным закладкам для обеспечения безопасности используемых ИС.

При рассмотрении возможных угроз безопасности, исходящих от аппаратной закладки, и определения ее влияния на информационную систему целесообразно структурировать характерные признаки троянов. Для описания таких характерных свойств было предложено несколько классификаций аппаратных троянов. Цели таких классификаций – систематизация изучения, разработка общих методов обнаружения и подходов, обеспечивающих подавление воздействия различных классов троянов, а также сравнение разных методов противодействия. На рис.1 приведена наиболее полная классификация аппаратных троянов, предложенная в статье [5]. В основе этой классификации учитываются как фазы разработки ИС, так и уровни возможного внедрения аппаратных троянов.

Разработка и изготовление ИС, как правило, включают такие этапы, как спецификация ИС, ее разработка, изготовление, тестирование и сборка. Они должны рассматриваться и как стадии, на которых злоумышленник может внедрить аппаратную закладку. На этапе спецификации (подготовки технического задания) определяются характеристики системы, в том числе используемые модели и предполагаемая функциональность ИС. После этого этапа характеристики системы реализуются на стадии проектирования в определенном целевом конструктивно-технологическом базисе с учетом функциональных и физических ограничений. На этапе производства ИС изготавливается комплект фотошаблонов, и проводится цикл изготовления кристаллов ИС на кремниевых пластинах с последующей проверкой их функциональных и физи-

hardware Trojan can long time to remain dormant and be activated after a specified time, by external influence or as a result of defined processes in the operation of IC. Range of hardware Trojans, the capabilities, sizes, principles of operation, power consumption, is huge, which together with the increasing complexity of IC, both on physical and functional levels, offer wide opportunities for the attacker to surreptitiously embed hardware Trojans.

The relative ease of insertion of hardware Trojans into modern IC is an additional cause for concern. Modifications can be made to the hardware both in the development phase and in the production process, including such stages as specification, design, verification and manufacturing. Moreover, a hardware Trojan can be included in already made IC [1]. The situation is complicated by the fact that current trends in the semiconductor industry are characterized by the separation of development and production of IC, and the latter can be done by several factories scattered around the world, mainly in Asia. Engaging third-party subcontractors is typical not only for IC manufacturing, but also for design: developers use third-party software and ready-made blocks (IP cores), designed by a third party. IP cores are often supplied in binary form and are designed by third-party firms specializing in certain technical projects. Therefore, a hardware Trojan can be a simple change of paragraph in the specification, an additional line in the source code written in hardware description language (HDL), or a modification of the silicon chip in a factory, for example, a small change in the topology of the transistor. If the change is made in the diffusion layer, on the chip it becomes practically "invisible" [2].

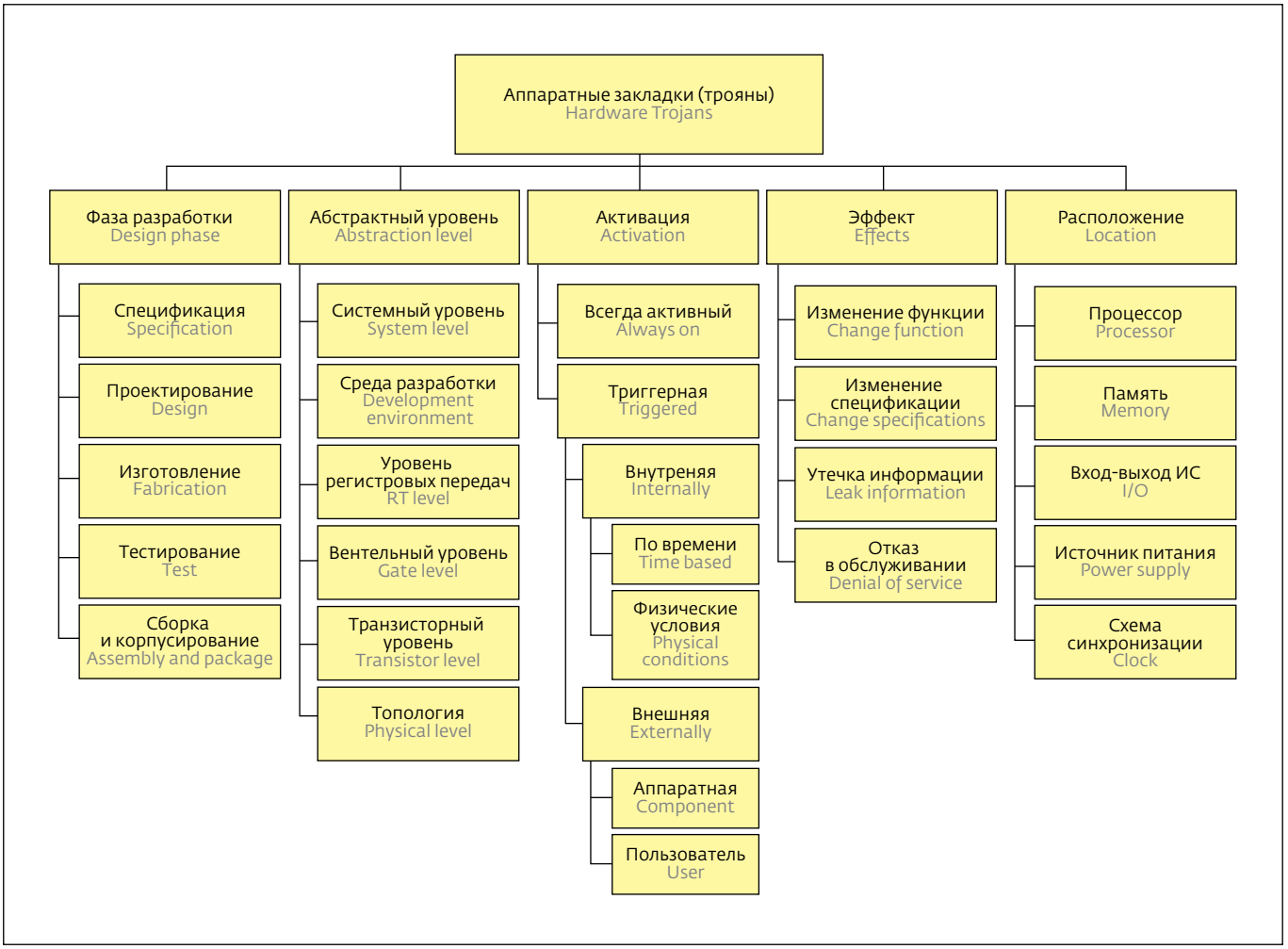

Рис.1. Классификация аппаратных троянов [5]
Fig.1. Classification of hardware trojans [5]

Currently, the problem of hardware Trojans is studied comprehensively in the world. For example, the Polytechnic Institute of New York University annually organizes competitions between teams for insertion and search of special devices [3], which contributes to the development of technologies for preventing the insertion and methods for the detection of hardware Trojans. The Defense Advanced Research Projects Agency (DARPA) of the United States Department of Defense has initiated in 2007 a special program to ensure the authenticity of IC used in military systems of the USA and conducts R&D on the development of methods and technologies to detect hardware Trojans [4]. The majority of other published studies is conducted in universities and mainly focuses on how to prevent the insertion of Trojans during the development of IC, as well as on methods for their identification in the IC after fabrication.

If a hardware Trojan was ever inserted into the system, it is always present regardless of whether is the device on or off. If the Trojan is inserted to any of system's IC, he has the potential to disrupt the entire system. The impact of hardware Trojans can range from a simple targeted attacks to complex attacks, which provide the fulcrum for high-level software-based attacks. Target attacks, in particular, include the following:

- change bits of information that violates the integrity of the stored data;
- weakening the functionality of the cryptographic cores;
- attack leading to the leakage of confidential information.

The system can be infected with several hardware Trojans, which joint actions undermine its security.

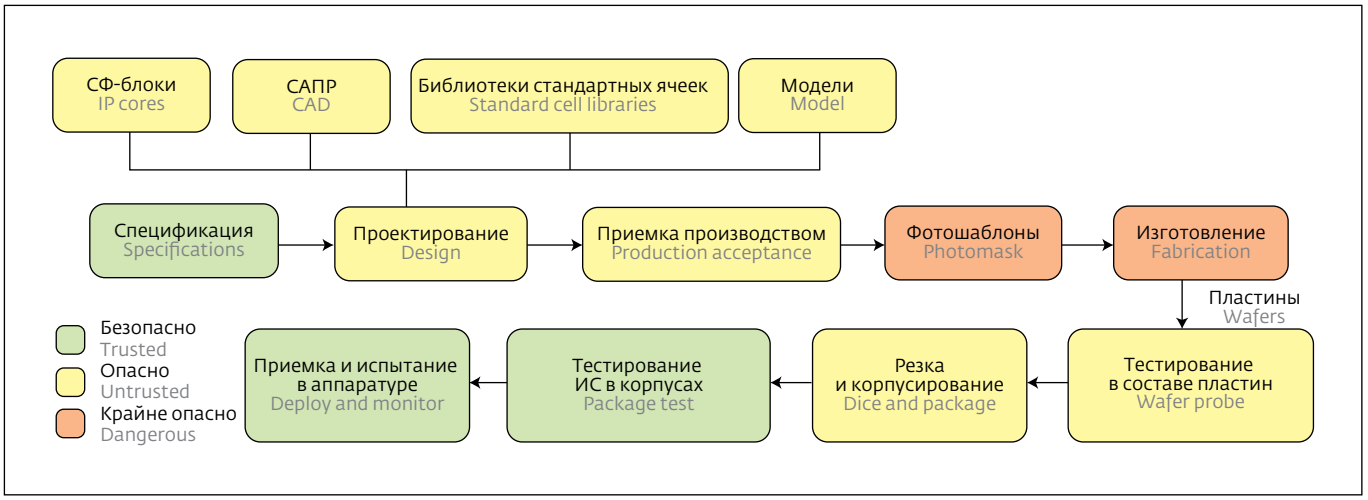

Рис.2. Стадии производства ИС и соответствующие уровни опасности внедрения аппаратной закладки [6]
Fig.2. Stages of IC manufacturing and corresponding levels of risk of insertion of hardware trojans [6]

ческих характеристик. Далее проводится резка пластин на чипы, их корпусирование, тестирование готовых к эксплуатации ИС, испытание и приемка. На рис.2 приведены стадии производства ИС и соответствующие им оценки уровней опасности внедрения аппаратной закладки [6].

Неуязвимыми с точки зрения внедрения аппаратных троянов являются только стадии спецификации, тестирования в корпусе, а также испытания и приемки. Все остальные стадии уязвимы к внедрению аппаратных троянов, и безопасность ИС на них определяется соисполнителями, которые обеспечивают изготовление ИС и ее тестирование, а также поставщиками средств разработки, IP-блоков и библиотек. Но даже стадии, которые отмечены выше как безопасные, могут быть подвержены влиянию злоумышленника, например, возможна настройка аппаратной закладки во время тестирования или во время поставки ИС. Поэтому полный цикл производства ИС должен быть всесторонне исследован с рассмотрением как стратегий эффективной профилактики внедрения троянов, так и технологий их обнаружения.

Трояны могут внедряться в любые элементы информационной системы. Локализация трояна

To fully understand the impact of hardware Trojans on the system and for their detection it is necessary to study the possibilities of data change in case of the insertion of Trojans, and also possible mechanisms of their activation. Therefore, investigation of the possible threats caused by Trojans, development of design and methods of their insertion and activation are a necessary part of the work in finding ways for prevention the insertion, and for detection and countering hardware Trojans to ensure the safety of the used IC.

For consideration of possible security threats caused by hardware Trojan, and determination of its impact on the information system, it is advisable to structure the characteristic signs of Trojans. To describe such characteristic properties several classifications of hardware Trojans were proposed. The purpose of such classifications is the systematization of the study, the development of common detection methods and approaches providing suppression of the effects of different classes of Trojans as well as comparison of different methods of counteraction. Fig.1 shows the most complete classification of hardware Trojans, proposed in the paper [5]. This classification takes into account both the phases of development of IC and levels of the possible insertion of hardware Trojans.

Development and manufacture of IC generally include such steps as specification of IC, its development, production, testing and packaging. They should be considered also as the stages on which the attacker can insert a hardware Trojan. At the specification stage, the characteristics of the system are defined, including used models and the estimated functionality of IC. After this phase the system features are implemented at

может ограничиваться отдельным компонентом, а может быть рассредоточена и на нескольких компонентах, таких как процессор, память, схемы входа-выхода, источники питания или схемы синхронизации. Особенность локализации определяется сложностью проекта ИС, трудностью внедрения и тем эффектом, который должен вызвать аппаратный троян. В связи с этим необходимо исследовать возможные механизмы работы аппаратных троянов, и на характерных примерах рассмотреть последствия, которые можно ожидать от их внедрения. Тем самым можно охарактеризовать угрозы, связанные с аппаратными троянами.

Аппаратные закладки являются относительно новыми угрозами кибербезопасности, при этом они существенно расширяют возможности для атаки на информационные системы. Ранее атаки ограничивались только программными средствами, сосредотачиваясь на слабых местах программного обеспечения. Средства защиты конкретного программного обеспечения разрабатывались исходя из аутентичности аппаратного обеспечения, поэтому общепринятые подходы к защите программными средствами не способны обеспечить безопасность от аппаратных троянов. С этой точки зрения аппаратные закладки представляют достаточно сложную проблему обеспечения безопасности.

Трояны могут быть внедрены в ИС специализированного назначения (ASIC), в коммерческие электронные компоненты, находящиеся в свободной продаже (COTS – Commercial Off The Shelf), микропроцессоры, цифровые сигнальные процессоры или в виде программных изменений в "прошивке" ПЛИС (FPGA). Учитывая, что изменения вносятся на самый низкий уровень системы, типы нарушающего действия могут иметь разнообразный характер. Эти воздействия можно условно классифицировать как изменение функциональности, изменения спецификации, утечка информации или отказ в обслуживании. Специфические аппаратные трояны могут реализовать любое из этих нарушающих воздействий.

Аппаратные трояны, изменяющие функциональность ИС через внедрение дополнительной логической схемы или посредством выключения части существующей логики, непосредственно ставят под угрозу целостность и сохранность информационной системы. Изменение данных в памяти, воздействие на вычислительные операции или на коммуникационный канал являются характерными целями рассматриваемого внедрения. Модификации функциональности могут носить очень разнообразный характер; воздействия этого класса аппаратных троянов ограничены только ресурсами системы, воображением и умением злоумышленника. Например, в [7] представлен сценарий, в котором простая деструктивная аппаратная закладка может вставить ошибку в алгоритм на основе китайской теоремы об остатках при вычислении криптографического алгоритма с открытым ключом (RSA), что приводит к компрометации RSA- ключа.

the design stage on a certain constructive and technological basis taking into account the functional and physical constraints. At the production stage a set of photomasks is prepared, and the manufacturing of the chips on silicon wafers with subsequent verification of their functional and physical characteristics is carried out. Further cutting of wafers, packaging of chips, testing of ready for operation IC and acceptance are carried out. Fig.2 shows the stages of production of IC and corresponding assessment levels of the risk of insertion of the hardware Trojans [6].

Only specification, test in package, and acceptance are invulnerable from the point of view of the insertion of hardware Trojans. All other stages are vulnerable to the insertion of hardware Trojans, and the security of the IC is determined by subcontractors, which provide production of IC and their testing, as well as by suppliers of development tools, IP cores and libraries. But even stages, which are marked above as "safe", can be influenced by an attacker, for example, it is possible to configure a hardware Trojan during testing or supply of IC. Therefore, a complete production cycle of IC needs to be thoroughly investigated with the consideration of strategies to effectively prevent the insertion of Trojans and technologies for their detection.

Trojans can be inserted in any elements of the information system. Localization of a Trojan may be limited to a separate component, and may be dispersed on several components such as processor, memory, input/output circuits, power supply or synchronization circuit. Location is determined by the complexity of the project, the difficulty of insertion, and the effect, which

В работе [5] приводится пример модификации, в результате которой модуль обнаружения ошибок принимает входные сигналы, которые должны быть отклонены.

Непосредственные ошибки в ИС, как например Pentium FDIV (ошибка в модуле операций с плавающей запятой в оригинальных процессорах Pentium выпуска 1994 года), могут быть воспроизведены аппаратной закладкой, причем для предотвращения ее обнаружения может использоваться выборочное включение. Специальные аппаратные трояны могут разрабатываться для изменения порядка выполнения инструкций центрального процессора, утечки данных через побочные каналы, изменения содержимого программируемой постоянной памяти (PROM).

Изменение функциональности системы может быть использовано для поддержки более широких атак. Так, в работе [6] отмечено, что возможности нанесения ущерба безопасности существенно увеличиваются при совместном использовании аппаратной и программной атаки. В качестве примера приведены изменения в центральном процессоре, поддерживающие атаку на программное обеспечение. В итоге предоставление доступа к памяти и модификация программы способствуют расширению полномочий с последующим доступом в систему через черный вход и атакой с кражей пароля.

Изменяющие спецификацию аппаратные трояны характеризуются тем, что искажают параметрические свойства целевой ИС или спецификации, не относящиеся к ее функциональности. Такие параметрические свойства включают синхронизацию или временные характеристики, а также потребляемую мощность ИС. Эффект достигается путем непосредственного изменения внутренних физических свойств – топологии межсоединений и геометрии транзисторных структур. В отличие от аппаратных троянов, которые влияют на функциональность, для этого класса характерны изменения топологии линий разводки и транзисторов, и их разрушительные действия могут приводить к отказам системы [6]. Можно предположить, что в дополнение к рассматриваемым модификациям может быть включена и такая аппаратная закладка, чтобы изменение спецификации имело триггерный или активационный механизм. Для рассматриваемого класса характерны различные типы воздействий на ИС, включая ограничение вычислительных возможностей системы путем внесения в схему генератора системной частоты, модификация вычислительных блоков или ячеек входа-выхода, при которой функциональность этих узлов не изменяется, но ухудшаются пропускные и динамические характеристики. Изменение размещения вентилей или разводки схемы, функционально эквивалентное, но при этом имеющее более высокие паразитные составляющие пассивных элементов, обуславливает ухудшение рабочих характеристик при высокой нагрузочной актив-

should be caused by hardware Trojan. In this regard, it is necessary to investigate the possible mechanisms of operation of hardware Trojans, and to consider, with examples, the effects that can be expected from their insertion. Thus it is possible to describe threats related to hardware Trojans.

Hardware Trojans are relatively new threats to cybersecurity, and they significantly expand the possibilities for attack on the information systems. Previously, attacks were limited to software only, focusing on weak areas of the software. Protection software was developing on the basis of the authenticity of the hardware, so conventional approaches to protecting software are not able to provide security against hardware Trojans. From this point of view, the hardware Trojans are rather complex problem of security.

Trojans can be embedded in the application-specific IC (ASIC), commercial off the shelf (COTS) IC, microprocessors, digital signal processors, or as software changes in the firmware for FPGA. Given that changes are made at the lowest level of the system, the type of violation may varies. These impacts can be classified as a change in functionality, changes in specifications, information leakage or denial of service. Specific hardware Trojans can implement any of these violations.

Hardware Trojans that change the functionality of IC through the insertion of additional logic circuitry or by switch-off of a part of the existing logic directly threaten the integrity and safety of an information system. Changing data in memory, the impact on computing or communication channel are typical goals of the considered insertion. Modification of functionality can be of very diverse nature; the impacts of this class of

ности и проявляется в возникновении временных ошибок. В работе [5] приведены примеры схем с перемычками в виде резистора, следствием которого становятся ошибки типа "закоротки" при некоторых режимах работы, и внесением конденсатора, приводящего к увеличению времени задержки за счет увеличения емкостной нагрузки.

Следующий класс троянов охватывает аппаратные модификации, направленные на скрытную передачу конфиденциальных данных от информационной системы злоумышленнику. Такая передача осуществляется без непосредственного участия системы и без ведома пользователя системы. Механизмы передачи могут задействовать как существующие внутренние и внешние каналы системы, так и побочные каналы. Например, в работе [6] отмечается, что утечка информации может происходить по радиочастотному, оптическому и тепловому побочным каналам. Информацию можно извлечь, анализируя потребляемую мощность ИС, ее шумовые характеристики, а также любые другие функциональные и физические характеристики. Интерфейсы RS232 и JTAG также могут быть использованы в качестве каналов утечки. Например, в работе [8] рассмотрена аппаратная закладка, которая позволяет определять ключи шифрования в беспроводной передаче по изменению амплитуды или частоты, которые возникают из-за вариаций технологии изготовления ИС. В работе [9] с использованием метода передачи сигналов с расширенным спектром информация о ключе шифрования извлекалась из изменения уровня собственных шумов КМОП ИС.

Системная модификация на самом низком уровне предоставляет широкий спектр возможностей для реализации ошибки типа "отказ в обслуживании" (DoS), которые варьируются от частичного проявления ошибки до полного и окончательного отключения системы внедрением так называемого "убивающего ключа" (kill switch) [11]. В работе [6] к этому классу отнесены трояны, которые влияют на обслуживание клиентов вычислительной системы через использование ограниченных ресурсов, таких как вычислительная способность, рабочий диапазон, мощность источника питания. Отмечается, что вносящие ошибку физические эффекты, изменение конфигурации системы или ее отключение могут быть временными или постоянными. Аппаратные закладки этого класса могут потреблять избыточную или всю энергию источника питания (аккумулятора), не позволяя системе перейти в спящий режим [11], или путем введения избыточных буферов в межсоединения ИС [12] уменьшать время работы устройства между подзарядками. Аппаратный троян может быть разработан с целью влияния на управление сигналом разрешения записи в память, перезаписывая существующее значение случайной величиной. Это ведет к побочным сбоям в работе служб или частичному и даже полному отключение системы. Ошибки "отказ в обслуживании",

hardware Trojans are limited only by system resources, imagination and skill of the attacker. For example, in [7] the scenario is presented, in which a simple destructive hardware Trojans can insert an error into the algorithm based on the Chinese remainder theorem for public-key cryptosystem (RSA), which leads to the compromise of the RSA key. In [5] an example of a modification is given, in which the error detection module accepts input signals that should be rejected.

The immediate errors in the IC, as for example the Pentium FDIV (error in the FPU in the original Pentium processors discovered in 1994), can be reproduced by the hardware Trojan, and to prevent its detection the selective switching can be used. Special hardware Trojans can be designed for change in execution order of CPU instructions, data leakage via side channels, change of the contents of a programmable memory (PROM).

Change in the functionality of the system can be used to support wider attacks. So, in paper [6] it is noted that the possibility of damage to the security is substantially increased, when the hardware and software attacks are used together. As an example, the changes in the central processor that supports an attack on software are described. As a result, all memory access and modification of the programme contribute to the empowerment, with subsequent access to the system through the back door and attack with the stolen password.

Hardware Trojans, which modify the specification, distort the parametric properties of the target IC or specifications that are not related to its functionality. Such parametric properties include synchronization, timing and power consumption of IC. The effect is achieved by directly modifying the internal physical

вызванные аппаратными троянами, могут быть связаны с преждевременным выходом устройства из строя. Так в работе [6] приведена схема, которая генерирует локальную избыточную мощность, что приводит к ускорению процесса старения ИС, сокращая срок ее службы без нарушения функциональности. Там же делается вывод, что с целью увеличения электромиграции возможно изменение химических компонентов в металлизированной разводке, причем эффект от этого может быть аналогичен увеличению напряжения питания или частоты синхронизации, что ведет к снижению времени наработки на отказ ИС.

***

Несанкционированные злоумышленные модификации ИС могут стать большой проблемой для обеспечения кибербезопасности электронных систем во всем мире, в особенности систем, задействованных в военной сфере и системах безопасности. В настоящее время военные ведомства многих стран не скрывают беспокойства в связи с расширяющимся аутсорсингом в области разработки и производства интегральных электронных компонентов, и зависимости новейших разработок от электронных компонентов, находящихся в свободной продаже. Аппаратные трояны угрожают нарушением целостности данных и функций, выполняемых любой вычислительной системой, которая содержит интегральные электронные компоненты. Суть возможных угроз заключается в функциональных и технических модификациях характеристик ИС, утечке конфиденциальной информации, а также атаках типа "отказ в обслуживании". Для предотвращения таких угроз необходима разработка комплексных методов и стратегий борьбы с аппаратными троянами, их предупреждения и выявления, а также мер противодействия им, что будет рассмотрено в последующих статьях цикла публикаций.

Статья подготовлена при финансовой поддержке Минобрнауки России в рамках выполнения государственного задания 8.527.2016/БЧ.

ЛИТЕРАТУРА

1. **Abramovici M., Bradley P.** Integrated circuit security: new threats and solutions //Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies. ACM, 2009. С. 55.
2. **Becker G.T.** et al. Stealthy dopant-level hardware trojans //Cryptographic Hardware and Embedded Systems-CHES 2013. Springer Berlin Heidelberg, 2013. С. 197–214.
3. Embedded System Challenge https://esc.isis.poly.ed
4. http://www.darpa.mil/Our_Work/MTO/Programs/Trusted_Integrated_Circuits_(TRUST).aspx
5. **Rajendran J.** et al. Towards a comprehensive and systematic classification of hardware trojans // Circuits and Systems (ISCAS), Proceedings of

properties – interconnection topology and geometry of transistor structures. In contrast to hardware Trojans, which affect the functionality, this class is characterized by changes in the topology of the wirings and transistors, and their destructive actions can lead to system failures [6]. We can assume that in addition to the considered modifications it may be activated hardware Trojans, which ensures change of the specifications with trigger or activation mechanism. Different types of impacts on IC are typical for this class, including limitation of computational capabilities of the system by insertion in the circuit of the system frequency generator, the modification of the computational units or input/output cells when the functionality of these nodes not change, but throughput and dynamic characteristics worsen. A change of the location of gates or wiring in the circuit may be functionally equivalent, but with a higher parasitic components of passive elements that leads to the performance degradation at high load and manifests in the appearance of transient errors. Paper [5] contains the examples of circuits with jumpers in the form of a resistor, a consequence of which are errors (short-circuits) in some modes, and addition of the capacitor, resulting in an increase in delay time due to the increase in capacitive load.

The next class of Trojans covers hardware modifications for transmission of confidential data from the information system to the attacker. Such transmission is carried out without direct participation of the system and without the knowledge of its user. The transfer mechanism can use existing internal and external channels, and side channels. For example, in [6] it is noted that leakage of information may occur via RF, optical and thermal side channels. Information

2010 IEEE International Symposium on. IEEE, 2010. C. 1871–1874.
6. **Chakraborty R.S., Narasimhan S., Bhunia S.** Hardware Trojan: Threats and emerging solutions // High Level Design Validation and Test Workshop. 2009. HLDVT 2009. IEEE International. IEEE, 2009. C. 166–171.
7. **Agrawal D.** et al. Trojan detection using IC fingerprinting //Security and Privacy, 2007. SP›07. IEEE Symposium on // IEEE, 2007. C. 296–310.
8. **Jin Y., Makris Y.** Hardware Trojans in wireless cryptographic integrated circuits // Design & Test, IEEE. Iss. 99. 2013. C. 1.
9. **Lin L., Burleson W., Paar C.** MOLES: malicious off-chip leakage enabled by side-channels // Proceedings of the 2009 International Conference on Computer-Aided Design. ACM, 2009. C. 117–122.
10. **Adee S.** The hunt for the kill switch // Spectrum, IEEE. 2008. T. 45. № 5. C. 34–39.
11. **Wolff F.** et al. Towards Trojan-free trusted ICs: Problem analysis and detection scheme // Proceedings of the conference on Design, automation and test in Europe. ACM, 2008. C. 1362–1365.
12. **Karri R.** et al. Trustworthy hardware: Identifying and classifying hardware trojans // Computer. 2010. T. 43. № 10. C. 39–46.

can be extracted by analyzing the power consumption of IC, its noise characteristics, as well as any other functional or physical characteristics. RS232 and JTAG interfaces can also be used as channels of leakage. For example, in [8] a hardware Trojan is described that allows to define the encryption keys in the wireless transmission with use of data about changing of the amplitude or frequency that occur due to variations of manufacturing technology. In [9], the information about the encryption key was retrieved from the change of the noise level of the CMOS IC using the signal transmission method with an expanded range.

System modification at the lowest level provides a wide range of opportunities for implementation of "denial of service" (DoS) errors, which range from the partial manifestation of the errors to the complete system shutdown by the insertion of so-called kill switch [11]. According to [6], this class includes Trojans that affect customer service in computer system through the use of limited resources such as computational capacity, operating range, power supply. It is noted that harmful physical effects, a change in system configuration or her shutdown may be temporary or permanent. Hardware Trojans of this class can consume excessive or the entire energy of the power supply (battery), not allowing the system to go into sleep mode [11], or by introducing excess buffers in the interconnects of IC [12] reduce the operating time of the device between charges. A hardware Trojan can be designed to distort the signal that enable writing to the memory by overwriting the existing value with a random value. This leads to collateral disruptions of services or partial, and even full system shutdown. DoS errors caused by hardware Trojans, can lead to premature failure of the device. Paper [6] describes a circuit that generates a local excess capacity, which leads to accelerating of aging of the IC, reduces its service life without breaking functionality. It is concluded in the same paper that to increase electromigration the change in the chemical components in the metallic wiring is possible, and the effect of this may be similar to increasing the voltage or frequency of synchronization that reduced the error-free running time of IC.

***

Unauthorized, malicious modification of the IC can become a big problem for the cyber security of electronic systems worldwide, in particular of systems for the military and security applications. Currently, the military departments of many countries do not hide the concern in connection with the expanding outsourcing in the field of development and production of integrated electronic components, and dependence of the latest developments from the COTS electronic components. Hardware Trojans threaten with violation of the integrity of the data and the functions performed by any computing system, which includes integral electronic components. The essence of possible challenges is in the functional and technical modifications of the characteristics of the IC, leakage of confidential information, as well as DoS attacks. To prevent such threats it is necessary to develop integrated methods and strategies against hardware Trojans, for their prevention and detection as well as responses to them that will be discussed in subsequent parts of this series of publications.

This paper was created with the financial support of the Ministry of Education and Science of the Russian Federation within the framework of the state order 8.527.2016/БЧ.