Аппаратные трояны: внедрение и проблемы обнаружения

А. Ю. Воронов, *В. Р. Стемпицкий*
Белорусский государственный университет информатики и радиоэлектроники,
г. Минск, Республика Беларусь

Увеличение разнообразия и спектров применения интегральных микросхем (далее – ИС) приводит к росту числа участников их производства и проектирования. Стороннее программное обеспечение для проектирования ИС, использование IP-блоков (Intellectual Property) других компаний значительно увеличивает риск внедрения в устройства вредоносных схем, называемых аппаратными троянами. Аппаратные трояны могут вызвать изменение функциональной работы устройства, утечку информации или вывод из строя [1]. В этом тезисе рассмотрен процесс внедрения аппаратных троянов с разными механизмами активации с помощью стороннего IP-блока, проведен анализ полученной структуры на схемотехническом уровне и на уровне программируемых блоков ПЛИС.

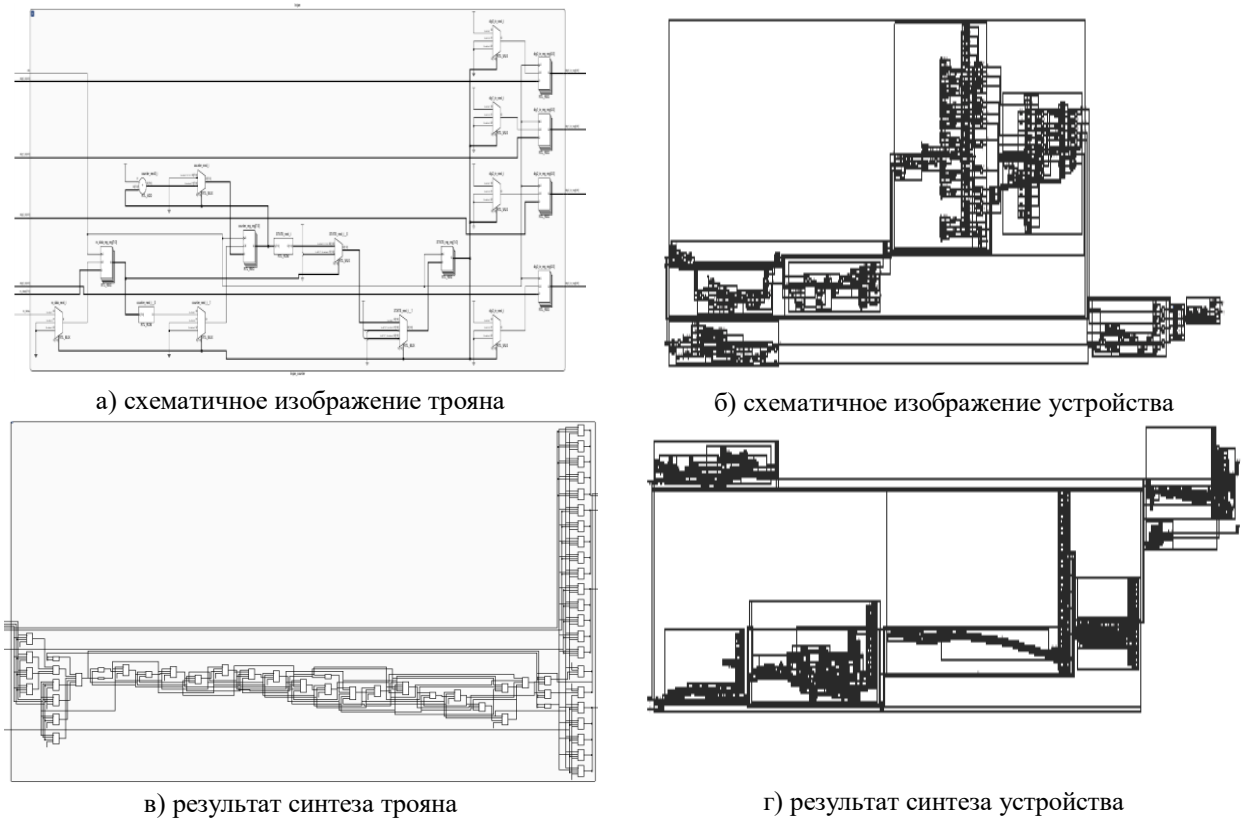
Ключевые слова: аппаратная безопасность, аппаратные трояны, ПЛИС.

С быстрым ростом информатизации общества популярность электронных устройств становится все выше и выше. В повседневной жизни люди используют электронные устройства для общения, совершения покупок и записи информации. В компаниях и банках данные обрабатываются и хранятся электронным оборудованием. Развивающиеся концепции умной окружающей среды, интернета вещей потребуют не только еще большего использования электронных устройств, но и увеличения их функционала и, следовательно, объема.

Как и программное обеспечение, аппаратное обеспечение имеет риски, связанные с безопасностью, а люди долгое время не знали о проблемах безопасности аппаратного обеспечения. В последние годы эксперты и ученые провели определенные исследования в области аппаратной безопасности, особенно в области безопасности микросхем, которые являются основной частью аппаратного обеспечения [2]. Как известно, процесс проектирования и производства ИС очень сложен. Для получения большей прибыли, привлекаются сторонние кампании, такие как проектировщики IP-блоков, поставщики программного обеспечения для автоматизированного проектирования и производственные предприятия. Перечисленные факторы сильно увеличивают риски внедрения аппаратных троянов а одном из этапов проектирования и производства ИС.

Стандартное определение аппаратным трояном было предложено фирмой IBM в 2007 году: аппаратные трояны относится к вредоносным схемам или вредоносным изменениям исходной схемы, которые существуют от стадии проектирования микросхемы до стадии тестирования упаковки микросхемы [3]. В данной работе будет рассмотрен процесс и результат внедрения аппаратного трояна в устройство, отвечающее за определение частоты и вывода ее значения на семисегментные индикаторы.

Для внедрения аппаратного трояна выбран определитель частоты, описанный на языке описания аппаратуры Verilog. Предполагается, что аппаратный троян встроен в IP-блок, реализующий UART-приемник (Universal Asynchronous Receiver / Transmitter), через который реализуется включение и выключение определителя частоты. Механизм активации первого встроенного аппаратного трояна является внутренним и представляет собой обычный восьмибитный счетчик. При достижении определенного значения, аппаратный троян переходит в состояние, при котором перестает отображаться реальное значение подаваемой частоты. Схематичное изображение устройства со встроенным трояном и реализация с помощью программируемых ресурсов ПЛИС изображена на рис. 1.



а) схематичное изображение трояна

б) схематичное изображение устройства

в) результат синтеза трояна

г) результат синтеза устройства

Рис. 1. Определитель частоты с аппаратным трояном с внутренним механизмом активации (счетчик)

Механизм активации второго аппаратного трояна, встроенного в рассматриваемое устройство, является внешним: при получении определенного значения по UART-приемнику, закладка влияет на схему также, как и в первом аппаратном трояне. Схематичное изображение устройства с трояном с внешним механизмом активации и его реализация с помощью программируемых ресурсов ПЛИС изображена на рис. 2.

Как видно из рис. 1 и 2, встроенные трояны, описанные на языках описания аппаратуры в виде автоматов с конечным состоянием, требует малых ресурсов для их реализации. На примере малого цифрового устройства, такого как определитель частоты, они занимают менее семи процентов, от общей схемы. Это делает крайне сложным определение внесение изменений в устройство путем анализа по потреблению электроэнергии, а для сверхбольших ИС и вовсе невозможным.

Легкость внедрения аппаратных троянов в ИС на одном из этапов проектирования и трудность их обнаружения делает их главной проблемой безопасности современных электронных устройств. На основе приведенных аппаратных закладок подтверждается их опасность.

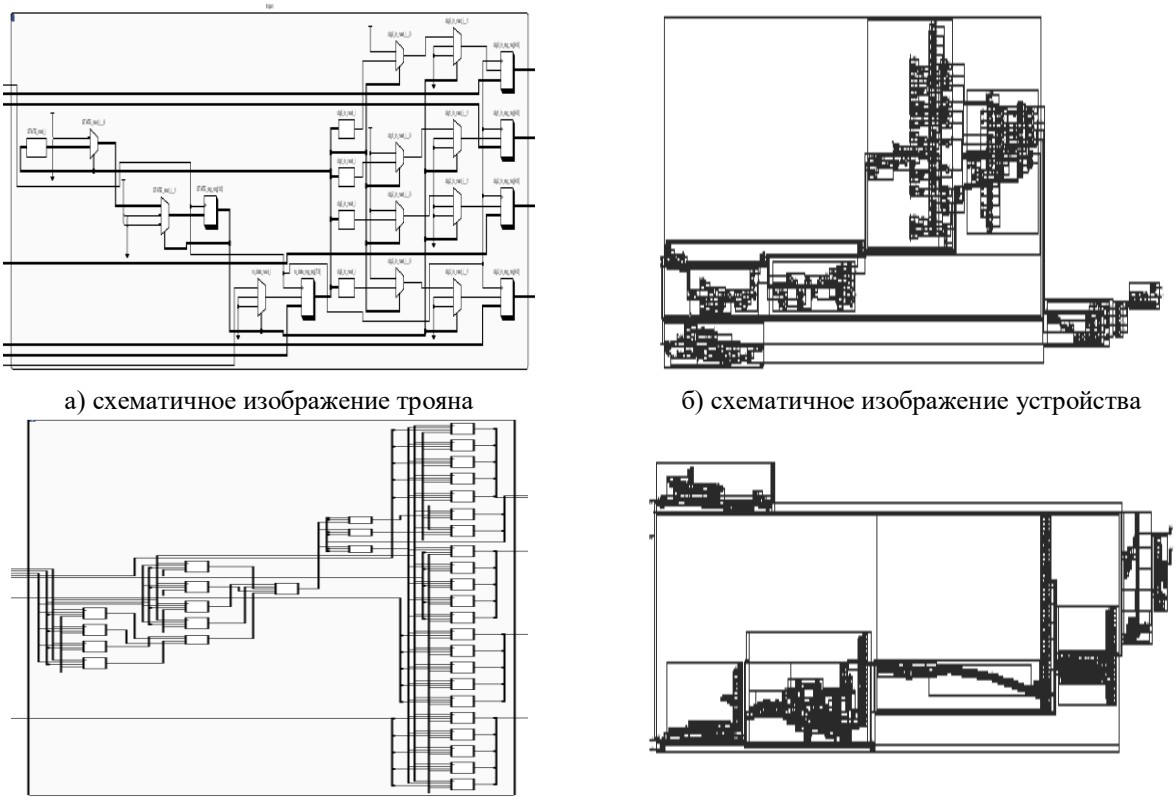
Список источников

[1] **Белоус, А. И.** Программные и аппаратные трояны – способы внедрения и методы противодействия. Первая техническая энциклопедия / А. И. Белоус, В. А. Солодуха, С. В. Шведов под общей редакцией А. И. Белоуса – М.: Техносфера, 2019 – 688 с

[2] **Dong, Ch.** Hardware Trojans in chips: A Survey for Detection and Prevention / Ch. Dong, Yi Xu, X. Liu – MDPI, Sensors 2020 – 37 p

[3] **Agrawal, D.** Trojan detection using IC fingerprinting. In Proceedings of the 2007 IEEE Symposium on Security and Privacy (SP’07) / D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi, B. Sunar – Berkeley, CA, USA, 20–23 May 2007 – p. 296–310.

[4] **Tripathi, A.** The economics of hardware trojans: An expert's opinion / A. Tripathi – Journal of Information Technology Case and Application Research, 2020 – 17 p
[5] **Xiao, K.** Hardware Trojans: Lessons Learned after One Decade of Research / K. Xiao, D. Forte, Y. Jin – ACM Transactions on Design Automation of Electronic Systems – 2016 – Vol. 22 – № 1 – Article 6
[6] **Xue, M.** Ten years of hardware Trojans: a survey from the attacker's perspective / M. Xue, Ch. Gu, W. Liu – IET Computers & Digital Techniques, 2020 – 16 p



а) схематичное изображение трояна б) схематичное изображение устройства

в) результат синтеза трояна г) результат синтеза устройства

Рис. 2. Определитель частоты с аппаратным трояном с внешним механизмом активации

Hardware trojans: implementation and detection's issues

A. Y. Voronov, V. R. Stempitsky
Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Annotation. The increase of integrated circuits (IC) diversity and range of applications leads to an increase participants number in their production and design. Third-party IC design software, the use of IP blocks (Intellectual Property) from other companies greatly increases the risk of implementation malicious schemes called hardware trojans into devices. Hardware trojans can cause a change in the functional operation of the device, information leakage or devise failure. This thesis considers the process of introducing hardware trojans with different activation mechanisms using a third-party IP block, analyzes the resulting structure at the schematic level and at the level of programmable FPGA blocks.

Keywords: Hardware security, Hardware trojans, FPGA.