КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ И АВТОМАТИЗАЦИЯ ПРОЕКТИРОВАНИЯ / COMPUTER MODELING AND DESIGN AUTOMATION

DOI: https://doi.org/10.60797/IRJ.2024.145.155

ОЦЕНКА КАЧЕСТВА СЛУЧАЙНЫХ ДВОИЧНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ С ПРИМЕНЕНИЕМ ПРОГРАММИРУЕМОЙ ЛОГИЧЕСКОЙ ИНТЕГРАЛЬНОЙ СХЕМЫ

Научная статья

Яковлев И.В.[1, *], Гузанов Р.О.[2], Панченко О.В.[3]

[1, 2, 3] Казанский национальный исследовательский технический университет им. А.Н. Туполева – КАИ, Казань, Российская Федерация

* Корреспондирующий автор (iakovleviv[at]gmail.com)

Аннотация

В данной статье рассматривается разработка и реализация устройства для оценки качества случайных двоичных последовательностей на базе программируемых логических интегральных схем (ПЛИС). Устройство предназначено для тестирования и проверки аппаратных генераторов случайных последовательностей, что играет критическую роль в обеспечении безопасности и точности в вычислениях в областях, где это особенно важно, таких как криптография и информационная безопасность. В статье подробно описывается процесс выбора аппаратной платформы, разработка методик и алгоритмов оценки, а также конечная реализация устройства с использованием отладочной платы Xilinx Spartan-6. Основное внимание уделено возможностям устройства проводить оценки в реальном времени, высокой точности результатов и экономичности использования ресурсов кристалла ПЛИС. Результаты тестирований подтвердили эффективность разработанной системы и её пригодность для использования в образовательных целях для демонстрации ключевых принципов криптографии и информационной безопасности.

Ключевые слова: программируемые логические интегральные схемы, оценка качества, случайные двоичные последовательности, криптография, информационная безопасность.

QUALITY ASSESSMENT OF RANDOM BINARY SEQUENCES USING A FIELD PROGRAMMABLE LOGIC DEVICE

Research article

Iakovlev I.V.[1, *], Guzanov R.O.[2], Panchenko O.V.[3]

[1, 2, 3] Kazan National Research Technical University named after A.N. Tupolev – KAI, Kazan, Russian Federation

* Corresponding author (iakovleviv[at]gmail.com)

Abstract

This article discusses the design and implementation of a programmable logic integrated circuit (FPLD)-based random binary sequence quality evaluation device. The purpose of the device is to test and validate hardware random sequence generators, which plays a critical role in ensuring security and accuracy in computing in areas where it is particularly important, such as cryptography and information security. The article details the hardware platform selection process, the development of evaluation techniques and algorithms, and the final implementation of the device using the Xilinx Spartan-6 debug board. The main attention is paid to the device's ability to perform real-time evaluation, high accuracy of results and economical use of FPLD crystal resources. Test results confirmed the effectiveness of the developed system and its suitability for educational use to demonstrate the key principles of cryptography and information security.

Keywords: field programmable logic device, quality assessment, random binary sequences, cryptography, information security.

Введение

В наше время случайные двоичные последовательности применяются в решении множества задач в математике, технике и криптографии. Они играют критическую роль в обеспечении безопасности и точности вычислений. Важным инструментом в этой области является устройство для оценки двоичных последовательностей на базе программируемых логических интегральных схем, предназначенное для тестирования и проверки аппаратных генераторов случайных последовательностей [1], [2]. Такое устройство позволяет оценивать качество генерирования последовательностей с высокой степенью точности и эффективности.

Основная цель данной работы – разработать и реализовать на ПЛИС блок оценки качества случайных двоичных последовательностей с использованием вероятностного подхода [3]. Реализация такого блока актуальна, так как позволяет гибко и эффективно тестировать аппаратные генераторы случайных последовательностей в режиме реального времени. Для достижения этой цели необходимо решить следующие задачи:

- изучить существующие методы оценки генераторов двоичных последовательностей на основе вероятности;
- выбрать подходящую аппаратную платформу для реализации устройства;
- разработать принципы функционирования и интерфейс взаимодействия с пользователем;
- спроектировать и реализовать блоки вычисления вероятности, управления параметрами, отображения на светодиодах, генерации случайных чисел;
- создать и настроить специализированный микроконтроллер, написать для него программное обеспечение;
- провести тестирование устройства и оценить его аппаратные затраты.

Применение данной разработки имеет значительный потенциал в образовательной сфере, где она может быть использована для создания лабораторных работ и курсов по криптографии и информационной безопасности. Описание функциональности устройства также может служить основой для практических занятий.

Техническая реализация устройства включает использование IP-ядра делителя для точного вычисления отношения количества единиц к общей длине двоичной последовательности. Это ядро позволяет пользователю задавать параметры деления и выбирать формат вывода результатов, что является ключевой особенностью системы.

Разработка такого устройства на отладочной плате Xilinx Spartan-6 LX9 MicroBoard [4], [5], использующей Vivado Design Suite для проектирования и отладки, обеспечивает доступ к необходимым ресурсам и интерфейсам для успешной реализации проекта.

Проектирование аппаратного блока

Устройство состоит из четырех блоков: генераторы последовательностей, вычисление вероятности, управление параметрами и контроллер с памятью. Пользователь выбирает тип генератора и задает длину выборки и частоту. Последовательность бит подается на блок подсчета статистики, который вычисляет вероятность получения единиц в последовательности. Эти данные отображаются на светодиодах и дисплее. Устройство имеет удобный интерфейс для взаимодействия с пользователем. Управление осуществляется с помощью переключателей и кнопок, а результаты отображаются на дисплее. Устройство работает в ручном и автоматическом режиме. Параметры и результаты отображаются на жидкокристаллическом дисплее.

Блок управления параметрами позволяет пользователю выбирать частоту синхронизации F и длину выборки N. Для каждого значения частоты и размера выборки представлены соответствующие двоичные коды. Таким образом, пользователь может указать нужные значения F и N, используя соответствующие двоичные комбинации.

Модуль предназначен для обработки случайных последовательностей длиной от 32 до 65535 бит. Интерфейс блока вычисления вероятности состоит из четырех входных и двух выходных портов. Входы включают в себя информацию о размере выборки, тактовую частоту, двоичную последовательность, сигнал очистки и сигнал запуска процесса оценки. Выходы предоставляют информацию о целой и дробной частях вероятности, а также сигнал о завершении вычислений. Функциональная схема модуля состоит из трех компонентов: блока для вычисления статистики единиц в последовательности, делителя и шинного мультиплексора. Дополнительное описание каждого компонента предоставлено в следующих разделах. Устройство STAT_BLOCK имеет те же входы, что и P_TESTER.

Оно предоставляет информацию о количестве единиц в последовательности, длине выборки и завершении вычислений через порты "n1(15:0)", "N_fix(15:0)" и "READY". Функциональная схема блока состоит из счетчиков, компаратора и регистров. Схема включает в себя два режима работы: ручной и автоматический. В ручном режиме корректность работы компонентов системы проверена. В автоматическом режиме статистика накапливается непрерывно за счет постоянного сигнала START, при этом длина выборки составляет 6.

В ходе выполнения работы были проведены следующие этапы схемотехнического проектирования: разработка IP-ядра делителя, проектирование шинного мультиплексора, создание генераторов двоичных, тестовых, псевдослучайных и истинно-случайных последовательностей, разработка блока управления параметрами, блока делителя частоты, блока отображения данных на светодиоды, а также проектирование периферийного микроконтроллера. Эти этапы позволяют создать и управлять сложной цифровой системой, обеспечивая необходимую функциональность и надежность ее работы. Комплексный подход к проектированию данных блоков способствует эффективной реализации цифровых устройств и систем, обеспечивая оптимальное соотношение между функциональностью, производительностью и ресурсами системы.

Схема сборки представлена на рисунке 1.

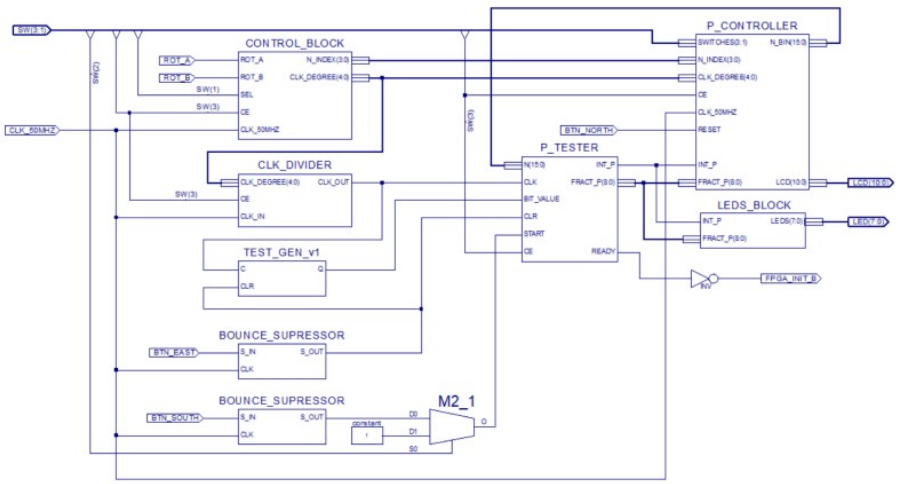

Рисунок 1 - Архитектура аппаратного блока

DOI: https://doi.org/10.60797/IRJ.2024.145.155.1

В состав этой схемы входят генератор двоичных последовательностей, блок вычисления вероятности, блок управления параметрами, делитель частоты, периферийный контроллер, блок отображения на светодиоды. В схеме

также присутствуют мультиплексор и два гасителя дребезгов [6], на входы которых подаются кнопки BTN_EAST и BTN_SOUT

Разработка программной части

При выполнении программной части в двоичном коде необходимо выбрать подходящую систему команд для процессора. В проекте были выбраны 18 команд, где каждая команда имеет свой уникальный шестиразрядный код CODE(5:0) и двенадцатиразрядное поле данных Data(11:0).

Таблицы подстановок, хранящиеся в памяти ROM_1024x18, являются важной частью работы и выполняют различные преобразования с данными. При выполнении программы или подпрограммы, устройство может обращаться к этим таблицам для выполнения соответствующих операций на основе заданных значений в таблицах. В проекте имеются следующие таблицы подстановок:

1. Таблица подстановки для двоично-десятичного кода вероятности. Используется в процессе преобразования двоичной дробной части вероятности в эквивалентный двоично-десятичный код. Она расположена во второй половине памяти ROM_1024x18, начиная с адреса 512 и заканчивая адресом 10.

2. Таблица подстановки для двоично-десятичного кода погрешности (см. табл.).

Таблица 1 - Подстановки для двоично-десятичного кода погрешности

DOI: https://doi.org/10.60797/IRJ.2024.145.155.2

DEC	B3	B2	B1	B0	N	Коэф. Стьюд. t	Погрешность выборки, DEC	Погрешность перевода, DEC	Суммарная погрешн., DEC
4	0	1	0	0	32	2,02	0,178544	0,000977	0,1795
5	0	1	0	1	64	1,96	0,1225	0,000977	0,1235
6	0	1	0	1	128	1,96	0,086621	0,000977	0,0876
7	0	1	0	1	256	1,96	0,06125	0,000977	0,0622
8	1	0	0	1	512	1,96	0,043321	0,000977	0,.0443
9	1	0	0	1	1024	1,96	0,030625	0,000977	0,0316
10	1	0	0	1	2048	1,96	0,021655	0,000977	0,0226
11	1	0	0	1	4096	1,96	0,015313	0,000977	0,0163
12	1	1	1	0	8192	1,96	0,010827	0,000977	0,0118
13	1	1	1	0	16384	1,96	0,007656	0,000977	0,0086
14	1	1	1	0	32768	1,96	0,005414	0,000977	0,0064
15	1	1	1	0	65535	1,96	0,003824	0,000977	0,0048

После выбора системы команд разработана подпрограмма, в которой осуществляется инициализация дисплея, программирование символов. В качестве примера на рисунке представлена диаграмма программы компонента COMMANDER.

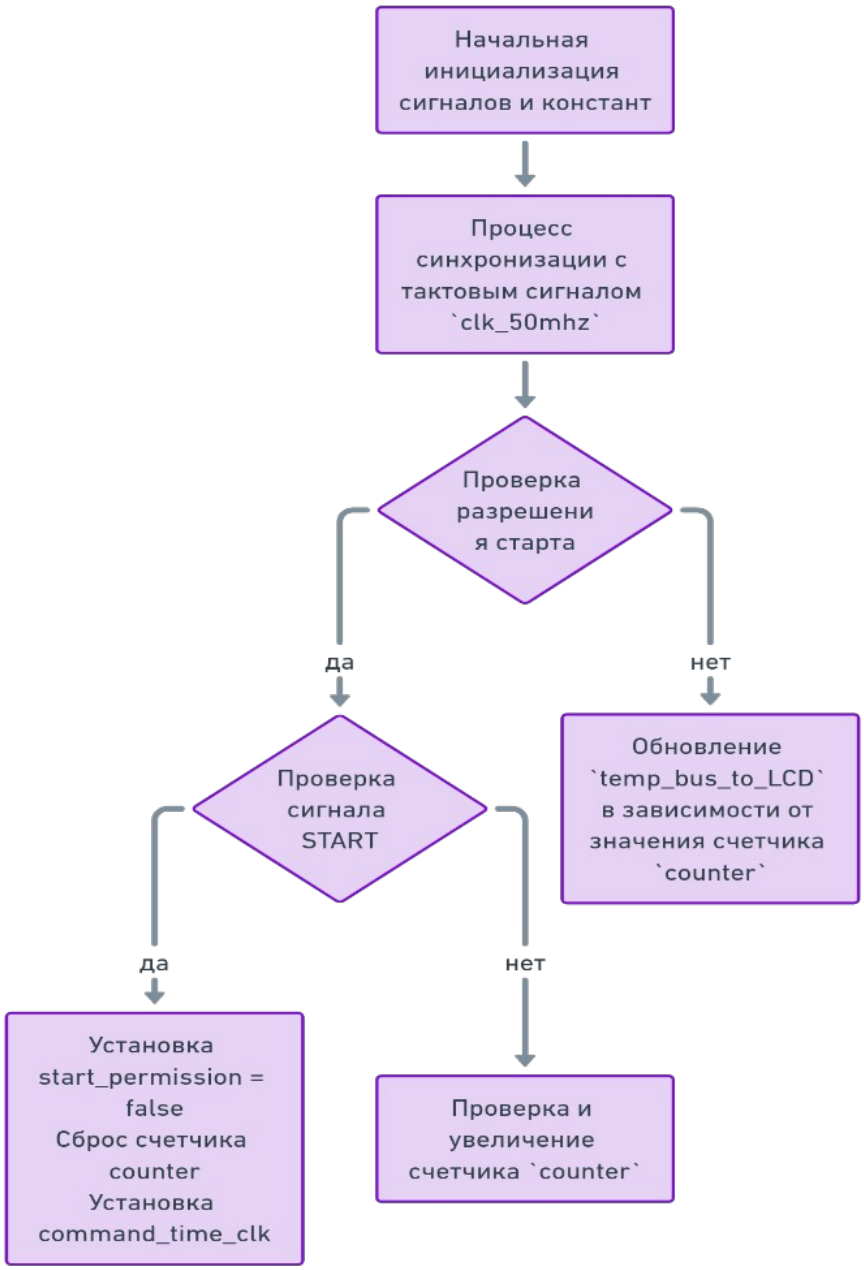

Рисунок 2 - Диаграмма программы компонента COMMANDER
DOI: https://doi.org/10.60797/IRJ.2024.145.155.3

В подпрограмме осуществляются команды вывода значения частоты, длины выборки, вероятности и погрешности. Кроме того, программируются таблицы подстановки для выборки N и погрешности. Подпрограмма занимает строчки с 50 по 511, при этом только 14 строк остаются неиспользованными.

Тестирование

Работоспособность спроектированного устройства с помощью тестового генератора TEST_GEN_v1 представлена на рисунках 3, 4, 5.

Количество разрядов 32			Начальное состояние регистра сдвига «01010101010101010101010101010101»	
№	N	F	Режим	Результат измерений
1	32	50 MHz	Ручной	
2	1024	97,66 KHz	Ручной	
3	65535	190,7 Hz	Ручной	

Рисунок 3 - Тестирования генератора TEST_GEN_v1

DOI: https://doi.org/10.60797/IRJ.2024.145.155.4

Количество разрядов 32			Начальное состояние регистра сдвига «11000000000000000000000000000011»	
№	N	F	Режим	Результат измерений
1	32	50 MHz	Автоматический	
2	1024	97,66 KHz	Автоматический	
3	65535	190,7 Hz	Автоматический	

Рисунок 4 - Тестирования генератора TEST_GEN_v1
DOI: https://doi.org/10.60797/IRJ.2024.145.155.5

После проверки работоспособности спроектированного устройства с помощью тестового генератора TEST_GEN_v1, запустим генератор TEST_GEN_v2 для дальнейшей оценки функциональности блока оценки качества двоичных последовательностей.

Количество разрядов 64			Начальное состояние регистра сдвига «0000000000000000000000000000000»& «11111111111111111111111111111111»	
№	N	F	Режим оценки	Результат измерений
1	32	50 MHz	Ручной	
2	32	50 MHz	Ручной	
3	256	50 MHz	Ручной	
4	1024	97,66 KHz	Ручной	
5	65535	190,7 Hz	Ручной	

Рисунок 5 - Тестирование генератора TEST_GEN_v2
DOI: https://doi.org/10.60797/IRJ.2024.145.155.6

Результаты оценки вероятности соответствуют ожидаемым значениям, что подтверждает правильную работу блока оценки качества. Анализ светодиодов позволяет определить наличие отклонений в сторону единиц и нулей, и в данном случае все результаты соответствуют ожиданиям.

По полученным оценкам аппаратных затрат ресурсов кристалла ПЛИС на реализацию блока оценки качества случайных двоичных последовательностей можно сделать вывод о затратах основных аппаратных ресурсов кристалла ПЛИС (триггеров, таблиц преобразования LUT, секций КЛБ) менее 11%, что свидетельствует об экономичности разработанной схемы устройства и хорошем качестве проектирования. В оценку аппаратных затрат блока оценка качества случайных двоичных последовательностей не вошёл периферийный контроллер, задача которого заключается

в реализации интерфейса взаимодействия с пользователем. Блок P_TESTER предоставляет гибкость при работе с выборками, так как он способен обрабатывать последовательности с фиксированной длиной выборки, а также с переменной длиной, что позволяет адаптировать его к различным аппаратным решениям.

В работе также были проведены эксперименты с использованием генераторов Фибоначчи [7] и Галуа [8] для создания псевдослучайных двоичных последовательностей. Целью было изучение свойств и сравнение качества генерируемых последовательностей при различных параметрах, таких как частота и длина выборки. Результаты показали, что генератор Фибоначчи имеет постоянную вероятность появления единиц из-за фиксированного периода, в то время как генератор Галуа обладает более высокой степенью случайности. При увеличении длины выборки к периоду генератора можно ожидать стабильные результаты. Однако дальнейшее увеличение длины выборки может не привести к значительным изменениям, так как генератор достигнет всевозможных состояний.

Также для проведения экспериментов были выбраны генераторы, основанные на цифровых элементах задержки. Эти генераторы имеют различное количество цифровых элементов задержки, такие как 1, 3, 5 и 7. Вероятность появления единиц в последовательностях генераторов на различном количестве элементов задержки может изменяться в зависимости от частоты и длины выборки. Разброс значений вероятности, выраженный через доверительные интервалы, уменьшается с увеличением длины выборки.

Заключение

В данной статье мы рассмотрели разработку и реализацию устройства для оценки качества случайных двоичных последовательностей на базе программируемых логических интегральных схем. Это устройство предоставляет возможность проведения точных и эффективных испытаний аппаратных генераторов случайных последовательностей, что крайне важно для обеспечения безопасности и точности в высокотехнологичных областях, таких как криптография и информационная безопасность.

Проект включал несколько ключевых этапов: от выбора аппаратной платформы и разработки алгоритмов до создания и тестирования готового устройства. Результаты тестирования подтвердили высокую эффективность разработанного блока оценки качества, что позволяет оценить генерируемые последовательности в реальном времени с высокой точностью.

Особое внимание было уделено удобству использования разработанного устройства, включая интуитивно понятный интерфейс и возможность работы в ручном и автоматическом режимах. Экономичность использования ресурсов кристалла ПЛИС и функциональность системы, позволяющая обрабатывать как фиксированную, так и переменную длину последовательностей, делают эту разработку пригодной не только для лабораторных исследований, но и для образовательных целей в курсах по криптографии и информационной безопасности [9], [10].

В заключение, данная разработка демонстрирует важность комплексного подхода к проектированию и реализации аппаратных систем, которые требуют высокой степени надежности и точности. Благодаря успешной реализации проекта и его потенциалу в образовательной сфере, ожидается, что устройство найдет широкое применение как в научных, так и в образовательных учреждениях, способствуя повышению качества обучения и исследований в области информационной безопасности.

Конфликт интересов

Не указан.

Рецензия

Все статьи проходят рецензирование. Но рецензент или автор статьи предпочли не публиковать рецензию к этой статье в открытом доступе. Рецензия может быть предоставлена компетентным органам по запросу.

Conflict of Interest

None declared.

Review

All articles are peer-reviewed. But the reviewer or the author of the article chose not to publish a review of this article in the public domain. The review can be provided to the competent authorities upon request.

Список литературы / References

1. Ivanyuk A.A. FPGA Based Arbiter Physical Unclonable Function Implementation with Reduced Hardware Overhead / A.A. Ivanyuk, S.S. Zalivako // Communications in Computer and Information Science. — 2019. — Vol. 1055. — P. 216-227. — DOI 10.1007/978-3-030-35430-5_18.

2. Строгонов А.В. Проектирование сложно-функциональных блоков в базисе ПЛИС: учебное пособие / А.В. Строгонов, С.А. Цыбин, А.В. Строгонов [и др.]; ГОУВПО "Воронежский гос. технический ун-т". — Воронеж: Воронежский гос. технический ун-т, 2010. — 333 с.

3. Эннс В.И. Проектирование специализированных гетерогенных ПЛИС с использованием программного прототипирования / В.И. Эннс // Проблемы разработки перспективных микро- и наноэлектронных систем (МЭС). — 2021. — № 4. — С. 22-26. — DOI 10.31114/2078-7707-2021-4-22-26.

4. Соловьев Д.М. Цифровая адаптивная система слежения за фазой и частотой сигнала на базе ПЛИС Xilinx Spartan-3A DSP / Д.М. Соловьев, Д. Э. Палей // Вестник Ярославского государственного университета им. П.Г. Демидова. Серия Естественные и технические науки. — 2011. — № 2. — С. 63-72.

5. Кульминский Д.Д. Разработка модели хаотического генератора с запаздывающей обратной связью на базе ПЛИС Xilinx семейства Spartan-6 / Д.Д. Кульминский, Ю.М. Ишбулатов, В.В. Сказкина // Наноэлектроника, нанофотоника и нелинейная физика: Сборник трудов XV Всероссийской конференции молодых ученых, Саратов, 08-10 сентября 2020 года. — Саратов: Техно-Декор, 2020. — С. 140.

6. Соловьев В.И. Исследование условий возникновения повторных замыканий герконов при разрыве тока / В.И. Соловьев, Ж.В. Солотенкова, В.А. Коротченко // Вестник Рязанского государственного радиотехнического университета. — 2011. — № 37. — С. 65-69.

7. Литюк В.И. Цифровой генератор чисел Фибоначчи / В.И. Литюк, Л.В. Литюк // Известия ТРТУ. — 2006. — № 9-1(64). — С. 29-30.

8. Логинов С.С. Генераторы псевдослучайных сигналов на основе систем с динамическим хаосом, реализованных над конечным полем Галуа / С.С. Логинов, М.Ю. Зуев // Системы синхронизации, формирования и обработки сигналов. — 2019. — Т. 10, № 2. — С. 24-27.

9. Утеев Г. Разработка децентрализованной системы идентификации личности по биометрическим данным с помощью технологии блокчейн и компьютерного зрения / Г. Утеев, Р.Ф. Гибадуллин // Международный научно-исследовательский журнал. — 2024. — № 4(142). — DOI 10.23670/IRJ.2024.142.6.

10. Ускорение AES шифрования на аппаратно-программной платформе NVIDIA CUDA / Р.Ф. Гибадуллин, А.С. Яковлев, А.А. Новиков и др. // Вестник Технологического университета. — 2017. — Т. 20, № 12. — С. 97-103.

Список литературы на английском языке / References in English

1. Ivanyuk A.A. FPGA Based Arbiter Physical Unclonable Function Implementation with Reduced Hardware Overhead / A.A. Ivanyuk, S.S. Zalivako // Communications in Computer and Information Science. — 2019. — Vol. 1055. — P. 216-227. — DOI 10.1007/978-3-030-35430-5_18.

2. Strogonov A.V. Proektirovanie slozhno-funkcional'nyh blokov v bazise PLIS: uchebnoe posobie [Designing complex functional blocks in the FPLD basis: a textbook] / A.V. Strogonov, S.A. Cybin, A.V. Strogonov [et al.]; GOUVPO " Voronezh State Technical University". — Voronezh : Voronezh State Technical University, 2010. — 333 p. [in Russian]

3. Enns V.I. Proektirovanie specializirovannyh geterogennyh PLIS s ispol'zovaniem programmnogo prototipirovaniya [Designing specialized heterogeneous FPLDs using software prototyping] / V.I. Enns // Problemy razrabotki perspektivnyh mikro- i nanoelektronnyh sistem (MES) [Problems of developing promising micro- and nanoelectronic systems (MES)]. — 2021. — № 4. — P. 22-26. — DOI 10.31114/2078-7707-2021-4-22-26 [in Russian].

4. Solov'ev D.M. Cifrovaya adaptivnaya sistema slezheniya za fazoj i chastotoj signala na baze PLIS Xilinx Spartan-3A DSP [Digital adaptive signal phase and frequency tracking system based on Xilinx Spartan-3A DSP FPGA] / D.M. Solov'ev, D. E. Palej // Vestnik YAroslavskogo gosudarstvennogo universiteta im. P.G. Demidova. Seriya Estestvennye i tekhnicheskie nauki [Bulletin of Yaroslavl State University named after P.G. Demidov. Natural and Technical Sciences Series]. — 2011. — № 2. — P. 63-72 [in Russian].

5. Kul'minskij D.D. Razrabotka modeli haoticheskogo generatora s zapazdyvayushchej obratnoj svyaz'yu na baze PLIS Xilinx semejstva Spartan-6 [Development of a model of a chaotic generator with delayed feedback based on the Xilinx FPGA of the Spartan-6 family] / D.D. Kul'minskij, YU.M. Ishbulatov, V.V. Skazkina // Nanoelektronika, nanofotonika i nelinejnaya fizika: Sbornik trudov XV Vserossijskoj konferencii molodyh uchenyh, Saratov, 08-10 sentyabrya 2020 goda [Nanoelectronics, Nanophotonics and nonlinear physics: Proceedings of the XV All-Russian Conference of Young Scientists, Saratov, September 08-10, 2020]. — Saratov: Tekhno-Dekor, 2020. — P. 140 [in Russian].

6. Solov'ev V.I. Issledovanie uslovij vozniknoveniya povtornyh zamykanij gerkonov pri razryve toka [Investigation of the conditions for the occurrence of repeated short circuits of reed switches during a current break] / V.I. Solov'ev, ZH.V. Solotenkova, V.A. Korotchenko // Vestnik Ryazanskogo gosudarstvennogo radiotekhnicheskogo universiteta [Bulletin of the Ryazan State Radio Engineering University]. — 2011. — № 37. — P. 65-69 [in Russian].

7. Lityuk V.I. Cifrovoj generator chisel Fibonachchi [Digital Fibonacci Number Generator] / V.I. Lityuk, L.V. Lityuk // Izvestiya TRTU [Proceedings of the TRYU]. — 2006. — № 9-1(64). — P. 29-30 [in Russian].

8. Loginov S.S. Generatory psevdosluchajnyh signalov na osnove sistem s dinamicheskim haosom, realizovannyh nad konechnym polem Galua [Pseudorandom signal generators based on dynamic chaos systems implemented over a finite Galua field] / S.S. Loginov, M.YU. Zuev // Sistemy sinhronizacii, formirovaniya i obrabotki signalov [Synchronization, signal generation and processing systems]. — 2019. — V. 10, № 2. — P. 24-27 [in Russian].

9. Uteev G. Razrabotka decentralizovannoj sistemy identifikacii lichnosti po biometricheskim dannym s pomoshch'yu tekhnologii blokchejn i komp'yuternogo zreniya [Development of a decentralized identity identification system based on biometric data using blockchain and computer vision technologies] / G. Uteev, R.F. Gibadullin // Mezhdunarodnyj nauchno-issledovatel'skij zhurnal [International Scientific Research Journal]. — 2024. — № 4(142). — DOI 10.23670/IRJ.2024.142.6 [in Russian].

10. Uskorenie AES shifrovaniya na apparatno-programmnoj platforme NVIDIA CUDA [Acceleration of AES encryption on the NVIDIA CUDA hardware and software platform] / R.F. Gibadullin, A.S. YAkovlev, A.A. Novikov et al. // Vestnik Tekhnologicheskogo universiteta [Bulletin of the Technological University]. — 2017. — V. 20, № 12. — P. 97-103 [in Russian].