# АННОТАЦИЯ

диссертации на соискание степени «доктора философии» (PhD) по образовательной программе «8D06201 – Радиотехника, электроника и телекоммуникации»

**СҚАБЫЛОВ ӘЛІШЕР ӘЛИҰЛЫ**

## АППАРАТНО-ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ШИФРОВАНИЕ ДАННЫХ НА ОСНОВЕ ПЛИС

**Общая характеристика работы**

Докторская диссертация, обсуждаемая в настоящем исследовании, направлена на реализацию аппаратного и программного обеспечения шифрования данных в телекоммуникационных сетях, включая интернет вещей и системы безопасной связи. Исследование предлагает подход, основанный на использовании программируемых логических интегральных схем (ПЛИС) для достижения высокоскоростного и надежного шифрования путем параллельной и конвейерной обработки данных. Ключевым аспектом работы является использование генераторов хаоса для генерации псевдослучайных чисел, используемых в качестве ключей, что значительно повышает безопасность зашифрованной информации. Алгоритм шифрования, представленный в диссертации, основан на непозиционной полиномиальной системе счисления (НПСС) и предлагает новые решения для защиты данных, которые отличаются от традиционных методов шифрования. Вводя этот алгоритм в ПЛИС, исследование направлено на создание отечественного аппаратно шифровального устройства, соответствующего современным стандартам информационной безопасности, обеспечивающего технологическую независимость и безопасность. Это исследование значительно продвигает разработку технологий для шифрования данных и создания надёжных методов повышения безопасности на основе информационно-коммуникационных технологий (ИКТ). Такой прогресс имеет важное значение для области информационной безопасности и защиты технологической конфиденциальности, влияя на основополагающие элементы защиты данных в системах современной связи.

**Актуальность исследования**

Актуальность данного исследования обусловлена возросшими требованиями к обеспечению защиты электронных информационных ресурсов, информационных систем и инфраструктуры связи, а также специализированных систем, таких как конфиденциальная связь и видеосвязь. В условиях постоянно растущего объема цифровой информации и ее стратегической значимости вопросы эффективного шифрования данных приобретают первостепенное значение.

ПЛИС предлагает уникальные возможности для решения этих проблем благодаря своей гибкости, масштабируемости и способности обрабатывать параллельные данные с высокой производительностью. В ПЛИС систем защиты информации позволяют значительно повысить скорость шифрования

данных, обеспечивая при этом высокую степень их конфиденциальности и целостности. Это делает ПЛИС предпочтительным решением где требования к безопасности и производительности выше.

Одним из ключевых аспектов этого исследования является использование генераторов хаоса в качестве источника псевдослучайных чисел для создания ключей шифрования. Такой подход значительно повышает безопасность данных, поскольку хаотические последовательности трудно предсказать и проанализировать, что делает процесс дешифрования без соответствующего ключа очень сложным.

Разработанный в рамках этого исследования алгоритм шифрования на основе НПСС – это решение, которое значительно отличается от традиционных методов шифрования. Это не только повышает уровень безопасности шифрования, но и повышает его эффективность за счет оптимизации процессов обработки данных.

Такой способ шифрования позволяет создать отечественное шифровальное устройство, отвечающее современным требованиям защиты информации. В современном мире, когда технологический суверенитет становится все более актуальным для обеспечения национальной безопасности, возможность создания собственных алгоритмов и технологий шифрования для каждой страны представляет собой стратегическое преимущество. Разработка и внедрение собственных решений в области шифрования данных не только обеспечивает надежную защиту информации, но и способствует развитию национальных технологических и научных компетенций, укрепляя технологическую независимость и безопасность страны.

Таким образом, актуальность данного исследования обусловлена не только техническими аспектами разработки эффективных и надежных методов шифрования данных, но и стратегической необходимостью обеспечения технологического суверенитета в области информационной безопасности.

**Целью диссертационной работы является** реализация и внедрение комплексного информационно-программного обеспечения шифрования данных на основе ПЛИС

**Предметом исследования являются** телекоммуникационные системы и специальные системы связи, включая программируемые логические интегральные схемы (ПЛИС), непозиционные полиномиальные системы счисления и генераторы псевдослучайных чисел.

**Задачи исследования**

1. Изучение алгоритмов шифрования данных: исследование и сравнение традиционных и современных методов шифрования, используемых для шифрования данных;

2. Оценка потенциала использования ПЛИС как основы систем шифрования данных. Создание аппаратной архитектуры на основе ПЛИС, оптимизация алгоритмов шифрования и интеграция программных и аппаратных компонентов;

3. Разработка алгоритма шифрования: создание эффективного алгоритма шифрования данных, основанного на НПСС и адаптированного для реализации в ПЛИС;

4. Использование генераторов хаоса: разработка методологии использования генераторов хаоса для генерации псевдослучайных чисел,

которые служат надежными ключами шифрования;

5. Оценка безопасности и эффективности: анализ производительности, мощности и эффективности разработанных инструментов по сравнению с другими методами шифрования данных в ИКТ;

6. Внедрение и тестирование алгоритма шифрования, реализованного в ПЛИС, для оценки его практического применения и производительности.

**Новизна и специфика диссертационной работы, впервые:**

1. внедрен и протестирован алгоритм шифрования ПЛИС на основе НПСС;

2. впервые было реализовано использование генераторов хаоса непосредственно в ПЛИС для генерации псевдослучайных чисел, которые служат ключами шифрования, что значительно повышает уровень безопасности системы;

3. впервые было предложено комплексное решение, объединяющее оборудование ПЛИС и специализированное программное обеспечение, способное обеспечить высокопроизводительное и безопасное шифрование данных в простых телекоммуникационных системах;

4.база данных непереводимых полиномов для использования в алгоритмах шифрования была впервые создана и систематизирована в ПЛИС, что является основным процессом выбора полиномов для генерации ключей шифрования. Аппаратная проверка неприводимости полиномов была впервые введена непосредственно в ПЛИС, что позволяет автоматизировать и ускорить процесс проверки полиномов, в том числе обеспечить высокую надежность и оперативность выбора ключей для шифрования данных.

**Основные концепции, предлагаемые для защиты:**

1. Разработанный генератор неприводимых полиномов для применения аппаратной защиты достигает до 16 битного ключа физического ресурса ПЛИС Артикс-7;

2. Генераторы хаотических сигналов и псевдослучайных чисел, реализованные на базе ПЛИС, способствуют повышению криптостойкости зашифрованной информации за счет случайного распределения длины информационных подблоков в передающих и принимающих устройствах.

3. Скорость аппаратной реализации алгоритма шифрования с открытым ключом на основе ПЛИС благодаря параллельным, конвейерным методам вычисления может быть доведена до 6,239 нс в одном такте.

**Теоретическая и практическая значимость работы**

Теоретическая значимость данного исследования заключается в разработке теоретических основ и понимания ИКТ и их применения в области шифрования и дешифрования данных, а также информационной безопасности. Исследование позволит глубже изучить принципы работы ИКТ, особенности шифрования и дешифрования данных, а также разработать новые методы и алгоритмы обеспечения информационной безопасности.

Практическая значимость исследования заключается в создании аппаратного и программного обеспечения на основе ПЛИС для внедрения эффективных и надежных систем шифрования и дешифрования данных. Это обеспечивает защиту информации от несанкционированного доступа и обеспечивает конфиденциальность передаваемых и хранящихся данных.

Результаты этого научного исследования аппаратные и программные решения на основе ПЛИС могут быть интегрированы в различные устройства и

системы ИКТ для обеспечения безопасности данных и защиты информации в различных областях, включая телекоммуникации, электронику, информационные системы и т. д. Это открывает новые возможности для разработки современных систем связи и передачи данных, обеспечивающих их надежность, конфиденциальность и целостность.

Полученные результаты и разработанные методы и алгоритмы шифрования и дешифрования данных на основе ПЛИС могут быть использованы в информационных и коммуникационных технологиях, облачном хранилище, системах электронной коммерции и других экспериментальных приложениях, требующих защиты информации. Это способствует развитию информационной безопасности и созданию более надежных и эффективных систем защиты данных.

Практическая значимость полученных результатов подтверждается публикациями в международных рецензируемых изданиях и участием в регулярных международных конференциях, а также авторским свидетельством РК № 22917.

**Достоверность и обоснованность полученных результатов**

Достоверность и обоснованность полученных результатов подтверждается публикациями в высокорейтинговых журналах дальнего зарубежья с высоким импакт-фактором и в изданиях, рекомендованных КОКСНВО МНВО РК для публикации основных результатов научной деятельности, и в трудах международных научных конференции ближнего и дальнего зарубежья.

**Личный вклад автора** заключается в том что, самостоятельно осуществил весь процесс исследования, от выбора метода исследования до разработки нормативно-технической документации. Автор также работал совместно с руководителями над постановкой задач и обсуждением результатов.

**Апробация диссертационной работы**

На основе материалов диссертационной работы опубликовано 10 печатных работ:

**Статьи с высоким импакт-фактором по базе данных Thomson Reuters или в публикациях, входящих в международную научную базу данных Scopus:**

1. Ibraimov M.K., Tynymbayev S.T., **Skabylov A.A.**, Kozhagulov Y., Zhexebay D.M. Development and design of an FPGA-based encoder for NPN //Cogent Engineering. – 2022. – Vol. 9, № 1. – 2008847 **[Q2, 67%]**
2. Aitkhozhayeva Y.Zh., Tynymbayev S., Adilbekkyzy S., Skabylov A., Ibraimov, M. Design and research of the behavioral model for the modular reduction device // Eurasian Physical Technical Journal 7. – 2020. – Vol. 17, № 1. – С. 151–156. **[Q3, 25%]**

**Научные публикации, рекомендованные КОКСНВО МНВО РК для публикации основных результатов научной деятельности**

1. Kalimoldayev M., Tynymbayev S., Almen D., **Skabylov A.** Implementation of the nonconductivity check algorithm for a given binary polynomial on the FPGA // Вестник КазНИТУ. – 2020. – Т. 141, № 5. – С. 629-635.

2. **Скабылов А.А.,** Ибраимов М.К., Жексебай Д.М., Кожагулов Е.Т. Программно-аппаратная реализация qpsk на базе zynq и matlab // Вестник КазНПУ им. Абая, серия «Физико-математические науки», №1(77), 2022 г.

3. **Скабылов А.А.,** Жексебай Д.М., Ибраимов М.К., Налибаев Е.Д. Применение хаотических генераторов для секретного ключа в приемо-передающих электронных устройствах // Вестник КазНПУ. – 2023. – Т. 82, № 2. – С. 194-201

**Публикации в сборниках тезисов международных конференций:**

1. Әлмен Д.Б., **Сқабылов Ә.Ә.** ПЛИС негізінде GF (2) ақырғы өрістегі келтірілмейтін полиномдар базасын құру //Международная научная конференция студентов и молодых ученых, «ФАРАБИ ӘЛЕМІ», 2020. – С. 269.

2. **Сқабылов Ә.Ә.,** Әлмен Д.Б., Жексебай Д.М., Азамат Р.М. Модуль бойынша бөлу құрылғысының әрекеттік моделін жобалау және зерттеу //Международная научная конференция студентов и молодых ученых, «ФАРАБИ ӘЛЕМІ», 2021. – С. 217.

3. **Сқабылов Ә.Ә.,** Әлмен Д.Б., Жексебай Д.М., Азамат Р.М. ПЛИС негізінде шифрлау және дешифрлау алгоритмін аппараттық жүзеге асыру //Международная научная конференция студентов и молодых ученых, «ФАРАБИ ӘЛЕМІ», 2021. – С. 218.

4. **Сқабылов Ә.Ә.,** Жексебай Д.М., Әлмен Д.Б., Ихсан Г.Б. FPGA негізінде qpsk бағдарламалық-ақпараттық комплекс //Международная научная конференция студентов и молодых ученых, «ФАРАБИ ӘЛЕМІ», 2022. – С. 215.

5. **Сқабылов Ә.Ә.,** Налибаев Е.Д., Ибраимов М.К., Данабеков Б., Азамат Р.М // «Бейсызық жүйелердегі хаос және құрылымдар. Теория және тәжірибе» XII Халықаралық ғылыми конференциясы, 2022. – С. 155.

**Авторское свидетельство:**

1. **Сқабылов Ә.Ә.,** Ибраимов М.К., Сахыбай Т., Жексебай Д.М., Кожагулов Е.Т. Аппаратный комплекс шифрования данных на основе ПЛИС //Авторлық куәлік, 2022. № 22917.

**Акт о внедрения завершенной научно-исследовательской работы в учебный процесс:**

1. Протокол №1 от 31 августа 2023 года

**Структура и объем диссертационной работы**

Диссертационная работа состоит из введения, трех глав, заключения и списка использованной литературы. Работа включает 54 рисунков, 20 формул, 6 таблиц, 117 списков литературы и 114 страниц.