ОТЧЕТ

о работе диссертационного совета «Информатика и информационные системы» при КазНУ имени аль-Фараби по защите диссертаций на присуждение степени доктора философии (PhD) за 2021 год

по группе специальностей: «6D07300, 8D06101 - Информационные системы», «6D070400 - Вычислительная техника и программное обеспечение (Компьютерная инженерия)», «6D075100 - Информатика, вычислительная техника и управление (Системная инженерия)», «6D060200 - Информатика (Компьютерные науки)», «6D100200, 8D06301 - Системы информационной безопасности», «6D070200 - Автоматизация и управление»

Председатель диссертационного совета доктор физико-математических наук, профессор, академик НАН РК Калимолдаев Максат Нурадилович.

Диссертационный совет утвержден приказом председателя правления - ректора КазНУ имени аль-Фараби №306 от 28.06.2021 г. на основании решения Ученого совета университета (протокол №11 от 22.06.2021 г.).

1. Данные о количестве проведенных заседаний. За отчетный 2021 год проведены 2 заседания диссертационного совета.

2. Фамилия, имя, отчество (при его наличии) членов диссертационного совета, посетивших менее половины заседаний. Всего членов диссертационного совета – 12 человек. Из них 6 человек (50%) являются постоянными членами диссертационного совета, 6 человек (50%) назначались временно на период защиты докторанта в зависимости от темы докторского исследования. Членов совета, посетивших менее половины заседаний, нет.

3. Список докторантов с указанием организации обучения

№	ФИО докторантов	Научные консультанты	ВУЗ, в котором обучался докторант
1	Алтыбай Аршын	Токмагамбетов Нияз Есенжолович – PhD, и.о. доцент, КазНУ им. аль-Фараби (г. Алматы, Казахстан); Michael Ruzhansky – PhD, Профессор, Гентский университет (г. Гент, Бельгия).	Казахский Национальный университет имени аль-Фараби
2	Алгазы Кунболат Тилеуханулы	Бияшев Рустем Гакашевич – доктор технических наук, профессор, Институт информационных и вычислительных технологий КН МОН РК (г. Алматы, Казахстан); Анджей Смолартс – доктор технических наук, профессор, Люблинский технический университет (г. Люблин, Польша).	Казахский Национальный университет имени аль-Фараби

4. Краткий анализ диссертаций, рассмотренных советом в течение отчетного года

Алтыбай Аршын. Тема диссертации: «Development of high-performance parallel algorithms and software complex for modeling hyperbolic type equations with singular coefficients: tsunami and acoustic wave propagation».

1) Анализ тематики рассмотренных работ.

Актуальность темы исследования. В настоящее время случайно происходящие и быстро меняющиеся физические процессы приводят к огромным экологическим и экономическим проблемам. Поэтому моделирование таких процессов очень важно. Многие такие задачи моделируются уравнениями гиперболического типа с сингулярными коэффициентами.

В соответствии со знаменитой работой Шварца об отсутствии классических решений уравнений с дистрибутивным сингулярным коэффициентом решение таких проблем является открытой проблемой, многие исследователи предлагают различные способы решения таких задач, один из которых использует концепцию очень слабых решений. То есть в данной работе рассматривается очень слабое решение уравнения цунами с сингулярным коэффициентом, и оно учитывается при теоретическом исследовании его единственности и сходимости.

Моделирование физических процессов, упомянутых выше, в больших масштабах и в течение длительного времени требует больших вычислительных затрат. Если вычислительный алгоритм является последовательным, то вычислительные затраты еще больше. Временным решением этой проблемы является распараллеливание.

Многие инженерные и научные приложения часто требуют одновременного решения большого количества уравнений с переменными коэффициентами. Основная цель диссертационной работы - использовать вычислительную мощность различных современных архитектур параллельных процессоров для увеличения скорости вычислений некоторых математических задач путем предоставления новых алгоритмов и решений.

Научная новизна. Доказательство существования, единственности и непротиворечивости очень слабых решений уравнения цунами и обоснование численным моделированием. Разработка параллельного алгоритма численного решения двумерного волнового уравнения с сингулярным коэффициентом с использованием технологии MPI на основе неявной разностной схемы. Разработка параллельного алгоритма численного решения двумерного уравнения цунами с использованием технологии CUDA на основе неявной разностной схемы. Разработка параллельного гибридного алгоритма численного решения двумерного волнового уравнения акустики на основе неявной разностной схемы. Разработка кроссплатформенного программного комплекса с открытым исходным кодом для численного решения и исследования уравнений гиперболического типа с сингулярными коэффициентами.

2) Связь тематики диссертаций с направлениями развития науки, которые сформированы Высшей научно-технической комиссией при Правительстве Республики Казахстан в соответствии с пунктом 3 статьи 18 Закона «О науке» и (или) государственными программами.

Диссертационная работа выполнялась в рамках проекта № AP08052028 «Нестандартный гармонический анализ связанный с операторами типа Бесселя и его применения».

3) Анализ уровня внедрения результатов диссертаций в практическую деятельность.

Практическая значимость работы. Разработанные параллельные алгоритмы численного решения гиперболических уравнений с сингулярными коэффициентами применяются для моделирования цунами в Каспийском море. Разработанное программное обеспечение может быть использовано для исследования волн в неоднородных средах в различных областях науки.

Алгазы Кунболат Тилеуханулы. Тема диссертации: «Разработка и исследование алгоритмов шифрования на базе различных подходов».

1) Анализ тематики рассмотренных работ.

Актуальность темы исследования обусловлена современным развитием информационно-коммуникационных технологий и необходимостью совершенствования моделей защиты электронной информации в целях обеспечения информационной безопасности. Процессы обработки, хранения, передачи и использования информации стали приоритетными в современном обществе и во многом зависят от уровня развития и использования средств связи и способов передачи информации. При нынешней ситуации необходимость защиты информации нужна не только государственному сектору, но и простому пользователю и негосударственным организациям. Одним из актуальных вопросов обеспечения безопасности информации является обеспечение необходимого уровня ее защиты путем создания современных средств защиты информации.

Информационные и коммуникационные технологии играют важную роль для суверенного государства. В Казахстане в 2017 году была принята Концепция кибербезопасности («Киберщит Казахстана»). Целью концепции является достижение и поддержание уровня защиты электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз для обеспечения устойчивого развития Республики Казахстан в условиях глобальной конкуренции. В связи с этим создание отечественных систем защиты информации, отвечающих современным требованиям информационной безопасности, является актуальным. В Казахстане в основном используют зарубежные криптографические средства и программное обеспечение для защиты информации, поэтому разработка

казахстанских отечественных средств криптографической защиты определенно актуальна и необходима.

Научная новизна. Построен новый симметричный алгоритм блочного шифрования с архитектурой подстановочно-перестановочной сети, отвечающий общим требованиям алгоритмов шифрования. Построен симметричный блочный алгоритм шифрования на основе нетрадиционного метода (НПСС), использование которого позволяет повысить криптостойкость алгоритма. Построены узлы нелинейной (S-блок) замены, которые имеют повышенные показатели стойкости к дифференциальному и линейному криптоанализу.

2) Связь тематики диссертаций с направлениями развития науки, которые сформированы Высшей научно-технической комиссией при Правительстве Республики Казахстан в соответствии с пунктом 3 статьи 18 Закона «О науке» и (или) государственными программами.

Диссертационная работа выполнялась в рамках проекта программно-целевого финансирования № BR05236757 «Разработка программных и программно-аппаратных средств для криптографической защиты информации при ее передаче и хранении в инфокоммуникационных системах и сетях общего назначения».

3) Анализ уровня внедрения результатов диссертаций в практическую деятельность.

Практическая значимость работы. Проведенные научные исследования и полученные результаты имеют высокую практическую значимость и могут быть использованы для защиты конфиденциальной информации при её хранении и передаче в инфокоммуникационных системах и сетях. Кроме того, эти результаты по созданию и развитию отечественных средств защиты информации расширяют теорию создания эффективных алгоритмов шифрования информации. Разработанный итеративный блочный алгоритм шифрования реализован и получено авторское свидетельство на «Qamal v 1.0.1», № 5200 от 6 сентября 2019 года, выданное Национальным институтом интеллектуальной собственности МЮ РК.

5. Анализ работы официальных рецензентов (с примерами наиболее некачественных отзывов).

Для изучения содержания диссертации и представления рецензий были назначены по два официальных рецензента для каждой диссертации, имеющих ученую степень доктора или кандидата наук, доктора философии (PhD) и не менее 5 (пяти) научных статей в области исследований докторанта.

При назначении официальных рецензентов диссертационный совет руководствовался принципом независимости друг от друга рецензентов и докторантов.

Официальные рецензенты представили в диссертационный совет письменные отзывы, в которых оценили соответствие диссертаций направлениям развития науки и (или) государственным программам,

актуальность, соответствие принципам новизны, самостоятельности, достоверности, внутреннего единства, практической ценности, академической честности, и дали заключения о возможности присуждения степени доктора философии (PhD). Копии отзывов официальных рецензентов были вручены докторантам и размещены на интернет-ресурсе университета более, чем за 5 (пять) рабочих дней до установленной даты защиты.

6. Предложения по дальнейшему совершенствованию системы подготовки научных кадров.

Нет.

7. Количество диссертаций на соискание степеней доктора философии (PhD), доктора по профилю в разрезе специальностей (направления подготовки кадров):

	6D07300, 8D06101 - Информационные системы	6D070400 - Вычислительная техника и программное обеспечение (Компьютерная инженерия)	6D075100 - Информатика, вычислительная техника и управление (Системная инженерия)	6D060200 - Информатика (Компьютерные науки)	6D100200, 8D06301 - Системы информационной безопасности	6D070200 - Автоматизация и управление
Диссертации, принятые к защите (в том числе докторантов из других вузов)	-	-	1	-	1	-
Диссертации, снятые с рассмотрения (в том числе докторантов из других вузов)	-	-	-	-	-	-
Диссертации, по которым получены отрицательные отзывы рецензентов (в том числе докторантов из других вузов)	-	-	-	-	-	-
Диссертации с отрицательным решением по итогам защиты (в том числе	-	-	-	-	-	-

докторантов из других вузов)						
Диссертации, направленные на доработку (в том числе докторантов из других вузов)	-	-	-	-	-	-
Диссертации, направленные на повторную защиту (в том числе докторантов из других вузов)	-	-	-	-	-	-

Председатель диссертационного совета _____ **Калимолдаев М.Н.**

Ученый секретарь диссертационного совета _____ **Дарибаев Б.С.**

Печать дата «30» декабря 2021 года