ОТЗЫВ

официального рецензента на диссертационную работу
Алгазы Кунболат Тилеуханулы на тему «Разработка и исследование алгоритмов шифрования на базе различных подходов», представленную на соискание степени доктора философии (PhD) по специальности «6D100200 - Системы информационной безопасности».

№п/п	Критерии	Соответствие критериям (необходимо отметить один из вариантов ответа)	Обоснование позиции официального рецензента
1.	Тема диссертации (на дату ее утверждения) соответствует направлениям развития науки и/или государственным программам	1.1 Соответствие приоритетным направлениям развития науки или государственным программам:	Диссертационная работа соответствует приоритетному направлению развития науки: «Информационные, коммуникационные и космические технологии» и Концепции кибербезопасности («Киберщит Казахстана») утвержденный постановлением Правительства Республики Казахстан от 30 июня 2017 года № 407.
		1) Диссертация выполнена в рамках проекта или целевой программы, финансируемого(ой) из государственного бюджета (указать название и номер проекта или программы) 2) Диссертация выполнена в рамках другой государственной программы (указать название программы) 3) Диссертация соответствует приоритетному направлению развития науки, утвержденному Высшей научно-технической комиссией при Правительстве Республики Казахстан (указать направление)	Диссертационная работа выполнена в рамках научно-исследовательских работ проекта программно-целевого финансирования «Разработка программных и программно-аппаратных средств для криптографической защиты информации при ее передаче и хранении в инфокоммуникационных системах и сетях общего назначения» (2018-2020 гг., государственный регистрационный номер: BR05236757).
2.	Важность для науки	Работа вносит/не вносит существенный вклад в науку, а ее важность хорошо раскрыта/не раскрыта	Полученные результаты вносят вклад в развитии и создании казахстанских средств криптографической защиты информации (СКЗИ). В дальнейшем могут быть использованы при создании СКЗИ с целью обеспечения информационной безопасности в различных инфокоммуникационных системах. В диссертационной

			работе разработан новый симметричный алгоритм блочного шифрования криптографической защиты информации. Построенный алгоритм состоит из преобразований mixer1, mixer2 и S-блока. Также приведен метод получения S-блоков, используемый в алгоритме и описан алгоритм генерации раундовых ключей. Вместе с тем, было исследовано влияние на криптографическую стойкость при использовании непозиционной полиномиальной системы счисления в алгоритме шифрования.
3.	Принцип самостоятельности	Уровень самостоятельности: 1) Высокий; 2) Средний; 3) Низкий; 4) Самостоятельности нет	Уровень самостоятельного написания диссертации докторанта высокий. Автором самостоятельно проведены все исследовательские работы и проведена обработка их результатов. Алгоритм блочного шифрования, разработанный в результате работы, был детально изучен с использованием современных методов криптографического анализа и показано конкретные результаты. Исследованы статистические свойства зашифрованного текста, полученного с помощью разработанных алгоритмов. Результаты криптоанализа использованного S-блока сравниваются с характеристиками S-блоков, используемых в других известных алгоритмах.
4.	Принцип внутреннего единства	4.1 Обоснование актуальности диссертации: 1) Обоснована; 2) Частично обоснована; 3) Не обоснована.	В настоящее время обладание информацией позволяет оказывать влияние на мировое сообщество в глобальном масштабе. Криптография позволяет передавать информацию в защищенной форме, обеспечивая безопасность, конфиденциальность и целостность данных. Криптографический метод защиты, безусловно, самый надежный метод защиты, так как охраняется непосредственно сама информация, а не доступ к ней, зашифрованный файл нельзя прочесть даже в случае кражи носителя. В РК цифровая информация защищается в основном зарубежными алгоритмами и средствами. В связи с этим, для РК создание отечественных средств защиты информации, в том числе

			криптографических, актуально и необходимо. *По данной диссертационной работе имеются следующие замечания:* *- в первом разделе диссертации было бы полезно предоставить больше информации о методах криптоанализа;* *- не было необходимости сравнивать результаты криптографического анализа представленного в алгоритме S-блока с S-блоком алгоритма DES, так как имеются различия в размерах.*
		4.2 Содержание диссертации отражает тему диссертации: 1) Отражает; 2) Частично отражает; 3) Не отражает	Содержание диссертации полностью отражает тему диссертации. Начина с введения, четырех разделов и заключения диссертация полном объеме излагает содержание полученных результатов соответственно теме научно-исследовательской работе. Общий объем диссертации: 118 страниц письменного текста, в том числе 23 рисунка, 42 таблицы, список литературы из 94 источников, 4 приложения
		4.3. Цель и задачи соответствуют теме диссертации: 1) соответствуют; 2) частично соответствуют; 3) не соответствуют	Цели и задачи исследования соответствуют теме диссертации. Цель диссертации: разработка алгоритмов блочного шифрования и алгоритмов раундового ключа с использованием непозиционных полиномиальных систем счисления и исследование их методами криптоанализа. Для достижения этой цели ставятся следующие задачи: анализ существующих симметричных блочных алгоритмов криптографической защиты информации; обзор и анализ известных методов криптографических атак; построение алгоритмов симметричного блочного шифрования на основе подстановочно-перестановочной сети и функции разворачивание раундовых ключей шифрования с применением непозиционных полиномиальных систем счисления (НПСС); исследование методами криптоанализа стойкости разработанных алгоритмов шифрования; программная реализация созданных алгоритмов шифрования.

		4.4 Все разделы и положения диссертации логически взаимосвязаны: 1) полностью взаимосвязаны; 2) взаимосвязь частичная; 3) взаимосвязь отсутствует	Структура диссертации состоит из введения, 4 разделов и заключения. Все разделы и структуры логически связаны. Во введении обосновывается актуальность диссертационной работы. Сформулированы цель работы, объект и предмет научно-исследовательской работы. В первом разделе описана классификация и основные направления исследований в алгоритмах защиты информации. Приведены термины, используемые в криптографии и диссертационной работе. Описываются криптоалгоритмы, разделенные по степени безопасности, требования к симметричным блочным шифрам и режимы шифрования, используемые при шифровании. Во втором разделе описаны новый алгоритм симметричного блочного шифрования «Qamal», разработанный на основе SP-сети и предложенная вторая версия этого алгоритма «Qamal NPNS» из-за особенностей использования ключа. Подробно описываются все используемые преобразования в этих алгоритмах. В третьем разделе представлены результаты, полученные при исследовании надежности разработанного алгоритма шифрования. Анализ начинается с проверки статистической безопасности зашифрованного текста, полученного с помощью алгоритма шифрования. Затем, проверяются свойства лавинного эффекта шифра, что является одним из необходимых условий в криптографии. Криптостойкость алгоритма проверена алгебраическими, дифференциальными, линейными и другими методами криптоанализа. В четвертом разделе приведено описание созданного программного обеспечения, реализующего разработанный симметричный блочный алгоритм шифрования.
		4.5 Предложенные автором новые решения (принципы, методы) аргументированы и оценены по сравнению с известными решениями:	Достоверность каждого научного результата, решения и вывода, сформулированных в диссертации, подтверждается данными, полученными в результате применения статистических тестов и методов криптографического анализа.

		1) критический анализ есть; 2) анализ частичный; 3) анализ представляет собой не собственные мнения, а цитаты других авторов	
5.	Принцип научной новизны	5.1 Научные результаты и положения являются новыми? 1) полностью новые; 2) частично новые (новыми являются 25-75%); 3) не новые (новыми являются менее 25%)	Научные результаты и принципы диссертации являются полностью новыми. Для криптографической защиты информации был разработан новый алгоритм симметричного блочного шифрования. Исследовано криптографическая стойкость структурных элементов (примитивов) разработанного алгоритма, а также влияние на стойкость применение непозиционной полиномиальной системе счисления. В структуре алгоритма используются новые S-блоки замены, полученные в результате проведенных исследований, которые обладают криптографическим свойствами, близкими к оптимальным теоретическим показателям.
		5.2 Выводы диссертации являются новыми? 1) полностью новые; 2) частично новые (новыми являются 25-75%); 3) не новые (новыми являются менее 25%)	Выводы диссертации являются полностью новыми, что подтверждается основных выводов работы в статье “Development and Analysis of Symmetric Encryption Algorithm Qamal Based on a Substitution-permutation Network” International journal of electronics and telecommunications, № 1, 2021, P. 127-132.
		5.3 Технические, технологические, экономические или управленческие решения являются новыми и обоснованными: 1) полностью новые; 2) частично новые (новыми являются 25-75%); 3) не новые (новыми являются менее 25%)	Структурная схема разработанного алгоритма зашифрования: алгоритм поддерживает длины блока и ключей в 128, 192 и 256 бит. От длины блока и ключа зависит число раундов шифрования. Ключам К длиной в 128, 192 и 256 бит соответствуют числа раундов шифрования 8, 10 и 12. Все раунды завершаются операцией сложения по модулю 2 с раундовым ключом. Алгоритм зашифрования включает разработанные процедуры наложения ключа с помощью операции побитового сложения (XOR), S-блока замены, процедур перемешивания Mixer1 и Mixer2.

6.	Обоснованность основных выводов	Все основные выводы основаны/не основаны на весомых с научной точки зрения доказательствах либо достаточно хорошо обоснованы (для qualitative research и направлений подготовки по искусству и гуманитарным наукам)	Результаты исследования диссертанта основаны на научных доказательствах. В третьей части работы представлены результаты исследования надежности алгоритма шифрования. Были проверены статистические свойства зашифрованных текстов, полученные с помощью разработанного алгоритма шифрования и последовательность раундовых ключей. Эта задача имеет значение в области криптографии. Для ее решения на практике использовался набор статистических тестов. В работе исследование криптостойкости алгоритма начинается с проведением криптоанализа для каждого используемого преобразования. Затем, в зависимости от полученных результатов, проводится анализ всего алгоритма. По результатам этих исследований можно сказать, что все выводы основаны на доказательствах.
7.	Основные положения, выносимые на защиту	Необходимо ответить на следующие вопросы по каждому положению в отдельности: 7.1 Доказано ли положение? 1) доказано; 2) скорее доказано; 3) скорее не доказано; 4) не доказано 7.2 Является ли тривиальным? 1) да; 2) нет 7.3 Является ли новым? 1) да; 2) нет 7.4 Уровень для применения: 1) узкий; 2) средний; 3) широкий	На защиту вынесены следующие положения: **1. Построен новый симметричный алгоритм блочного шифрования с архитектурой подстановочно-перестановочной сети, отвечающий общим требованиям алгоритмов шифрования.** 7.1 доказано; 7.2 нет; 7.3 да; 7.4 широкий; 7.5 да, K.T. Algazy, L.K. Babenko, R.G. Biyashev, E.A. Ishchukova, N.A. Kapalova, S.E. Nysynbaeva, Andrzej Smolarz Differential Cryptanalysis of New Qamal Encryption Algorithm // International journal of electronics and telecommunications, № 4, 2020, P. 647-653 2. **Построен симметричный блочный алгоритм шифрования на основе нетрадиционного метода (НПСС), использование которого позволяет повысить криптостойкость алгоритма.**

		7.5 Доказано ли в статье? 1) да; 2) нет	7.1 доказано; 7.2 нет; 7.3 да; 7.4 широкий; 7.5 да, R.G. Biyashev, A. Smolarz, K. T. Algazy, A.Khompysh. Encryption algorithm "Qamal NPNS" based on a nonpositional polynomial notation // Вестник КазНУ им. аль-Фараби. – Алматы, 2020. – № 1. – С. 198-208. **3. Построены узлы нелинейной (S-блок) замены, которые имеют повышенные показатели стойкости к дифференциальному и линейному криптоанализу.** 7.1 доказано; 7.2 нет; 7.3 да; 7.4 широкий; 7.5 да, Бияшев Р.Г., Алгазы К.Т., Дюсенбаев Д.С., Сакан К.С. Результаты линейного криптоанализа шифра Qamal // Вестник АУЭС. – Алматы, 2020. – № 2. – С. 96-105.
8.	Принцип достоверности Достоверность источников и предоставляемой информации	8.1 Выбор методологии - обоснован или методология достаточно подробно описана 1) да; 2) нет	В диссертационной работе выбранная методология основана и подробно описана. Алгоритмы симметричного блочного шифрования являются основным криптографическим инструментом для обеспечения конфиденциальности обработки информации и защиты информации в информационно-коммуникационных системах. В работе отмечены основные преимущества блочных шифров.

		8.2 Результаты диссертационной работы получены с использованием современных методов научных исследований и методик обработки и интерпретации данных с применением компьютерных технологий: 1) да; 2) нет	Сегодня криптографическая защита информации невозможна без использования компьютерных технологий. В связи с этим результаты диссертации были получены с использованием современных методов научного исследования и обработки и интерпретации данных с использованием компьютерных технологий.
		8.3 Теоретические выводы, модели, выявленные взаимосвязи и закономерности доказаны и подтверждены экспериментальным исследованием (для направлений подготовки по педагогическим наукам результаты доказаны на основе педагогического эксперимента): 1) да; 2) нет	Теоретические выводы, модели, выявленные взаимосвязи и закономерности были доказаны и подтверждены экспериментальными исследованиями. Криптографическая стойкость разработанного алгоритма шифрования подтверждена различными исследованиями. Статистические свойства зашифрованных текстов исследовались с использованием набора тестов NIST и Кнута. Вместе с тем, еще одно необходимое свойство шифра – лавинный эффект, было проверено на практике. В целом были получены удовлетворительные результаты. Криптографическая стойкость шифра подтверждается результатами дифференциальных, линейных, алгебраических атак и атаки методом бумеранга. Они проиллюстрированы не только теоретическими оценками, но и конкретными примерами. Криптографические характеристики нелинейного узла, используемого в алгоритме шифрования, показаны в сравнении с другими известными алгоритмами.
		8.4 Важные утверждения подтверждены/частично подтверждены/не подтверждены ссылками на актуальную и достоверную научную литературу	Важные утверждения подтверждаются ссылками на актуальную и достоверную научную литературу.
		8.5 Использованные источники литературы достаточны/не достаточны для литературного обзора	Список использованной литературы включает 94 ссылки на английском, русском и казахском языках. Среди них много высокорейтинговых зарубежных изданий, опубликованных в последнее время, которых достаточно для общего литературного

			обзора.
9	Принцип практической ценности	9.1 Диссертация имеет теоретическое значение: 1) да; 2) нет	Диссертация имеет теоретическое значение. В ходе исследовательских работ было доказано, что использование ключа в непозиционной полиномиальной системе счисления повышает криптографическую стойкость. Кроме того, результаты работы будут способствовать созданию и развитию отечественных средств защиты информации для РК, расширят теорию создания эффективных алгоритмов шифрования информации.
		9.2 Диссертация имеет практическое значение и существует высокая вероятность применения полученных результатов на практике: 1) да; 2) нет	Результаты, полученные в ходе исследовательских работ, имеют высокую практическую ценность и могут быть использованы для защиты конфиденциальной информации в информационно-коммуникационных системах и сетях.
		9.3 Предложения для практики являются новыми? 1) полностью новые; 2) частично новые (новыми являются 25-75%); 3) не новые (новыми являются менее 25%)	Разработан новый алгоритм симметричного блочного шифрования для криптографической защиты информации, который может быть использован для создания отечественных средств защиты информации в республике Казахстан.
10.	Качество написания и оформления	Качество академического письма: 1) высокое; 2) среднее; 3) ниже среднего; 4) низкое.	Диссертация подготовлена в соответствии с требованиями.

В отзывах официальные рецензенты указывают одно из следующих решений:

1) присудить степень доктора философии (PhD) или доктора по профилю;

2) направить диссертацию на доработку (кроме случаев защиты диссертации в форме серии статей);

3) отказать в присуждении степени доктора философии (PhD) или доктора по профилю.

Копии отзывов официальных рецензентов вручаются докторанту не позднее, чем за 5 (пять) рабочих дней до защиты диссертации.

Официальный рецензент:
Заместитель декана факультета «Кибербезопасности, компьютерной и программной инженерии» Национального авиационного университета
д.т.н., профессор **С.А.Гнатюк**