

ОТЗЫВ

официального рецензента на диссертационную работу Қадыржан Аружан Булатовна по теме «Разработка новых средств защиты информации в зоне прямой радиовидимости», представленную на соискание степени доктора философии (PhD) по образовательной программе 8D07104 – Приборостроение

№ п/п	Критерии	Соответствие критериям (подчеркнуть один из вариантов ответа)	Обоснование позиции официального рецензента (замечания выделить курсивом)
1.	Тема диссертации (на дату ее утверждения) соответствует направлениям развития науки и/или государственным программам	<p>1.1 Соответствие приоритетным направлениям развития науки или государственным программам:</p> <p>1) диссертация выполнена в рамках проекта или целевой программы, финансируемого(ой) из государственного бюджета (указать название и номер проекта или программы);</p> <p>2) диссертация выполнена в рамках другой государственной программы (указать название программы);</p> <p>3) диссертация соответствует приоритетному направлению развития науки, утвержденному Высшей научно-технической комиссией при Правительстве Республики Казахстан (указать направление).</p>	Тема исследования полностью соответствует приоритетным направлениям развития науки, утвержденным ВНТК при Правительстве Республики Казахстан, в части «Передовое производство, цифровые и космические технологии», поскольку ориентирована на повышение устойчивости и скрытности каналов управления группами БПЛА в зоне прямой радиовидимости.
2.	Важность для науки	Работа <u>вносит/не вносит</u> существенный вклад в науку, а ее важность хорошо <u>раскрыта/не раскрыта</u> .	Работа вносит существенный вклад в науку, а её важность раскрыта полноценно. Это подтверждается полученными теоретическими и экспериментальными результатами: предложен и апробирован метод измерения мгновенных значений частоты, фазы и амплитуды квазигармонического колебания по фазовому портрету. Разработан алгоритм идентификации местоположения источника радиосигнала по совокупности времени распространения до приемниках группы БПЛА с использованием оптоволоконной синхронизации внутри группы БПЛА. Показано, что на данной основе может быть реализован метод защиты информации по принципу «свой/чужой». Предложен метод обфускации данных, основанный на вычислении дискретных логарифмов в полях $GF(2^{n+1})$, включая аппаратно-ориентированную реализацию для 256-уровневого канала.
3.	Принцип самостоятельности	<p>Уровень самостоятельности:</p> <p>1) <u>высокий</u>;</p> <p>2) средний;</p> <p>3) низкий;</p> <p>4) самостоятельности нет.</p>	Уровень самостоятельности оценивается как высокий. Автором выполнены постановка задач, разработка методов и алгоритмов (включая метод измерения мгновенных значений частоты, фазы и амплитуды квазигармонического колебания по фазовому портрету и алгоритм обфускации на основе

			дискретного логарифмирования), проведены схемотехническая реализация ключевых узлов и стендовые эксперименты. Личный вклад автора состоит в самостоятельном планировании и выполнении основного объема работ.	
4.	Принцип внутреннего единства	4.1 Обоснование актуальности диссертации:	Актуальность исследования обусловлена ростом роли группового применения БПЛА и усилением радиоэлектронного противоборства (подавление, обнаружение и подмена каналов управления). В условиях прямой радиовидимости критичны низкая заметность, помехоустойчивость и малая задержка при ограниченных бортовых ресурсах. Предлагаемый подход сочетает геометрическую аутентификацию источника и внутригрупповую синхронизацию, уменьшая риск спуфинга и снижая зависимость от ресурсоёмкой криптографии.	
		1) обоснована;		
		2) частично обоснована;		
		3) не обоснована.		
		4.2 Содержание диссертации отражает тему диссертации:		Содержание диссертации соответствует заявленной теме: рассматриваются угрозы и требования к защищённому каналу управления в условиях прямой радиовидимости, предлагаются методы измерения параметров радиосигнала и геометрической идентификации источника, обосновывается архитектура с внутригрупповой оптоволоконной линией, а также развиваются алгоритмы обфускации на базе конечных полей.
		1) отражает;		
		2) частично отражает;		
		3) не отражает.		
		4.3 Цель и задачи соответствуют теме диссертации:		Цель и задачи диссертации согласованы с темой: разработка системы защиты информации для передачи команд группе БПЛА в условиях прямой радиовидимости подкреплена задачами по построению защищённого канала, измерению мгновенных параметров сигнала, схемотехнической реализации и разработке метода обфускации данных на базе дискретного логарифмирования.
		1) соответствуют;		
		2) частично соответствуют;		
		3) не соответствуют.		
		4.4 Все разделы и положения диссертации логически взаимосвязаны:		Работа обладает целостностью: обзор и постановка задач приводят к выбору измерительных и вычислительных методов, далее — к разработке архитектуры и аппаратной реализации, после чего предлагаются и анализируются средства обфускации. Результаты глав взаимно дополняют друг друга и формируют завершённый контур решения.
		1) полностью взаимосвязаны;		
		2) взаимосвязь частичная;		
3) взаимосвязь отсутствует.				
4.5 Предложенные автором новые решения (принципы, методы) аргументированы и оценены по сравнению с известными решениями:	Автором выполнено обоснование и сопоставление предложенных решений с распространёнными подходами (TDOA/FDOA/Дф-методы, методы извлечения мгновенных характеристик сигналов). Для вычисления дискретных логарифмов рассмотрены особенности классических алгоритмов и предложены улучшения для специальных классов полей.			
1) критический анализ есть;				
2) анализ частичный;				
3) анализ представляет собой не собственные мнения, а цитаты других авторов;				

		4) анализ отсутствует.			
5.	Принцип научной новизны	5.1 Научные результаты и положения являются новыми?	Ключевые результаты обладают научной новизной: метод измерения мгновенных значений частоты, фазы и амплитуды квазигармонического колебания по фазовому портрету; геометрическая аутентификация источника радиосигнала в архитектуре защищённого канала в зоне прямой радиовидимости; метод вычисления дискретных логарифмов в полях $GF(2^{n+1})$, позволяющий реализовать обфускацию данных для 256-уровневых каналов.		
		1) полностью новые;			
		2) частично новые (новыми являются 25-75%);			
		3) не новые (новыми являются менее 25%).			
		5.2 Выводы диссертации являются новыми?		Выводы содержат новые для рассматриваемого класса задач утверждения о применимости измерения мгновенных значений частоты, фазы и амплитуды квазигармонического колебания по фазовому портрету для создания защищенного канала связи и о возможности аппаратно-ориентированной обфускации на базе дискретного логарифмирования в специальных конечных полях.	
		1) полностью новые;			
		2) частично новые (новыми являются 25-75%);			
		3) не новые (новыми являются менее 25%).			
		5.3 Технические, технологические, экономические или управленческие решения являются новыми и обоснованными:			Технические решения обоснованы и доведены до аппаратной апробации: описан измерительный тракт и цифровая обработка (в т.ч. синхронизация таймерами и использование DMA), а также аппаратное представление элементов поля для реализации обфускации (например, для $GF(257)$).
		1) полностью новые;			
		2) частично новые (новыми являются 25-75%);			
		3) не новые (новыми являются менее 25%).			
6.	Обоснованность основных выводов	Все основные выводы <u>основаны</u> /не основаны на весомых с научной точки зрения доказательствах либо достаточно хорошо обоснованы (для qualitative research (куолилатив ресеч) и направлений подготовки по искусству и гуманитарным наукам).	Основные выводы подтверждаются математическими выводами, моделированием и экспериментальной отработкой электронных схем. В диссертации приведены сведения о разработанной аппаратной реализации и результатах обработки сигналов, что в целом обеспечивает достаточный уровень доказательности для диссертационной работы.		
7.	Основные положения, выносимые на защиту	Необходимо ответить на следующие вопросы по каждому положению в отдельности:	7.1. По материалам диссертации каждое из положений, выносимых на защиту, подтверждено: теоретические утверждения — строгими выводами и/или корректными постановками моделей, прикладные результаты — демонстрацией работоспособности на уровне алгоритмов и схемотехнической апробации. В работе прослеживается причинно-следственная связь «постановка задачи – метод – алгоритм – проверка работоспособности», что позволяет считать положения обоснованными. 7.2. Положения, выносимые на защиту, не являются тривиальными, поскольку опираются не на известные « типовые »		
		7.1 Доказано ли положение?			
		1) доказано;			
		2) скорее доказано;			
		3) скорее не доказано;			
		4) не доказано;			
		5) в текущей формулировке проверить доказанность положения невозможно.			
		7.2 Является ли тривиальным?			
		1) да;			
		2) нет;			

		3) в текущей формулировке проверить тривиальность положения невозможно.	<p>решения в готовом виде, а на специализированные комбинации методов, ориентированные на ограничения групповых БПЛА (по ресурсу канала, вычислительным возможностям и требованиям к устойчивости): использование внутригрупповой проводной/оптоволоконной составляющей, радиотехническая идентификация источника, а также алгоритмическая обфускация, основанная на вычислении дискретного логарифма в специальных конечных полях.</p> <p>7.3. Все положения обладают признаками научной новизны: новизна выражается в постановке и реализации комплексного подхода к защите командно-информационного обмена в группе БПЛА, а также в разработке/адаптации методов обработки и преобразования сигналов и данных под целевую архитектуру и аппаратно-ориентированные ограничения. Существенно, что предлагаемые решения образуют взаимосвязанную систему (а не набор разрозненных частных приёмов).</p> <p>7.4. Уровень применимости положений оценивается как широкий: результаты могут быть использованы при проектировании защищённых каналов управления и телеметрии для групповых робототехнических комплексов (в том числе БПЛА), в задачах радиомониторинга и идентификации источников сигналов, а также при создании встраиваемых устройств обработки/маскирования данных, где критичны скорость и простота аппаратной реализации.</p> <p>7.5. Положения диссертации отражены в публикациях по теме исследования, перечисленных в автореферате, а также подтверждаются результатами апробации (доклады/выступления) и патентной активностью; это обеспечивает проверяемость и воспроизводимость ключевых результатов научным сообществом.</p>
		7.3 Является ли новым?	
		1) да;	
		2) нет;	
		3) в текущей формулировке проверить новизну положения невозможно.	
		7.4 Уровень для применения:	
		1) узкий;	
		2) средний;	
		3) широкий;	
		4) в текущей формулировке проверить уровень применения положения невозможно.	
		7.5 Доказано ли в статье?	
		1) да;	
		2) нет;	
		3) в текущей формулировке проверить доказанность положения в статье невозможно.	
8.	Принцип достоверности.	8.1 Выбор методологии - обоснован или методология достаточно подробно описана:	
	Достоверность источников и предоставляемой информации	1) да;	
		2) нет.	

		8.2 Результаты диссертационной работы получены с использованием современных методов научных исследований и методик обработки и интерпретации данных с применением компьютерных технологий:	Использованы современные аппаратно-программные средства оцифровывания и обработки сигналов, а также численные расчёты и моделирование для подтверждения выводов.	
		1) да;		
		2) нет.		
		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):	Теоретические положения подкреплены экспериментальной проверкой работоспособности электронных схем и обработкой измерительных данных с использованием фазовых портретов.	
		1) да;		
		2) нет.		
		8.4 Важные утверждения подтверждены/частично подтверждены/не подтверждены ссылками на актуальную и достоверную научную литературу.	Литературный обзор охватывает ключевые направления (TDOA/FDOA/ $\Delta\phi$, методы оценивания мгновенных параметров, вычисление дискретных логарифмов). Наличие публикаций автора 2024–2026 гг. по теме подтверждает актуальность и соответствие современному уровню исследований.	
		8.5 Используемые источники литературы достаточны/не достаточны для литературного обзора.	Используемые источники представляют достаточную базу для постановки задач и выбора методических подходов; обзор позволяет определить место предлагаемого подхода среди существующих решений.	
9	Принцип практической ценности	9.1 Диссертация имеет теоретическое значение:	Работа имеет теоретическое значение: развиты методы оценивания параметров квазигармонических сигналов на сверхкоротких интервалах, а также предложены математические конструкции для обфускации данных на основе конечных полей.	
		1) да;		
		2) нет.		
		9.2 Диссертация имеет практическое значение и существует высокая вероятность применения полученных результатов на практике:		Практическая значимость подтверждается схемотехнической реализацией и апробацией. Результаты применимы при проектировании малозаметных каналов управления и аутентификации источников сигналов для групп БПЛА и родственных задач робототехники и мониторинга.
		1) да;		
		2) нет.		
		9.3 Предложения для практики являются новыми:		Практико-ориентированные предложения в значительной степени новые за счёт комбинирования геометрической аутентификации, внутригрупповой оптоволоконной синхронизации и аппаратно-ориентированной обфускации. Отдельные компоненты опираются на известные подходы цифровой обработки сигналов и конечных полей, что соответствует прикладному характеру работы.
1) полностью новые;				
2) частично новые (новыми являются 25-75%);				
		3) не новые (новыми являются менее 25%).		
10.		Качество академического письма:		

	Качество написания и оформления	1) высокое; 2) среднее; 3) ниже среднего; 4) низкое.	Работа в целом оформлена и написана на должном уровне, соответствующим требованиям научного стиля, материал изложен последовательно. Имеются небольшие стилистические ошибки в диссертационной работе.
11.	Замечания к диссертации	Замечания отсутствуют	
12.	Научный уровень статей докторанта по теме исследования (в случае защиты диссертации в форме серии статей официальные рецензенты комментируют научный уровень каждой статьи докторанта по теме исследования)		
13.	Решение официального рецензента (согласно пункту 28 настоящего Типового положения)	Диссертационная работа Кадыржан Аружан Булатовна на тему «Разработка новых средств защиты информации в зоне прямой радиовидимости» представляет собой завершённое научное исследование, соответствует требованиям, предъявляемым к диссертациям на соискание степени доктора философии (PhD), и обладает научной новизной и практической значимостью.	

Официальный рецензент:

PhD, асоц.профессор кафедры «Радиотехника, электроника и телекоммуникации» Евразийского национального университета имени Л.Н. Гумилева.

Медетов Б.Ж.

