ОТЗЫВ

официального рецензента на диссертационную работу Қадыржан Аружан Булатовны 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	1.1 Соответствие приоритетным направлениям развития науки или государственным программам: 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).	Тема диссертационного исследования соответствует актуальным направлениям развития науки и технологий в части цифровизации, информационной безопасности и развития беспилотных систем. Рассматриваемые средства защиты каналов управления группой БПЛА в зоне прямой радиовидимости соотносятся с приоритетами, ориентированными на развитие высокотехнологичных и цифровых решений, включая средства связи и навигации для робототехнических комплексов.
2.	Важность для науки	Работа вносит/не вносит существенный вклад в науку, а ее важность хорошо раскрыта/не раскрыта.	Диссертация вносит существенный вклад в развитие прикладных аспектов защиты информации в радиоканалах управления БПЛА. Научная значимость определяется тем, что автором предложена комплексная концепция защиты, объединяющая: требования к защищенному каналу управления в зоне прямой радиовидимости; идентификацию и аутентификацию источника радиосигнала радиотехническими методами; метод измерения мгновенных параметров квазигармонического сигнала (частоты, амплитуды и фазы) на основе фазовых портретов; аппаратно-ориентированный метод обфускации данных на базе дискретного логарифмирования в специальных конечных полях.
3.	Принцип самостоятельности	Уровень самостоятельности: 1) высокий; 2) средний; 3) низкий; 4) самостоятельности нет.	Уровень самостоятельности автора оценивается как высокий. Это подтверждается тем, что автором выполнены постановка задачи, разработка методик обработки сигналов и вычислительных алгоритмов, а также схемотехническая проверка работоспособности ключевых узлов.
4.	Принцип внутреннего единства	4.1 Обоснование актуальности диссертации: 1) обоснована; 2) частично обоснована;	Актуальность диссертационной работы обоснована современными тенденциями применения БПЛА вблизи линии боевого соприкосновения и ростом роли

		3) не обоснована.	радиоэлектронной борьбы. В условиях прямой радиовидимости повышаются риски обнаружения, подавления и подмены каналов управления. В этой связи востребованы решения, обеспечивающие устойчивость и верификацию источника команд при ограниченных вычислительных и энергетических ресурсах бортовой электроники.
		4.2 Содержание диссертации отражает тему диссертации: 1) отражает; 2) частично отражает; 3) не отражает.	Содержание диссертации соответствует заявленной теме: рассмотрены требования к защищенному каналу управления в зоне прямой радиовидимости, предложены методы извлечения информативных параметров радиосигнала и реализован аппаратно-ориентированный механизм обфускации данных, что в совокупности поддерживает заявленную цель — повышение скрытности и устойчивости передачи команд группе БПЛА.
		4.3. Цель и задачи соответствуют теме диссертации: 1) соответствуют; 2) частично соответствуют; 3) не соответствуют.	Цель и задачи сформулированы корректно и логически вытекают из предмета исследования: от анализа архитектуры защищенного канала к разработке методов измерения параметров сигнала и далее — к практической схемотехнической реализации и прикладной обфускации данных.
		4.4 Все разделы и положения диссертации логически взаимосвязаны: 1) полностью взаимосвязаны; 2) взаимосвязь частичная; 3) взаимосвязь отсутствует.	Разделы работы выстроены последовательно: постановка проблемы и архитектурные решения, далее — методика обработки сигналов, затем — аппаратная реализация и алгоритм обфускации. Переходы между разделами мотивированы требованиями к управлению БПЛА (задержка, надежность, ресурсы).
		4.5 Предложенные автором новые решения (принципы, методы) аргументированы и оценены по сравнению с известными решениями: 1) критический анализ есть; 2) анализ частичный; 3) анализ представляет собой не собственные мнения, а цитаты других авторов; 4) анализ отсутствует.	Автор сопоставляет предложенные решения с традиционными подходами защиты радиоканала и обсуждает вычислительную сложность ключевых процедур. В части дискретного логарифмирования показана целесообразность аппаратной оптимизации для малых квази-мерсенновских полей (например, GF(257)), что является релевантным для 256-уровневых представлений данных.
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 обладают новизной за счет комбинирования методов физического уровня (идентификация/контроль источника по динамике сигнала) и вычислительно-легких преобразований данных для повышения скрытности передачи команд в условиях прямой радиовидимости.
		5.2 Выводы диссертации являются новыми?	Выводы диссертации отличаются новизной и отражают предложенные

		1) полностью новые;	автором конструктивные решения: обоснование архитектуры защищенного канала, описание алгоритмов извлечения мгновенных параметров и аппаратно-ориентированного дискретного логарифмирования для обфускации.
		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:	Предложенные технические решения обоснованы с инженерной точки зрения: автор ориентирует алгоритмы на реализацию в электронных узлах и демонстрирует возможность построения модулей обработки/обфускации с предсказуемой задержкой и ограниченными ресурсами.
		1) полностью новые;	
		2) частично новые (новыми являются 25-75%);	
		3) не новые (новыми являются менее 25%).	
6.	Обоснованность основных выводов	Все основные выводы основаны/не основаны на весомых с научной точки зрения доказательствах либо достаточно хорошо обоснованы (для qualitative research (куолитатив ресеч) и направлений подготовки по искусству и гуманитарным наукам).	Обоснованность выводов подтверждается математическими выкладками, моделированием и анализом алгоритмов, а также результатами схемотехнической отработки отдельных решений. Представленная аргументация в целом достаточна для диссертационной работы.
7.	Основные положения, выносимые на защиту	Необходимо ответить на следующие вопросы по каждому положению в отдельности:	7.1. Полученные в диссертации теоретические и прикладные результаты по всем положениям, выносимым на защиту, обоснованы и подтверждены совокупностью аналитических выводов, математического моделирования и экспериментально-схемотехнической апробации отдельных узлов и алгоритмов. 7.2. Все положения, выносимые на защиту, являются оригинальными и не сводятся к тривиальным известным решениям, так как основаны на (i) комбинированной архитектуре защищённой передачи команд для группы БПЛА, (ii) применении метода фазовых портретов для извлечения мгновенных параметров квазигармонического сигнала в задачах радиотехнической идентификации, (iii) аппаратно-ориентированном вычислении дискретных логарифмов в квазимерсенновских полях Галуа с последующим использованием результата для обфускации данных. 7.3. Все три положения, выносимые на защиту, являются новыми. Новизна обусловлена тем, что предложенные методы и алгоритмы ориентированы на практическую реализацию в условиях ограниченных ресурсов канала/вычислений и формируют целостную технологическую основу для защиты командно-информационного обмена в системах группового применения БПЛА.
		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.	
		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.	7.4. Положения, выносимые на защиту, обладают широким уровнем применимости: результаты могут использоваться при разработке средств защиты каналов передачи команд и телеметрии для групп БПЛА и других распределённых робототехнических систем, а также в смежных задачах радиотехнической идентификации источника сигнала и аппаратной реализации алгоритмов преобразования/обфускации данных на встраиваемых платформах. 7.5. Основные положения диссертации отражены в научных публикациях по теме работы (включая публикации в изданиях, индексируемых международными базами, и в журнале из перечня КОКСОН), а также подтверждаются наличием патента на изобретение и поданной заявкой на изобретение по тематике исследования; подготовлена тематическая монография.
8.	Принцип достоверности.	8.1 Выбор методологии - обоснован или методология достаточно подробно описана:	Выбор методологии и инструментария представляется обоснованным: работа сочетает методы цифровой обработки сигналов, математическое моделирование, элементы теории конечных полей и аппаратно-схемотехническую проверку. Результаты сопоставлены с известными подходами; приведена библиографическая база и публикации автора, что повышает достоверность выводов.
	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.	Важные утверждения подтверждены ссылками на актуальную научную литературу по радиотехнической идентификации источников, методам обработки сигналов и вычислению дискретных логарифмов. Наличие публикаций автора по теме исследования дополнительно подтверждает

			проработанность и актуальность результатов.
		8.5 Использованные источники литературы достаточны/не достаточны для литературного обзора.	Использованные источники литературы представляют достаточную базу для постановки задач и выбора методических подходов; обзор позволяет корректно позиционировать предлагаемые решения среди известных методов.
9	Принцип практической ценности	9.1 Диссертация имеет теоретическое значение: 1) да; 2) нет.	Работа имеет теоретическое значение: развиты методы оценивания параметров квазигармонических сигналов на сверхкоротких интервалах и предложены математические конструкции для аппаратно-ориентированной обфускации данных на основе конечных полей.
		9.2 Диссертация имеет практическое значение и существует высокая вероятность применения полученных результатов на практике: 1) да; 2) нет.	Практическая значимость подтверждается ориентацией на реализацию на бортовой электронике и схемотехнической апробацией ключевых узлов. Предлагаемые решения могут быть использованы при проектировании защищенных каналов управления группой БПЛА, а также в смежных задачах робототехники и мониторинга.
		9.3 Предложения для практики являются новыми: 1) полностью новые; 2) частично новые (новыми являются 25-75%); 3) не новые (новыми являются менее 25%).	Практико-ориентированные предложения частично являются новыми: отдельные компоненты опираются на известные подходы ЦОС и теории конечных полей, однако их сочетание и адаптация к условиям прямой радиовидимости канала управления группой БПЛА, а также аппаратная реализация метода обфускации образуют новое прикладное решение.
10.	Качество написания и оформления	Качество академического письма: 1) высокое; 2) среднее; 3) ниже среднего; 4) низкое.	Работа в целом написана и оформлена на высоком/хорошем уровне, материал изложен последовательно и логично.
11.	Замечания к диссертации	1. В работе целесообразно более формально задать модель угроз и целевые метрики (вероятность перехвата/подмены, устойчивость к помехам, критерии безопасности для обфускации и аутентификации). 2. Для радиотехнической идентификации источника ($\Delta t/\Delta\varphi$) желательно шире оценить влияние многолучевости, доплеровских сдвигов и маневров на точность и устойчивость, приведя результаты моделирования в усложненных сценариях. 3. В диссертации полезно более подробно описать протокольные аспекты: инициализацию, управление ключами/параметрами, защиту от повторной передачи и синхронизационные процедуры внутри группы.	

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 Қадыржан Аружан Булатовна на тему «Разработка новых средств защиты информации в зоне прямой радиовидимости» является завершенным научным исследованием, соответствует требованиям, предъявляемым к диссертациям на соискание степени доктора философии (PhD) по образовательной программе 8D07104 – Приборостроение, и обладает научной новизной и практической значимостью. С учетом изложенного считаю, что автор заслуживает присуждения степени доктора философии (PhD) по образовательной программе 8D07104 – Приборостроение.

Официальный рецензент:

Профессор
Международного университета
информационных технологий — Айтмагамбетов А.З.

Подпись указанного лица удостоверяю
Менеджер по персоналу