

Федеральное агентство связи
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Сибирский государственный университет телекоммуникаций и
информатики»
(СибГУТИ)

ОТЗЫВ

на выпускную квалификационную работу магистранта гр. МГ-171
Анискиной А.Д. по теме «Исследование и анализ надёжности шифра
Шеннона»

В 2016 году были теоретически описаны и строго доказаны свойства двух шифров Шеннона. Основной целью данной работы является исследование надёжности реализации одного из этих шифров Шеннона для поточного шифрования данных, передаваемых по сети. Помимо теоретического обоснования надёжности шифра, одной из важнейших задач является доказательство надёжности его реализации, потому как уязвимости зачастую находятся именно в тех нюансах, которые отличают практическую реализацию от теории.

В рамках работы Анискиной А.Д. необходимо было выполнить масштабное исследование и проверку адаптации шифра Шеннона, нацеленной на возможность его применения на практике для поточного шифрования данных. Перед автором стояла задача изучить и применить к рассматриваемой реализации все известные в настоящее время атаки на поточные шифры, исследовать возможность других атак и постараться выявить уязвимости, либо параметры шифра, при которых он наиболее уязвим. Кроме того, требовалось оценить трудоёмкость взлома зашифрованных данных с учётом применения всех возможных атак и либо подтвердить его надёжность, либо предложить рекомендации по её повышению.

Автором работы были выполнены все поставленные задачи, в результате была показана устойчивость шифра ко всем видам атак, исследованы и оценены различные параметры шифра.

Существенных замечаний к оформлению нет, все этапы работы выполнены в срок и на высоком уровне. По результатам проверки на сайте *antiplagiat* оригинальность работы составляет 85,09%, что полностью соответствует требованиям, предъявляемым к ВКР. Поэтому работу магистранта Анискиной А.Д. оцениваю на **«отлично»** и рекомендую для публикации в рецензируемом научном издании. Считаю, что Анискина А.Д. заслуживает присвоения квалификации «магистр» по направлению 09.04.01 - «Информатика и вычислительная техника» и рекомендую её для поступления в аспирантуру.

Компетенции		Уровень сформированности компетенций		
		высокий	Средний	низкий
Общекультурные	ОК-1 Способность совершенствовать и развивать свой интеллектуальный и общекультурный уровень	+		
	ОК-3 Способность к самостоятельному обучению новым методам исследования, к изменению научного и научно-производственного профиля своей профессиональной деятельности	+		
	ОК-4 Способность заниматься научными исследованиями	+		
	ОК-5 Использование на практике умений и навыков в организации исследовательских и проектных работ, в управлении коллективом	+		
	ОК-6 Способность проявлять инициативу, в том числе в ситуациях риска, брать на себя всю полноту ответственности	+		
	ОК-9 Умение оформлять отчеты о проведенной научно-исследовательской работе и подготавливать публикации по результатам исследования	+		
Общепрофессиональные	ОПК-3 Способность анализировать и оценивать уровни своих компетенций в сочетании со способностью и готовностью к саморегулированию дальнейшего образования и профессиональной мобильности	+		
	ОПК-5 Владение методами и средствами получения, хранения, переработки и трансляции информации посредством современных компьютерных технологий, в том числе в глобальных компьютерных сетях	+		
Профессиональные	ПК-2 знанием методов научных исследований и владение навыками их проведения	+		
	ПК-7 применением перспективных методов исследования и решения профессиональных задач на основе знания мировых тенденций развития вычислительной техники и информационных технологий	+		
	ПК-17 способностью к организации промышленного тестирования создаваемого программного обеспечения	+		

Работа имеет практическую ценность
 Работа имеет теоретическую значимость
 Работа внедрена
 Рекомендую работу к опубликованию
 Работа выполнена в рамках гранта НИОКР

+
+
+

Тема предложена предприятием
 Тема предложена студентом
 Тема является фундаментальной
 Рекомендую студента в аспирантуру
 Имеются публикации по теме работы

+
+
+

Доц. каф. ПММК, к.т.н.
 Должность руководителя

подпись

Ракитский Антон Андреевич
 ФИО руководителя