Отзыв научного руководителя на диссертацию
Казакова Ильи Борисовича
«Математические модели передачи информации через
зашумленные скрытые каналы»

Работа И. Б. Казакова посвящена исследованию проблемы передачи информации через зашумленные скрытые каналы.

Содержательно под скрытым каналом понимается передача информации способом, не предусмотренным при проектировании системы. В качестве примеров можно привести модуляцию разделяемых ресурсов (процессорного времени, объема оперативной памяти), кодирование информации в служебных полях сетевых пакетов (порядковый номер, приоритет) или в передвижении персонажа многопользовательской игры. Так как скрытые каналы не рассматривались при проектировании и анализе безопасности, возникает риск нарушения политики безопасности. Важность этой угрозы была отмечена еще в “Оранжевой книге” — одном из первых стандартов в области безопасности. В системах с повышенными требованиями к защищенности в соответствии с этим стандартом необходимо идентифицировать скрытые каналы и понизить их пропускную способность до приемлемого уровня (не больше 100 бит в секунду). Распространенный способ понижения пропускной способности заключается в добавлении шума, однако при этом естественным образом снижается производительность системы. Таким образом, задача оценки пропускной способности зашумленного скрытого канала является безусловно **актуальной и практически значимой**.

Основной целью работы И. Б. Казакова является рассмотрение ряда математических моделей зашумленных скрытых каналов передачи информации, построение способов надежной передачи и оценка пропускной способности.

Возникают следующие подзадачи:

1. рассмотрение скрытого канала, основанного на перестановке сетевых пакетов, с моделями ошибок передачи, порожденных транспозициями пакетов и/или потерями пакетов; построение кодов, исправляющих заданное количество ошибок;
2. рассмотрение скрытого канала, основанного на манипулировании объемом занимаемой памяти; организация надежной передачи по каналу и оценка пропускной способности;
3. рассмотрение скрытого канала, основанного на перемещении персонажа многопользовательской игры; рассмотрение случая, когда

некоторые направления движения могут блокироваться (“канал с запрещениями”), и случая, когда персонаж-передатчик может выпасть из области видимости персонажа-приемника (“канал со стираниями”); исследование возможности надежной передачи и оценка пропускной способности.

Содержание диссертации отражает приведенные постановки.

Во **введении** описываются цели работы, обосновывается актуальность и практическая значимость, приводятся основные результаты.

Глава 1 является обзором, посвященным скрытым каналам. Автор анализирует существующие подходы к определению скрытого канала, приводит широкий класс примеров, рассматривает различные источники шума.

Вторая глава посвящена каналу, основанному на перестановке порядка отправки сетевых пакетов. Выбирается натуральный параметр n , и в качестве сообщений выступают перестановки из множества S_n . В процессе передачи могут происходить ошибки: пара пакетов может поменяться местами, пакет может потеряться. Автор вводит граф кода, в котором смежность вершин порождается соответствующей моделью ошибки, сводит задачу построения кода, исправляющего заданное число ошибок, к построению независимого множества, и численно решает задачу построения надежных кодов для практически интересных значений n и числа ошибок. Кроме того, приводится теоретическая оценка мощности оптимального кода для случая, когда допускается одна транспозиция пакетов (теорема 1).

В **третьей главе** изучается канал, основанный на манипулировании объемом памяти, занимаемым процессом-передатчиком. Автор приводит явную реализацию канала, основанную на так называемом разностном коде. Ошибка возникает, если между двумя последовательными записями в канал не происходит чтения. Для обеспечения надежности предлагается разбить сообщение на блоки небольшой длины и передавать блоки циклически. В случае, если ошибки независимы и равновероятны, доказано утверждение о среднем времени передачи (теорема 2). Это время логарифмически зависит от длины сообщения, то есть передача оказывается достаточно эффективной. Еще один важный результат — утверждение о неулучшаемости стратегии передачи (теорема 3). Автором также создана программная реализация канала, показавшая адекватность принятых в модели предположений.

Глава 4 посвящена так называемому каналу с запрещениями. Содержательно задача возникла из рассмотрения передачи информации посредством движения персонажа по игровому полю, когда механизмы

игры могут блокировать те или иные направления движения. Формально на каждом такте из всего n -буквенного алфавита выбирается множество мощности не менее k доступных для передачи символов. Требуется организовать протокол гарантированной отправки одного бита информации. Оказывается, что решение этой задачи существует тогда и только тогда, когда выполнено неравенство $n \leq 2k - 2$ (теорема 4). Интересно, что если разрешить менять запреты не чаще, чем раз в два такта, условия существования протокола принимают вид $k > 1$.

В **пятой главе** исследуется механизм блужданий по игровому полю. Предполагается, что приемник видит передающего игрока только в отдельные такты, то есть вместо всей траектории видимыми оказываются некоторые фрагменты. Решается задача проверки эквивалентности пары траекторий, то есть совпадения положений игрока во все моменты видимости. Блуждание по плоскости изоморфным образом сводится к блужданию на графе, а проблема совпадения конца траекторий решается в терминах проверки равенства пары многочленов специального вида (теорема 5).

Наконец, **глава 6** посвящена передаче информации через канал частичного стирания, когда вместо символов исходного алфавита приемник получает на вход элементы классов эквивалентности. Сперва изучается случай равномерного кода, в котором каждый символ кодируется траекторией движения одной и той же длины. Как и в третьей главе, надежность передачи обеспечивается с помощью повторов. Формулируется и доказывается аналогичная теореме 2 теорема 6 о среднем времени передачи сообщения заданной длины. Выполненная программная реализация и проведенные численные эксперименты показали адекватность предположений, принятых в математической модели. Во второй части главы предположение о равномерности снимается. Автор изучает возможность однозначного онлайн-декодирования (при этом некоторые декодированные символы могут заменяться на специальный символ стирания). В этом направлении удалось найти критериальные условия на передатчик (теоремы 7 и 9) и оптимальную структуру приемника (теорема 8).

В **заключении** перечисляются основные результаты диссертации.

Содержание работы **свидетельствует** о том, что полученные в ходе ее создания **результаты являются новыми и вносят вклад в решение научной задачи — изучения надежности и пропускной способности зашумленных скрытых каналов.**

Практическая значимость полученных результатов состоит в возможности применения результатов в анализе защищенности реальных систем.

Основные результаты диссертации докладывались на «Ломоносов-

ских чтениях» в 2017 и 2018 году, на XVIII Международной конференции «Алгебра, теория чисел и дискретная геометрия: современные проблемы, приложения и проблемы истории» (ТГПУ им. Л. Н. Толстого, 23-26 сентября 2020 г.), на XXVII Международной научной конференции студентов, аспирантов и молодых ученых «Ломоносов 2020» (МГУ имени М.В. Ломоносова, 10-27 ноября 2020 г.), на семинаре «Intelligent Systems Workshop» (Huawei Moscow Research Center, 16 декабря 2020 г.), а также неоднократно на специальных семинарах механико-математического факультета. По результатам работы автором опубликовано 7 статей, включая одну статью в журнале, индексируемом в Scopus, и четыре статьи в журналах из RSCI.

Достоверность и обоснованность результатов подтверждается:

- четкостью формулировок утверждений и строгостью представленных доказательств;
- апробацией на семинарах и конференциях;
- опубликованием основных результатов в рецензируемых журналах из списков ВАК, RSCI и Scopus.

С учетом изложенного считаю, что **работа И. Б. Казакова соответствует критериям, установленным в “Положении о присуждении ученых степеней в Московском государственном университете имени М.В.Ломоносова”, и рекомендуется к защите в диссертационном совете МГУ 05.01 ФГБОУ ВО МГУ по специальности 05.13.19 — методы и системы защиты информации, информационная безопасность, а ее автор, несомненно, заслуживает присуждения ему ученой степени кандидата физико-математических наук.**

Научный руководитель
кандидат физико-математических наук,
старший научный сотрудник
кафедры математической теории
интеллектуальных систем

А.В. Галатенко

Подпись старшего научного сотрудника А. В. Галатенко удостоверяю.

Декан механико-математического
факультета МГУ имени М.В.Ломоносова
д.ф.-м.н., профессор,
член-корреспондент РАН

А. И. Шафаревич