ОТЗЫВ

официального оппонента на диссертационную работу
Казакова Ильи Борисовича
**«Математические модели передачи информации через зашумлённые
скрытые каналы»**, представленную на соискание ученой степени
кандидата физико-математических наук по специальности 05.13.19 –
«Методы и системы защиты информации, информационная безопасность»
(физико-математические науки)

Исследование характеристик скрытых каналов передачи информации играет важную роль в задачах информационной безопасности. Наличие скрытого канала в системе является существенной угрозой её безопасности, так как такой канал позволяет передавать информацию трудно выявляемым способом. Одной из существенных характеристик скрытого канала является его пропускная способность. Наличие скрытых каналов низкой пропускной способности принято считать допустимым. В силу своих особенностей, скрытый канал передачи информации, как правило, является зашумлённым. В диссертационной работе рассматриваются вопросы, связанные с определением возможности передачи информации по зашумлённым каналам и оценкой их пропускной способности.

Диссертационная работа состоит из введения, шести глав и заключения. Общий объем работы составляет 184 страницы, список используемой литературы содержит 96 наименований, включая 7 работ автора по теме диссертационного исследования.

Во введении определяются цели и задачи исследования, обосновывается теоретическая и практическая значимость работы.

Первая глава имеет обзорный характер. В ней приводятся определения скрытых каналов, обосновывается важность получения оценок их пропускной способности, обсуждаются особенности зашумлённых скрытых каналов.

Во второй главе исследуется канал на основе изменения порядка передачи сетевых пакетов. В качестве модели ошибок рассматриваются перестановки и потери пакетов, которые могут возникать в сети передачи данных. Для множества перестановок S_n строится исправляющий ошибки код, приводятся экспериментальные оценки мощности кодов при различных значениях n и максимального числа ошибок. Для модели ошибки, допускающей только перестановку пакетов, доказывается нижней оценки мощности кода, допускающего эффективный алгоритм построения.

В третьей главе изучается скрытый канал на основе изменения объёма занятой процессом виртуальной памяти. В предлагаемом протоколе процесс-передатчик изменяет объём занятой памяти таким образом, что разность значений в соседние моменты времени кодирует значение передаваемого байта. В качестве модели ошибок рассматривается пропуск чтения, когда процесс-приёмник по каким-либо причинам не успел прочитать переданный символ. Предлагается разделение передаваемого сообщения на блоки и циклическая стратегия передачи блоков сообщения. Для заданной вероятности возникновения ошибки чтения вычисляется математическое ожидание количества циклов передачи, при котором сообщение будет передано. Согласно теореме 2 среднее количество циклов логарифмически увеличивается в зависимости от числа передаваемых блоков. Далее формально доказывается неуплучшаемость циклической стратегии передачи.

В главах с четвёртой по шестую рассматривается оригинальная задача построения скрытого канала на основе блуждания по плоскости с ограничениями. Одной из возможных интерпретаций данной задачи может быть передача данных в рамках компьютерной игры, когда один из участников имеет возможность наблюдать за движениями другого, траектория движения которого кодирует передаваемое сообщение, при этом движения игрока-передатчика могут быть ограничены некоторыми условиями, а игрок-приёмник наблюдает положение игрока-передатчика только в некоторые моменты времени. В главе 4 доказываются критерий возможности передачи одного бита информации при полной наблюдаемости передатчика и запрете на передачу некоторых символов в каждый такт времени (теорема 4). В главе 5 вводится формализация понятия блуждания по плоскости и разрабатывается техника для анализа траекторий блуждания по плоскости при частичном наблюдении.

В шестой главе вводится понятия структуры и канала частичного стирания, которые являются формализацией рассмотренной ранее модели движения персонажа компьютерной игры по игровому полю. Символы передаваемого сообщения кодируются словами в алфавите возможных перемещений. Декодирование символа s , представленного словом $w(s)$, возможно в том случае, когда наблюдаемым перемещениям отправителя, то есть разреженному подслову w , может соответствовать только один символ s . Для равномерного кодирования, по аналогии с подходом циклической передачи для канала с изменением объёма памяти, оценивается среднее количество циклов передачи. В заключительной части главы вводится понятие корректного протокола, который может использовать произвольные

коды, и доказываются критерий существования корректного протокола в канале частичного стирания.

В заключении формулируются основные результаты работы.

К числу наиболее важных результатов можно отнести следующее.

- Построена модель односторонней поблочной передачи информации. Получена оценка среднего времени, необходимого для завершения передачи, доказана оптимальность циклической стратегии передачи блоков.
- Разработана модель каналов с запрещениями. Сформулирован и доказан критерий надёжной передачи информации по такому каналу.
- Введено понятие канала частичного стирания и корректного протокола в таком канале. Получены оценки среднего времени передачи в канале частичного стирания с равномерным кодированием. Формулируется и доказываются критерий существования корректного протокола передачи в общем случае.

Достоинства диссертации.

1. В работе получены оценки пропускной способности для различных скрытых каналов передачи информации, что может иметь практическое значение при анализе уровня защищенности конкретных информационных систем.

2. Введено новое понятие канала частичного стирания. Разработан математический аппарат для анализа каналов частичного стирания на основе блуждания по плоскости, который может применяться для анализа других аналогичных каналов.

3. Рассмотренные в диссертационной работе скрытые каналы были реализованы в виде программного обеспечения, получены результаты численных экспериментов оценки пропускной способности при различных значениях параметров соответствующих скрытых каналов.

4. Все модели и утверждения строго формализованы и доказаны.

5. Работа написана понятным языком, с рассмотрением содержательных примеров. Доказательства утверждений, которые в некоторых случаях являются достаточно громоздкими, вынесены в отдельный раздел, что значительно упрощает чтение текста работы.

Недостатки. В работе можно выделить три части, которые довольно слабо связаны друг с другом. Главы 2, 3 и с четвёртой по шестую объединяет только то, что все они связаны с анализом характеристик скрытых каналов передачи данных. Однако, и методы технической реализации исследуемых каналов, и разработанный для их анализа математический аппарат различаются. Как отмечается во введении данной работы, известно большое число практических реализаций каналов скрытой передачи информации. В этой связи обоснование выбора именно таких каналов заслуживает большего внимания.

В главе 3 при рассмотрении канала передачи на основе манипулирования размером занятой процессом-передатчиком оперативной памяти утверждается, что в силу особенностей возникающих ошибок приёма информации, когда соседние значения «склеиваются», применение известных кодов, исправляющих ошибки затруднено. Предлагается протокол, который удаляет полученный блок данных, если в процессе его передачи возникла ошибка. Подобная модель процесса-получателя представляется упрощённой. Если при двукратной передаче блока каждый раз возникала ошибка, но при приёме разных символов исходного сообщения, сообщение может быть восстановлено путём сравнения двух блоков с искажениями. Аналогичное замечание относится и к каналу частичного стирания. В случае повторной передачи кода входного символа может быть принят другой класс эквивалентности, который не может использоваться для независимого восстановления переданного символа, но может разрешить неоднозначность, возникшую на первом цикле передачи.

В работе также имеются неточности изложения. Рассматриваемая циклическая стратегия передачи предполагает передачу блоков до успешной передачи всего сообщения. Однако, предполагается, что процесс-передатчик не имеет обратной связи от процесса-получателя. Оценка среднего количества циклов передачи не гарантирует успешности процесса. В формулировке теоремы 1 на стр. 46 используется обозначение для максимальной мощности независимого множества графа. Это обозначение пояснялось в одном из предыдущих утверждений, но, строго говоря, в формулировке теоремы оно могло иметь и другой смысл. На стр. 115 не оговаривается, что z_0 является примитивным корнем степени j . В нескольких местах частичная сумма гармонического ряда называется суммой гармонического ряда.

Перечисленные замечания не оказывают влияния на общую положительную оценку работы.

Заключение по диссертации. В работе получены новые теоретические результаты, которые могут использоваться в области разработки прикладных систем обработки конфиденциальной информации.

Автореферат корректно и полно отражает содержание диссертационной работы. Основные результаты были опубликованы в рецензируемых периодических изданиях, включая пять публикаций в журналах из списка Scopus/Web of Science, и докладывались на различных профильных конференциях и семинарах.

Диссертация Казакова Ильи Борисовича «Математические модели передачи информации через зашумлённые скрытые каналы» соответствует всем требованиям, предъявляемым Положением о присуждении учёных степеней в Московском государственном университете имени М.В. Ломоносова к диссертациям на соискание учёной степени кандидата наук, а её автор заслуживает присуждения учёной степени кандидата физико-математических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» (физико-математические науки).

Официальный оппонент:

кандидат физико-математических наук,

ведущий научный сотрудник

Научно-исследовательского института механики

МГУ им. М. В. Ломоносова

Афонин Сергей Александрович

22 ноября 2021 г.

Контактные данные: тел. +7 (495) 939-53-06, e-mail: serg@msu.ru

Адрес места работы:

119192, Москва, Мичуринский проспект, д. 1, НИИ механики МГУ.

Специальность, по которой официальным оппонентом защищена диссертация: 05.13.11 – «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей» (физико-математические науки).

Подпись ведущего научного сотрудника С. А. Афонина удостоверяю.