

ОТЗЫВ

на автореферат диссертации Казакова Ильи Борисовича
«Математические модели передачи информации через зашумлённые скрытые каналы»,
представленной на соискание ученой степени кандидата
физико-математических наук по специальности 05.13.19 – «Методы и
системы защиты информации, информационная безопасность»

Согласно представленному тексту автореферата, диссертация Казакова И.Б. посвящена способам оценки пропускной способности скрытых каналов в условиях зашумления. Скрытый канал — это коммуникационный канал, пересылающий информацию методом, который не был для этого предназначен. С помощью скрытых каналов могут быть реализованы такие нарушения политики безопасности, как утечка паролей и внедрение вредоносных программ. Таким образом, наличие скрытых каналов нежелательно с точки зрения безопасности системы, а если их наличие неизбежно, то их пропускная способность должна быть как можно меньше. Требования к выявлению и ограничению скрытых каналов присутствует в различных стандартах безопасности.

Для исследования автором выбран ряд модельных примеров скрытых каналов: канал перестановки пакетов, канал манипуляции объёмом виртуальной памяти и канал блужданий по плоскости. Решаемая автором задача состоит в том, чтобы исследовать возможность надёжной передачи информации и оценить пропускную способность при заданном типе и уровне шумов.

В разделе автореферата, посвященном краткому содержанию диссертации, представлены результаты исследований. Результаты, относящиеся к скрытому каналу перестановки пакетов, сводятся к характеристикам, полученным с помощью численного эксперимента по поиску максимальных исправляющих ошибки кодов, а также к оценкам мощности так называемого «послойного кода». На основе полученных численных значений и формальных утверждений несложно вычислить пропускную способность реализации канала. Для канала, основанного на манипуляции занимаемой виртуальной памяти, построена математическая модель и получены теоремы о логарифмическом росте времени передачи и неувлучшаемости циклической стратегии. Поскольку логарифм — это медленно растущая функция, то большие объёмы информации могут быть передаваемы достаточно эффективно. Изучение канала блужданий по плоскости разбивается на три темы: структура блужданий по плоскости, канал с запрещениями и канал частичного стирания. Выявлено, что блуждания по плоскости сводятся к блужданиям по счётному графу, вершинам которого могут быть приписаны целочисленные координаты. Получен критерий надёжности канала с запрещениями. Представлены новые понятия структуры и канала частичного стирания. Рассмотрено семейство протоколов, называемое «схемой равномерного кодирования». Также рассмотрен протокол в общем случае, найдено накладываемое на приемника критериальное условие существования согласованного передатчика.

Результаты диссертации опубликованы в 5 печатных работах в изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность», а также в двух работах, опубликованных в журналах из списка ВАК. Также результаты прошли апробацию на пяти всероссийских и международных конференциях и трех специальных семинарах.

К автореферату имеются следующие замечания:

1. Было бы полезно снабдить полученные теоретические результаты иллюстрациями, выукло

отражающими возможность практического использования, в частности, оценками пропускной способности возможных реализаций.

2. В разделе, посвященном опубликованным работам, не указано разделение публикаций на типы (в изданиях из списка рекомендованных к защите и в прочих изданиях).

Перечисленные замечания не влияют на общую положительную оценку диссертационной работы.

Содержание автореферата диссертации соответствуют специальности 05.13.19 - «Методы и системы защиты информации, информационная безопасность», а также критериям, установленным в Положении о присуждении ученых степеней в Московском государственном университете имени М.В. Ломоносова, а её автор, Казаков Илья Борисович, заслуживает присуждения ему ученой степени кандидата физико-математических наук по специальности 05.13.19 - «Методы и системы защиты информации, информационная безопасность».

Ст. преподаватель кафедры
Прикладной математики и кибернетики
Петрозаводского государственного университета,
Кандидат технических наук

Р.В. Сошкин

2 декабря 2021

Контактные данные:

тел. +7 911 406 7026

e-mail: soshkin@mail.ru

Адрес места работы:

185910, Республика Карелия,
Петрозаводск, пр. Ленина 33