ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

на диссертацию **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

Диссертация И.Б. Казакова посвящена исследованию скрытых каналов передачи информации. Автор пользуется определением скрытого канала, введенным в работе Лэмпсона: канал называется скрытым, если информация передается способом, не предусмотренным для передачи при проектировании системы. Близкими понятиями являются стеганография, когда безопасность передачи обеспечивается сокрытием самого факта передачи, а также цифровые водяные знаки, когда в файл-контейнер встраивается дополнительная информация, причем встраивание не должно приводить к заметной модификации контейнера. В литературе приведено большое количество примеров скрытых каналов разного типа – внутрихостовых и сетевых, по времени и по памяти, детерминированных и вероятностных… Требования, связанные с необходимостью выявления и ограничения пропускной способности скрытых каналов, присутствуют в стандартах информационной безопасности, начиная с «Оранжевой книги». Если канал невозможно выявить и полностью заблокировать (известны теоремы о существовании невыявляемых скрытых каналов, в частности, принадлежащие А.А. Грушо и Е.Е. Тимониной), можно привнести шум, который, с одной стороны, может сломать или хотя бы замедлить скрытые каналы, но, с другой стороны, приведет к деградации производительности системы. Таким образом, с точки зрения обеспечения безопасности актуальна задача анализа надежности системы и пропускной способности зашумленных скрытых каналов – решение этой задачи позволит

оптимизировать подбор параметров шума для достижения заданного уровня защищенности системы. В работе И.Б. Казакова рассматривается интересный и достаточно репрезентативный ряд примеров скрытых каналов и моделей ошибки передачи информации по ним, привносимой шумом. Таким образом, диссертация соответствует паспорту специальности 05.13.19 – методы и системы защиты информации, информационная безопасность (пункт 5 – Методы и средства (комплексы средств) информационного противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет, пункт 7 – Анализ рисков нарушения информационной безопасности и уязвимости процессов переработки информации в информационных системах любого вида и области применения, а также пункт 9 – Модели и методы оценки защищенности информации и информационной безопасности объекта).

Работа состоит из введения, шести глав и заключения. Во введении автор формулирует цели исследования, обосновывает актуальность и практическую ценность поставленных задач, приводит основные результаты.

Первая глава носит преимущественно обзорный характер. Описываются существующие подходы к определению понятия скрытого канала (и обосновывается выбор определения Лэмпсона), приводится ряд известных примеров скрытых каналов, анализируются источники и типы шума.

Во второй главе изучается скрытый канал передачи информации, основанный на модуляции порядка отправки сетевых пакетов. На практике это может быть реализовано в терминах порядковых номеров пакетов, выбора номера порта источника или ip-адреса получателя. Предполагается, что в процессе передачи в системе (например, в результате «зашумляющего» преобразования) пакеты могут быть переставлены местами и/или потеряться (это актуально для транспортного протокола UDP). Автор вводит математическую модель, в которой сообщения кодируются перестановками на заданном конечном множестве, а ошибки передачи задают отношение смежности в графе, вершинам которого соответствуют возможные сообщения

на стороне приемника. Задача построения оптимального кода, гарантированно исправляющего заданное число ошибок, сводится к задаче о построении максимального независимого множества в графе. Автор сначала решает задачу численно (для множеств небольшого порядка), затем для одной из моделей ошибки приводит аналитическое решение и оценивает мощность получающегося кода.

В третьей главе автор переходит от сетевого случая к внутрихостовому и от гарантированно надежной передачи к вероятностной. Субъект-передатчик кодирует информацию в объеме собственной памяти (точнее, в изменении этого объема с течением времени). Возможные ошибки сводятся к «склейке» нескольких передаваемых значений в одно, а надежность обеспечивается многократным повторением сообщения. В рамках формальной модели циклически передается сообщение из n блоков, причем вероятность успешной передачи каждого отдельного блока фиксирована и не зависит от вероятностей, соответствующих другим блокам. Показано, что среднее время успешной передачи сообщения растет логарифмически по n, а также что циклическая стратегия передачи является оптимальной.

В четвертой главе тип изучаемого скрытого канала вновь меняется. Автор переходит к рассмотрению случая, когда приемник и передатчик играют в многопользовательскую игру, а передача производится с помощью ходов игрового персонажа. Вводится дополнительная сущность – субъект, который на каждом такте может блокировать заданное подмножество ходов. Содержательно запреты могут быть реализованы, например, с помощью игровых сущностей типа монстров. Требуется понять, при каких условиях можно организовать гарантированно надежную передачу информации. Автору удалось полностью решить поставленную задачу. В случае, когда запреты меняются не чаще, чем один раз в два такта, надежная передача возможна всегда. Если же запреты могут меняться каждый такт, предлагается критерий, связывающий мощность алфавита (множества ходов) и мощность множества запретов.

В пятой главе субъект-блокировщик исключается из рассмотрения. Вместо этого вводится класс ошибок, связанный с выпадением игрока-передатчика из области видимости игрока-приемника (формально приемник наблюдает положение передатчика в какое-то подмножество моментов времени). Изучается вопрос, какие последовательности ходов могут приводить к полному совпадению положений в моменты видимости. От блужданий по игровому полю автор переходит к блужданию на графе, а критерий совпадения концов траекторий элегантно формулирует в терминах совпадения пары многочленов.

В шестой главе изучается возможность построения каналов передачи информации в модели, введенной в пятой главе. Возникает понятие стирания, содержательно имеющее тот же смысл, что и в теории кодирования. Сначала рассматривается случай равномерного алфавитного кода, в котором все элементарные кодовые слова состоят из одинакового числа символов-ходов, а надежность, как и в третьей главе, обеспечивается циклической передачей. В этом случае удается получить утверждения о среднем времени передачи, аналогичное утверждению из третьей главы. Затем ограничения существенно смягчаются – разрешается использовать кодовые слова разной длины и менять кодовые слова в зависимости от времени (это имеет смысл, например, в случае существенных неоднородностей игрового поля). Решается следующая задача. Предполагается, что процесс-передатчик – детерминированная функция; по заданной функции и модели ошибки требуется понять, существует ли возможность онлайн-декодирования сообщения с возможной заменой некоторых букв на специальный символ стирания. Здесь И.Б. Казакову удалось получить критерий возможности такого декодирования. В случае положительного ответа приводится описание оптимального приемника.

Наконец, в заключении перечисляются основные результаты диссертации.

Достоинства диссертации

1. Четкость изложения. Работа написана на хорошем математическом языке, утверждения сформулированы строго и корректно, доказательства верные,

полные и понятные. Можно также отметить безупречный русский язык, что не всегда встречается в диссертациях.

2. Нетривиальность результатов. Доказательства некоторых утверждений работы оказались достаточно объемными и непростыми. Особенно следует отметить критерий существования надежной передачи в условиях блокировок (теорема 4) и конструкцию для оптимального приемника (теорема 8).

3. Широта технического арсенала. Автор продемонстрировал владение методами из разных областей математики; в частности, в пятой главе используются довольно тонкие алгебраические конструкции, в третьей главе потребовалось обратиться к методам математического анализа. Кроме того, для обоснования практической адекватности формальных моделей был написан ряд программ и проведены содержательные эксперименты.

4. Широта охвата. В работе изучаются разные классы скрытых каналов, моделей ошибки и способов достижения надежности. При этом не возникает ощущения эклектичности – диссертация оставляет целостное впечатление.

Недостатки диссертации

1. Работа имеет теоретический характер, но могла бы содержать рекомендации, как нужно разрушать и/или ограничивать скрытые каналы рассмотренных типов в реальных системах. В работе приводится ряд общих соображений, однако ожидается большая конкретизация (например, в виде списка действий, обеспечивающих падение пропускной способности до заданного приемлемого уровня).

2. Не рассматривается случай ограниченно детерминированного передатчика в главе 6. Детерминированные функции образуют континуальное множество, что препятствует конструктивному рассмотрению. Представляется, что условие ограниченной детерминированности позволило бы перейти к алгоритмической реализации процедур проверки корректности кодирования и построения оптимального декодера.

3. Библиографию по скрытым каналам в многопользовательских играх автор ограничил одним примером, тогда как число публикаций много больше.

4. Наличие погрешностей в оформлении, в основном при форматировании текста и формул (стр. 31, 61, 95, 146 и др.).

В целом работа оставляет хорошее впечатление. Полученные результаты являются новыми, материал изложен полно и подробно, решенные задачи актуальны и содержательны.

Автореферат полно и строго отражает цели и задачи исследования, постановки и основные результаты. Содержание диссертации в достаточной степени отражено в печатных работах (одной статье в журнале из списка Scopus, четырех статьях в журналах из списка RSCI и двух публикациях в журналах из списка ВАК).

Вместе с тем, указанные выше замечания не умаляют значимости диссертационного исследования. Диссертация И.Б. Казакова «Математические модели передачи информации через зашумлённые скрытые каналы» является законченным научным исследованием и отвечает требованиям, установленным Московским государственным университетом имени М.В. Ломоносова к работам подобного рода. Содержание диссертации соответствует паспорту специальности 05.13.19 – «методы и системы защиты информации, информационная безопасность» (по физико-математическим наукам), а также критериям, определенным пп. 2.1-2.5 Положения о присуждении ученых степеней в Московском государственном университете имени М.В. Ломоносова, а также оформлена, согласно приложениям № 5, 6 Положения о диссертационном совете Московского государственного университета имени М.В. Ломоносова.

Таким образом, соискатель Казаков Илья Борисович заслуживает присуждения ученой степени кандидата физико-математических наук по специальности 05.13.19 – «методы и системы защиты информации, информационная безопасность».

Официальный оппонент:

Доктор технических наук, профессор кафедры математического и компьютерного моделирования Института информационных и вычислительных технологий ФГБОУ ВО «НИУ «МЭИ»

Фролов Александр Борисович

19 ноября 2021 г.

Контактные данные:

тел. , e-mail: frolovab@mpei.ru

Специальность, по которой официальным оппонентом защищена диссертация:

05.13.01 – Системный анализ, управление и обработка информации (по отраслям)

Адрес места работы:

111250, г.Москва, вн. тер. г. муниципальный округ Лефортово, ул. Красноказарменная, д.14, стр. 1. ФГБОУ ВО «НИУ «МЭИ», кафедра математического и компьютерного моделирования. Тел.: +7(495)362-77-74; e-mail: universe@mpei.ac.ru