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)

Диссертация И.Б. Казакова посвящена изучению надежности и пропускной способности скрытых каналов передачи информации. Канал считается скрытым, если информация по этому каналу передается способом, не предусмотренным при проектировании информационной системы. В качестве примеров можно привести кодирование информации в неиспользуемых полях заголовков или в номерах сетевых пакетов, в модуляции загрузки разделяемого ресурса – процессорного времени, памяти, очереди печати, в именах временных файлов или параметрах счета за услуги. Так как изначально возможность передачи по скрытым каналам не рассматривалась, наличие скрытых каналов значительно увеличивает риск организации невыявляемых утечек информации или удаленной настройки программно-аппаратных закладок. Необходимо заметить, что полное блокирование скрытых каналов часто оказывается практически невозможным; скажем, при наличии разделяемых ресурсов в системах с многоуровневой безопасностью (MultiLevel Security, MLS) для предотвращения несанкционированных информационных потоков либо нужно разрешать все конфликты доступа в пользу менее привилегированных пользователей (и существенно затруднить работу более привилегированных пользователей), либо смириться с существованием скрытых каналов. Возможным выходом из положения представляется привнесение шума, из-за которого в канале возникнут помехи и скорость передачи информации значительно понизится. Шумы могут возникать естественным образом – сетевые пакеты могут пропадать из-за перегрузки каналов связи, разделяемые ресурсы могут использоваться другими процессами, временный файл с нужным именем может уже быть создан другим пользователем и т. д. – или в результате специальных мер по противодействию скрытым каналам.

В работе И.Б. Казакова рассматривается следующий класс задач. Зафиксирован механизм, на котором основан скрытый канал (автор рассматривает три постановки – кодирование информации через перестановку сетевых пакетов, через модуляцию объема памяти процесса и через перемещения персонажа по игровому полю), и класс шумов – в первом случае это не более, чем заданное число перестановок и/или потерь сетевых пакетов, во втором – вероятность неуспешной передачи блока информации, в третьем – либо изменяемый во времени запрет на использование части символов (направлений движения), либо пропадание игрока-передатчика из области видимости игрока-приемника. Требуется понять, при каких условиях возможна надежная передача информации, а также, в случае существования надежного механизма передачи, оценить пропускную способность скрытого канала. Решение задачи позволит анализировать защищенность систем от скрытых каналов, а также подбирать параметры противодействия, обеспечивающие заданную верхнюю границу пропускной способности.

Краткая характеристика работы и основные результаты

Диссертация И.Б. Казакова состоит из введения, шести глав и заключения.

Во введении приводятся цели исследования, обосновывается актуальность и практическая ценность работы, формулируются основные результаты.

Первая глава является обзором. В ней определяются основные понятия из области скрытых каналов, приводится ряд примеров скрытых каналов различных типов, проводится анализ источников шумов.

Вторая глава посвящена изучению скрытого канала на основе изменения порядка отправки сетевых пакетов. Сообщение кодируется перестановкой. Рассматривается два класса ошибок, которые могут произойти при передаче: перестановка порядка пары пакетов и потеря пакета. Вводится граф, вершинами которого являются элементы множества сообщений на выходе из канала передачи, а отношение смежности порождено ошибками. Показывается, что построение кодового множества, гарантированно исправляющего заданное множество ошибок, эквивалентно поиску независимого множества в графе или поиску клики в графе-дополнении. С помощью численного эксперимента строятся максимальные или близкие к максимальным кодовые множества для перестановок на множествах небольшого порядка – от 3 до 7. Для случая перестановки пары пакетов приводится конструкция так называемого послойного кода, исправляющего ошибки. В теореме 1 доказывается нижняя оценка на мощность кода.

В третьей главе автор переходит к передаче информации на основе изменения объема памяти процесса-передатчика. Предлагается протокол, в котором процесс-передатчик циклически побайтово передает сообщение, при передаче одного байта соответствует одно изменение объема, а процесс-приемник осуществляет циклическое считывание. Если между парой «записей» не происходит ни одного чтения, два байта на входе канала склеиваются в один байт на выходе. С помощью внедренных в протокол механизмов контроля целостности процесс-приемник обнаруживает, что блок из N байтов передан некорректно, и прием этого блока откладывается на следующую итерацию цикла. Предполагается, что ошибки передачи блока независимы и равновероятны. При таких предположениях доказана теорема 2 о среднем числе итераций, требуемом на успешную передачу сообщения из n блоков (оно логарифмически зависит от n), и теорема 3 о том, что циклическая стратегия передачи сообщения является неулучшаемой, то есть передача блоков в любом другом порядке не приведет к снижению среднего количества итераций. Отдельно отметим подраздел 3.1.3, в котором автор приводит ряд рекомендаций по противодействию рассмотренному скрытому каналу.

В четвертой главе автор переходит к изучению передачи информации посредством передвижений персонажей многопользовательских игр, то есть кодовый алфавит состоит из ходов в одном из направлений из заданного конечного множества мощности n. В данной главе явно возникает субъект, противодействующий передаче. На каждом такте этот субъект, названный автором Евой, блокирует произвольные n-k кодовых символов, поэтому у передатчика остается k вариантов выбора хода. Ставится вопрос, при каких значениях n и k возможно гарантированно передать один бит информации. Ответ дается в теореме 4: необходимым и достаточным условием существования такого протокола является выполнение неравенства $n <= 2k$-2. Интересно, что если разрешить менять блокировки каждые два такта, то критерий существенно упростится и примет вид $k > 1$.

Пятая глава является по сути вспомогательной. Автор больше не рассматривает блокировки, вместо этого предполагается, что игрок-передатчик время от времени выпадает из области видимости игрока-приемника, так что видны известны не все местоположения, а только некоторое подмножество. В результате некоторые различные последовательности ходов могут порождать последовательности позиций, совпадающих во все моменты видимости, так что сообщения могут склеиваться. Глава содержательно посвящена алгоритму поиска склеек. В теореме 5 доказывается, что движение по игровому полю сводится к блужданию по специальному графу, а совпадение концов пары траекторий — к проверке совпадения пары многочленов с целыми коэффициентами. В заключение раздела перечисляются некоторые соображения, связанные с противодействием скрытым каналам, основанным на перемещениях в многопользовательских играх.

В шестой главе происходит возврат к непосредственному изучению скрытых каналов. В рамках предположений, введенных в главе 5, рассматривается две постановки. В первом случае все кодовые слова имеют одинаковую длину, то есть состоят из одинакового числа ходов, поэтому задача разделения сообщения на кодовые слова решается тривиально. Предполагается, что при

передаче каждого кодового слова с некоторой вероятностью может произойти ошибка; ошибки происходят независимо, а вероятности ошибки передачи разных кодовых слов могут отличаться. По аналогии с главой 3 сообщение передается циклическим образом. Доказывается теорема 6 о среднем числе итераций, требующемся для успешной передачи сообщения из n блоков. Также приводятся результаты расчета пропускной способности модельной реализации такого канала. Во втором случае происходит отказ от условия равномерности кода. Предполагается, что при передаче каждого символа исходного сообщения схема кодирования может меняться. Это предположение является практически осмысленным, так как игровое поле, вообще говоря, является конечным и неоднородным. В результате возникает континуальное семейство передатчиков-кодировщиков. Возникает вопрос, можно ли по заданному передатчику и модели ошибки создать корректный приемник-декодер. Автор, с одной стороны, накладывает дополнительное требование онлайн-декодирования, то есть возможности декодирования начала сообщения без зачитывания всего сообщения; с другой стороны, допускаются стирания, то есть замена части символов на специальный символ «*». Критерий существования корректного приемника представлен в теореме 7 (в силу континуальности множества передатчиков критерий не является конструктивным). В теореме 8 доказывается существование и способ построения оптимального, то есть выдающего минимальное число символов стираний, декодера.

В заключении перечислены основные результаты диссертации.

Полученные автором результаты являются новыми. Работа носит преимущественно теоретический характер. Введенные автором модели и доказанные теоремы могут быть полезны специалистам по информационной безопасности при анализе новых классов скрытых каналов, а также могут использоваться в рамках чтения курсов для студентов, специализирующихся в области защиты информации. Созданные автором программы могут применяться для оценки численных характеристик изученных скрытых каналов при конкретных параметрах, в том числе связанных с мерами противодействия.

Достоверность результатов и апробация работы

Диссертация И.Б. Казакова написана на высоком математическом уровне. Автор приводит все необходимые определения, четко и строго формулирует утверждения. Доказательства полны, понятны и корректны.

Результаты работы неоднократно докладывались на всероссийских и международных конференциях, а также на специальных семинарах механико-математического факультета МГУ имени М.В. Ломоносова.

Недостатки работы

1. Автор не приводит практически важные характеристики изученных скрытых каналов. В частности, для канала на основе перестановки пакетов и канала на основе изменения объема памяти не приведена пропускная способность, из-за чего затруднительно оценить степень угрозы, представляемой такими каналами; нет численной оценки эффективности предлагаемых в работе методов противодействия.
2. В рамках изучения скрытых каналов в многопользовательских играх приводятся две несвязанные постановки — с использованием блокировок («канал с запрещениями» в терминологии автора) и с возможностью выпадения из области видимости («канал частичного стирания»). Естественно было бы попытаться связать два механизма в рамках единой модели. Кроме того, в случае канала с запрещениями было бы интересно перейти от слишком консервативного предположения об идеальном выборе блокировок к более содержательному и практически интересному случаю случайных блокировок.
3. При написании обзорной части автору стоило ознакомиться с рядом русскоязычных источников, в частности, диссертацией оппонента «Анализ угроз скрытых каналов и методы

построения гарантированно защищенных распределенных автоматизированных систем», а также с обзорными статьями оппонента и научного руководителя в журнале JetInfo.

Приведенные недостатки не являются существенными и не влияют на общую положительную оценку работы.

Заключение

Диссертационная работа Казакова Ильи Борисовича «Математические модели передачи информации через зашумлённые скрытые каналы» представляет собой законченное научное исследование, в котором решены актуальные задачи. Полученные автором результаты являются достоверными и новыми.

Основное содержание работы опубликовано в семи статьях, в том числе пяти статьях в рецензируемых журналах, рекомендованных для защиты в диссертационном совете МГУ по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» (одна в журнале из списка Scopus и четыре в журналах из списка RSCI). Результаты докладывались на пяти всероссийских и международных конференциях и трех специальных семинарах.

Автореферат в полной мере соответствует содержанию диссертационной работы.

Диссертация Казакова Ильи Борисовича «Математические модели передачи информации через зашумлённые скрытые каналы» отвечает всем требованиям, установленным Московским государственным университетом имени М.В. Ломоносова к кандидатским диссертациям. Содержание диссертации соответствует паспорту специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» (физико-математические науки), а также критериям, определенным пп. 2.1-2.5 Положения о присуждении ученых степеней в Московском государственном университете имени М.В. Ломоносова. Работа оформлена согласно приложениям № 5, 6 Положения о диссертационном совете Московского государственного университета имени М.В. Ломоносова.

Соискатель Казаков Илья Борисович заслуживает присуждения ученой степени кандидата физико-математических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» (физико-математические науки).

Официальный оппонент
Тимонина Елена Евгеньевна,
ведущий научный сотрудник,
доктор технических наук,
профессор

Е.Е. Тимонина
«21» ноября 2021 г.

Федеральный исследовательский центр
«Информатика и управление» РАН,
119333, Москва, ул. Вавилова, д.44, кор.2,
тел.: +7 (499) 135-62-60,
email: ipiran@ipiran.ru

Подпись Е.Е. Тимониной заверяю
ИУ РАН
ов
2021 г.

Подпись Тимониной Е.Е. заверяю.

«___» ноября 2021 г.