ОТЗЫВ

официального оппонента доктора технических наук
Воловача Владимира Ивановича - доктора технических наук, доцента,
ФГБОУ ВО «Поволжский государственный университет сервиса»,
заведующего кафедрой информационного и электронного сервиса,
на диссертацию
Кузнецова Николая Алексеевича «Разработка алгоритмов, и моделирование обеспечения целостности данных в информационных системах обмена дискретной информацией», представленную на соискание ученой степени кандидата технических наук по специальности 05.13.18 - «Математическое моделирование, численные методы и комплексы программ»

Структура и краткое содержание диссертации

Диссертационная работа подготовлена в ФГБОУ «Ульяновский государственный университет» на кафедре телекоммуникационных технологий и сетей. Диссертация состоит из введения, 4 глав, заключения, списка используемых источников. Содержит 131 стр. машинописного текста, библиография включает 92 наименования.

Во введении соискателем сформулированы положения, выносимые на защиту, представлена практическая ценность работы, ее апробация и научная новизна.

В первой главе диссертации выполнен анализ состояния проблемы целостности данных, выявлены причины их нарушения, составлена классификация угроз, без знания особенностей которых трудно оценить возможные потери и разрабатывать способы их обнаружения и восстановления искаженных данных. Предложена концептуальная модель системы передачи-приема данных (СППД) с нарушением целостности, которая служит информационно-понятийной базой и основой для проведения моделирования. Оценены возможности известных моделей обеспечения целостности данных.

Во второй главе предложен подход к моделированию СППД с использованием теории массового обслуживания, в которой пакеты передаваемых данных интерпретируются заявками, очереди заявок - с потоком пакетов. Исследования предложено проводить в варианте одноканальной системы массового обслуживания и простейшим потоком заявок и диагностировать признак несанкционированного доступа к СППД, как отклонения временных параметров доставки пакетов.

Обнаружение несанкционированного доступа производилось путем вычисления значений интенсивностей поступивших пакетов данных, интенсивностей принятых к обработке пакетов данных и интенсивностей, находящихся в очереди и ожидающих обработки пакетов данных, величины которых устанавливаются протоколами передачи телеметрии, согласно разработанному автором алгоритму.

Разработана математическая модель подсистемы обнаружения признаков несанкционированного доступа к СППД на основе предложенного подхода с применением эффективных методов аппроксимации, точечных процессов, индикаторных функций и их компенсаторов в семимартингальном описании.

В третьей главе работы произведен сравнительный анализ наиболее часто используемых на практике приемов и средств обнаружения и исправления ошибок в пакетах данных при передаче по СППД, возникающих при воздействии случайных факторов в передающей среде. Подробно рассмотрен подход к обнаружению и исправлению ошибок на основе применения кодов с переменными весами. Обоснована эффективность их применения в СППД. Предложены структурные решения применения их в реальных условиях.

Четвертая глава посвящена разработке математической модели подсистемы оценки риска повторных ошибок, вызванных сбоями приемной аппаратуры и программных средств СППД. Для повышения эффективности предложено использовать сигмовидную функцию Гомперца, применение которой позволяет обнаруживать местоположения пачек ошибок, вычислять наибольшую вероятность присутствия этих ошибок. Разработана программа для проведения имитационного моделирования, приведены основные результаты экспериментальных исследований.

В заключении сформулированы основные результаты и выводы по выполненной научно-квалификационной работе.

Актуальность темы диссертации

Актуальность состоит в необходимости повышать эффективности сохранения целостности передаваемой информации из-за возрастания атак и несанкционированного доступа нарушителей, взломщиков, а также других негативных событий, вызванных ростом числа подключений пользователей к сети Интернет, ее разрастанием и, как следствие, усложнением.

Немаловажную роль играет появление новых услуг, таких как Интернет вещей, которые активно развиваются и охватывают все больше и большее население стран мира. Уже сейчас имеется немало примеров атак на Интернет вещей, круг которых постоянно расширяется. Интеллектуальные

технологии все чаще внедряются в производство, науку, банковскую и социальную среду и становятся объектами для исполнения преступных целей.

Основой предоставления различных Интернет-услуг являются сети передачи данных, которые могут осуществлять обмен информации на большом расстоянии. Примером являются сети связи между удаленными местами добычи полезных ископаемых в районах Сибири и центрами их управления. Здесь передаваемая информация может носить закрытый производственный и экономический характер, который может представлять интерес для конкурентов и может затрагивать государственные экономические интересы.

Расположенность сетей на большой территории часто вызывает необходимость использования различных сред передачи данных, что ведет к неоднородности и необходимости их точной стыковки, переформатированию сигнальной информации, удовлетворению требованиям различных сетевых протоколов.

Эти факторы также могут вызвать нарушения целостности передаваемых данных. Например, обеспечивающие с той или иной степенью эффективности задачи целостности данных решаются по отдельности, однако отсутствуют подходы к построению интегрированных систем, предназначенных для защиты от всей совокупности неблагоприятных воздействий. В связи с этим диссертационная работа, направленная на комплексное решение проблемы защиты информации, может считаться актуальной.

Научная новизна

Научная новизна диссертации заключается в следующем:

- разработан комплексный подход для построения средств выявления признаков нарушения целостности телеметрических данных, передаваемых по дискретным каналам связи, и обеспечивающий контроль их искажения от постороннего доступа и влияния случайных факторов со стороны среды передачи и приемной аппаратуры. Комплексность приводит к интеграции аппаратных средств и позволяет улучшить распознавание причин возникающих угроз и принятия решений по ликвидации последствий.

Отсюда выделяются три задачи: это задача обнаружения признаков несанкционированного вмешательства в процесс передачи данных по каналу связи, задача обнаружения искажения данных, вызванных средой передачи, и задача обнаружения повторных искажений за счет ошибок, возникающих в аппаратуре приема и обработки поступивших данных.

С этой целью автор построил математические модели средств обеспечения целостности данных, включающие способы обнаружения признаков несанкционированного доступа, выявления и исправления ошибок, вычисления риска возникновения повторных ошибок, вызванных средой передачи данных и сбоев приемной аппаратуры:

- для решения первой задачи разработана математическая модель процесса приема и обработки информации на основе аппарата теории массового обслуживания;
- для решения второй задачи предложено использовать матрично-алгоритмическую организацию построения кодов с переменным весом, обнаруживающих ошибки, вызванные шумами среды передачи данных, и позволяющих их исправлять, а также алгоритмическую модель генератора кодов переменного веса и численного метода быстрого вычисления веса двоичных последовательностей телеметрических данных для проведения их структурного анализа;
- для решения третьей задачи разработана математическая модель оценки риска возникновения повторных ошибок, вызванных сбоями приемной аппаратуры и программных средств;
- для проведения экспериментальных исследований разработан комплекс программных средств имитационного моделирования обнаружения признаков несанкционированного доступа, выявления и исправления ошибок в передаваемых пакетах данных в условиях отрицательно действующих факторов и риска возникновения повторных ошибок.

Следует отметить, что при решении поставленных задач получен ряд новых научных результатов:

- применен комплексный подход к решению основной задачи работы путем декомпозиции ее на составные части: обнаружение фактов несанкционированного доступа; эффективное применение кодов с переменным весом; оценка риска возникновения повторных ошибок, позволяющий при решении указанных задач дифференцировать виды и угрозы нарушения целостности и, тем самым, производить оценки угроз, возможных последствий, применять корректно способы и средства их устранения;
- обнаружение фактов несанкционированного доступа на основе построения модели системы передачи-приема данных в виде системы массового обслуживания путем введения семимартингального описания точечных процессов, индикаторных функций и их компенсаторов, что позволяет повысить точность обнаружения признаков несанкционированного

доступа и расширить область эффективного применения предложенной модели;

- эффективное применение кодов с переменным весом, позволяющих обнаруживать ошибки, вызванные шумами среды передачи данных, и с помощью разработанного численного метода быстро вычислять веса двоичных последовательностей для проведения их структурного анализа и восстановления;

- оценки риска возникновения повторных ошибок, вызванных средой передачи данных и сбоями приемной аппаратуры, систем передачи-приема данных с использованием сигмовидной функции Гомперца, позволяющей описывать с более высокой точностью угрозы нарушения целостности данных на начальной и завершающей стадиях функционирования СППД.

Методика исследования

В работе использовались методы математического моделирования. численные методы, теория вероятностей, теория алгоритмов, системный подход к проектированию вычислительных систем.

В работе предлагается подход к созданию средств, включающих в свой состав модели проведения анализа нештатных ситуаций, в которых возникает необходимость защиты целостности передаваемых по каналам потоков данных, в виде трех взаимодействующих подсистем.

Первая подсистема позволяет обнаруживать признаки несанкционированного доступа в СППД. В ее основу заложен аппарат теории массового обслуживания, позволяющий выявлять задержки, возникающие при передаче пакетов данных, которые можно интерпретировать как вмешательство в порядок очереди и в сами пакеты данных. Таким образом, можно регистрировать сам факт нарушения целостности.

Вторая подсистема позволяет обеспечивать целостность телеметрических данных на основе кодов переменного веса. В ее основу заложено применение трех методов: метода обнаружения ошибок на основе контроля веса двоичного кода, метода генерации кодов переменного веса и метода подсчета веса двоичного кода. Эта подсистема позволяет идентифицировать места локализации как пачек ошибок, так и единичных аддитивных ошибок различной кратности.

Третья подсистема служит для оценки риска повторных ошибок, вызванных сбоями приемной аппаратуры и программных средств СППД, и выполняет вычисление значений показателя этого риска, тем самым, позволяя определять приемлемый уровень достоверности принимаемых данных.

Практическая значимость

Полученные результаты, такие как модели процессов обнаружения целостности передаваемых данных, средства имитационного моделирования и полученные результаты моделирования могут найти применение для проектирования защищенных систем передачи и приема данных по дискретным каналам передачи информации, а также реализованы как отдельные экспериментальные подсистемы с соответствующим согласованием в реальных приемо-передающих комплексах.

Достоверность результатов и выводов диссертационной работы обеспечивается корректностью применения аппарата теории вероятностей, полным обоснованием всех разработанных алгоритмов с использованием численных методов, совпадением результатов численного эксперимента на разработанном программном комплексе с имеющимися аналитическими результатами.

Публикации и апробация работы

По результатам диссертационного исследования опубликовано 7 печатных работ. Среди них 4 работы опубликованы в изданиях, включенных в перечень ВАК, 3 работы опубликованы в иных печатных изданиях.

Основные результаты диссертации докладывались и обсуждались на следующих конференциях и семинарах: XXIII Всероссийская межведомственная научно-техническая конференция школы-семинара «Информационная безопасность - актуальная проблема современности», Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С.М. Штеменко Министерства обороны Российской Федерации, г. Краснодар, 22.09.2021-03.10.2021 (открытая секция); Всероссийская научно-практическая конференция «Траектории взаимодействия в развитии цифровых навыков», УлГПУ им. Н.И. Ульянова, г. Ульяновск, 25.12.2021; Международная научно-техническая конференция «Перспективные информационные технологии», г. Самара, 18.04.2022; совместные научные семинары кафедры телекоммуникационных технологий и сетей УлГУ и НИТИ им. С.П. Капицы (2021 - 2022 гг.); научном семинаре 23 кафедры 2 факультета Краснодарского высшего военного орденов Жукова и Октябрьской Революции Краснознаменного училища имени генерала армии С.М. Штеменко Министерства обороны Российской Федерации, г. Краснодар, 22.02.2022.

Оформление материалов диссертации и личный вклад соискателя

Диссертация написана понятным для специалиста языком, иллюстративный материал корректно отображает содержание работы,

которая носит связный логический характер со всеми необходимыми ссылками на приведенные в конце диссертации источники.

Автореферат правильно и полно отражает основные идеи, содержание и выводы диссертации. Все результаты и положения, выносимые на защиту, получены автором самостоятельно.

Замечания по диссертации

В целом диссертационная работа оставляет хорошее впечатление. Вместе с тем, по представленной работе возникли следующие замечания:

1. При получении оценок риска повторных ошибок не приведена информация об их частоте появления в подсистемах приема-передачи, об их происхождении и искажениях данных, не указан тип аппаратуры, в которых риск наиболее вероятен;
2. Не показано, как в случае встраивания программных средств обнаружения вмешательства в процесс передачи данных по каналам будет происходить согласование с принятыми и используемыми на практике телекоммуникационными протоколами;
3. Недостаточно информации, по каким критериям оценивается эффективность применения кодов с переменным весом по сравнению с используемыми на практике;
4. Не показано, какова необходимость разделения потока пакетов на находящихся в очереди и ожидающих обслуживания и как это будет осуществляться на практике;
5. Нет подробной информации о формировании потока заявок-пакетов, которые будут обслуживаться, как в структуру пакета будут записываться необходимые данные, на основании значений которых на приемной стороне будут рассчитываться интенсивности и определяться признаки несанкционированного доступа.

Следует отметить, что указанные замечания не являются принципиальными и не подвергают сомнению достоверность результатов и обоснованность полученных выводов.

Заключение

Диссертация Кузнецова Н.А. является научно-квалификационной работой, в которой изложены научно обоснованные технические решения, направленные на обеспечение целостности данных в информационных системах обмена дискретной информацией и имеющие существенное значение для развития соответствующей области знаний. По научному содержанию и полноте выполненных исследований диссертационная работа соответствует требованиям п. 9 «Положения о присуждении ученых степеней» ВАК РФ, предъявляемым к

кандидатским диссертациям, а ее автор – Кузнецов Николай Алексеевич заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.18 – «Математическое моделирование, численные методы и комплексы программ».

Официальный оппонент
доктор технических наук, доцент,
ФГБОУ ВО «Поволжский государственный
университет сервиса»,
заведующий кафедрой информационного
и электронного сервиса

Владимир Иванович Воловач

Подпись Воловача Владимира Ивановича
подтверждаю:

Официальный оппонент Воловач Владимир Иванович, доктор технических наук по специальности 05.12.04 «Радиотехника, в том числе системы и устройства телевидения», доцент, заведующий кафедрой информационного и электронного сервиса ФГБОУ ВО «Поволжский государственный университет сервиса», Российская Федерация, 445017, Самарская область, г. Тольятти, ул. Гагарина, д. 4 , тел. +7 (8482) 26-35-38, e-mail: office@tolgas.ru