Отзыв официального оппонента

на диссертационную работу Корнева Дмитрия Александровича «Разработка и исследование средств взаимодействия приложений и методов защиты вычислительного комплекса транспортной системы», представленную на соискание ученой степени кандидата технических наук по специальности 05.13.15 – «Вычислительные машины, комплексы и компьютерные сети»

Высокоскоростной железнодорожный транспорт - одна из наиболее значимых технологических инноваций последнего времени. Востребованность современных, надежных и безопасных транспортных систем в мире настолько высока, что, как показывает опыт европейских стран, строительство скоростных магистралей окупается уже через пять лет после ввода их в эксплуатацию.

Однако эффективность использования высокоскоростного транспорта во многом определяется возможностью моделирования транспортных потоков, что реализуемо только при создании информационной транспортной системы.

В представленной работе решена задача создания вычислительной части информационной транспортной системы на базе индустрии цифровых технологий, обеспечивающей высокий уровень взаимодействия участников движения при эффективной информационной защите. С учетом значимости проблемы эффективного использования железнодорожного транспорта актуальность разработки вычислительного комплекса его информационной системы не вызывает сомнений.

Во введении к диссертации автором сформулирована задача исследования и обоснована ее актуальность. Важно отметить, что транспортную систему предложено создать на базе уже эксплуатирующихся и хорошо зарекомендовавших себя систем диспетчерской централизации и автоведении поездов; это позволит снизить проектные и эксплуатационные

расходы, а также гарантирует надежность функционирования системы поскольку использует технические решения, проверенные эксплуатацией.

Реализация вычислительной части транспортной системы предложена с использованием технологии виртуализации, что имеет преимущества для систем повышенной категории ответственности, поскольку за счет разграничения решаемых задач отказ одного из приложений не приведет к полной потере контроля движения, а резервируемые мощности позволят быстро восстановить режим ее штатного функционирования. При этом нужно отметить, что автором справедливо отмечены основные недостатки систем виртуализации, главным из которых является требование дополнительных вычислительных ресурсов. Однако большие мощности современных серверов в сочетании с возможностью создать вычислительный комплекс единую физическую архитектуру с разграничением приложений обосновывают выбор для него принципа виртуализации.

В соответствии с требованиями к структуре диссертации во введении указаны цель работы и ее практическая значимость, научная новизна результатов, выносимых на защиту.

Первая глава диссертации посвящена разработке структуры вычислительного комплекса во взаимодействии с системами диспетчерской централизации, автоведения поезда и комплексного локомотивного устройства безопасности. Автором определены функции вычислительного комплекса, каналы связи с локальной сетью диспетчерской централизации и мобильной сетью локомотива, а также объем и вид информации, которая должна передаваться по этим каналам связи. В работе приведена необходимая информация об алгоритме программы системы автоведения: периодах исполнения, сигналах управления, запросах данных от линейных пунктов диспетчерской централизации. Важно отметить, что для расчета нагрузки на ресурс вычислительного комплекса по заявке локомотива использовалась действующая техническая документация на работу систем

автоведения и диспетчерской централизации, ссылки на которую приведены в списке используемой литературы.

На основании алгоритма взаимодействия участников перевозочного процесса автором разработана архитектура вычислительного комплекса с разделением ресурса под выполнение конкретных приложений, предусматривающая наличие резерва, который можно использовать для расширения алгоритма управления или при внезапных отказах приложений.

Для выбора реализации вычислительного комплекса автором проанализированы существующие технологии виртуализации. На основании сопоставления их характеристик им обосновано применение нативной виртуализация с высокими удельными показателями быстродействия, что особенно важно для управления транспортной системой. Поскольку разрабатываемая система связана с безопасностью движения, анализ характеристик различных типов виртуализации выполнялся в комплексе с их уязвимостями.

В связи с тем, что ОАО «РЖД» предъявляет особые требования к защите информационных систем, в работе выполнен обзор стандартов безопасности, действующих в России, и анализ специфики стандарта ОАО «РЖД» 1.18.002-2009 «Управление информационной безопасностью. Общие положения».

В выводах к первой главе утверждается, что разработанная система управления движением поездов позволит повысить уровень взаимодействия участников перевозочного процесса за счет передачи части полномочий вычислительному комплексу и удовлетворяет требованиям ОСТ 32.146-2000 «Аппаратура железнодорожной автоматики, телемеханики и связи. Общие технические условия».

Вторая глава диссертации посвящена расчету характеристик разрабатываемого вычислительного комплекса транспортной системы.

Автором выполнен подробный анализ работ, в которых рассматриваются методы исследования виртуальных вычислительных

систем, и показано, что с их помощью преимущественно решаются задачи оптимального распределения ресурса по критерию производительности сервера. Задача создания вычислительного комплекса интеллектуальной транспортной системы связана, прежде всего, с обеспечением устойчивого взаимодействия участников перевозочного процесса с учетом асинхронных и параллельных процессов алгоритма взаимодействия, проводимых вычислений и формирования управлений.

В связи с этим автором была разработана оригинальная имитационная модель функционирования виртуального вычислительного комплекса, учитывающая алгоритм взаимодействия его приложений. Для моделирования обосновано выбран математический аппарат сетей Петри, который позволяет создавать имитационные модели работы сложных систем с учетом их взаимодействия с внешними объектами. С помощью разработанной модели возможно рассчитывать нагрузку на ресурс по заявкам систем автоведения локомотивов при любых вероятностных характеристик этого взаимодействия, а также в соответствии с алгоритмом работы самой системы.

Верификация разработанной модели выполнялась при имитации предельных нагрузок на ресурс по заявкам систем автоведения локомотивов для участка ж.д. протяженностью 200 км (минимальная рекомендуемая длина участка обслуживания пунктом диспетчеризации); при этом контролировался алгоритм взаимодействия виртуальных машин и ресурса при поступлении заявки от системы автоведения.

Разработанная модель позволила автору определить требования к ресурсу сервера при разных значениях параметров распределения его нагрузки. В соответствии с полученным значением максимальной нагрузки и требованиями к быстродействию вычислительного комплекса им обосновано предложен сервер типа IBM Flex System x240 со встроенной фабрикой IBM® Virtual Fabric, который обладает большой вычислительной мощностью,

адаптирован к использованию на его базе технологии виртуализации и имеет простое управление при разворачивании резерва.

В этой же главе решена задача определения оптимальной длины участка железной дороги, обслуживаемой вычислительным комплексом на базе сервера IBM Flex System x240. Задача решалась методом векторной оптимизации по двум противоречивым критериями, в качестве которых автор справедливо использовал мощность и цену серверов этого ряда, а в качестве управления принял число поездов, запросы от которых сервер может обслуживать одновременно. Целевая функция определялась минимизацией отклонения функции неулучшаемых решений от утопической точки. Важно отметить, что при определении целевой функции автором предложен метод, позволяющий не учитывать весовые коэффициенты критериев, а использовать их относительные значения.

Полученный результат - 950 км - хорошо коррелируется с допустимой длиной участка дороги, контролируемого диспетчерской централизацией – 1000 км.

Третья глава работы посвящена анализу работоспособности вычислительного комплекса при внезапных отказах и попытках получения несанкционированного доступа к системе.

На первом этапе исследовалась возможность разворачивания резерва комплекса при отказе одной виртуальной машины за время, предусмотренное на обслуживание заявки системы автоведения. Имитация данного процесса выполнялась с использованием разработанной модели вычислительного комплекса, дополненной модулями загрузки резервной виртуальной машины. Расчетные результаты были подтверждены методами экспериментальных исследований, которые также показали, что за заданное время на ресурсе хоста комплекса невозможно развернуть резервную виртуальную машину.

На основании этого автором принято правильное решение о резервировании вычислительного комплекса. Поскольку современные серверы обладают значительным ресурсом безотказной работы, для

вычислительного комплекса предложено мажоритарное резервирование с голосованием, что повысит надежность и точность работы системы автоведения в целом. С учетом заявленного ресурса сервера Flex System x240 принятая система резервирования обеспечит его штатную работу при внезапных отказах виртуальных машин в течение почти девяти лет.

Для анализа устойчивости вычислительного комплекса к действиям нарушителей автор разработал дерево маршрутов атак, исходя из условия, что наиболее вероятно проведение MITM-атаки на систему, вследствие изолированности сети Intranet, используемой информационными системами железнодорожного транспорта. С целью поиска методов противодействия нарушителям создана модель проведения MITM-атаки на вычислительный комплекс на базе математического аппарата сетей Петри.

Несомненное преимущество такого подхода к разработке частных моделей функционирования вычислительного комплекса - это возможность создания общей имитационной модели работы системы, описывающей ее динамические свойства в разных условиях эксплуатации: в штатных условиях, при внезапном отказе одного из элементов и при попытке проведения информационной атаки.

Такая модель была использована автором в четвертой главе при поиске эффективной системы защиты вычислительного комплекса. В работе рассмотрены четыре основных типа защит: защита виртуальной машины; защита "диска" виртуальной машины; защита хостовой системы; использование средств обеспечения безопасности сетевой инфраструктуры.

Поскольку информационная атака проводится в условиях полной неопределенности выбора маршрута атаки и действий нарушителя по преодолению защит, в работе удачно использован метод статистических испытаний Монте-Карло, который позволяет процедурой розыгрыша получить достоверный результат в системах со сложным взаимодействием различных факторов.

Исследования эффективности защит выполнялись с использованием разработанной модели проведения MITM-атаки на вычислительный комплекс с криптографической защитой информации. Разработанная методика определения эффективности применяемой защиты не вызывает сомнений, поскольку предусматривает разыгрывание комбинаций случайных величин, которые полностью определяют вероятность прохождения нарушителя по выбранному маршруту атаки. Данные распределений разыгрываемых величин получены автором из ежегодных отчетов по статистике уязвимостей корпоративных информационных систем, публикуемых компанией Positive Technologies, которая осуществляет контроль и устранение уязвимостей информационных систем.

Считаю, что автором получен достоверный результат по прогнозированию уровня эффективности рассматриваемых защит и принято верное решение о применении комплексной защиты, обеспечивающей снижение вероятности доступа к информации вычислительного комплекса до 35%.

Заключение диссертации соответствует ее основным положениям.

В приложении к работе приведены описание виртуального комплекса задания параметров движения автономного подвижного состава и интерфейса программы расчета эффективности средств обеспечения безопасности виртуального комплекса.

Несмотря на высокий уровень представленного материала, по диссертации имеются следующее замечание:

Разработанная структура вычислительного комплекса предусматривает обслуживание запросов от систем автоведения тепловозов и нигде не указывается, сможет ли тот же самый комплекс обслуживать запросы, поступающие от электровозов и электропоездов, поскольку на большинстве участков железной дороги могут эксплуатироваться и электровозы и тепловозы.

На основании изучения материалов диссертации, автореферата и публикаций, представленных автором работы, можно сделать следующие выводы:

На основании анализа работы систем железнодорожной автоматики и связи аргументировано обоснована структура вычислительного комплекса системы управления движением поездов, использующая технологию виртуализации.

С использованием методов теоретических и экспериментальных исследований высокую степень обоснованности получили следующие результаты работы:

расчетная мощность сервера вычислительного комплекса системы управления движением поездов;

необходимость применения резервирования разработанного вычислительного комплекса для обеспечения надежного функционирования системы управления движением поездов при внезапных отказах его приложений;

целесообразность применения комплексной системы защиты разработанного вычислительного комплекса от проведения информационных атак;

Достоверность научных положений, выводов и рекомендаций, сформулированных в диссертации, подтверждается использованием технической документации на существующие средства автоматики и связи железнодорожного транспорта, на базе которых разработана структура вычислительного комплекса, и применением современных средств теоретических и экспериментальных исследований сложных технических объектов.

Научные положения, выводы и рекомендации, сформулированные в диссертации имеют высокую степень новизны, прошли апробацию при публикации результатов работы в ведущих изданиях, рекомендованных ВАК Минобрнауки России, а также докладах автора на отраслевых и

международных конференциях, посвященных развитию железнодорожного транспорта.

Результаты работы получили внедрение при создании виртуального комплекса задания параметров движения автономного моторвагонного подвижного состава и тепловозов на базе Научно-исследовательского института железнодорожного транспорта, что подтверждено представленным актом о внедрении.

На основании сказанного можно заключить, что диссертационная работа Корнева Д.А. на соискание ученой степени кандидата технических наук является законченной научно-квалификационной работой, в которой решена актуальная задача разработки вычислительного комплекса системы управления движением поездов, имеющая существенное значения для развития транспортной системы страны, что соответствует требованиям п.9 «Положения о порядке присуждения ученых степеней», а ее автор заслуживает присуждения искомой ученой степени по специальности 05.13.15 - «Вычислительные машины, комплексы и компьютерные сети».

Официальный оппонент,
д.т.н., профессор А.И. Дивеев
«7» апреля 2015г.

Подпись руки тов. Дивеева А.И.
ЗАВЕРЯЮ
Секретарь ВЦ РАН
«07» апреля 2015 г.

Сведения об оппоненте:
Дивеев Асхат Ибрагимович,
доктор технических наук, профессор,
заведующий сектором Проблем кибернетики
ФГБУН Вычислительный центр им. А.А. Дородницына
Москва, 119333, ул. Вавилова, 40.
Рабочий телефон: 8-499-135-61-95
Электронная почта: aidiveev@mail.ru