УТВЕРЖДАЮ

Проректор по научной работе

ФГБОУ ВПО

Московский энергетический институт

(Национальный исследовательский университет)

НИУ "МЭИ"

д.т.н., профессор Драгунов Виктор Карпович

111250, Москва, ул. Красноказарменная,

д. 14, каб. И-312

телефон: +7 495 362-77-22

e-mail: DragunovVK@mpei.ru

24 марта 2015 г.

Отзыв

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

Значимость диссертационной работы обусловлена необходимостью повышения безопасности движения поездов и пропускной способности железных дорог. Направление выполненных исследований соответствует актуальной стратегии развития железнодорожного транспорта до 2030 года, где предусмотрено создание технологической платформы «Высокоскоростной интеллектуальный железнодорожный транспорт» как единой системы управления движением и обеспечения безопасности за счет создания интеллектуальной среды эксплуатации железнодорожного транспорта. В диссертации решена задача определения параметров вычислительного комплекса с высоким уровнем информационной

защиты единой системы управления движением на полигоне железных дорог, обеспечивающего высокий уровень взаимодействия между системами автоведения поездов и службами диспетчерской централизации для эффективного управления движением в соответствии с текущей поездной ситуацией.

Диссертационная работа состоит из введения, четырех глав, заключения и двух приложений. Список источников литературы насчитывает 196 наименований.

Во введении автором рассмотрены основные функции, которые определяются Технологической платформой интеллектуального железнодорожного транспорта в управлении перевозочным процессом, и существующие средства автоматизации, которые могут быть использованы для ее создания, а также обосновывается использование средств виртуализации для создания вычислительного комплекса Технологической платформы.

В соответствии с требованиями к диссертациям во введении сформулированы цель и задачи проведенных исследований, научная новизна и практическая значимость работы; обоснована достоверность выполненных исследований.

Первая глава посвящена разработке архитектуры вычислительного комплекса системы управления движением. Для этого автором определена нагрузка на его ресурс от участников перевозочного процесса с учетом характеристик передаваемой и обрабатываемой информации и алгоритма их взаимодействия. Нагрузка рассчитывалась на основании ТУ функционирования существующих средств автоматизации диспетчерской централизации и систем управления локомотивами с учетом требований к выполнению графика движения поездов.

Для выбора принципа реализации вычислительного комплекса, ресурс которого наилучшим образом обеспечивает разделение решаемых задач и взаимодействие приложений с учетом требований к быстродействию, рассмотрены характеристики систем виртуализации, их уязвимости и возможные средства защиты. На основании проведенного анализа автором обосновано применение технологии нативной виртуализации платформы, как наиболее полно удовлетворяющей условиям по эффективному использованию ресурса и высокому быстродействию.

Поскольку функционирование разрабатываемого вычислительного комплекса определяет работу полигона железной дороги, в последнем параграфе первой главы выполнен обзор нормативной и законодательной базы в области информационной безопасности, в том числе, особенностей требований к информационным и вычислительным системам, используемым в структуре «РЖД».

Результаты исследований, изложенные в первой главе, обстоятельно обосновывают научную новизну предложенной автором архитектуры комплексной системы управления движением поездов как единого информационно-коммуникационного пространства на основе средств цифровой связи со стандартизованными технологиями идентификации, навигации и позиционирования.

Вторая глава диссертации посвящена разработке математической модели

вычислительного комплекса с целью исследования процессов взаимодействия приложений при решении задачи управления движением.

С целью выбора математического аппарата для решения задачи управления движением автором выполнен обзор существующих моделей исследования виртуальных вычислительных систем и показано, что их основным недостатком является абстрагирование расчетов распределения ресурса от алгоритма решаемой задачи, что снижает точность расчета нагрузки на ресурс и прогнозирование эффективности его использования.

Применительно к решаемой задаче автором выбран метод имитационного моделирования функционирования вычислительного комплекса на базе математического аппарата сетей Петри, который позволяет не только учесть характер взаимодействия приложений, но и использовать методы теории вероятностей для получения количественных показателей работы системы.

Для подтверждения адекватности разработанной модели физической реализации вычислительного комплекса была выполнена ее верификация при моделировании алгоритма взаимодействия приложений по заявке на обслуживание одного локомотива и расчете минимальной и максимальной нагрузки на ресурс при взаимодействии участников перевозочного процесса.

С использованием разработанной модели рассчитана нагрузка на ресурс вычислительного комплекса от участников перевозочного процесса при различных вероятностных характеристиках времени поступления и времени обслуживания заявок систем автоведения локомотивов. Результаты расчетов показали неэффективное использование вычислительных ресурсов разрабатываемого комплекса в общем расходе ресурсов на поддержание системы виртуализации и мониторинга для минимальной протяженности участка железной дороги, обслуживаемой диспетчерской централизацией (200 км), даже при допустимом интервале следования поездов.

В связи с этим в работе решена задача определения протяженности полигона железной дороги, для которого вычислительные ресурсы разрабатываемого комплекса использовались бы наиболее эффективно.

Практическую реализацию вычислительного комплекса автор предложил выполнить на базе сервера IBM Flex System x240 с встроенной фабрикой IBM® Virtual Fabric, поскольку он оптимизирован для реализации технологий виртуализации, обладает высокой производительностью для поддержания широкого спектра рабочих нагрузок. С учетом характеристик и стоимости серверов этой серии была решена оптимизационная задача по определению числа поездов, обслуживаемых вычислительным комплексом при эффективном использовании его ресурса. Задача решалась методом векторной оптимизации по противоречивым критериям.

Результаты исследований, изложенные во второй главе, обстоятельно обосновывают научную новизну предложенной автором математическая модель вычислительного комплекса на базе математического аппарата сетей Петри.

В третьей главе рассмотрены внештатные режимы функционирования вычислительного комплекса и методы повышения безотказности его работы. С использованием разработанной модели были выполнены расчеты времени разворачивания внезапно отказавших виртуальных машин на базе его резерва. Результаты моделирования сопоставлялись с результатами экспериментального исследования аналогичных процессов. Было получено, что время, необходимое для разворачивания на резерве комплекса виртуальной машины, не соответствует требованиям алгоритма взаимодействия его приложений при организации управления движением поездов. В связи с эти автором предложен способ мажоритарного резервирования вычислительного комплекса с голосованием «2 из 3» и выполнен расчет его ресурса по среднему времени безотказной работы сервера и IBM Flex System x240, гарантируемого производителем. Получено, что данный метод резервирования обеспечивает надежную работу вычислительного комплекса при внезапных отказах в течении 8,9 лет.

При анализе уязвимостей вычислительного комплекса в случае проведения на него информационной атаки показано, что вследствие закрытой структуры комплексной системы управления движением поездов наиболее вероятным методом воздействия на систему является MITM-атака.

С целью анализа влияния нарушителя на маршрут передачи информации и создания общей имитационной модели взаимодействия ресурса и приложений при попытках получения несанкционированного доступа к информации разработана математическая модель MITM-атаки на вычислительный комплекс с использованием математического аппарата сетей Петри. Разработанная модель может быть использована для любого маршрута проводимой атаки и отражает реальный процесс пакетной передачи данных по лигитимным или модифицированным каналам связи. Также она может быть расширена, детализована или модифицирована под другие условия передачи данных, что позволяет адаптировать ее для вычислительной сети другой структуры.

Иерархическое дерево маршрутов атак на вычислительный комплекс разрабатывалось с использованием методики формализованных моделей информационных атак. Возможные маршруты атак были использованы автором при расчете уровня защищенности вычислительного комплекса системы управления движением поездов.

Результаты исследований, изложенные в третьей главе, обстоятельно обосновывают научную новизну предложенной автором математической модели MITM-атаки на вычислительный комплекс на базе математического аппарата расширенных сетей Петри.

Четвертая глава работы посвящена выбору типа защиты вычислительного комплекса.

Для определения количественных показателей эффективности применяемой системы защиты автором разработана методика, в основу которой положен алгоритм MITM-атаки на вычислительный комплекс с криптографической защитой

информации в интегральной модели маршрутов атак. Особенностью данной методики является использование метода Монте- Карло в имитационной модели функционирования вычислительного комплекса в условиях проведения атаки. При этом в алгоритме моделирования действий нарушителя учитывались разветвленные конфигурации системы защиты и маршрутов атак, а также случайный характер параметров атаки и системы защиты.

С использованием разработанной модели были определены расчетные значения вероятностей защищенности вычислительного комплекса при основных типах защиты: стандартных мерах на основе мониторинга сетевых процессов и разграничения прав доступа к ресурсам; защите виртуальной машины; защите "диска" виртуальной защиты; защите хостовой системы; использовании средств обеспечения безопасности сетевой инфраструктуры, а также комплексной системы защиты, объединяющей все типы защит.

Получено, что применение комплексной системы защиты вычислительного комплекса более чем в три раза снижает вероятность доступа к информации по сравнению с самой эффективной системой защиты - защиты хостовой системы. Поскольку работа вычислительного комплекса связана с безопасностью движения поездов и эффективностью перевозочного процесс для него автор рекомендует использовать комплексную систему защиты.

Результаты исследований, изложенные в четвертой главе, обстоятельно обосновывают научную новизну предложенной автором вероятностный метод расчета эффективности защиты вычислительного комплекса.

По диссертационной работе имеются следующие замечания:

1) Представленная работа в большей степени соответствует названию «Разработка метода проектирования защищенного вычислительного комплекса системы управления движением поездов с использованием средств виртуализации»
2) В качестве исследуемого ресурса, влияющего на оценку качества функционирования виртуального вычислительного комплекса автор рассматривает только емкость памяти. Однако не менее важным параметром в условиях управления в реальном времени является время доставки и обработки данных, которое следует учитывать при построении модели.
3) В диссертации отсутствует сравнительный анализ методов моделирования, который должен обосновать использование при моделировании аппарата сетей Петри.
4) Для повышения надежности функционирования вычислительной системы автором применена система мажоритарного резервирования, при построении модели которой учитываются вероятности отказов вычислительных комплексов (ВК), но не учитывается вероятность отказа мажоритарного элемента системы резервирования (МЭВК), что приводит к завышенной оценки надежности вычислительной системы.
5) В диссертации отсутствует отдельный раздел, посвященный доказательству

адекватности предложенных автором моделей.

Заключение о соответствии диссертационной работы, предъявляемым требованиям.

Диссертационная работа Корнева Дмитрия Александровича является законченным исследованием на актуальную тему и выполнена автором самостоятельно, на высоком научном уровне.

Работа написана технически квалифицированно и аккуратно оформлена, по каждой главе в работе имеются выводы.

Основное содержание работы, выводы и результаты достаточно полно представлены в автореферате. Приведенные замечания не снижают общего высокого научного уровня и практического значения проведенного исследования.

Рассмотренная диссертационная работа отвечает требованиям пункта 9 «Положения о порядке присуждения ученых степеней ВАК, предъявляемым к кандидатским диссертациям по специальности 05.13.15 «Вычислительные машины, комплексы и компьютерные сети», а ее автор Корнев Д.А. заслуживает присуждения ученой степени кандидата технических наук

Отзыв рассмотрен на заседании кафедры вычислительных машин, систем и сетей НИУ «МЭИ» 26 » февраля 2015 г.

Зав. кафедрой "Вычислительные машины, системы и сети"
ФГБОУ ВПО Московский энергетический институт
(Национальный исследовательский университет)

д.т.н., профессор _____ Крюков Александр Федорович
адрес: 111250, Москва, ул. Красноказарменная, д. 17, ауд. Б-209
телефон: +7 495 362-77-77
e-mail: PK@mpei.ru

Профессор кафедры "Вычислительные машины, системы и сети"
ФГБОУ ВПО Московский энергетический институт
(Национальный исследовательский университет)

д.т.н., профессор _____ Абросимов Леонид Иванович
адрес: 111250, Москва, ул. Красноказарменная д.14
телефон: +7 495 362-70-72
e-mail: AbrosimovLI@mpei.ru