На правах рукописи

Корнев
Дмитрий Александрович

РАЗРАБОТКА И ИССЛЕДОВАНИЕ СРЕДСТВ ВЗАИМОДЕЙСТВИЯ ПРИЛОЖЕНИЙ И МЕТОДОВ ЗАЩИТЫ ВЫЧИСЛИТЕЛЬНОГО КОМПЛЕКСА ТРАНСПОРТНОЙ СИСТЕМЫ

Специальность 05.13.15 – Вычислительные машины, комплексы и компьютерные сети

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Москва - 2015 г.

Работа выполнена в Федеральном государственном бюджетном образовательном учреждении высшего профессионального образования "Московский государственный университет путей сообщения" на кафедре “Информационные технологии”

Научный руководитель: Соловьев Владимир Павлович, кандидат технических наук, доцент
Заведующий кафедрой "Информационные технологии" ФГБОУ ВПО "Московский государственный университет путей сообщения", ученый секретарь Ученого совета университета

Официальные оппоненты: Дивеев Асхат Ибрагимович, доктор технических наук, профессор
Заведующий сектором Проблем кибернетики ФГБУН Вычислительного центра имени А.А. Дородницына РАН.

Пруцков Александр Викторович, кандидат технических наук, доцент
Доцент кафедры "Вычислительная и прикладная математика" ФГБОУ ВПО "Рязанский государственный радиотехнический университет"

Ведущая организация: ФГБОУ ВПО "Московский энергетический институт" (национальный исследовательский университет)

Защита диссертации состоится «28» апреля 2015 г. в 14^{00} часов на заседании диссертационного совета Д 212.125.01 на базе Московского авиационного института (национального исследовательского университета) по адресу: Волоколамское шоссе, д. 4, г. Москва, А-80, ГСП-3, 125993
С диссертацией можно ознакомиться в библиотеке университета

Автореферат разослан «___» _____ 2015 г.

Ученый секретарь диссертационного совета
Корнеенкова Анна Викторовна _____

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность работы. Стратегией развития железнодорожного транспорта России до 2030 года предусмотрено создание технологической платформы «Высокоскоростной интеллектуальный железнодорожный транспорт» - единой системы управления движением, многоуровневой безопасности и интеллектуальной среды эксплуатации железнодорожного транспорта. Это обосновано необходимостью повышения пропускной способности ж.д. с учетом специфики их эксплуатации - организация движения высокоскоростного подвижного состава в графике движения поездов со средними эксплуатационными характеристиками. Реализация технологической платформы требует, в том числе, создание единого информационно-коммуникационного пространства с высоким уровнем информационной защиты.

Для организации и обеспечения безопасности движения поездов на ж.д. России используется цифровая система диспетчерской централизации (ДЦ) «Сетунь», которая включает в себя современную систему телемеханики с высокоскоростным обменом информацией между центральным распорядительным постом и линейными пунктами по сети рабочей связи. С другой стороны, развитие цифровых технологий позволило внедрить на локомотивах систему автоведения, которая осуществляет управление движением поездов по критерию минимизации энергозатрат в зависимости от характеристик участка пути. Однако на настоящий момент отсутствует комплексное взаимодействие между участниками перевозочного процесса, что делает невозможным определение оптимального закона управления локомотивом с учетом текущих характеристик его энергетического оборудования и меняющейся поездной ситуации. Мощности современных вычислительных систем позволяют успешно решить эту задачу, а технологии виртуализации – обеспечить распределение вычислительных ресурсов для решения частных задач организации движения поездов.

Большие вычислительные мощности современных серверов делают экономически целесообразным их использование для решения комплексных задач, требующих значительных ресурсов для взаимодействия сетей и приложений, в частности решения задачи управления движением на участке ж.д. большой протяженности.

Диссертация посвящена актуальной теме разработки защищенного вычислительного комплекса системы управления движением поездов как составляющей единого информационно-коммуникационного пространства, значимость которой для науки и практики заключается в развитии методов создания и защиты интеллектуальных логистических систем управления перевозочным процессом.

Научно-технической задачей диссертации является создание метода разработки защищенного вычислительного комплекса системы управления движением поездов с использованием средств виртуализации.

Объект исследования: вычислительный комплекс для решения задачи повышения эффективности и безопасности перевозочного процесса по сети ж.д.

Предмет исследования: методы взаимодействия компьютерных сетей и приложений.

Целью диссертационной работы является разработка и исследование функционирования вычислительного комплекса с эффективной системой защиты для решения задачи управления движением поездов на участке железной дороги, контролируемом диспетчерской централизацией.

Поставленная цель определяет основные задачи диссертационной работы:

1. Определение объемов и характеристик информации, обеспечивающей выполнение алгоритма взаимодействия участников перевозочного процесса (систем диспетчерской централизации, автоведения и комплексного устройства безопасности локомотива).
2. Разработка структуры и алгоритма функционирования вычислительного комплекса для логистического управления перевозочным процессом.
3. Разработка программно - ориентированного метода взаимодействия элементов вычислительного комплекса с возможностью расчета нагрузки на его ресурс от участников перевозочного процесса.
4. Обеспечение надежности функционирования вычислительного комплекса при внезапном отказе его элемента.
5. Определение уязвимостей вычислительного комплекса при информационной атаке на него.
6. Разработка метода определения средств эффективной защиты вычислительного комплекса с учетом его структуры и возможных маршрутов проведения атак.

Результаты, выносимые на защиту и их научная новизна:

1. Структура комплексной системы управления движением поездов как единого информационно-коммуникационного пространства на основе средств цифровой связи со стандартизованными технологиями идентификации, навигации и позиционирования, отличающаяся от существующих тем, что она позволяет повысить уровень взаимодействия участников перевозочного процесса за счет интеграции их полномочий на базе вычислительного комплекса.
2. Разработана математическая модель вычислительного комплекса на базе математического аппарата сетей Петри, отличающаяся от известных тем, что объединяя преимущества графового представления состояний и дискретной модели системы позволяет имитировать динамический процесс распределения ресурса между приложениями в виртуальной инфраструктуре с учетом парал-

лельных и асинхронных процессов их взаимодействия и рассчитывать количественные показатели работы системы, в том числе, при моделировании сценариев использования резервных элементов комплекса.

3. Разработана математическая модель MITM-атаки на вычислительный комплекс на базе математического аппарата расширенных сетей Петри, которая в отличие от известных моделей позволяет имитировать динамический процесс изменения маршрутизации трафика нарушителем при любом возможном алгоритме проведения атаки.

4. Разработан вероятностный метод расчета эффективности защиты вычислительного комплекса, отличающийся от известных тем, что позволяет имитировать динамический процесс проведения MITM-атаки в интегральной модели маршрутов несанкционированного доступа с учетом характеристик защит элементов комплекса; основу метода составляют модель MITM-атаки на вычислительный комплекс с криптографической защитой информации и метод Монте-Карло с разыгрыванием случайных параметров атак и уровней защиты его элементов.

Достоверность результатов диссертации обеспечивается корректным применением методов математического моделирования процессов взаимодействия вычислительного ресурса и его приложений на базе математического аппарата сетей Петри, методов математической статистики и векторной оптимизации, а также подтверждается совпадением результатов имитационного моделирования и экспериментального исследования вычислительных процессов.

Соответствие паспорту специальности. Содержание диссертации соответствует п. 5 паспорта специальности 05.13.15 «Вычислительные машины, комплексы и компьютерные сети», поскольку в ней разработан алгоритм создания структуры вычислительного комплекса с эффективной системой защиты для сети управления движением поездов.

Практическая значимость работы:

Разработан инженерный метод создания защищенного вычислительного комплекса логистической системы управления движением поездов, обеспечивающей эффективность и безопасность перевозочного процесса.

Практическое использование результатов работы. Полученные результаты были использованы при создании виртуального комплекса задания параметров движения автономного моторвагонного подвижного состава и тепловозов с гидравлической тяговой передачей с использованием сигналов GPS-навигатора, а также для организации каналов взаимодействия этих приложений.

Апробация работы. Основные положения диссертационной работы докладывались и обсуждались на заседаниях кафедры «Информационные технологии» МИИТа в 2012-2014 гг. а также на следующих конференциях:

Двенадцатая научно-практическая конференция «Безопасность движения поездов». Московский государственный университет путей сообщения (МИИТ), 2011г.

Научно-практическая конференция «Неделя науки – 2012. НАУКА МИИТа - ТРАНСПОРТУ». Московский государственный университет путей сообщения (МИИТ), 2012г.

Тринадцатая научно-практическая конференция «Безопасность движения поездов». Московский государственный университет путей сообщения (МИИТ), 2012г.

Научно-практическая конференция «Неделя науки – 2013. НАУКА МИИТа - ТРАНСПОРТУ». Московский государственный университет путей сообщения (МИИТ), 2013г.

VII Международный транспортный форум, I Форум транспортного образования «Молодые ученые транспортной отрасли»; Московский государственный университет путей сообщения, 2013г.

Международная научно-практическая конференция «Современные проблемы развития интеллектуальных транспортных систем»; Днепропетровский Национальный Университет Железнодорожного Транспорта, 2014г.

IV международная научно-практическая конференция «ИнтеллектТранс-2014»; Санкт-Петербургский государственный университет путей сообщения, 2014г.

Публикации. По направлению исследований было опубликовано двенадцать работ, из них 5 статей – в изданиях, рекомендованных ВАК Минобрнауки России.

Личный вклад автора. Все выносимые на защиту научные результаты получены автором лично. В работах, опубликованных в соавторстве, личный вклад соискателя сводится к следующему: [2, 11] - разработка программы имитационного моделирования движения локомотива; [3] - разработка методики и программы расчета влияния характеристик информации на вероятность проведения атак на ресурс; [4] - обзор и анализ современного программного обеспечения в сфере виртуализации; [11] - обоснование структуры системы управления безопасностью работы железнодорожного транспорта.

Структура диссертации. Диссертация включает: введение, четыре главы, заключение, список использованных источников – 196 наименований. Общий объем диссертации – 145 с., из которых основного текста –133 с., 45 рисунков, 7 таблиц, 2 приложения.

СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность решаемой задачи, сформулированы цель, научная новизна, теоретическая и практическая значимость исследований.

В первой главе разработана архитектура вычислительного комплекса (ВК) с использованием средств виртуализации который позволяет осуществлять взаимодействие системы автоведения поезда УСАВП-Т, и ДЦ «Сетунь» участка железной дороги. При этом ВК формируется из 10 виртуальных машин (ВМ), которые принимают на себя функции:
ВМ0: шлюз – для получения входной информации от локальной вычислительной сети ДЦ, УСАВП-Т и комплекса локомотивных устройств безопасности (КЛУБ), а также передачи выходной информации соответствующим системам;
ВМ1: формирование базы данных о характеристиках участка железной дороги, постоянных и временных ограничениях скорости, текущей координате поезда;
ВМ2: формирование базы данных о параметрах поезда (тип поезда, вес поезда, ограничения режимов нагрузок, число локомотивов и вагонов поезда);
ВМ3: формирование базы данных кассеты регистрации КЛУБ;
ВМ4: расчет мощности, которая может быть реализована локомотивом;
ВМ5: решение задачи оптимального управления локомотивом;
ВМ6: формирование базы данных о срабатывании систем защиты локомотива, получаемых от системы автоматики локомотива УСТА;
ВМ7: формирование базы данных о значениях текущих параметров режимов работы локомотива, получаемых от системы автоматики локомотива УСТА; расчет прогнозируемой надежности систем и агрегатов локомотива;
ВМ8: мониторинг ВК;
ВМ9: резерв.

Для обоснования принципа реализации ВК рассмотрены характеристики систем виртуализации и их уязвимости, выполнен анализ существующих средств защиты, а также обзор законодательной базы в области информационной безопасности, в том числе, особенности требований к информационным и вычислительных систем, используемым в структуре «РЖД».

Вторая глава посвящена разработке математической модели ВК для определения требуемых характеристик при работе в комплексной системе управления движением.

Теоретическим основам построения и исследования систем виртуализации посвящены работы отечественных и зарубежных авторов: Дубинина В.Н., Заикина С.А., Рослякова А.В., Тормасова А.Г. , Barrett D., Boomer J.; Carbone J., Crawford L. S., von Hagen W., Haletky E., Halter E. M., Keefer R. M.; Kipper G., Larson R., Lowe S., Olzak T., Sabovik J., Takemura C., , Vacca J. R., Chris Wolf C. и др. Проведенный анализ выполненных исследований показал, что в них решается задача оптимального распределения ресурса в виртуальной компьютерной системе с фиксированной структурой или задача построения виртуальной системы, где основным критерием эффективности является интегральный показатель стоимости и суммарной нагрузки приложений, определяемой по

производительности сервера. Для создания математических моделей управления ресурсами используются преимущественно методы дискретной математики и алгебры, вычислительной математики, методы математической статистики, методы теории операционных систем и системного программирования, математический аппарат логико-алгебраических описаний, формализма сетей абстрактных машин и иерархических алгебраических систем.

Основным недостатком этих моделей является абстрагирование расчета распределения ресурса от алгоритма функционирования вычислительной системы для решения конкретной задачи. Это снижает точность расчета нагрузки на ресурс и прогнозирования эффективности его использования.

Для решения поставленной задачи разработана динамическая модель ВК, описывающая процессы взаимодействия ресурса и приложений, обеспечивающих заданный алгоритм взаимодействия участников перевозочного процесса. В модели использован математический аппарат расширенных сетей Петри, объединяющий преимущества графовой и дискретной динамической модели и позволяющий рассчитывать количественные показатели работы вычислительной системы, характеризующейся параллельными и асинхронными процессами.

Математическая модель ВК в терминах сетей Петри определяется совокупностью объектов (рисунок 1) :

$$\Pi = \{P, T, I, O, \mu\}, \qquad (1)$$

где $P = \{p_1,\ p_2, \dots, p_i, \dots, p_n\}$ - непустое конечное множество позиций;

$T = \{t_1, t_2, \dots, t_j, \dots, t_m\}$ - непустое конечное множество переходов;

I - входная функция переходов, определяющая кратность входных дуг переходов $I(t_j)$;

O - выходная функция переходов, определяющая кратность выходных дуг переходов $O(t_j)$;

μ - вектор маркировки.

Разрешение на выполнение перехода $t_i \in T$ определяется условием

$$t_j: \mu(p_i) \geq \#(p_i, I(t_j)),\ p_i \in P, \qquad (2)$$

где $(p_i, I(t_j))$ - кратность входной позиции p_i для перехода t_j.

Результатом выполнения разрешенного перехода $t_i \in T$ является новая маркировка μ':

$$\mu'(p_i) = \mu(p_i) - \#(p_i, I(t_j)) + \#(p_i, O(t_j)). \qquad (3)$$

Динамическая модель ВК определяется системой, состоящей из 71 логических уравнений типа (2) и (3).

Для моделирования процессов в ВК разработана программа, базирующаяся на объектно-ориентированном подходе, для чего были созданы специализированные классы, описывающие состояния, переходы, дуги и функционирование сети Петри в целом. В программной реализации модели для задания случайных величин использовался стандартный генератор псевдослучайных чисел.

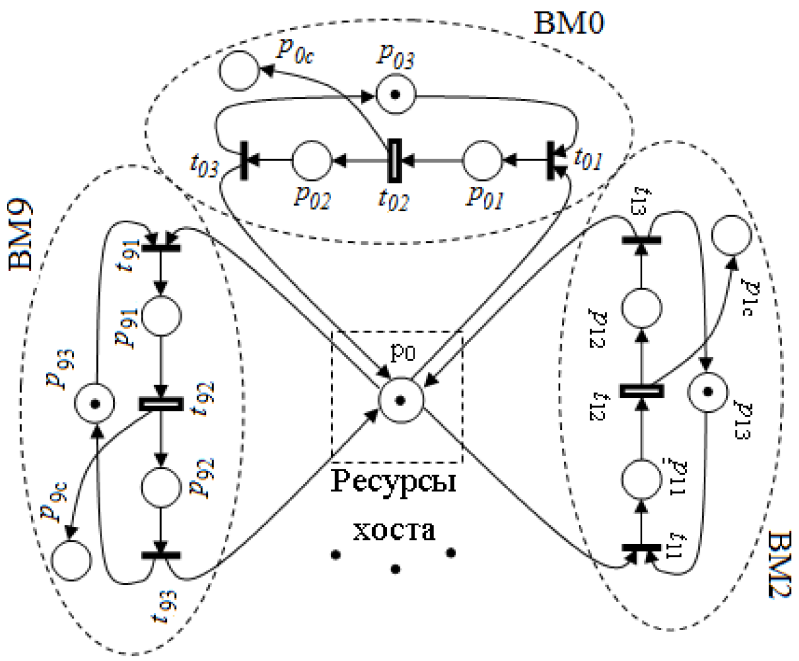


Рисунок 1. Модель ВК в терминах сетей Петри: p_0 – ресурс хоста; p_{01}-p_{03}, ...p_{91}-p_{93}-состояние ВМ0-9: p_{01}, ...,p_{91}-предоставление ресурсов; p_{02},... ,p_{92} - освобождение ресурсов; p_{03},...,p_{93} -ожидание ресурсов; p_{0c}, ...,p_{9c}-счетчики операций; t_{01} – t_{03}, ... t_{91}- t_{93}- распределения ресурсов ВМ0-9: t_{01},,...,t_{91} - выделение ресурсов; t_{02},...t_{92} - работа с ресурсами; t_{03},... ,t_{93} - возвращение ресурсов хосту

Исходными данными для расчета требуемых характеристик ВК являлись алгоритм работы системы УСАВП-Т, объем и характер информации, необходимой для взаимодействия участников перевозочного процесса: 100 мс – время выполнения циклической программы системы УСАВП-Т; объем информации 2530 КБ – на обслуживание заявки УСАВП-Т одного локомотива (принималась на основании ТУ на функционирование систем ДЦ «Сетунь», КЛУБ, УСАВП-Т, УСТА). Максимальная нагрузка на ресурс ВК для полигона ж.д. протяженностью 200 км (минимальная рекомендуемая длина участка, обслуживаемого ДЦ «Сетунь») определялась с учетом допустимых интервалов следования поездов при двухпутном движении, требований ресурса системами виртуализации и мониторинга состояния самого ВК; ее значение составило 6,23 ГБ. В соответствии с Инструкцией по определению станционных и межпоездных интервалов № ЦД-361 на участке ж.д. с указанными характеристиками одновременно могут находиться до 68 поездов.

Верификация модели выполнялось для двух режимов работы ВК:

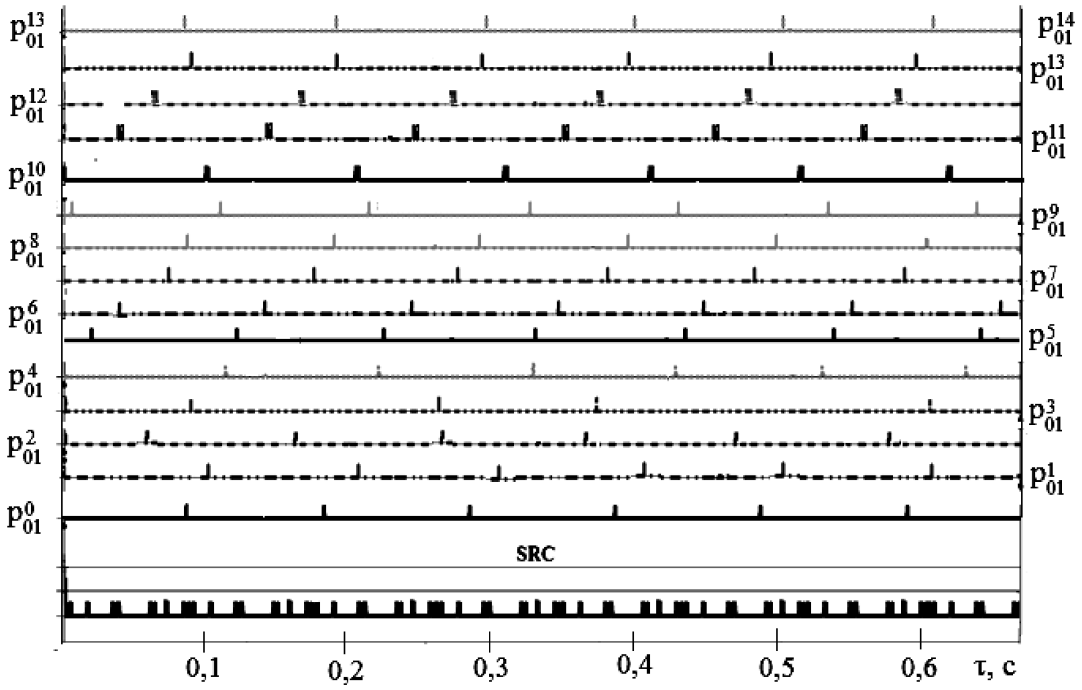
- расчете нагрузки на ресурс от системы УСАВП-Т одного локомотива (минимальная нагрузка) с контролем обеспечения алгоритма взаимодействия участников перевозочного процесса (распределения ресурса между ВМ при получении заявки на обслуживание от системы автоведения локомотива);

- расчете нагрузки на ресурс ВК при допустимых интервалах следования поездов и синхронных запросах на обслуживание систем УСАВП-Т локомотивов всех поездов (максимальная нагрузка).

Тестирование разработанной модели ВК показало, что она адекватно отражает процессы распределения ресурса в соответствии с алгоритмом взаимодействия участников перевозочного процесса и верно определяет требования к ресурсу на режимах максимальной и минимальной нагрузки.

Разработанная модель позволила установить требования к алгоритму взаимодействия приложений вычислительного ресурса ВК с учетом параметров работы циклической программы управления системы УСАВП-Т и скорости передачи информации по канала связи между участниками перевозочного процесса 1 Гбит/с. Получено, что максимально допустимое время работы циклической программы ВМ5 не должно превышать τ_{BM5}=99,5 мс.

В реальных условиях эксплуатации заявки на обслуживание участников перевозочного процесса будут поступать на ВК в разные моменты времени. На рисунке 2 представлен процесс моделирования использования ресурса ВК при обслуживании заявок участников перевозочного процесса с использованием математического аппарата сетей Петри.



p_{01}^{0} - p_{01}^{14} –обращение к ВМ0 по заявкам 0-14 локомотивов; SRC – использование ресурсов хоста при обслуживании заявок УСАВП-Т 68 поездов

Рисунок 2. Процесс моделирования использования ресурса ВК с использованием математического аппарата сетей Петри при равномерном распределении заявок на обслуживание, поступающих на ВМ0 от УСАВП-Т 68 поездов

Для определения эффективности использования ресурса ВК в реальных условиях выполнялся расчет его нагрузки при случайных распределениях потока заявок на обслуживание и математического ожидания времени обслуживания заявок. Получено, что при обслуживании заявок 68 поездов, имеющих равномерное распределение с математическим ожиданием времени обслуживания 15 мс максимальная нагрузка на ресурс ВК не превысит 30% от номинального значения ресурса, предусмотренного на обслуживание в системе управления движением. В том случае, если математическое ожидание времени обслуживания одной заявки системы УСАВП-Т возрастает до 50 мс пиковое значение нагрузки на ресурс достигает 320 МБ - 62% от того же ресурса (рисунок 3).

Проведенные исследования показали, что для участка ж.д. протяженностью 200 км средние затраты ресурса ВК на обслуживание заявок УСАВП-Т поездов не превышают 10% в общем расходе ресурса на поддержание всей структуры с учетом мониторинга. Поэтому важно было определить при какой длине участка ж.д., обслуживаемого комплексной системой управления движением, ресурс ВК будет использоваться наиболее эффективно.

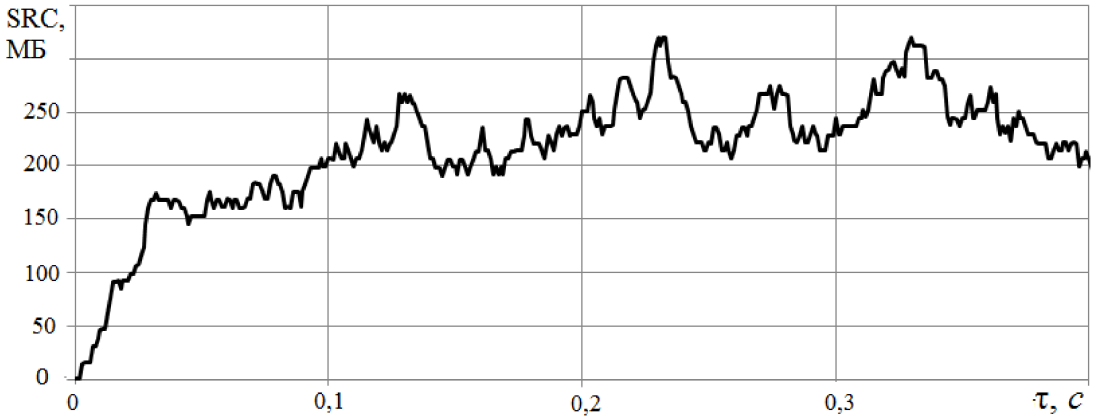


Рисунок 3. Нагрузка на ресурс ВК при равномерных распределениях заявок на обслуживание, поступающих от УСАВП-Т 68 поездов, и математическом ожидании времени обслуживания одной заявки 50 с

Для реализации разрабатываемого ВК предлагается использовать сервер IBM Flex System x240 с встроенной фабрикой IBM® Virtual Fabric. Этот тип сервера применяется для обслуживания больших вычислительных мощностей. Его особенностями являются:

-оптимизация с точки зрения виртуализации, производительности и высокой масштабируемости сетевых подключений;

- упрощенное развертывание и управление.

С целью удовлетворения современных сложных и постоянно изменяющихся бизнес-требований вычислительный узел IBM Flex System x240 (элемент IBM PureFlex System) оптимизирован с точки зрения виртуализации, производительности и высокой масштабируемости ввода-вывода для поддержания широкого спектра рабочих нагрузок. Вычислительные узлы Flex System x240 доступны для решений PureFlex System или IBM Flex System.

Для определения рациональной длины участка ж.д., обслуживаемой ВК, была решена задача оптимизации с векторной целевой функцией:

$$Ц(u) = \{K_1(u), K_2(u), ..., K_l(u), ..., K_L(u)\} \to \min ,$$

где $K_1(u), K_2(u), ..., K_l(u), ..., K_L(u)$ - частные критерии оптимизации, u - параметр управления, принадлежащий множеству возможных управлений U, $u \in U$.

Для ВК в качестве основных критериев эффективности работы выступают ресурс, необходимый для обслуживания систем УСАВП-Т поездов, находящихся на контролируемом участке, и его цена, а в качестве параметра управления – возможное число локомотивов G на этом же участке.

$$\begin{cases} K_1(G) \to \min \\ K_2(G) \to \max \end{cases}, \qquad (4)$$

где K_1 – цена сервера; K_2 – ресурс сервера, необходимый для обслуживания заявок УСАВП-Т.

Поиск оптимального распределения ресурсов такой системы сводится к определению множества неулучшаемых решений (оптимизации по Парето), т.е. приближению параметров управления к значению, при котором обеспечивается приближение $Ц(u)$ к утопической точке $K_{ут}$. При равнозначимости критериев $K_1(G)$ и $K_2(G)$ с учетом (4) оптимальное решение находилось минимизацией расстояния до $K_{ут}$ на плоскости критериев $(K_1, 0, K_2)$.

$$\begin{cases} Ц(G) \to \min ; \\ Ц^2(G) = [K_1(G) - K_{1\min}]^2 + [K_2(G) - K_{2\max}]^2 . \end{cases}$$

Значения критериев $K_1(G)$ и $K_2(G)$ могут отличаться на несколько порядков (в зависимости от масштабов измерения величин), поэтому целевая функция для определения эффективности работы ВК определялась через их относительные значения

$$Ц(g) = \sqrt{\left(\frac{K_1(G) - K_1^*}{K_1^{**} - K_1^*}\right)^2 + \left(\frac{K_2(G) - K_2^{**}}{K_2^{**} - K_2^*}\right)^2} \to \min \qquad (5)$$

где $K_1^*, K_2^*, K_1^{**}, K_2^{**}$ - соответственно минимальные и максимальные значения частных критериев, найденных при решении задачи оптимизации по заданному

критерию; $K_1(G)$, $K_2(G)$ - текущие значения частных критериев, полученные при параметрах управления, расположенных в множестве Парето.

В соответствии с (5) были рассчитаны значения $Ц(G)$ для Ярославского направления ж.д. при допустимом интервале следования поездов (рисунок 4).

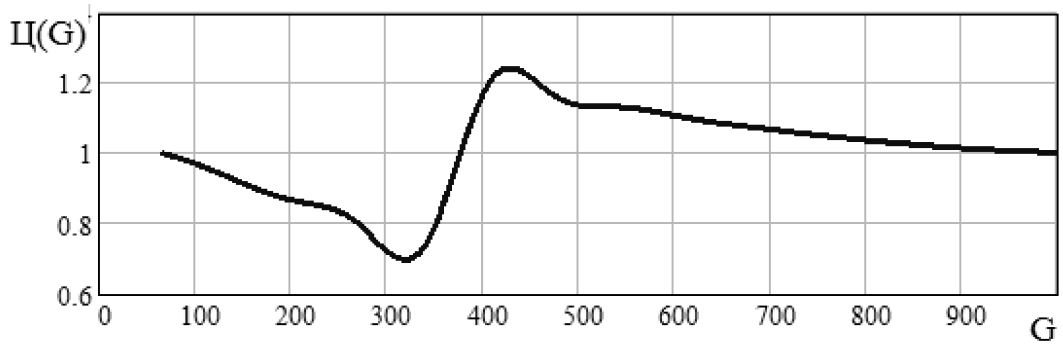


Рисунок 4. Значения целевой функции эффективности использования ресурса ВК в зависимости от числа локомотивов на обслуживаемом участке ж.д. при допустимом интервале следования поездов

Таким образом, при равной значимости частных критериев оптимизации $\overline{K}_1(G)$ и $\overline{K}_2(G)$ для Ярославского направления ж.д. ресурс ВК будет использоваться наиболее эффективно, если комплексная система управления движением будет обслуживать 320 поездов, т.е. участок протяженностью 950 км.

В третьей главе рассмотрены уязвимости ВК и предложен способ его резервирования в соответствии с требованиями к вычислительным ресурсам стандарта СТО РЖД 1.18.002-2009.

С помощью разработанной модели ВК выполнено моделирование динамического процесса отказа снапшота ВМ и разворачивания аналогичного резервного приложения. При этом предполагалось, что исправные ВМ работают в штатном режиме, создавая соответствующую нагрузку на ресурс. По условиям моделирования время получения запросов на обслуживание систем автоведения и время загрузки ресурса ВМ5 имели равномерное распределение в соответствии с ограничениями T2=100мс и $\tau_{ВМ5}$=99,5 мс.

Результаты моделирования показали, что время загрузки снапшота составляет 15,0 с. Эксперименты по разворачиванию снапшота на физическом хосте дали аналогичный результат: в зависимости от степени загрузки ресурса хоста это время может составлять от 11 до 17 с. При загрузке на хостовую систему ВМ только с базовой ОС время ее разворачивания составляет от 7 до 12 с. (при расчетном времени – 7,9 с.), что еще раз подтвердило адекватность модели ВК его физической реализации. Аналогичные исследования были проведены для режимов разворачивания на хостовой системе ВМ для формирования баз данных и ПО системы автоведения.

Таким образом, при отказе одной из ВМ использование резерва ресурса не позволит развернуть на хосте дополнительную ВМ и передать ей функции управления за 100 мс в соответствии с требованиями алгоритма функционирования системы автоведения. Это потребовало разработки системы резервирования ВК. На основании анализа характеристик систем резервирования для ВК принято мажоритарное резервирование с голосованием «2 из 3», что позволит защититься не только от отказов, но и от воздействия помех, обеспечивая более высокую точность управления.

Для определения надежности ВК с мажоритарным резервированием были использованы данные производителя сервера IBM Flex System x240, в соответствии с которыми время наработки до первого отказа этого сервера составляет $1{,}0 \cdot 10^5 - 1{,}25 \cdot 10^5$ часов. При среднем времени наработки до первого отказа $1{,}125 \cdot 10^5$ часов было получено, что время работоспособного состояния ВК с мажоритарным резервированием составит $0{,}937 \cdot 10^5$ часов. При этом для времени эксплуатации менее $0{,}78104 \cdot 10^5$ часов (менее 8,9 лет), ВК с мажоритарным резервированием будет иметь большие значения вероятности безотказной работы, чем ВК без резервирования (рисунок 5).

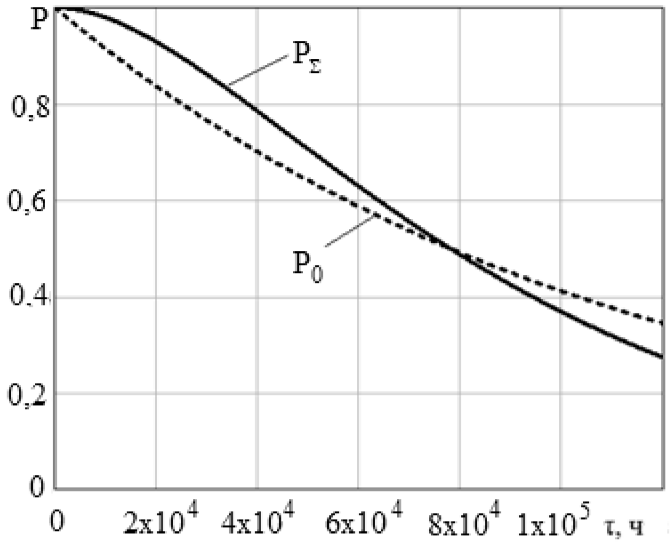


Рисунок 5. Вероятность безотказной работы ВК без резервирования (P_0) и ВК с мажоритарным резервированием с голосованием “2 из 3” (P_Σ)

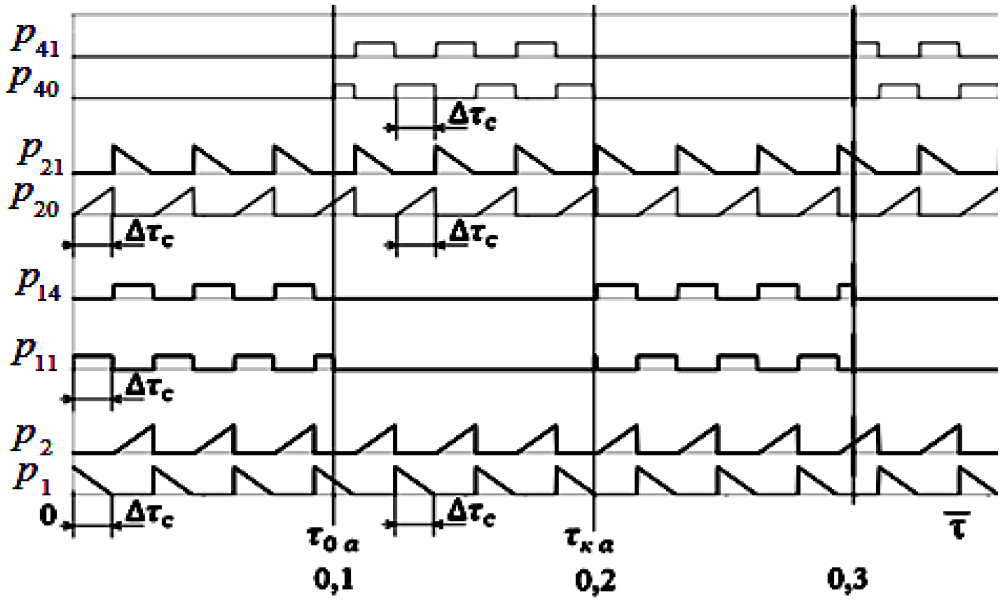
Второй уязвимостью ВК является проведение информационной атаки. Вследствие закрытости структуры комплексной системы управления движением поездов проведение DoS-атаки маловероятно, а MITM-атака является вероятным методом воздействия на систему. При этом наиболее уязвимой точкой для несанкционированного подключения является радиоканал между системой автоведения поезда и ВК, образуя канал взаимодействия «система автоведения поезда – атакующий – ВК».

При проведении MITM-атаки нарушитель осуществляет вмешательство в протокол передачи информации, считывая или искажая ее. Основными типами MITM-атак являются: атака в пределах одного LAN (LocalAddressNetwork),

осуществляемая на канальном уровне модели OSI; DNS Spoofing, используемый для предоставления ложной DNS-информации; кража cookie при HTTP-сеансах; MITM-атака с использованием Wi-Fi-маршрутизатора.

Для анализа действий нарушителя и выбора эффективной системы защиты была разработана математическая модель MITM-атаки на информационный ресурс с использованием математического аппарата расширенных сетей Петри. Модель представляет собой направленный маркированный граф, состояние которого описывается системой из 31 логических уравнений типа (2) и (3), где кроме состояний ресурса, легитимного пользователя, атакующего и каналов связи между ними представлена конфигурация средств маршрутизации, модифицируемая атакующим.

На рисунке 6 представлена сокращенная диаграмма, отражающая функционирование сети между ВМ и ресурсом при передаче информации пакетами в штатном режиме и в режиме перехвата трафика.



$\Delta\tau_c$ - интервал времени передачи информации; $\tau_{0\,a}$- момент начала атаки; $\tau_{к\,a}$ - момент завершения атаки

Рисунок 6. Моделирование работы каналов передачи информации при MITM-атаке на ВК

В начальный момент времени запрос от ВМ передается ресурсу по легитимному каналу p_1-p_{11}-p_{20}; при этом объем информации в буфере p_1 уменьшается, в буфере p_{20} - увеличивается. После получения всего запроса ресурс генерирует ответ объемом в 150 пакетов в буфере p_{21} и передает его ВМ по каналу p_{21}-p_{14}-p_2 (объем информации в буфере ресурса p_{21} уменьшается, а в буфере ВМ p_2 – увеличивается). В момент времени $\tau_{0\,a}$ в сеть включается атакующий, считывая информацию через состояния p_{40}, и p_{41}, а штатные каналы передачи информации (состояния p_{11}, p_{14}) не используются. Для перехвата информации ата-

кующий модифицирует базовую конфигурацию средства маршрутизации, перенаправляя трафик через себя. При этом характер передачи информации не меняется ни для ВМ, ни для ресурса. В произвольный момент времени $\tau_{ка}$ нарушитель покидает сессию, восстанавливая базовую конфигурацию средств маршрутизации.

Маршруты попыток несанкционированного доступа к ресурсу ВК определялась с использованием методики формализованных моделей информационных атак, разработанной Б. Шнайером, в основе которой лежит иерархическое дерево атак. Особенностью дерева атак виртуальной инфраструктуры является наличие ветви, которая показывает, что за счет трансляции трафика через сетевой интерфейс хоста возможно провести атаку на ВМ, существенно снизив при этом риск обнаружения атаки. Данная модель может быть легко расширена, детализована или модифицирована под другие условия, что позволяет ее адаптировать для вычислительной сети другой структуры.

Возможные маршруты атак были использованы при расчете характеристик систем защиты ВК.

Четвертая глава посвящена разработке метода определения эффективности системы защиты ВК. Параметры распределения характеристик его уязвимостей и проводимых атак принимались на основании результатов тестирования на проникновение в информационные системы крупных предприятий в 2011—2012 г., проведенного компанией Positive Technologies, в том числе, и для определения масштаба времени при моделировании процессов компрометации.

Вопросам информационной безопасности посвящены работы российских и зарубежных специалистов: Безрукова Н.Н., Водолазкого В.В., Герасименко В.А., Грушо А.А., Девянина П.Н., Домарева В.В., Зегжды Д.П., Касперски К., Корниенко А.А., Лукацкого А.Г., Молдовяна А.А., Щербакова А.Ю., Bell D.E., Bishop M., Bragg R., Jensen Ch.D., LaPadula L.J.,McNab C.,Vitek J., и других.

В настоящее время для анализа работы информационных систем в условиях проведения атак разработаны модели и методики: сценарная логико-вероятностная модель сети как системы массового обслуживания - для решения задачи защиты от распределенных атак; графо-вероятностная модель обнаружения нелегитимного программного обеспечения; поведенческая и формальная модели анализа состояния компьютерных систем, основанные на математических аппаратах теории графов и теории конечных автоматов - для выявления атак на Web-серверы и анализа условий предотвращения несанкционированных доступов к информации; модель нечеткого логического вывода, позволяющая выявлять вероятность атаки по совокупности аномальных событий в системе; методика покрытия тестами программного обеспечения - для исследования его на наличие уязвимостей по исполняемым файлам.

Для расчета вероятности доступа к ВК разработана математическая модель с использованием математического аппарата расширенных цветных сетей

Петри, описывающая динамические процессы в системе с шифрованной информацией при проведении MITM-атаки (рисунок 7). Результатом моделирования является отображение текущих состояний основных элементов структуры ВК (хоста, гипервизора, объектов сетевой структуры) на основании маршрутов дерева атак, разработанного в третьей главе.

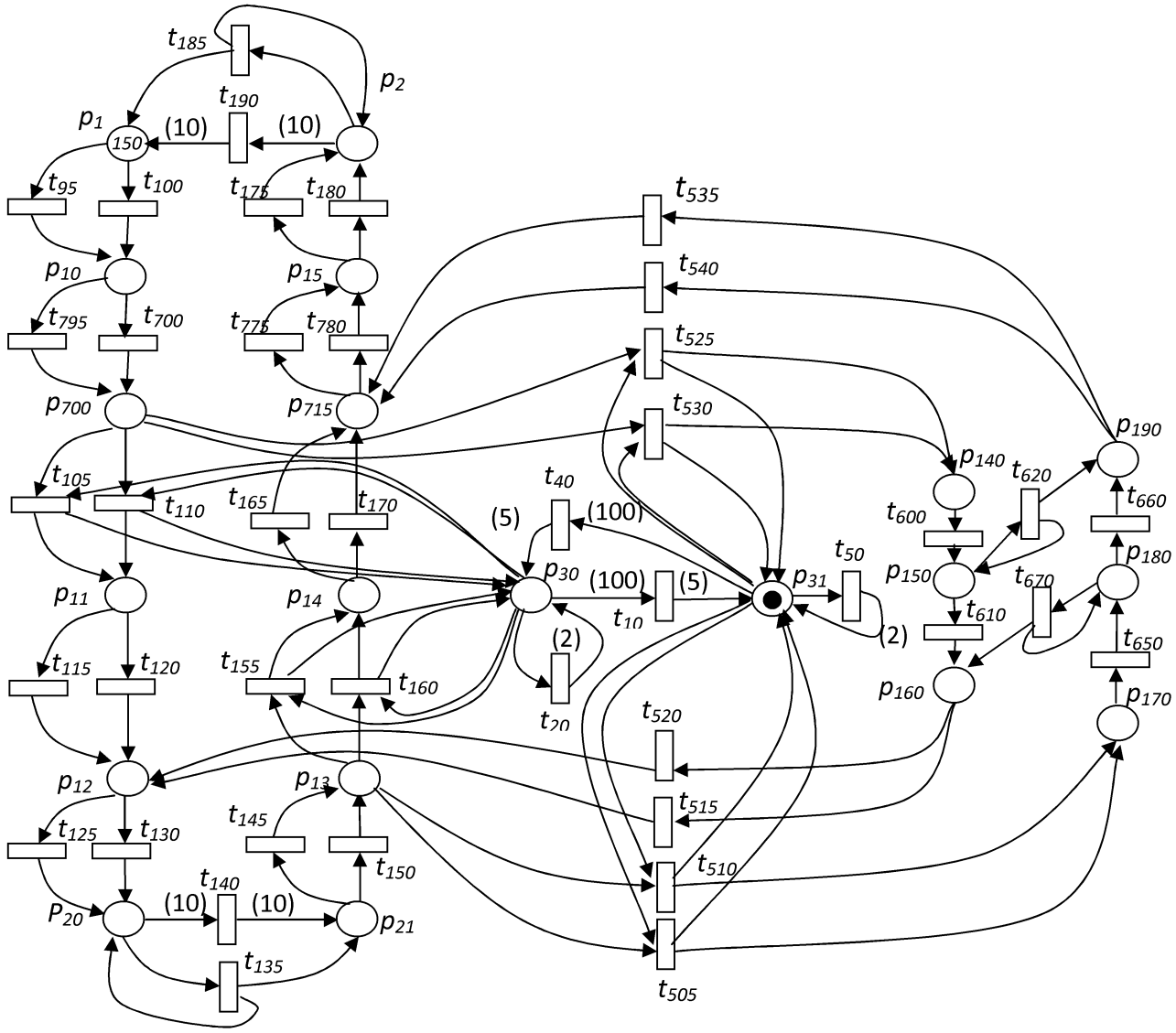


Рисунок 7 . Модель атаки на ВК с криптографической защитой информации в терминах расширенных сетей Петри

При моделировании маршрутов в маркированном графе цветных сетей Петри разрешение на выполнение перехода $t_i \in T$ определяется условием:

$$t_j : \mu : (p_i) \geq \#(p_i : color, I : color(t_j)),\ p_i \in P \qquad (6)$$

где $(p_i : color, I : color(t_j))$ - кратность входной позиции p_i, соответствующего цвета, для дуги перехода t_j этого же цвета.

Результатом выполнения разрешенного перехода $t_i \in T$ является новая маркировка μ':

$$\mu'(p_i) = \mu(p_i) - \#: color(p_i, I(t_j)) + \#: color(p_i, O(t_j)) . \qquad (7)$$

Динамические процессы в защищенном ВК при совершении атаки на него описываются системой из 57 логических уравнений типа (6) и (7) и определяются позициями и переходами:

p_1, p_2 – передача и получение информации клиентом; p_{20}, p_{21} – получение и передача информации ресурсом; p_{30}, p_{31}- легитимные и скомпрометированные настройки систем маршрутизации; p_{10}, …, p_{15} - легитимные каналы передачи данных между ресурсом и клиентом; p_{700}, p_{715} - передача запроса клиента и ответа ресурса; p_{140},p_{170} - получение атакующим зашифрованного пакета от клиента и от ресурса; p_{150} ,p_{160}, p_{180},p_{190} - пакеты клиента и ресурса расшифрованы и зашифрованы атакующим; t_{190}, t_{140}- формирование ответов клиентом и ресурсом; t_{100}, t_{110}, t_{120}, t_{130}, t_{150} , t_{160}, t_{170}, t_{180} - шифрование, передача и дешифрование информации в легитимных каналах; t_{95}, t_{105}, t_{115}, t_{125}, t_{725}, t_{135}, t_{145}, t_{155}, t_{165}, t_{175} t_{185}, t_{775}- формирование и передача подтверждения получения пакета информации клиентом и ресурсом; t_{700}, t_{715} - передача запроса клиента и ответа ресурса гипервизором на хост; t_{20}, t_{50} - воздействие на средства маршрутизации атакующим; t_{10},t_{40} - перенаправление трафика через атакующего и легитимные каналы связи; t_{505} - передача подтверждений получения пакета от ресурса и клиента к атакующему; t_{510}, t_{540}- передача информации от ресурса к атакующему и от атакующего к клиенту; t_{515}, t_{535}- передача подтверждения получения пакетов клиентом и ресурсом, сфальсифицированное атакущим; t_{530}, t_{520} - передача информации от клиента к атакующему и от атакующего к ресурсу; t_{610}, t_{600}, t_{650} - шифрование и расшифровка пакета клиента и ресурса атакующим; t_{620}, t_{670}- фальсификация получения пакета ресурсом и клиентом.

В штатном режиме работы системы, маркеры, отображающие функционирование средств маршрутизации, находятся в состоянии p_{30}, а передача информации осуществляется через легитимные каналы (p_{11} и p_{14}). В случайный момент времени атакующий воздействует на средства маршрутизации (t_{20}) и при успехе перенаправляет информацию через себя (t_{10}, p_{31}). Трафик между клиентом и ресурсом проходит через атакующего (t_{505}, t_{510}, , p_{140} и t_{525}, t_{530}, p_{170}). Он дешифрует пакеты (t_{600}, t_{650}), получая доступ к информации (p_{150} и p_{180}), фальсифицирует подтверждения о получении пакетов (t_{620}, t_{670}) и передает их клиенту (t_{535}) или ресурсу (t_{515}). «Прочитав» каждый пакет, он снова шифрует его (t_{610}, t_{660}), и передает ресурсу или клиенту (t_{540}, t_{520}). Время прослушивания информации определяется функционированием перехода t_{50}. Собрав информацию, нарушитель уходит из сети и легитимные каналы передачи информации восстанавливаются, что соответствует срабатыванию перехода t_{40}.

Для определения эффективной системы защиты ВК была разработана методика, в основу которой положен алгоритм MITM-атаки на ВК с криптографической защитой трафика. Новизной методики является использование метода

Монте-Карло для статистического анализа текущего состояния защищенной структуры ВК, представленной в терминах расширенных сетей Петри, при случайных характеристиках проводимых атак.

В алгоритме моделирования процесса «MITM-атака»-«защита» учитывалась разветвленная конфигурация системы защиты и случайный характер параметров проведения атаки и параметров системы защиты.

Начало атаки определялось воздействием на одну из листовых вершин дерева атак, причем вершина маршрута атаки задавалась случайным числом с равномерным распределением $R0 = \{1,2,\dots,9\}$. Параметр квалификации атакующего для каждой моделируемой атаки задавался количеством маркеров в исходной вершине маршрута $\mu_{0,m}$:$\mu_{0,m} = R1_m$, где $R1_m$- случайная величина с диапазоном изменения $1 \leq R1_m \leq 100$ и шагом $\Delta R1_m = 1$, m - номер ветви атаки.

Результирующее время срабатывания каждого перехода $\tau_{j,m}$ определялось в модели значениями трех случайных параметров: сложностью проводимой атаки $R2_{j,m}$, квалификацией атакующего для преодоления текущего перехода $R3_{j,m}$ $(1 \leq R3_{j,m} \leq R1_m)$ и собственно временем проведения атаки $R4_{j,m}$:

$$\tau_{j,m} = k2_{j,m} \cdot R2_{j,m} + k3_{j,m} \cdot R3_{j,m} + k4_{j,m} \cdot R4_{j,m} ,$$

где $k2_{j,m}$, $k3_{j,m}$, $k4_{j,m}$- масштабные коэффициенты соответствующих параметров атаки.

Процедура отыскания и эксплуатации уязвимости на переходе $t_{j,m}$ дерева атак была представлена в математической модели срабатыванием соответствующего перехода $t_{j,m}$.

Кратность входной дуги перехода $I(t_{j,m})$ задавалась параметром сложности проводимой атаки на соответствующем переходе

$$I(t_{j,m}) = R2_{j,m};$$

кратность выходной дуги перехода $O(t_{j,m})$ задавалась параметром квалификации атакующего для соответствующего перехода

$$O(t_{j,m}) = R3_{j,m}.$$

В соответствии с алгоритмом модели срабатывание перехода $t_{j,m}$ могло быть реализовано только при выполнении условия:

$$\mu(\mathrm{p_{i,m}}) \geq \#(\mathrm{p_{j,m}}, \mathrm{I(t_{j,m})}), \qquad (8)$$

где $\mu(p_{j,m})$ - случайное числом маркеров в состоянии, предшествующем переходу $t_{j,m}$; оно зависит от числа выходных дуг предыдущего перехода $O(t_{j-1,m})$ и от числа циклов $N_{\text{п}}$, определяющих срабатывание предыдущего перехода $t_{j-1,m}$. Поэтому процедура эксплуатации уязвимости определялась числом циклов программы, при которых $\mu(p_{i,m}) < \#(p_{j,m}, I(t_{j,m}))$.

Количество необходимых процедур $N_{\text{п}}$ для выполнения условия (8)

$$N_{\text{п}} = R4_{j,m}.$$

Таким образом, при моделировании процесса «атака-защита» в ВК с использованием математического аппарата расширенных цветных сетей Петри выполнялось разыгрывание пяти случайных величин $R0$, $R1_m$, $R2_{j,m}$, $R3_{j,m}$, $R4_{j,m}$. имеющих различные законы распределения.

В соответствии с разработанным алгоритмом выполнено моделирование динамического процесса атаки на ВК с различными типами защит. При моделировании был принят «уровень доверия» $\varepsilon = 0{,}03$, что обеспечивалось числом розыгрышей в каждом варианте защиты L = 65250.

В качестве базовой системы защиты, успешная атака на которую может быть реализована за контрольное время 168 ч., принят стандартный комплекс мер на основе мониторинга сетевых процессов и разграничения прав доступа к ресурсам без использования специализированного анализирующего или защитного ПО.

С использованием разработанной модели были определены расчетные значения вероятностей несанкционированного доступа к информации ресурса при использовании четырех типов защит:

- защита виртуальной машины;
- защита «диска» виртуальной машины;
- защита хостовой системы;
- средств обеспечения безопасности сетевой инфраструктуры.

Результаты моделирования процессов в ВК с защитой ВМ при проведении MITM-атаки показали, что на момент контрольного времени (168 ч.) вероятность защиты от несанкционированного доступа к информации составила 0,14 (рисунок 8). Поскольку хост и гипервизор ВК не получили дополнительной защиты время доступа к ним не меняется по сравнению с базовой системой защиты.

В том случае, если в ВК используются комплекс защитных средств и ПО для обеспечения конфиденциальности «диска» ВМ, на момент контрольного времени вероятность защиты от несанкционированного доступа к информации составила 0,12, а время доступа к гипервизору увеличилось на 2 часа (3%) по сравнению с базовой системой.

Наиболее эффективной системой для защиты информации ВК оказывается комплекс защитного ПО для хоста. Его использование увеличивает вероятность защиты за контрольное время до 0,2, при этом хост оказывается доступен атакующему через 90 ч, а гипервизор - через 120 ч. Ориентировочное время доступа к информации составит 240 ч.

Использование средств обеспечения безопасности сетевой инфраструктуры ВК оказалось наименее эффективным средством защиты. К контрольному

времени информация будет защищена с вероятностью 0,1; время доступа к хосту составит 67 ч., а к гипервизору - 90 ч.

Поскольку надежное функционирование ВК связано с безопасностью движения поездов он требует высокого уровня защиты. В связи с этим были выполнены расчеты вероятности обеспечения конфиденциальности информации ВК при комплексной защите, т.е. использования всех четырех типов рассмотренных защит (рисунок 8). Результаты показали, что в этом случае за контрольное время информация будет защищена с вероятностью 65%.

Для возможности оценки эффективности применяемых средств защиты виртуального вычислительного комплекса системы управления движением поездов разработана программа, использующая CLI - интерфейс.

Рисунок 8. Вероятностные характеристики защиты ВК при проведении MITM-атаки и различных системах используемой защиты: base - стандартный комплекс мер на основе мониторинга сетевых процессов и разграничения прав доступа к ресурсам без использования специализированного анализирующего или защитного ПО; I- защита ВМ; II – защита "диска" ВМ; III- защита хостовой системы; IV - средства обеспечения безопасности сетевой инфраструктуры; V – комплексная защита, включающая I, II, III и IV типы защит

ЗАКЛЮЧЕНИЕ

В диссертационной работе были выполнены исследования и разработан

метод создания вычислительного комплекса с эффективной системой защиты и использованием средств виртуализации для решения задачи управления движением поездов на участке железной дороги, контролируемом диспетчерской централизацией.

При выполнении работы были получены теоретические и практические результаты:

1. Определены объемы и характеристики информации, использующейся для выполнения алгоритма взаимодействия систем диспетчерской централизации, автоведения поездов и локомотивных устройств безопасности как единого информационно-коммуникационного пространства.

2. Разработана структура комплексной системы управления движением поездов на основе средств цифровой связи со стандартизованными технологиями идентификации, навигации и позиционирования, отличающаяся от существующих тем, что она позволяет повысить уровень взаимодействия участников перевозочного процесса за счет интеграции их полномочий на базе вычислительного комплекса.

3. Разработан программно ориентированный метод взаимодействия элементов вычислительного комплекса на базе математического аппарата сетей Петри. Показано, что данный метод позволяет рассчитывать нагрузки на ресурс от элементов вычислительного комплекса при различных характеристиках потока заявок от участников перевозочного процесса с учетом параллельных и асинхронных процессов их взаимодействия.

4. Разработана методика расчета оптимальной длинны участка ж.д., контролируемого вычислительным комплексом системы управления движением. Показано, что для полигона ж.д. Ярославского направления при допустимом интервале следования поездов и использовании в вычислительном комплексе сервера IBM Flex System x240 длинна такого участка составляет 950км.

5. Разработана система резервирования вычислительного комплекса в соответствии с требованием стандарта СТО РЖД 1.18.002-2009 «Управление информационной безопасностью. Общие положения».

6. Определены возможные маршруты атак на вычислительный комплекс; наибольшую уязвимость вычислительный комплекс имеет при проведении MITM-атаки, а точкой для несанкционированного подключения будет являться радиоканал между системой автоведения поезда и вычислительным комплексом.

7. Разработан вероятностный метод расчета эффективности защиты вычислительного комплекса, который позволил определить значения вероятностей и времени несанкционированного доступа к информации ресурса при случайных параметрах атак и уровней защиты его элементов.

8. Поучено, что за контрольное время защита сетевой инфраструктуры вычислительного комплекса обеспечивает вероятность получения доступа к информации 0,95 по сравнению со стандартным комплексом мер защиты, защита "диска" ВМ – 0,88, защита ВМ – 0,86, защита хостовой системы - 0,8 и увеличивает время доступа в полтора раза.

9. Для вычислительного комплекса системы управления движением поездов рекомендовано использование интегральной системы защиты, обеспечивающей вероятность сохранения конфиденциальности информации 0,65 за контрольное время доступа.

ОСНОВНЫЕ ПУБЛИКАЦИИ ПО ТЕМЕ РАБОТЫ

Публикации в изданиях, рекомендованных ВАК Минобрнауки России:

1. Корнев, Д.А. Критерии логической сети обслуживания./ Д.А. Корнев // Мир транспорта - 2012.-№2. - С. 134-139.

2. Корнев, Д.А. Симулятор системы управления и обеспечения безопасности железнодорожного транспорта на базе сетевых технологий./ Д.А. Корнев Шамров М.И. Гринфельд И.Н. // Информационные технологии в проектировании и производстве – 2013. - № 2.- С.36 -40.

3. Корнев, Д.А. Влияние характеристик источника информации на вероятность проведения атак. / В.П. Соловьев, Д.А. Корнев // Вопросы защиты информации - 2014. - №2 (105). - С. 37 – 42.

4. Корнев, Д.А. Сетевое взаимодействие в системах виртуализации VirtualBox и VMWare./ В.П. Соловьев, Д.А. Корнев // Программная инженерия - 2013. - №9. - С. 42 – 47.

5. Корнев, Д.А. Моделирование динамического состояния виртуальной инфраструктуры с использованием сетей Петри./ Д.А. Корнев // Программная инженерия - 2014. - №5. - С. 14 – 19.

Публикации, не входящие в перечень изданий, рекомендованный ВАК Минобрнауки России:

6. Корнев, Д.А. Уязвимости луковичной маршрутизации в обеспечении безопасности функционирования информационной сети: тез. докл. науч.-практ. конф. / Д.А. Корнев // Труды тринадцатой научно-практической конференции «Безопасность движения поездов». - М.: Московский государственный университет путей сообщения (МИИТ), 2012. - С. VIII-2.

7. Корнев, Д.А. Реализация сетевой MITM-атаки в виртуальных компьютерных сетях : тез. докл. науч.-практ. конф. / Д.А. Корнев // Труды научно-практической конференции «Неделя науки – 2012. НАУКА МИИТа - ТРАНСПОРТУ».- М.: Московский государственный университет путей сообщения (МИИТ), 2012.- С. VII-9.

8. Корнев, Д.А. Повышение конфиденциальности информации виртуальных систем путем использования средств анонимизации: тез. докл. науч.-практ.

конф. / Д.А. Корнев // Труды научно-практической конференции «Неделя науки – 2013. НАУКА МИИТа - ТРАНСПОРТУ».- М.: Московский государственный университет путей сообщения (МИИТ), 2013. - С. VII-5 - VII-6.

9. Корнев, Д.А. Дерево атак на виртуальную инфраструктуру: тез. докл. науч.-практ. конф. / Д.А. Корнев// VII Международный транспортный форум, I Форум транспортного образования «Молодые ученые транспортной отрасли» - М.: Московский государственный университет путей сообщения (МИИТ), 2013.- С.17.

10. Корнев, Д.А. Моделирование атак на информационную систему в терминах сетей Петри/ Д.А. Корнев// Труды IV международная научно-практическая конференция «ИнтеллектТранс-2014» / Под ред. А.А. Корниенко.- СПб.: Санкт-Петербургский государственный университет путей сообщения (ПГУПС).- С. 243-249.

11.Корнев, Д.А. Виртуальная система контроля и управления безопасностью работы железнодорожного транспорта/ В.П.Соловьев, Д.А. Корнев // Труды двенадцатой научно-практической конференции «Безопасность движения поездов».- М.: Московский государственный университет путей сообщения (МИИТ), 2011.- С. I-6.

12. Корнев, Д.А. Методика построения вероятностной модели оценки угроз на информационный ресурс: тез. докл. науч.-практ. конф. / Д.А. Корнев// Международная научно-практическая конференция «Современные проблемы развития интеллектуальных систем транспорта» - Днепропетровск: Днепропетровский национальный университет железнодорожного транспорта (ДНУЖТ), 2014.- С.68-69.