Федеральное государственное бюджетное образовательное учреждение

высшего профессионального образования

«Московский Государственный Университет Путей Сообщения»

МГУПС (МИИТ)

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

Диссертация
на соискание ученой степени кандидата технических наук

Научный руководитель

кандидат технических наук, доцент

Соловьев Владимир Павлович

Москва - 2015 г.

ВВЕДЕНИЕ

Стратегией развития железнодорожного транспорта в Российской Федерации до 2030 года определена важная роль развития высокоскоростного железнодорожного транспорта и создания технологической платформы «Высокоскоростной интеллектуальный железнодорожный транспорт» [1].

На ближайшую перспективу целью разработки Технологической платформы является внедрение единой комплексной системы управления движением высокоскоростных поездов (до 400 км/ч) с многоуровневым обеспечением безопасности движения, а также создание интеллектуальной среды эксплуатации высокоскоростного железнодорожного транспорта.

К основным задачам и функциям Технологической платформы относятся:

1. интеграция современных машиностроительных и информационных технологий и средств автоматизации в транспортную инфраструктуру для повышения безопасности и эффективности транспортного процесса;

2. разработка интеллектуальных логистических систем управления перевозочным процессом для высокоскоростного железнодорожного транспорта в увязке с другими транспортными системами, в том числе для обеспечения энергоэффективного управления движением; создание «интеллектуального» поезда со встроенной системой автоведения и самодиагностики;

3. создание единого информационно-коммуникационного пространства транспорта с обеспечением информационной защиты на основе средств цифровой связи со стандартизованными технологиями идентификации, навигации и позиционирования, а также применения спутниковых технологий ГЛОНАСС/GPS.

Из-за большой протяженности железных дорог России (86 тыс. км дорог общего назначения), высокой стоимости прокладки и обслуживания особенность их эксплуатации заключается в том, что одно и то же полотно используется как для грузового, так и пассажирского движения. Учитывая значительные расстояния между городами, связываемыми высокоскоростным движением, прокладка специальных линий на настоящий момент экономически не оправдана и в ближайшее время не планируется. В связи с этим перед службами РЖД встает проблема организации движения высокоскоростного подвижного состава в графике движения поездов со средними эксплуатационными характеристиками. При этом организация движения должна соответствовать принципам оптимизации по времени следования поездов и их энергозатратам. Реализовать это можно только за счет повышения пропускной способности железных дорог.

Для обеспечения безопасности движения поездов на железной дороге (ж.д.) используется диспетчерская централизация (ДЦ), выполняющая управление из одного пункта стрелка-

ми и светофорами ряда станций и перегонов в зависимости от их занятости, а также автоматическую запись графика исполненного движения поездов.

С 1990г. года на ж.д. начала внедряться автоматическая система ДЦ «Сетунь» с высокоскоростным обменом информацией между центральным распорядительным постом и линейными исполнительными и контролируемыми пунктами [2]. Эта система позволяет осуществлять организацию движения на контролируемом участке, а также выполнять сбор, обработку и отображение информации в реальном масштабе времени о местоположении поездов, их номерах и состоянии других объектов контроля. Обмен информацией между центральным постом и линейными пунктами осуществляется по сети рабочей связи, которая имеет возможность осуществлять удаленный мониторинг программного обеспечения линейных пунктов и состояния интерфейсов и осуществляет реконфигурацию опроса линейных пунктов при возникновении проблем на линии связи (с одновременной индикацией неисправности). Длина управляемого и контролируемого участка ДЦ «Сетунь» – 200 – 1000 километров (в зависимости от интенсивности движения поездов).

Однако применение цифровой системой ДЦ при наличии «человеческого фактора» в управлении подвижным составом является недостаточным мероприятием для обеспечения максимальной пропускной способности железной дороги. Второй составляющей Технологической платформы является система автоведения поезда, которой уже в настоящее время оборудуются опытные магистральные локомотивы и электропоезда [3]. Однако на настоящий момент комплексное взаимодействие системы ДЦ с системами автоведения поездов, находящихся в зоне контролируемого участка, отсутствует. Алгоритм управления локомотивом система автоведения рассчитывает исходя из постоянной информации о параметрах профиля участка и сигналов безопасности, получаемых с ближайшего светофора. Отсутствие информации о поездной ситуации на всем участке следования проводит к необходимости использования поездом режимов торможения, что снижает участковую скорость движения и энергетическую эффективность работы локомотива, а также повышает износ колесных пар и тормозного оборудования поезда. Интеграция системы автоведения локомотива в систему ДЦ участка ж.д. позволит оптимальным образом согласовать текущую поездную ситуацию участка, характеристики его профиля и режим движения поезда. Это обеспечит не только максимальную пропускную способность железных дорог, но снизит вероятность возникновения аварийных ситуаций и повысит экономичность работы локомотивов. Мощности современных вычислительных систем позволяют успешно решить задачу взаимодействия систем автоведения поездов с системой диспетчерской централизации, а технологии виртуализации – обеспечить распределение вычислительных сред для решения принципиально разных задач: контроля, прогнозирования и организации движения в конкретной поездной ситуации. Кроме того, такому вычис-

лительному комплексу (ВК) можно передать часть функций системы автоведения, разгрузив ее процессор, а также в режиме реального времени контролировать действия машиниста и всех систем локомотива, повышая безопасность движения и прогнозируя надежность работы локомотивов, что даст возможность наилучшим образом организовать их эксплуатацию и обслуживание на линии.

Виртуальная вычислительная среда позволяет реализовать любой алгоритм управления вычислительными процессами отдельных приложений, получить высокий уровень доступности ресурсов, сократить расходы, благодаря более эффективному использованию аппаратных средств, обеспечить более высокий уровень безопасности и более совершенную систему восстановления в аварийных ситуациях.

Однако существуют и недостатки виртуализации. В первую очередь виртуальная среда требует дополнительных ресурсов на обслуживание каждой виртуальной машины (ВМ), хоста и т. д. Потери могут быть довольно велики - до 20-30% ресурсов процессора (в зависимости от нагрузки), минимум 20% физической памяти (обычно больше) [4]. Поэтому виртуальные машины всегда работают медленнее, чем хост. Другое следствие требования дополнительных ресурсов системами виртуализации - невозможность использования множества ВМ на одном физическом устройстве. Обычно допустимое число ВМ составляет от 2-4 на обычной персональной машине и до 50 - на высокопроизводительных серверах. Кроме того, уплотнение информации на одном физическом оборудовании всегда ведет к повышению риска ее потери или компрометации; в случае «заражения» хоста и «прослушивания» его сетевых интерфейсов нарушитель может видеть всю информацию, передаваемую ВМ в сеть.

Однако, вследствие большой вычислительной мощности современного сервера экономически целесообразно его использование для решения комплексных задач, требующих значительных ресурсов, в частности решения задачи оптимального управления движением поездов на участке ж.д. значительной протяженности, а технологии виртуализации позволят наиболее эффективным образом распределить ресурс сервера для решения частных задач эксплуатации и безопасности движения поездов с разными техническими характеристиками. При этом следует иметь в виду, что вследствие большой протяженности участка ж.д., обслуживаемого ВК, взаимодействие между локомотивами и собственно ВК будет включать каналы радиосвязи, что делает возможным проведение информационных атак на систему с целью нарушения движения на ж.д. Это может привести к остановке движения на любом из направлений и большим экономическим потерям. Для снижения вероятности информационных атак ВК системы управления движением должен иметь эффективные средства защиты.

Диссертация посвящена актуальной теме разработки защищенного вычислительного комплекса системы управления движением поездов как составляющей единого информацион-

но-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 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 поезда 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 преиму-

щества графового представления состояний и дискретной модели системы позволяет имитировать динамический процесс распределения ресурса между приложениями в виртуальной инфраструктуре с учетом параллельных и асинхронных процессов их взаимодействия и рассчитывать количественные показатели работы системы, в том числе, при моделировании сценариев испльзования 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.

IV международная научно-практическая конференция «ИнтеллектТранс-2014», 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.

I. СТРУКТУРА ВЫЧИСЛИТЕЛЬНОГО КОМПЛЕКСА СИСТЕМЫ УПРАВЛЕНИЯ ДВИЖЕНИЕМ ПОЕЗДОВ

1.1. Разработка системы управления движением поездов для участка железной дороги с диспетчерской централизацией

1.1.1. Анализ структуры и функционирования системы диспетчерской централизации «Сетунь»

Система ДЦ «Сетунь» предназначена для контроля и управления движением на железнодорожных узлах и участках дорог при однопутном и многопутном движении поездов. Она включает в себя современную систему телемеханики с высокоскоростным обменом информацией между центральным распорядительным постом и линейными исполнительными пунктами (ЛП) и выполняет следующие функции непрерывного управления и контроля поездной ситуации на участке ж.д. [5, 6, 7] (рисунок 1.1):

- контроль и отображение состояния путевых объектов;
- непрерывный контроль поездной ситуации на участке в автоматическом режиме с учетом номеров, индексов поездов и других данных;
- передача штатных команд на ЛП;
- передача ответственных команд на ЛП;
- ведение системного журнала (технологического протокола);
- ведение графика исполненного движения поездов с его анализом;
- обмен информацией с компонентами ДЦ «Сетунь» соседних участков и с информационно - управляющими системами верхнего уровня (АСОУП) и едиными базами данных региональных центров управления перевозками.

Структура ДЦ имеет два взаимосвязанных уровня: аппаратуру центрального поста (ЦП), включающую в себя персональные ЭВМ, устройства ввода, отображения и регистрации информации, и аппаратуру ЛП, в состав которой входят управляющая ЭВМ, устройства ввода информации, интерфейс связи с устройствами автоматики на станциях и перегонах. Диспетчерская централизация может работать в автоматическом, полуавтоматическом и ручном режимах, осуществлять логическое закрытие путей, перегонов и стрелочных секций с блокированием соответствующих кнопок телеуправления.

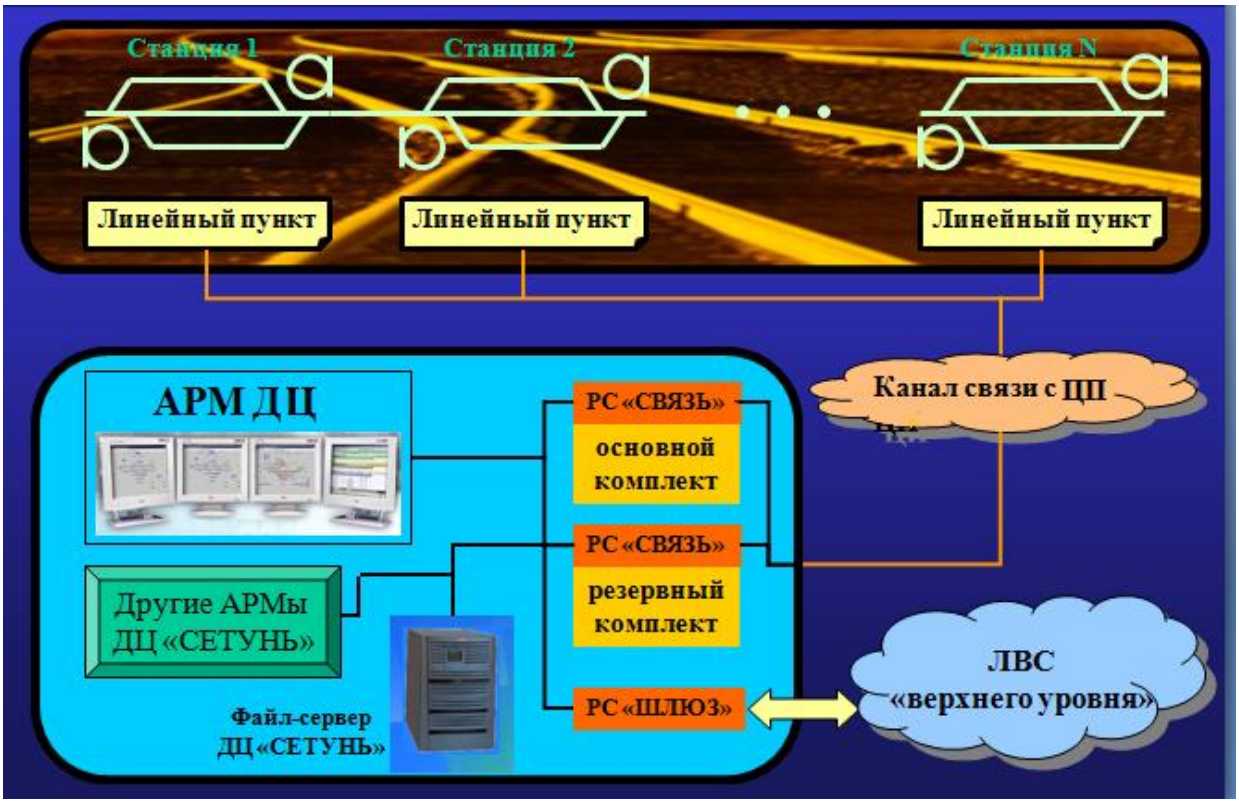


Рисунок 1.1. Схема взаимодействия элементов ДЦ «Сетунь»

На центральном посту ЦП располагаются автоматизированные рабочие места поездных диспетчеров АРМ ДЦ, сервер для хранения всей оперативной и справочной информации и компьютеры рабочих станций РС «Связь», объединенные в локальную вычислительную сеть (ЛВС). С помощью сервера осуществляется взаимодействие ДЦ с информационными системами. Рабочие станции «Связь» осуществляют взаимодействие с линейными пунктами ДЦ по линиям связи через встроенные в них модемы.

1.1.2. Анализ структуры и функционирования системы автоведения поездов

В последние десятилетия активно велись работы по созданию систем автоведения поездов и в настоящее времени ими оборудовано более пяти тысяч магистральных локомотивов и электропоездов (ВЛ10, ВЛ11, ВЛ80С, ВЛ85, 2ЭС5К 3ЭС5К, ЭП20, ТЭП70 и др.) [3]. Система автоведения - это аппаратно-вычислительный комплекс, который рассчитывает оптимальный алгоритм следования поезда. Результаты мониторинга движения пассажирских поездов показали, что доля поездов, отклонявшихся от энергооптимального графика при автоведении в 3–4 раза меньше, чем при ручном управлении, а экономия электроэнергии составляет в среднем от 3 до 10 % .

Системы автоведения могут работать в двух режимах:

• режим автоведения, когда система полностью контролирует движение поезда, управляя локомотивом;

• режим советчика, когда поездом управляет машинист, а система выводит на экран рекомендации по энергооптимальному алгоритму ведения поезда и отображает текущую информацию о режиме движения.

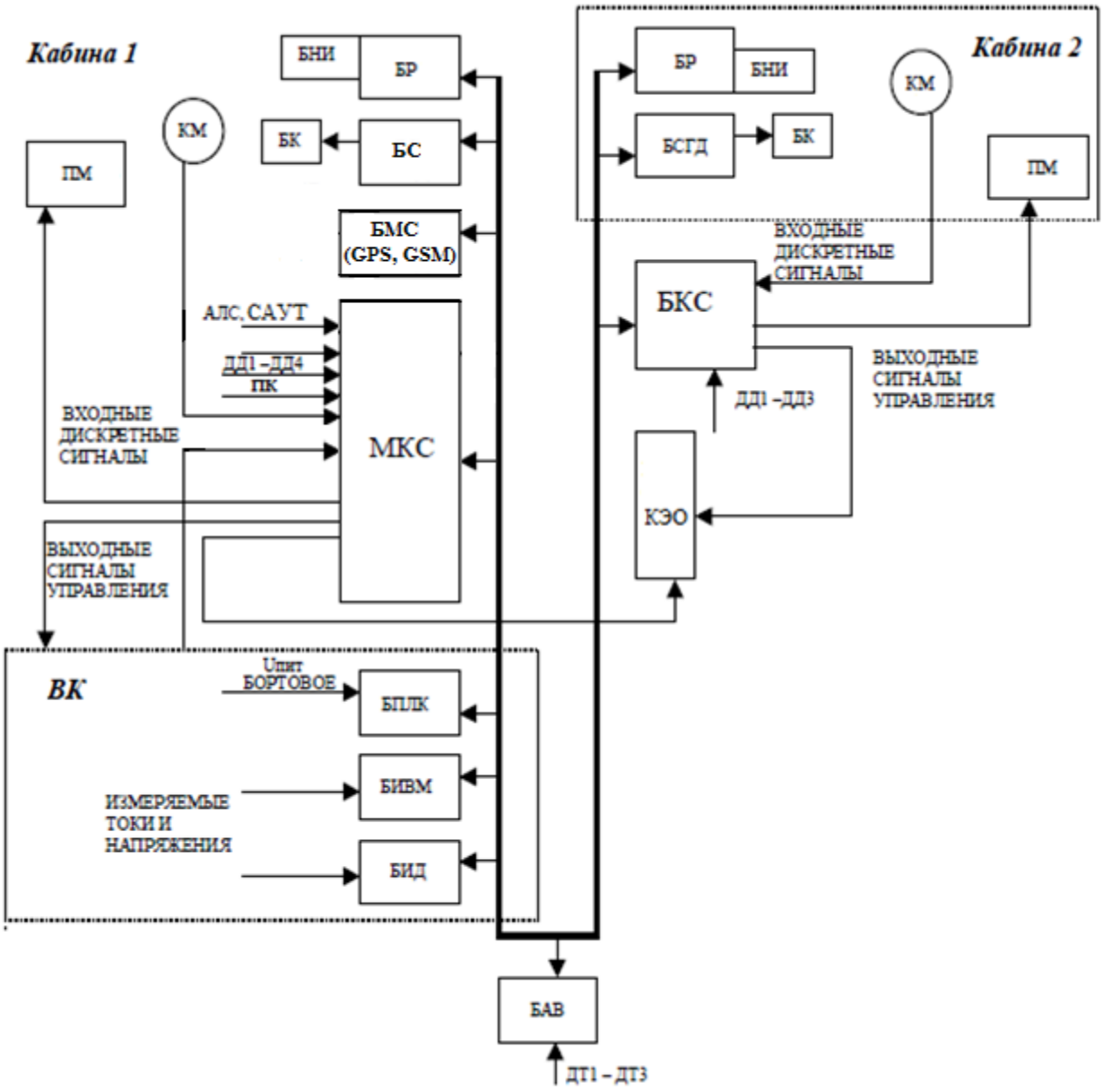
Примером системы автоведения является универсальная система автоведения магистрального тепловоза УСАВП-Т [8,9], которая обеспечивает движение поезда на заданном участке с соблюдением установленных ограничений скорости по сигналам автоматической локомотивной сигнализации (АЛС) в соответствии с оптимальным графиком движения. В системном блоке УСАВП-Т хранится база постоянных данных с электронной картой участка следования. Составляющей системы автоведения является подсистема регистрации параметров движения тепловоза РПДА-ТМ, выполняющая сбор, обработку, регистрацию данных о текущей координате, расходе топлива и режимах работы систем тепловоза на съемный носитель, а также их передачу по цифровому радиоканалу (рисунок 1.2) [3]. Питание УСАВП-Т осуществляется от блока питания БПЛК; блоки системы объединяются в одну общую CAN-сеть. Запись информации о параметрах движения осуществляется блоком регистрации (БР) на съемный накопитель информации (БНИ). Открытая структура УСАВП-Т позволила расширить ее возможности путем применения подсистем беспроводного приема данных GPRS и спутниковой навигации.

Блок БС является центральным блоком системы автоведения. В распределенной CAN-сети он выполняет функции шлюза внутренней сети, к которому подключаются остальные блоки системы, а также системы автоматического управления торможением САУТ и комплексного локомотивного устройства безопасности КЛУБ-У [10, 11, 12].

В состав блока входят источник стабилизированного напряжения 48В, два процессорных модуля CPU686 с двумя CAN-интерфейсами каждый и мастер-модуль, реализующий сетевые функции. Блок БС представляет собой высокопроизводительный компьютер, предназначенный для реализации алгоритмов управления тепловозом, вывода визуальной и речевой информации, связи по каналу CAN с напольными приборами безопасности. Он имеет постоянную память, в которую заносят информацию об участке обслуживания, тяговые характеристики тепловоза и расписание движения. Кроме того, часть памяти зарезервирована для хранения переменной (изменяемой) информации: номер поезда, количество вагонов, мест временных ограничений скорости и т.п. Эта информация при необходимости может быть оперативно изменена машинистом.

Модуль коммутации и сопряжения (МКС) осуществляет управление тепловозом на режимах тяги и торможения, контролирует состояния входных и выходных сигналов. Блок МКС обрабатывает и передает в общую информационную шину данных (ИШД) информацию о

входных дискретных и аналоговых сигналах, в том числе о состоянии цепей управления и регулирования, сигнализации тепловоза, тормозной системы, системах дизеля.



КМ- контроллер машиниста; АЛС – автоматическая локомотивная сигнализация; МКС – модуль коммутации и сопряжения; БС – блок процессорный; БМС – блок мобильной связи; БПЛК – блок питания локомотивный; БИВМ – блок измерения высоковольтный модульный; БИД – блок измерения диагностический; БКС – блок коммутации и сопряжения; БНИ – блок накопления информации; БАВ – блок аналогового ввода; БК - бортовой компьютер; БР – блок регистрации; БСГД - блок процессорный с графическим дисплеем; ВК – высоковольтная камера; КЭО - электропневматический клапан тепловоза; ПМ – пневмомодуль; ДД1-ДД4 – датчики давления тормозной системы; ДТ1 – ДТ3 – датчики топливной системы и температуры наружного воздуха; пк – позиция контроллера машиниста

Рисунок 1.2. Структурная блок-схема системы УСАВП-Т

Блок коммутации и сопряжения (БКС) выполняет управление тепловозом из второй кабины, обрабатывает и передает в ИШД информацию о входных дискретных и аналоговых сигналах.

Блок измерения высоковольтный (БИВМ) предназначен для измерения напряжения и тока тягового генератора, токов тяговых двигателей, расчета мощности тягового генератора, а также передачи цифровой информации в ИШД.

Диагностический блок (БИД) предназначен для измерения напряжения и тока во вспомогательных электрических цепях тепловоза, а блок аналогового ввода (БАВ) – для подключения каналов датчиков температуры; показания обоих блоков в виде цифровой информации передаются в ИШД.

Блок мобильной связи (БМС) передает информацию с тепловоза на удаленное расстояние по каналам спутниковой связи и определяет местоположение и скорость тепловоза по сигналам спутниковой системы навигации GPS.

Для взаимодействия блоков системы УСАВП-Т в ней предусмотрены два канала обмена информацией (порта интерфейса CAN), один из которых является основным, связывающим в единую сеть все блоки УСАВП-Т, а второй посредством блока «Шлюз-CAN» используется для подключения к комплексному локомотивному устройству безопасности КЛУБ-У. Загрузка ПО в блок БС осуществляется по каналу RS232. Для записи и хранения зарегистрированной информации используется переносной блок накопления информации (картридж), позволяющий зафиксировать данные в течение 24 часов работы.

Система непрерывно контролирует правильность работы аппаратуры, осуществляя при этом функцию самодиагностики по следующим параметрам:

- правильность обмена информацией по внутреннему каналу связи CAN;
- диагностику работы шины CAN;
- правильность срабатывания электронных управляющих ключей.

Объем памяти картриджа БНИ – 64 Мб со скоростью обмена до 1 Мбит/с и временем стирания не более 1с. [10]; объем встроенной энергонезависимой памяти блока БР– 128 Мб.

Система УСАВП-Т снимает с датчиков и аппаратов каждой секции тепловоза более 50 дискретных и аналоговых сигналов: для величин, определяющих безаварийность работы систем – с интервалом времени 10 мс; для величин, определяющих режим управления тепловозом – с интервалом времени 100 мс [13].

Кроме того, для диагностирования состояния тепловоза она измеряет и сохраняет 65 параметров режимов работы систем тепловоза (на картридж через подсистему РПДА).

1.1.3. Структура вычислительного комплекса системы управления движением поездов

Эффективность системы централизованного управления автоведением поездов на линии метрополитена подтверждена в [14,15,16,17]. Для реализации оптимального управления поездом метрополитена система использует информацию о протяженности и профилях участков линии, существующих ограничениях и расчетной тяговой характеристике подвижного состава. Подобные системы позволяет осуществлять централизованное управление поездами на линии, минимизируя энергопотребление и время хода, но не учитывают фактических текущих характеристик подвижного состава и их возможность реализовать оптимальное управление. Кроме того, данная система строится на использовании графика движения поездов, который в условиях метрополитена не меняется и выполняется строго.

На линиях ж.д. график движения поездов постоянно корректируется с учетом выполнения необходимого перевозочного процесса. Кроме того, в процессе эксплуатации тяговые характеристики локомотивов могут меняться, например, в зависимости от погодных условий (снижение коэффициента сцепления колеса с рельсом, увеличение отбора мощности на привод вспомогательного оборудования) или отказа отдельных систем (например, переход на систему аварийного возбуждения тягового генератора). Организовать оптимальное управление работой участка железной дороги без полной информации о поездной ситуации и текущих характеристик локомотивов как тяговых единиц – невозможно.

В [18] предлагается система управления движением поездов, которая включает в себя центральный пункт управления, распределенные ЛП с блоками устройств ДЦ и магистральную линию связи, соединенную с центральным пунктом. На каждом из локомотивов предполагается наличие бортовой ЭВМ с антенным блоком, а на центральном пункте управления и всех ЛП - блоков стационарных радиомодемов цифрового радиоканала связи. В постоянной энергонезависимой памяти блока бортовой ЭВМ каждого локомотива записана информация о путевом развитии всех участков диспетчерского круга вместе с соответствующими им вариантами возможных маршрутов передвижения локомотивов. На центральном пункте стационарная ЭВМ должна быть соединена через спутниковую связь с бортовыми антеннами локомотивов.

Данная система управления предполагает более развитую и гибкую ДЦ, однако и здесь каждый локомотив имеет собственную систему автоведения, которая не может определять оптимальное управление по условиям поездной ситуации на всем участке ж.д. с учетом технического состояния локомотива.

С целью интеграции системы автоведения локомотива в систему ДЦ «Сетунь» разработана структура системы, содержащей дополнительный вычислительный комплекс (ВК), который позволяет осуществлять текущее взаимодействие обеих систем при рациональном ис-

пользовании вычислительных ресурсов (рисунок 1.3). На центральном посту располагаются рабочие места диспетчеров АРМ ДЦ, сервер для хранения оперативной и справочной информации и компьютеры рабочих станций РС «Связь», объединенные в локальную вычислительную сеть ЛВС. Сервер осуществляет взаимодействие ДЦ с информационными системами, а рабочие станции «Связь» - с линейными пунктами ЛП по линиям связи через встроенные модемы.

Вычислительный комплекс принимает, распределяет, обрабатывает и передает оперативную информацию между локальной вычислительной сетью (ЛВС) ДЦ и системами автоведения локомотивов, находящихся на участке ж.д., контролируемом ДЦ. При этом ВК выполняет функции:

1. шлюза – для получения входной информации от ЛВС ДЦ, системы автоведения локомотива, комплекса локомотивных устройств обеспечения безопасности КЛУБ, а также передачи выходной информации соответствующим системам;
2. формирование базы данных о характеристиках участка железной дороги, обслуживаемом данной системой ДЦ (профили и длины соответствующих участков), а также о постоянных и временных ограничениях скорости, текущей координате поезда;
3. формирование базы данных о параметрах поезда (тип поезда, вес поезда, ограничения режимов движения, число локомотивов, число вагонов поезда);
4. формирование базы данных кассеты регистрации комплексного устройства КЛУБ;
5. формирование базы данных о срабатывании систем защиты локомотива;
6. формирование базы данных о значениях текущих параметров режимов работы локомотива; расчет прогнозируемой надежности систем и агрегатов локомотива;
7. расчет мощности, которая может быть реализована локомотивом;
8. решение задачи оптимального управления локомотивом;
9. мониторинг ВК.

Вся информация, сосредоточенная на ВК, должна быть доступна для сервера ДЦ «Сетунь» или передаваться на него в режиме реального времени. Аналогичным образом вся оперативная информация, необходимая для управления локомотивом должна передаваться на его бортовой компьютер. Взаимодействие системы автоведения локомотивов с ВК предлагается осуществлять по каналам спутниковой связи посредством блоков мобильной связи БМС и AIRT (тепловоза) – AIR ВК, а с сервером ДЦ – по локальной сети ETHERNET.

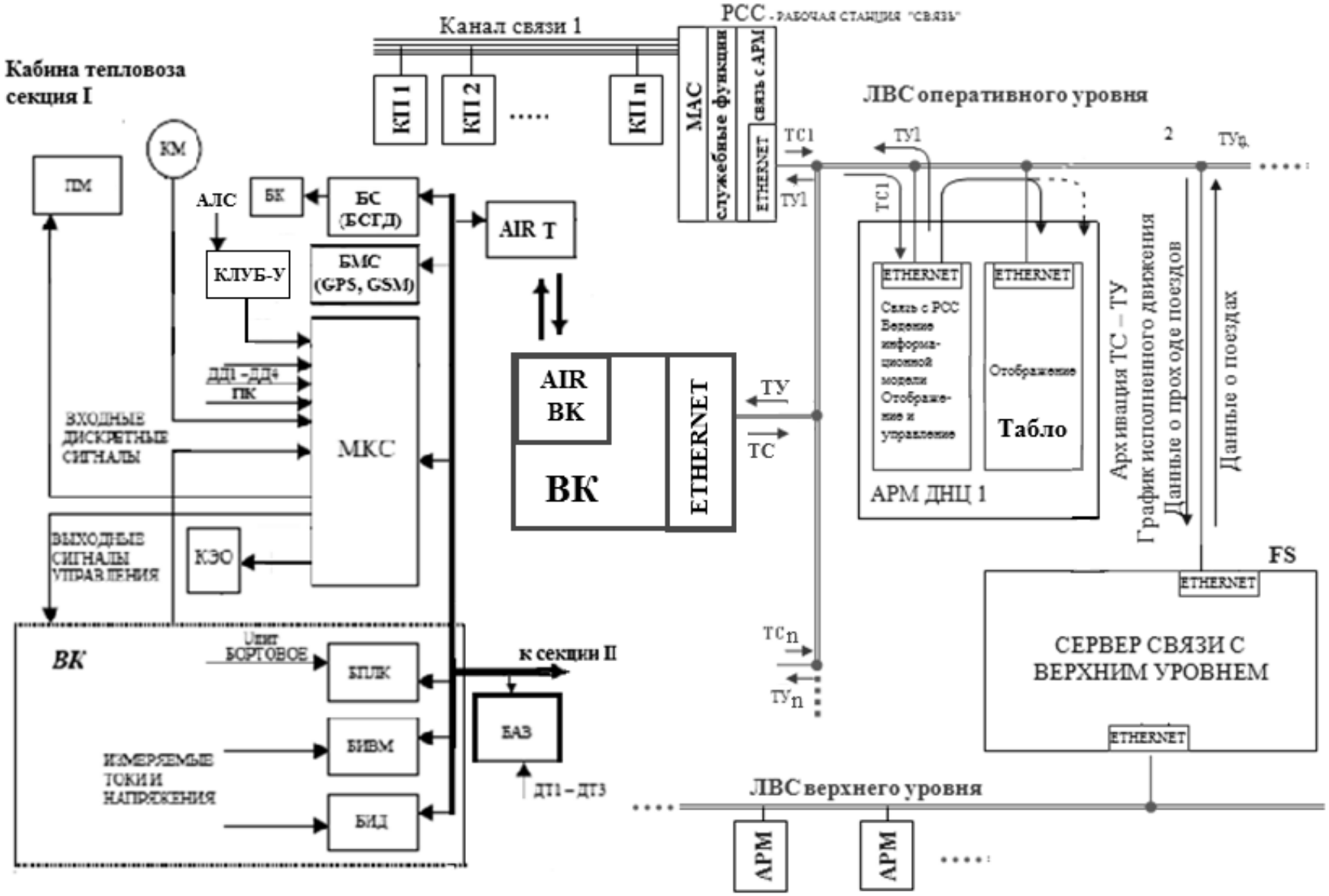


Рисунок 1.3. Структура взаимодействия системы автоведения поезда и ВК на базе системы диспетчерской централизации «Сетунь»

Информация, передаваемая на ВК, должна позволять управлять каждым поездом по оптимальному алгоритму с учетом поездной ситуации на всем участке ДЦ (а не только по показаниям ближайших напольных устройств сигнализации), что дает возможность минимизировать энергозатраты, диагностировать состояние каждого локомотива, находящегося в зоне действия ДЦ и прогнозировать его возможные отказы, контролировать состояние машиниста.

Функции, передаваемые ВК, дают возможность отказаться от части блоков системы автоведения. В частности, из системы автоведения локомотива могут быть исключены блоки накопления информации БНИ и регистрации БР.

Внедрение комплексной системы управления движением поездов позволит повысить пропускную способность ж.д. за счет создания единого центра управления движением на участке ДЦ с возможностью расчета текущего оптимального графика движения с учетом поездной ситуации и фактических характеристик подвижного состава. Практическая реализация такого графика движения обеспечит не только снижение времени следования поезда и его энергозатраты, но и повысит эффективность использования подвижного состава за счет рациональной организации работы службы ремонта.

С целью расчета необходимого ресурса ВК, как основного элемента системы управления движением, были обобщены сводные данные, необходимые для работы системы автоведения поезда. Поскольку энергетическая система тепловоза имеет более сложную структуру из-за наличия дизеля и его вспомогательных систем, совместная работа которых и определяет мощность, передаваемую на тягу, расчет технических и аппаратных ресурсов ВК выполнялся исходя из алгоритма функционирования системы автоведения тепловоза 2ТЭ116 [13] и признаков работы его систем защит и управления вспомогательными агрегатами [19, 20] (таблица 1.1).

Таблица 1.1

Величины, передаваемые ВК от одной секции тепловоза

Система тепловоза и период измерения контролируемых величин	Аналоговые сигналы	Дискретные сигналы
1	2	3
Система защиты электрического оборудования Т1= 10 мс[13]	Напряжение генератора, ток генератора, напряжение стартер-генератора, ток 1-6 тяговых двигателей; перемещение реек	Признак Внешнее короткое замыкание - от реле максимального тока РМ1, внутреннее короткое замыкание

1	2	3
	топливного насоса высокого давления дизеля, напряжение на выходе индуктивного датчика, ток возбуждения тяговых двигателей в тормозном режиме	– от реле РМ2; пробой изоляции в цепи высокого напряжения – от реле заземления РЗ; открытие дверей высоковольтной камеры – от блокировочных контактов БД1, БД2, БУ; превышение допустимого тока торможения – от реле РМТ; признак вентиляторов тормозных резисторов – от реле РТП
Система управления скоростью Т2=100 мс [13]	Текущее время, частота вращения вала дизеля, позиция контроллера в тяговом режиме; позиция контроллера в тормозном режиме; положение реверсора; давление в уравнительном резервуаре 1-ой и 2-ой кабины, давление в тормозном цилиндре; давление в тормозной магистрали; управление ШИМ 1-6 тяговых двигателей; управление ШИМ стартер-генератоа; частота вращения 1-6 колесной пары; линейная скорость локомотива	Признак: Режим боксования или юза – от промежуточных реле РУ11, РУ17; включение нагрузки – от реле включения тяги РУ5;обрыв обмоток электродвигателей – от реле РОП; включение возбуждения генератора – от контактора КВ; включение двигателя компрессора – от контактора КДК; включение ослабления возбуждения тяговых двигателей – от контакторов ВШ1, ВШ2; включение электромагнитов регулятора дизеля– от электромагнитов МР1-МР4; аварийное возбуждения стартер-генератора – от реле РУ16; включение режима электрического торможения – от промежуточного реле РТ4; вентиль блокировки пневматического тормоза РТ1; вентиль жалюзи тормозного режима ОТ

1	2	3
		Включение тумблеров: управления переходами УП; аварийного возбуждения генератора АП; отключения моторов ОМ1-М6; включение электрического торможения ОТ
Система диагностирования состояния дизеля Т2=100 мс	Температура воды дизеля и масла дизеля – от электрических датчиков ДВО, ДВ1, ДВ2, ДМО, ДМ1, ДМ2; давление масла в системе дизеля – от реле РДМ1; температура наддувочного воздуха – от датчика температуры; температура топлива – от датчика температуры	Признак: Пониженный уровень воды в расширительном баке - от датчика уровня; пробой газов в картер дизеля - от электропневматического вентиля ВА; перегрев воды или масла - от датчиков-реле ТРВ1, ТРВ2; положение жалюзи и включение вентиляторов дизеля – от электропневматических вентилей ВП1- ВП6; тепловая защита тормозных резисторов РТП
Система безопасности движения Т2=100 мс[14]	Принимаемые сигналы устройства КЛУБ: табельный номер машиниста; номер поезда; длина состава в осях; длина состава в условных вагонах; номер локомотива или ведущей секции многосекционного локомотива; масса поезда; значение установленной на данной дороге максимальной скорости движения локомотива; значение скорости движения на сигнал «КЖ» БИЛ-У; расчетная длина блок-участка; диаметр бандажа	Признак устройства КЛУБ: тип локомотива; категория поезда; изменение координаты пути (возрастание или убывание); состояние рукояток бдительности; включение компрессоров; включение генераторов управления; включение питания электромагнитов ЭПК; состояние ключа ЭПК: режим ”ЭПТ” - контроль цепи; режим ”ЭПТ” - перекрыша; режим ”ЭПТ” - торможение; включение тифона; включение свистка; конфигурация

1	2	3
	1-ой и 2-ой колесных пар (на которых установлены датчики измерения пути и скорости); число зубцов датчика измерения пути и скорости; значение допустимой скорости движения на сигнал «З» БИЛ-У; пробег локомотива; показание светофора; количество свободных блок-участков; длинна блок участка; допустимая и фактическая скорость; железнодорожная координата локомотива по сигналам датчиков пути и скорости и от навигационной спутниковой системы GPS/ГЛОНАСС; текущее время; текущая дата; фактическое направление движения; расстояние до цели; вид цели; допустимая скорость движения на «Зеленый»; контролируемая скорость движения на «Желтый»;уровень бодрствования машиниста; позиция контроллера машиниста; код рукоятки / клавиши; категория поезда; категория по давлению в тормозной магистрали; код серии локомотива	установки датчиков измерения пути и скорости;активность радиоканала; сигнал от ДЦ о принудительной (экстренной) остановке поезда

С учетом разноплановости задач, решаемых ВК, его структуру целесообразно реализовать с использованием средств виртуализации, предусмотрев возможность развертывания до-

полнительной ВМ в случае необходимости расширения функционала ВК или потери любой из существующих ВМ. Такая структура ВК позволяет:

- разделить задачи организации движения, управления локомотивами, контроля действий машинистов и диагностирования состояния локомотивов с целью разграничения доступа к информации и повышения безопасности движения;

- снизить вероятность потери информации;

- эффективно использовать ресурсы хоста как вычислительной среды.

В соответствии с решаемыми задачами ВК должен иметь структуру, состоящую из десяти ВМ (рисунок 1.4).

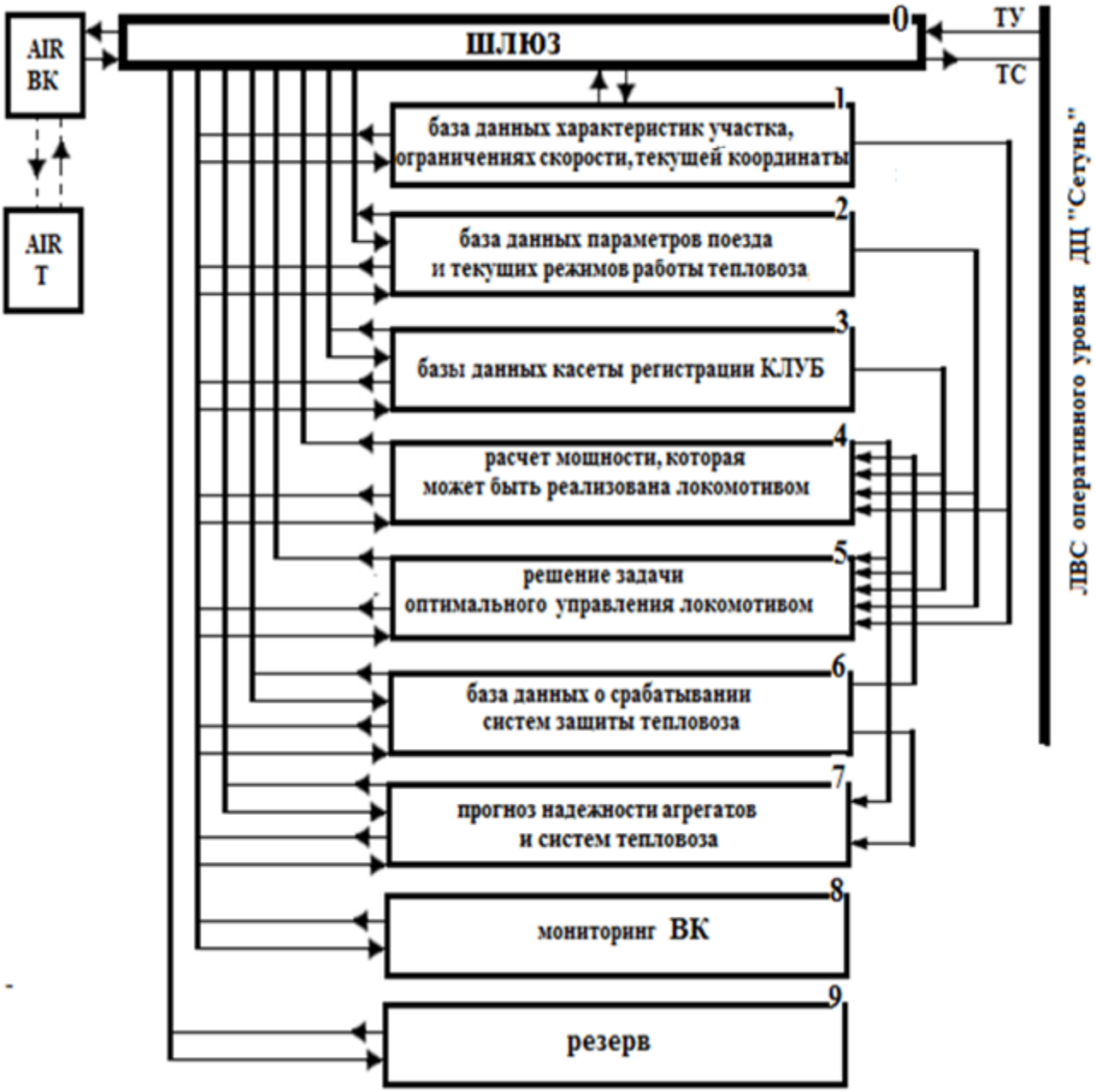


Рисунок 1.4. Архитектура ВК системы управления движением поездов на участке ДЦ «Сетунь» ж.д.

При этом ВК, являющийся элементом информационной сети, связанной с безопасностью жизнедеятельности, должен быть оборудован системой защиты. Приоритетный тип защиты должен выбираться по характеристикам ее эффективности с учетом структуры ВК и возможных видов атак на него, приводящих к наиболее тяжелым последствиям (блокирование участка железной дороги или крушение на нем).

Для расчета оптимального алгоритма управления локомотивом ВК должен иметь полную информацию о поездной ситуации на участке движения. Поэтому по запросу ему должна передаваться информация о сигналах объектов контроля и объектов управления на участке. В соответствии с Руководством на программное обеспечение автоматизированного рабочего места поездного диспетчера ДЦ «Сетунь» в пределах диспетчерского круга должно быть не более 20 рабочих станций «Связь»; при этом емкость канала управления (ТУ) составляет 1120 объектов, а емкость канала контроля (ТС) – 1380 объектов [21,22]. Каждый сигнал управления представляется 19 импульсами, а каждый сигнал контроля – 20 импульсами. Таким образом, по запросу ВК от ДЦ ему должна передаваться информация о 2500 аналоговых сигналах с периодом Т2=100 мс.

1.2. Структура и классификация систем виртуализации

В настоящее время используется несколько подходов к принципам виртуализации, отличающихся между собой уровнем абстрагирования создаваемой ВМ от хоста. В соответствии с этими принципами системы виртуализации классифицируются по двум основным реализациям: виртуализация платформ и виртуализация ресурсов [23] (рисунок 1.5).

Продуктом принципа виртуализации платформ являются ВМ, функционирующие на хосте. Существуют различные методы обеспечения взаимодействия виртуальных платформ и хоста, отличающиеся степенью абстрагирования гостевой операционной системы (ОС) от программно-аппаратных средств хоста.

1. Полная программная эмуляция, преимуществом которой является возможность виртуализировать различные архитектуры, т.к. ВМ полностью абстрагирует все аппаратное обеспечение при сохранении гостевой операционной системы в неизменном виде. Основной недостаток метода полной эмуляции - низкое быстродействие гостевой системы.

Примерами продуктов программной эмуляции являются системы: Bochs, PearPC, QEMU (без ускорения), Hercules Emulator.

2. Нативная виртуализация, принципиальной особенностью которой является наличие гипервизора, что позволяет гостевой системе напрямую обращаться к ресурсам хоста. Это значительно увеличивает быстродействие виртуальной платформы, приближая его к быстродействию физической системы, и позволяет ВМ эмулировать лишь необходимое количе-

ство аппаратного обеспечения. Существенным недостатком нативной виртуализации является требования идентичности архитектуры всех гостевых систем и хоста, что ограничивает возможности эмулирования различных ВМ.

Примерами продуктов нативной виртуализации являются системы: VMware, Virtual Iron, Virtual PC, VirtualBox, Parallels Desktop и другие.

Рисунок 1.5. Классификация систем виртуализации

3. Виртуализация адресного пространства, преимуществом которого является отсутствие необходимости создания изолированных гостевых систем, за счет чего происходит экономия вычислительных ресурсов и повышается быстродействие ВМ по сравнению с методом нативной виртуализацией. Однако замена ВМ изолированным адресным пространством повышает уязвимость системы в целом.

Примером виртуализации адресного пространства является режим User-mode Linux (UML).

4. Паравиртуализация. Особенностью этого метода является использование программного интерфейса API для взаимодействия гостевых операционных систем (ОС) с хостом. При этом паравиртуализация требует модификации кода гостевой системы, что значительно усложняет работу с ней и исключает возможность использования операционных систем с закрытым исходным кодом.

В настоящее время паравиртуализация применяется в системах XenSource и Virtual Iron.

5. Виртуализация уровня операционной системы. Основным преимуществом данного метода является обеспечение быстродействия гостевых систем соответствующего быстродействию хоста, что выделяет его среди всех систем виртуализации. Поэтому основное применение он нашел при организации систем хостинга, требующих специфической архитектуры хоста.

Однако при таком подходе все гостевые системы разделяют ядро хостовой ОС, а каждая ВМ является лишь программным окружением для изолированных приложений, что повышает уязвимость системы в целом.

Примерами виртуализации уровня ОС являются: Linux-VServer, Virtuozzo, OpenVZ, Solaris Containers и FreeBSD Jails.

6. Виртуализация уровня приложений используется для частичной изоляции отдельного приложения от окружающей его ОС, что позволяет ему свободно мигрировать между однотипными операционными системами. Такой метод виртуализации исключает несовместимости и конфликты между приложением и ОС хоста и требует меньшего объема ресурсов по сравнению с эмуляцией всей ОС.

Виртуализация ресурса предполагает абстрагирование ряда операций над виртуализируемым ресурсом от физической реализации хоста и разграничение доступа к разделяемым ресурсам. В зависимости от назначения систему виртуализации ресурсов можно реализовать тремя основными методами.

1. Агрегация компонентов позволяет объединять множество однотипных аппаратных объектов в единый логический объект с общим набором интерфейсов. Агрегация компонентов обеспечивает удобство работы с большим числом отдельных объектов, скрывая реализацию этого процесса, но имеет низкий уровень контроля за процессом взаимодействия аппаратных объектов, что может привести к потере информации, искажению трафика и т.д.

Примерами использования метода агрегации компонентов являются RAID-массивы, NAT и VPN, кластеры, позволяющие создавать виртуальные пространства сетевых имен и адресов, и т.д.

2. Разделение ресурсов - метод виртуализации, обратный агрегации компонентов. Пре-

имуществом данного метода является упрощение процедуры разграничения доступа к логическим объектам и их администрирование, что повышает безопасность системы в целом, а основным недостатком - низкий уровень контроля за взаимодействием отдельных логических объектов и разделяемой среды.

3. Инкапсуляция. Данный метод виртуализации используется для скрытия особенностей реализации используемого объекта и упрощения процесса взаимодействия с ним. Преимуществом инкапсуляции является оптимизация интерфейса и упрощение программного обеспечения, а недостатком - снижение, по сравнению с исходными, уровня контроля за взаимодействием виртуализируемых систем и быстродействия.

Среди различных видов виртуализации платформ наибольшее распространение на практике получила нативная виртуализация, поскольку оптимальным образом позволяет сочетать требования к ресурсам, абстрагирование ВМ от хоста и быстродействие. Кроме того, решению задач информационной безопасности больше соответствует виртуализация платформ, т.к. обеспечивает более высокий уровень абстрагирования отдельных логических объектов и разграничения доступа к ним, чем виртуализация ресурсов.

Возможности нативной виртуализации определяются в основном характеристиками гипервизора. Гипервизоры можно классифицировать:

- по методу функционирования [24]: гипервизор нативный, запускаемый на аппаратном обеспечении хоста; гипервизор хостовый, запускаемый в ОС хоста; гипервизор гибридный, включающий сервисную хостовую ОС;

-по архитектуре [25]: гипервизор монолитный; гипервизор микроядерный.

Нативный гипервизор функционирует непосредственно на аппаратном обеспечении хоста и управляет его аппаратным обеспечением. Гостевые ОС, запущенные на ВМ, располагаются уровнем выше (рисунок 1.6) [24]. Нативные гипервизоры используются во многих решениях Enterprise-класса: Microsoft Hyper-V, VMware ESX Server, Citrix Xen Server .

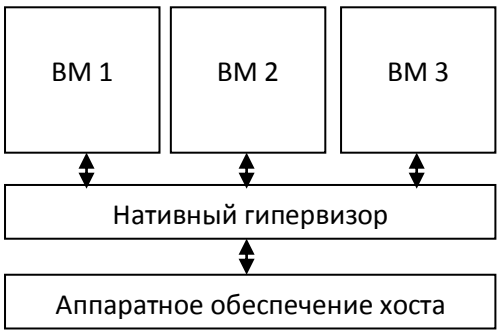


Рисунок 1.6. Блок-схема функционирования нативного гипервизора

Хостовый гипервизор функционирует внутри хостовой ОС, поэтому и ВМ запускается в пользовательском пространстве хостовой ОС (рисунок 1.7.). Это снижает ее производительность по сравнению с ВМ, использующей нативный гипервизор. Примерами использования хостовых гипервизоров являются MS Virtual Server и VMware Server, MS VirtualPC, VMware Workstation и Oracle Virtual Box.

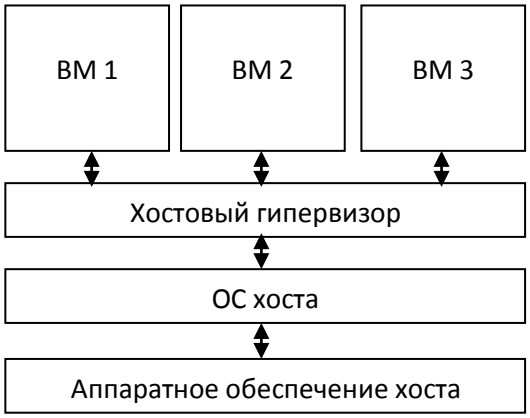


Рисунок 1.7. Блок-схема функционирования хостового гипервизора

Гибридный гипервизор объединяет функции нативного и хостового гипервизоров (рисунок 1.8). В нем управление аппаратными средствами выполняются тонким гипервизором и специальной сервисной ОС, работающей под управлением тонкого гипервизора. Обычно гипервизор управляет напрямую процессором и памятью компьютера, а ВМ работают с остальными аппаратными компонентами через сервисную ОС.

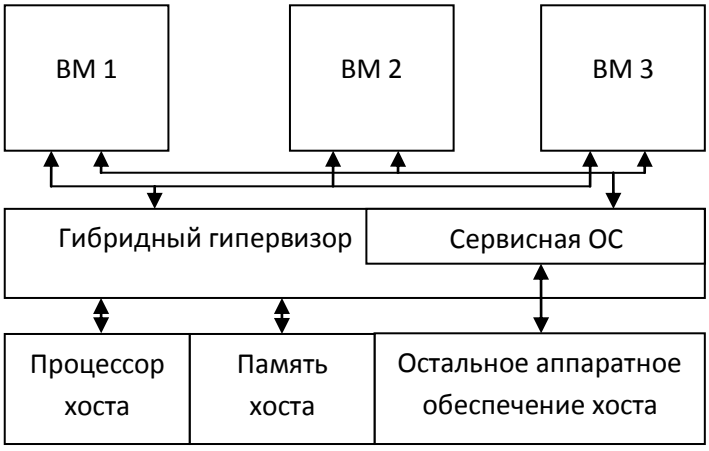


Рисунок 1.8. Структурная схема функционирования гибридного гипервизора

Гипервизор с архитектурой монолитного ядра является автономной системой, вклю-

чающей, в том числе, и драйверы для работы с оборудованием. Он обеспечивает высокую степень изоляции ВМ, независимость от ПО сторонних разработчиков и надежность системы в целом. Примером такого гипервизора является продукция компании VMware**;** ее ESX Server состоит из собственно гипервизора, среды исполнения (ESXi) и сервисной консоли на базе ядра Linux. Недостатком такого гипервизора является сложность исполнения полностью автономной системы, в частности, необходимость создания и развития собственной модели драйверов.

При реализации гипервизора с архитектурой микроядра его функции разделяются по разным модулям и уровням разным модулям и уровням. Сам гипервизор, как правило, выполняет функции управления памятью и процессором, а для взаимодействия с внешними устройствами используется хостовая ОС. Примером тому является Hyper-V, разработанный компанией Microsoft. Гипервизор такого типа наиболее эффективен при большой вычислительной нагрузке, т.к. он позволяет использовать оригинальные драйвера входящие в состав ОС.

1.3. Анализ уязвимостей виртуальной компьютерной сети и средств ее защиты

Для систематизации угроз безопасности применительно к ИС используется таксономия, как теория классификации и систематизации сложно организованных областей деятельности [26, 27, 28, 29, 30, 31, 32, 33]. В [26] отмечается, что проблема обеспечения безопасности входит в число наиболее сложных при создании любых сетей, а наилучшие результаты в решении этих проблем были достигнуты благодаря решению задач по таксономии в этой области. В качестве примера в [27] приводится новая редакция стандарта США «Common Criteria for Information Technology Security Evaluation», где приведены принципы для решения задач таксономии угроз безопасности ИС [34].

В [26, 35, 36, 37, 38, 39, 40] приведен системный анализ угроз безопасности. Применительно к виртуальной инфраструктуре (ВИ) угрозы во многом идентичны угрозам физической инфраструктуре, но имеют ряд специфических возможностей для реализации атак:

1. Угроза атаки на сервер виртуализации и средства управления ВИ [41]. Этот вид атаки реализуется за счет несанкционированного доступа к аппаратному обеспечению, средствам администрирования или использования уязвимостей ПО виртуализации.

Угроза атаки на сервер виртуализации может возникать как вне ВИ, так и внутри нее. При появлении в виртуальной среде «UnmanagedVM» (давно не обновлявшихся ВМ), содержащих многочисленные уязвимости, уровень безопасности среды резко снижается. Используя «UnmanagedVM», нарушитель может получить доступ к управляющим элементам ВИ или использовать уязвимости в системе виртуализации. Кроме того, реализация подобной атаки позволяет легко удалить "следы" компрометации. Для этого достаточно вернуть ВМ к исходно-

му состоянию из резервной копии (snapshoot) [42]. Поэтому бесконтрольное разрастание числа ВМ (Virtual Sprawl) в силу простоты их создания приводит к снижению уровня безопасности ВИ, особенно при отсутствии должного уровня администрирования.

2. Угроза атаки на виртуальную платформу со стороны скомпрометированного хоста или гипервизора. Данная атака может быть проведена, если нарушитель получает доступ к среде виртуализации. При этом операционная среда ВМ вместе с традиционными системами защиты информации оказываются полностью скомпрометированными.

3. Угроза атаки на диск ВМ. Данный тип атаки реализуется за счет несанкционированного доступа к системе хранения данных или сети передачи данных через скомпрометированные элементы виртуальной или физической инфраструктуры.

4. Угроза атаки на виртуальную машину с другой виртуальной машины. Этот тип атаки может быть проведен за счет использования трафика, передающегося между ВМ одной платформы, который зачастую не покидает пределов хоста. Такой алгоритм передачи информации не позволяет использовать внешние межсетевые экраны и другие средства разграничения и фильтрации трафика, что упрощает проведение атак между ВМ, расположенными на одном хосте.

5. Угроза атаки на виртуальную среду в результате отсутствия физической защиты серверов виртуализации, хостов, и сетевого оборудования.

Среди уязвимостей для проведения атаки в обход используемых механизмов защиты лидируют [43]:

- переполнение буфера;

-инжекция SQL-команд;

-вирусные атаки.

Успешному проведению атак данного типа способствуют ошибки в ПО и некорректные настройки механизмов защиты. По данным Web Application Security Consortium (WASC) около 49%Web-приложений содержат уязвимости высокой степени риска (Urgent и Critical), обнаруженные при автоматическом сканировании системы [44]. Однако при детальной ручной и автоматизированной оценке методом «белого ящика» вероятность обнаружения уязвимостей высокой степени риска достигает 80-90%. Причиной большинства типов уязвимости может быть ошибка в исполняемом бинарном файле.

По данным различных источников основными условиями, которые способствуют нарушению безопасности информации, являются следующие [45]:

- разглашение (излишняя болтливость сотрудников) – 32%;

- несанкционированный доступ путем подкупа и склонения к сотрудничеству со стороны конкурентов и преступных группировок – 24%;

- отсутствие надлежащего контроля и условий обеспечения ИБ– 14%;

- традиционный обмен производственным опытом – 12%;

- бесконтрольное использование ИС– 10%;

- наличие предпосылок возникновения среди сотрудников конфликтных ситуаций - 8%.

Виртуальная инфраструктура обладает таким же ограниченным уровнем защиты, что и физическая, и при этом имеет дополнительные уязвимости:

- классические средства обеспечения ИБ не способны обнаружить компрометацию данных на ВМ со стороны гипервизора; при этом гипервизор имеет доступ ко всем информационным ресурсам, расположенным на ВМ;

- средства управления ВИ могут являться самостоятельными объектами атак; доступ нарушителя к ним позволяет получить контроль над гипервизорами, ВМ и расположенными на них данными;

- возможность создания в конфигурации ВМ неразрешенных устройств (в том числе хранилищ данных), на которых нарушитель может выполнять копирование конфиденциальной информации;

- ВИ обладает повышенной уязвимостью со стороны средств администрирования, имеющих доступ к информационным ресурсам, минуя существующую политику ИБ;

- сетевые хранилища жестких дисков гостевых машин требуют самостоятельных средств защиты;

- поскольку традиционные межсетевые экраны не контролируют трафик внутри сервера виртуализации, компрометация одной ВМ может привести к компрометации прочих ВМ, расположенных на этом сервере;

- требование к скорости передачи информации между серверами виртуализации делает нецелесообразным установку средств защиты на служебных каналах передачи данных, что повышает уязвимость инфраструктуры в целом.

Требования законодательства по обеспечению IT-безопасности не делают различий между физической и виртуальной средой обработки информации; согласно нормативным актам, применяемые средства защиты должны быть сертифицированы и не иметь недекларируемых возможностей.

На практике применяют два распространенных метода обнаружения вторжений: методы, основанные на сигнатурах и аномалиях [46]. Сигнатурный метод сравнивает процессы, происходящие в системе, с известными шаблонами атак, на основании чего происходит идентификация известной атаки. Метод аномалий использует принцип сравнения заданного профиля штатного функционирования системы с протекающими в ней процессами с последую-

щим выявлением аномалий. Метод, основанный на аномалиях, позволяет выявить новые типы вторжений, но имеет низкую надежность и высокую вероятность ложного срабатывания.

В зависимости от требуемого уровня защиты ВИ могут использоваться различные модели администрирования [47, 48, 49, 50]:

- дискреционный метод контроля доступа;
- обязательный метод контроля доступа;
- ролевой метод контроля доступа.

Система дискреционного управления доступом подразумевает, что все ресурсы принадлежат пользователям и контролировать доступ к ресурсу каждой ВМ должен ее пользователь. Такие системы в основном рассчитаны на небольшое число пользователей, т.к. при его росте количество работ по администрированию системы возрастает многократно.

Ролевой метод управления доступом может считаться модификацией модели обязательного контроля за доступом, но при его реализации не обязательно требование к многоуровневой системе безопасности.

При ролевой модели администрирования имеется опасность «самосанкционирования» администратором прав нарушителя, т.к. он имеет доступ к управлению ВИ. Чтобы избежать это, используется ролевая модель управления, основанная на базе делегирования административных прав от главного администратора к подчиненным, с целью уменьшения границ предоставляемых полномочий и повышения контроля за состоянием инфраструктуры [41].

Для обеспечения безопасности информации в сетевых хранилищах данных необходимо реконфигурировать сеть таким образом, чтобы файлы-образы ВМ размещались в изолированном сетевом хранилище, доступ к которому контролируется межсетевым экраном. При этом важно обеспечить модель безопасности, при которой администратор может в полном объеме выполнять свои функции по администрированию, но не имеет доступа к данным ВИ, которые создаются их пользователями.

Основой формального описания систем защиты традиционно считается модель защиты с полным перекрытием, в которой рассматривается взаимодействие трех множеств – «области угроз», «защищаемой области», «системы защиты». Элементы этих множеств находятся между собой в определенных отношениях, собственно и описывающих систему защиты [51, 52, 53].

При создании системы защиты необходимо учитывать затраты, которые могут быть не оправданы в случае обеспечения ее высокого уровня. Для рационального решения задачи безопасности проводят анализ рисков, которые служат показателями полноты, комплексности и эффективности системы защиты [54]. Значение риска рассчитывается как произведение вероятности реализации угрозы по отношению к ресурсу и ущерба от реализации угрозы.

В настоящее время распространено несколько методов оценки составляющих рисков. Наиболее распространено использование экспертных оценок в совокупности с бальными шкалами значений, что не позволяет получить объективные показатели уровня защиты [55]. В связи с этим актуальной задачей является разработка метода определения эффективности системы защиты, опирающегося на количественные показатели критериев оценки.

1.4. Законодательная база информационной безопасности

Системы виртуализации, как и ИС в целом, должны удовлетворять стандартам ИБ.

Основой всех международных стандартов в области ИБ является Британский стандарт BS 7799. Стандарт определил лучшие методы контроля для построения системы управления ИБ, полученные на основе мирового опыта в данной области. Его первая часть BS 7799-1 «Code of Practice for Information Security Management» была разработана Британским Институтом стандартов в 1995г. по заказу Британского правительства. В 1998 г. появилась вторая часть этого стандарта BS 7799-2 «Information Security management — specification for information security management systems», определившая общую модель построения системы управления ИБ и набор обязательных требований для сертификации.

В 2000 г. технический комитет Международной организации по стандартизации (ISO)и Международная электротехническая комиссия (IEC) приняли BS 7799-1 в качестве международного стандарта ISO 17799 [55], а в 2005 г. переименовал стандарт ISO 17799 в стандарт ISO/ IEC 27002 «Information technology —Security techniques — Code of practice for information security management». Британский стандарт BS 7799-2 технический комитет ISO и IEC приняли в качестве международного стандарта ISO/IEC 27001 «Information technology — Security techniques — Information security management systems — Requirements».

В 2005 г. и 2013г оба международных стандарта были пересмотрены под теми же номерами [56, 57] .

Стандарт ISO/IEC 27001 является моделью для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения системы менеджмента ИБ, а стандарт ISO/ IEC 27002 предоставляет лучшие практические рекомендации по менеджменту ИБ для тех, кто отвечает за их создание, реализацию или обслуживание. Информационная безопасность определяется стандартом как «сохранение конфиденциальности, целостности и доступности».

Международный стандарт ISO/IEC 27005:2008 «Information technology — Security techniques —Information security risk management» определяет общие направления по управлению рисками информационной безопасности [58]. Этот стандарт согласуется с концепциями стандарта ISO/IEC 27001, и имеет целью «содействие адекватному обеспечению ИБ на основе риск

- ориентированного подхода». Стандарт ISO/IEC 27005 рекомендован для использования в организациях, управляющих рисками ИБ.

Международный стандарт ISO/IEC 15408:2005 «Common Criteria for Information Technology Security Evaluation» («Общие критерии») введен в декабре 1999 года и пересмотрен в 2005 г [34]. Стандарт определяет оценку безопасности ИТ, как исследование свойств безопасности изделия или системы, называемых объектами оценки, и выделяет три группы пользователей с общим интересом к этим оценкам: потребители объекта оценки, разработчики объекта оценки и оценщики объекта оценки. «Общие критерии» разработаны таким образом, чтобы удовлетворить потребности всех трех групп пользователей.

Наряду с международными стандартами ряд стран создают национальные стандарты в области ИБ.

Стандарт BSI «Bundesamt für Sicherheit in der Informations technik: IT-Grundschutzhandbuch» («Руководство по обеспечению безопасности ИТ») разработан в Германии и впервые опубликован немецким агентством по безопасности в ИТ (German Information Security Agency) в 1994 г [59]. Он определяет меры по безопасности в ИТ для защиты среднего уровня и содержит рекомендации относительно обязанностей персонала и аудита.. В приложении стандарта для определения эффективных мер безопасности BSI приводит типичные угрозы с их детальным описанием. Каждый год BSI обновляет документ дополнениями и новыми техническими решениями.

Наиболее значимыми национальными стандартами ИБ США является «Trusted Computer System Evaluation Criteria» (1985 г.), получивший из-за цвета обложки название «Оранжевая книга» [60]. В стандарте определен понятийный базис ИБ: безопасная система, доверенная система, политика безопасности, уровень гарантированности, подотчетность, доверенная вычислительная база, монитор обращений, ядро безопасности, периметр безопасности. Безопасность и доверие оцениваются в данном стандарте с точки зрения управления доступом к информации, что и является средством обеспечения конфиденциальности и целостности. Оранжевая книга является некоторым аналогом международного стандарта ISO/IEC 15408 (стандарт ISO/IEC 15408 - более универсальный), но с учетом американской юрисдикции документов.

В настоящее время в США действует серя стандартов по ИБ NISTSP 800: NISTSP 800-30 [61], NISTSP 800-35 [62], NISTSP 800-39 [63].

В России вопросы ИБ нормируются Государственными Стандартами [64, 65, 66, 77, 68, 69, 70, 71, 72, 73]. ГОСТ Р ИСО/МЭК 15408 - (1, 2, 3)-2008 «Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» введен в 2002 г. и пересмотрен в 2008 г.; он состоит из трех частей [64, 65, 66] и является фактически перево-

дом стандарта ИСО/МЭК 15408:

- часть 1. Ведение и общая модель [64];

- часть 2. Функциональные требования безопасности [65];

- часть 3. Требования доверия и безопасности [66].

ГОСТ Р ИСО/МЭК 15408 содержит перечень и описание функциональных требований безопасности, которые могут применяться при создании доверенных продуктов или систем ИТ, отвечающих потребностям рынка. Однако в [74] отмечается, что его использование не позволяет обеспечить решение всех задач защиты ИС и лишь представляет современный уровень спецификации требований и оценки безопасности, которые на момент издания стандарта были известны и одобрены его разработчиками.

Наряду с ИСО/МЭК 15408 в России как национальные приняты международные стандарты ГОСТ Р ИСО/МЭК 17799 [67], ГОСТ Р ИСО/МЭК 15446 [68], ГОСТ Р ИСО/МЭК 18044 [69], ГОСТ Р ИСО/МЭК 27033 [70] .

Для защиты пользователей ИТ Российская законодательная система разрабатывает оригинальные стандарты безопасности [71, 72, 73], а крупные российские компании, обладающие значительным риском в информационной среде, создают собственные стандарты с учетом решения конкретных задач. В частности, такие стандарты имеют РЖД [75], банковская отрасль [76] и др.

Основные положения, определяющие требования к аппаратуре железнодорожной автоматики, телемеханики и связи изложены в ОСТ 32.146-2000 «Аппаратура железнодорожной автоматики, телемеханики и связи. Общие технические условия». В ОСТе, наряду с требованиями к конструктивными параметрам аппаратуры, содержатся требования к процессу разработки программного обеспечения для систем автоматики, телемеханики и связи (АИТС). В частности указано, что при разработке программного обеспечения должны быть выполнены требования по спецификации защищенности, в том числе связанные с риском для информации, требующей защиты.

Дальнейшее развитие вопросов информационной безопасности дано в стандарте СТО РЖД 1.18.002-2009 «Управление информационной безопасностью. Общие положения», который базируется на действующих в Российской Федерации законодательных и нормативных документах и международных стандартах: ГОСТ Р 51275-99, ГОСТ Р 51624-2000, ГОСТ Р 51583-2000, ГОСТ Р ИСО/МЭК 15408-2002, ISO/IEC 17799:2005, ISO/IEC 27001:2005 и др., но содержит ряд специальных базовых принципов.

Этот стандарт устанавливает задачи и принципы построения системы управления информационной безопасностью ОАО «РЖД», требования к организационной структуре и мерам управления информационной безопасностью в отрасли, принципы организации планиро-

вания мероприятий по управлению информационной безопасностью и основные меры управления информационной безопасностью. В частности в нем указано, что при управлении информационной безопасности должны решаться задачи:

- анализ уязвимостей, построение моделей нарушителей и угроз безопасности информационных активов;

- анализ и оценка рисков нарушения информационной безопасности АИТС и информационных активов; разработка моделей их защиты;

- формирование требований безопасности информационных активов, предъявляемых к АИТС ОАО «РЖД»;

- определение направлений обеспечения информационной безопасности АИТС ОАО «РЖД» и разработка общих тактико-технических требований по обеспечению безопасности информации;

- разработка требований к подсистемам обеспечения информационной безопасности АИТС, оценка их соответствия и контроль выполнения;

- обеспечение требуемого уровня информационной безопасности посредством проектирования, разработки, внедрения, оценки соответствия и сопровождения систем обеспечения информационной безопасности;

В СТО РЖД 1.18.002 указано, что все создаваемые АИТС ОАО «РЖД» должны разрабатываться с учетом требований нормативно-правовых документов, российских и международных национальных стандартов, а также приведены основные принципы оценки информационной безопасности.

Важно отметить, что стандарт определяет принцип функциональной интеграции специализированных программно-технических комплексов защиты с программно-техническими комплексами передачи и обработки информации, имеющими собственные встроенные средства защиты с мощной функциональностью (операционные системы рабочих станций и серверов, активное сетевое оборудование). Это обеспечивает достижение высокого уровня защищенности при минимизации затрат на внедрение. Еще один базовый принцип построения АИТС должен состоять в сегментировании сети по территориально-производственной принадлежности с разделением функций и ролей. Этот принцип подразумевает физическое или виртуальное разделение локальных вычислительных сетей и информационных ресурсов структурных единиц ОАО «РЖД» с жестким распределением прав доступа к ресурсам между персоналом.

1.5. Выводы по главе I

Для интеграции современных информационных технологий в транспортную инфра-

структуру с целью повышения безопасности и внедрения интеллектуальных логистических систем управления перевозочным процессом для высокоскоростного железнодорожного транспорта в увязке с другими транспортными системами, а также обеспечения энергоэффективного управления движением:

1. Предложена 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. Определены функции вычислительного комплекса в общей системе управления движением и разработана его структура с использованием средства нативной виртуализации, что позволяет разграничить вычислительные процессы и их взаимодействие с базами данных и участниками перевозочного процесса, повысить надежность и защищенность отдельных элементов при разграничении прав доступа к ним.

3. Подтверждено соответствие разработанной структуры вычислительного комплекса законодательной базе стандарта ОАО «РЖД» 1.18.002-2009 «Управление информационной безопасностью. Общие положения», подразумевающего разделение информационных ресурсов структурных единиц и использование собственных средств защиты.

4. Исследование процесса взаимодействия вычислительного комплекса с участниками перевозочного процесса требует создания его имитационной модели, использующей алгоритм работы системы автоведения поезда с учетом текущей поездной ситуации.

II. РАЗРАБОТКА МОДЕЛИ ФУНКЦИОНИРОВАНИЯ ВИРТУАЛЬНОГО ВЫЧИСЛИТЕЛЬНОГО КОМПЛЕКСА

2.1. Анализ алгоритмов и моделей функционирования виртуальных компьютерных систем

В связи с тем, что разрабатываемый ВК предназначен для создания комплексной системы управления движением поездов и связан с безопасностью движения, необходимо выполнить тестирование его работы как в режиме нормального функционирования, так и при возникновении внештатных ситуаций – отказов отдельных ВМ и информационных атак, поскольку основное из требований стандарта СТО РЖД 1.18.002-2009 к вычислительным ресурсам – это надежность функционирования и собственные встроенные средства защиты [75].

Для возможности выполнения тестирования системы со сложными динамическими параллельными и асинхронными процессами должна быть разработана модель, позволяющая анализировать ее функциональность для решения основной задачи при нормальном режиме и внештатных ситуациях.

В настоящее время средства виртуализации являются одним из основных принцепов создания корпоративных ИС. Поскольку задачи распределения ресурсов должны решаться еще на стадии проектирования системы, к настоящему времени разработаны различные методы моделирования и прогнозирования функционирования таких ИС.

Теоретические основы систем виртуализации рассмотрены в трудах отечественных и зарубежных авторов: Дубинина В.Н. [57], Заикина С.А. [77], Рослякова А.В. [78], Barrett D. [79], Boomer J. [80]; Carbone J.[81], Luca S. Crawford [82], William von Hagen [83], Haletky E. [84], Erick M. Halter [85], Keefer R. M. [80]; Kipper G. [79], Larson R. [81], Lowe S. [86], Olzak T. [80], Sabovik J. [80], Chris Takemura [82], Chris Wolf [85].

Ряд работ посвящены решению частных задач систем виртуализации, основными из которых являются задачи оптимального распределения ресурсов и данных в виртуальной компьютерной сети. Для создания математических моделей и алгоритмов управления ресурсами и данными в виртуальных системах авторы используют преимущественно методы дискретной и вычислительной математики, математической статистики, теории операционных систем и системного программирования, а также математический аппарат логико-алгебраических описаний, формализма сетей абстрактных машин и иерархических алгебраических систем.

Развитию теоретических основ архитектурной, функционально-структурной организации и виртуализации систем и сетей внешнего хранения и обработки данных посвящена работа [87]. В ней обоснован и исследован синтез структур и алгоритмов функционирования систем и сетей хранения и обработки данных на базе виртуализации и интеграции сетевых ресур-

сов с вычислительными ресурсами. Для создания имитационных моделей дискретных систем с событийно-временной координацией взаимодействующих процессов автор использует математический аппарат логико-алгебраических описаний, формализм сетей абстрактных машин и иерархические алгебраические системы. На основании проведенных исследований предложена архитектурная и функционально-структурная организация систем и сетей внешнего хранения и обработки данных с развитыми функциональными возможностями и высокой производительностью, ориентированная на универсальные и специализированные приложения.

Теория математического моделирования средств управления ресурсами и данными в распределенных и виртуализованных средах разработана в [4, 88]. В ней сформулирован подход к созданию распределенных и виртуализованных сред, ориентированных на размещение, хранение и управление ресурсами и данными, а также построению и анализу математических моделей систем виртуализации. Автором разработаны модели, описывающие компоненты такой среды, в том числе, математические модели интегрированных средств контроля доступа для них. В частности, в работе представлены модель виртуализации объектов уровня операционной системы путем разделения их в пространстве имен и обобщенная математическая модель и алгоритмы группового многоуровневого управления ресурсами, необходимые для виртуализации уровня ОС и других технологий виртуализации. Для разработки математических моделей и алгоритмов управления ресурсами и данными в распределенных и виртуализованных средах автором использовались методы дискретной математики и алгебры, вычислительной математики, методы математической статистики, методы теории операционных систем и системного программирования. На основании выполненных исследований предложены принципы функционирования средств размещения и управления ресурсами и данными как распределенной, саморегулирующейся виртуализованной мобильной среды, являющейся совокупностью вычислительных ресурсов и хранилищ данных, объединенных коммуникационной инфраструктурой. Кроме того, разработаны принципы функционирования распределенной среды с открытой коммуникационной инфраструктурой и возможностью переноса защиты с серверов и коммуникаций на клиентские узлы путем использования предложенной модели интегрированной системы контроля доступа, базирующейся на понятии «декларируемых полномочий».

В [89] разработаны математическая модель и метод управления ресурсами центрального процессора в условиях функционирования виртуальных выделенных серверов с целью ограничения потребления времени центрального процессора. Использование этого метода позволяет осуществлять текущее распределение ресурсов между вычислительными задачами в операционных систем с закрытыми исходными кодами. При отыскании алгоритма управления

автор использовал аналитические методы теории массового обслуживания, теории операционных систем, теории цифровой фильтрации и др.

Аналогичная задача автоматизации распределения вычислительных ресурсов в виртуальном комплексе на основе эффективной стратегии управления, регламентирующей качество оказываемых приложениями услуг, была решена в [90]. В основе метода лежит модель оптимального управления ресурсами для совокупности виртуальных серверов, где для каждого момента определяются характеристики приложений и выбираются весовые коэффициенты значимости для каждого приложения и его характеристик. В качестве решения задачи оптимизации распределения ресурсов системы предлагается минимизация отклонения функции суммарной оценки приложений системы с учетом весовых коэффициентов самих приложений и их характеристик от некоторого целевого значения.

Моделям и алгоритмам распределения ресурсов виртуализованных вычислительных кластеров посвящена работа [91]. В ней разработана математическая модель статического распределения ресурсов виртуальзованных кластеров для обеспечения надежности и контроля функционирования программной и аппаратной части устройств вычислительной техники. Целевая функция минимизирует стоимость серверов при ограничениях разового распределения каждого сервиса (приложения) и суммарной нагрузки приложений возможностям физического сервера. Задание значений параметров серверов в модели предлагается определять по результатам тестирования и исследования его производительности. Предложенная модель позволяет определять количественно возможность уменьшения стоимости физических ресурсов кластера на основе статистических данных. При этом в работе справедливо отмечается, что при оптимизации структуры виртуализованного кластера необходимо учитывать пороговое значение коэффициента загрузки сервера, обеспечивающего работу его компонент.

Решению задачи комплексного планирования операций и распределения ресурсов в корпоративной информационной системе для повышения оперативности и качества ее функционирования посвящена работа [92]. В ней предложен вариант построения аналитической концептуальной модели функционирования корпоративной информационной системы, в составе которой выделены как основные компоненты процессы, операции, потоки и ресурсы, формализованные с использованием теоретико-множественного подхода. Теоретико-множественная модель планирования операций в корпоративной информационной системе определена автором в виде математической структуры выбора с предпочтением. В результате, задача планирования сведена к классу задач формирования множества альтернатив предпочтения и выбора наилучшей альтернативы из множества Парето. Автор аргументировано обосновывает, что для исследования корпоративной информационной системы целесообразно ис-

пользовать класс динамических моделей, которые повышают оперативность решения задач планирования.

В [93] решена задача повышения эффективности проектирования и расширение функциональных и эксплуатационных возможностей предметно-ориентированных облачных сред за счет виртуализации их функциональной и системной архитектур. Автор работы анализирует принципы построения облачных сред, базирующихся на виртуализации системной архитектуры, и формулирует требования к предметно-ориентированной облачной среде, обеспечивающей доступ приложений к высокопроизводительному программному обеспечению. Для проектирования архитектуры виртуализованных предметно-ориентированных облачных сред используется математический аппарат многоосных алгебраических систем построения формализованных поведенческих логико-алгебраических моделей. Полученные результаты позволили сформулировать предложения по повышению производительности системы при запуске приложений и при загрузке заданий на внешний вычислительный ресурс.

Проведенный анализ выполненных исследований показал, что в основном в них решается задача оптимального распределения ресурса в виртуальной компьютерной системе с фиксированной архитектурой или задача построения виртуальной системы без учета алгоритма ее взаимодействия с внешней системой. При решении данного класса задач основным критерием эффективности выступает стоимостной показатель и показатель суммарной нагрузки приложений, определяемый по результатам тестирования производительности сервера.

При решении задачи создания ВК для комплексной системы управления движением поездов одно из основных требований к вычислительному ресурсу – устойчивое взаимодействие с внешними системами и выполнение циклической программы за заданный интервал времени, в том числе, и при любых внештатных ситуациях. Таким образом, разрабатываемая модель должна позволять выполнять расчет динамической нагрузки на ресурс ВК, тестирование работы ВК при его взаимодействиями с внешними системами, а также в случае аварийного нарушения распределения его ресурсов и при попытке проведения информационной атаки, что соответствует требованиям СТО РЖД 1.18.002-2009 к вычислительным ресурсам [75]. Этим требованиям соответствует динамическая имитационная модель функционирования ВК с учетом параллельных и асинхронных процессов взаимодействия ресурса и приложений, обеспечивающих устойчивое взаимодействие участников перевозочного процесса.

2.2. Расчет нагрузки на ресурс вычислительного комплекса для обеспечения функционирования системы управления движением поездов

Расчет требуемого ресурса ВК выполнялся исходя из алгоритмов функционирования ДЦ «Сетунь» и системы автоведения поезда, приведенных в п. 1.3.

В таблице 2.1 приведены данные расчета нагрузки на ресурс ВК при управлении одной секцией тепловоза полученные на основании табл. 1.1. В расчетах принималось, что в соответствии с требованиями алгоритма работы системы автоведения поезда информация на ВК от каждой секции локомотива и от ДЦ «Сетунь» должна передается пакетами данных с периодом Т2=100 мс [13].

Таблица 2.1.

Нагрузка на ресурс ВК от одной секции локомотива

	Принимаемая и обрабатываемая информация с интервалом Т2=100 мс, КБ	Источник информации	Примечание
1	2	3	4
ВМ1 «База данных характеристик участка, ограничений скорости, текущей координаты»	20,0·4	ДЦ «Сетунь»	Получение данных от шлюза; передача данных на ВМ4, ВМ5
ВМ2 «База данных параметров поезда и текущих режимов работы»	9,0·4	Тепловоз	Получение и передача данных ВМ4, ВМ5; возвращение данных
ВМ3 «База данных кассеты регистрации КЛУБ»	14,0·4	Тепловоз	Получение данных; передача данных ВМ4, ВМ5; возвращение данных
ВМ4 «Расчет мощности, которая может быть реализована локомотивом»	20,3·2	Тепловоз [13] (принято для микроконтроллера АТ89С55 микропроцессорной системы управления)	Получение данных; выполнение расчетов; передача данных ВМ5; возвращение данных
ВМ5 «Решение задачи оптимального управления локомотивом»	2115	Тепловоз, ДЦ «Сетунь» (принято с учетом параметров микроконтроллера АТ89С55 [13] и	Получение данных от ВМ1- ВМ3, ВМ6; выполнение расчетов; передача данных на шлюз

1	2	3	4
		взаимодействия с базами данных ВМ1-ВМ4, ВМ6, ВМ7)	
ВМ6 «База данных о срабатывании систем защиты»	1,0·2	Тепловоз	Получение данных; передача данных ВМ4, ВМ5, ВМ7; возвращение данных
ВМ7 «Прогноз надежности агрегатов и систем тепловоза»	20,3·2	Тепловоз [13] (принято для микроконтроллера AT89C55)	Получение данных от шлюза и ВМ6; возвращение данных
ВМ8 «Мониторинг ВК»	$256 \cdot 10^3$		[94]
ВМ9 «Резерв»	0		
Шлюз	20,3·4+20,0·4	Тепловоз, ДЦ «Сетунь»	Получение данных от тепловоза, ДЦ; передача данных ВМ1-ВМ3,ВМ6, ВМ7; передача ответных данных на тепловоз, ДЦ

Анализ показывает, что наиболее нагружена будет оперативная память ВК от ВМ5, выполняющей решение задачи оптимального управления движением. Сводные данные для определения ресурса ВК приведены в таблице 2.2.

Таблица 2.2

Расчет ресурса ВК при полной нагрузке

	Нагрузка, КБ	Примечание
1	2	3
Нагрузка на ресурс ВК от одной секции тепловоза	2532	При максимальной нагрузке на ресурс, когда одновременно выполняется расчет ВМ4 и ВМ5, а на прочие ВМ загружаются базы данных
Нагрузка на ресурс ВК от трехсекционного тепловоза	7596	
Нагрузка на ресурс ВК от 68	$516,0 \cdot 10^3$	Нагрузка рассчитывалась из условия

1	2	3
трехсекционных тепловозов		длины участка ж.д., контролируемом ДЦ «Сетунь» - 200 км. При двухпутном движении с интервалом 7 минут [95] на участке может находиться 68 поездов
Нагрузка на ресурс ВК от 68 трехсекционных тепловозов с учетом режима мониторинга	$(516+256)\cdot10^3/0,7=1103\cdot10^3$	В расчетах принимается рекомендация [96] 70% загрузки оперативной памяти процессора
Нагрузка на ресурс от ОС и программного обеспечения одной ВМ	$512\cdot10^3$	[97]
Нагрузка на ресурс от ОС и программного обеспечения десяти ВМ	$5120\cdot10^3$	
Требуемый ресурс ВК	$6,223\cdot10^6$	

2.3. Разработка модели вычислительного комплекса и ее тестирование

Для анализа процессов, происходящих в ВК, и определения эффективности применяемой системы защиты необходимо соблюдение двух принципиально важных условий: наличие правдоподобных траекторий нагрузки на ресурс и надежная среда, в которой можно было бы проводить численные эксперименты [98]. Как отмечено в [99, 100] анализ динамики ресурсных потоков целесообразно выполнять с использованием аппарата сетей Петри. Этот аппарат позволяет объединить преимущества графового представления и дискретной динамической модели системы, рассчитывать количественные показатели её работы, которые характеризуются параллельными и асинхронными процессами. Аппарат сетей Петри может быть использован и для определения эффективности работы ВК.

Моделирование в терминах сетей Петри осуществляется на событийном уровне. Переходы отображают действия, происходящие в системе, а позиции - состояния, предшествующие этим действиям, и состояния, принимаемые системой после выполнения действий. Анализ результатов моделирования позволяет определить динамическое состояние системы при любых алгоритмах управления и выполняемых процедурах.

Рассмотрим виртуальный ВК, созданный на базе хоста, и состоящий собственно из хоста и виртуальных машин. Обобщенные ресурсы хоста SRC (объем оперативной памяти, тактовая частота процессора, емкость, количество операций ввода-вывода в секунду и время обращения к жесткому диску) позволяют одновременно функционировать десяти ВМ (SRC=10).

Связь каждой ВМ с хостом и отдельных ВМ между собой осуществляется через гипервизор, который обеспечивает распределение ресурсов хоста между всеми ВМ и определяет эффективность работы ВК на доступном аппаратном обеспечении.

Для исследования работы ВК разработана его динамическая модель в терминах сетей Петри, которая определяется совокупностью объектов (рисунок 2.1) [99,100, 101]:

$$П = \{P, T, I, O, \mu\}, \qquad (2.1)$$

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.

Функции входа и выхода определяются отображением бинарного произведения множества переходов и множества позиций на множество $\{0,1\}$:

$$I: T \times P \to \{0,1\};$$
$$O: T \times P \to \{0,1\}.$$

Маркировка сети определяется отображением множества позиций на множество натуральных чисел N

$$\mu: P \to N.$$

Графически, в терминах расширенных сетей Петри, модель ВК представляется как ориентированный маркированный граф, состоящий из вершин двух типов - позиций и переходов, соединенных между собой дугами.

Моделирование маршрутов в маркированном графе сетей Петри должно удовлетворять условиям:

$$|I(p_i)| = \left|\{t_j | p_i \in O(t_j)\}\right| = 1;$$
$$|O(p_i)| = \left|\{t_j | p_i \in I(t_j)\}\right| = 1,$$

где $\{t_j | p_i \in O(t_j)\}$ - множество переходов, для которых p_i является выходом;

$\{t_j | p_i \in I(t_j)\}$ - множество переходов, для которых p_i является входом.

Разрешение на выполнение перехода $t_i \in T$ определяется условием [99, 100]

$$t_j: \mu(p_i) \geq \#(p_i, I(t_j)) \quad \forall p_i \in P, \qquad (2.2)$$

где $(p_i, I(t_j))$ - кратность входной позиции p_i для перехода t_j; т.е. переход t_j разрешен, при некоторой маркировке $\mu(p_i)$, если позиция $p_i \in P$ имеет разметку не меньшую чем кратность дуги, соединяющей p_i и t_j.

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

$$\mu'(p_i) = \mu(p_i) - \#(p_i, I(t_j)) + \#(p_i, O(t_j)) . \qquad (2.3)$$

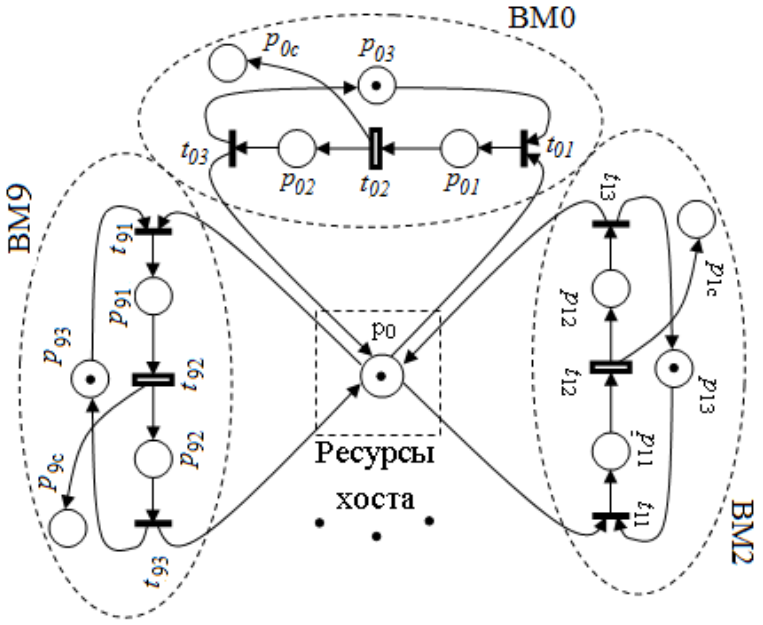


Рисунок 2.1. Модель функционирования ВК с SRC=10 в терминах сетей Петри

С учетом изложенного модель функционирования ВК с SRC=10, представленная в терминах сетей Петри, содержит 41 позицию и 30 переходов:

$$P = \{p_0, p_{01}, p_{02}, p_{03}, p_{0c}, p_{11}, \dots, p_{gl}, \dots, p_{93}, p_{9c}\};$$

$$T = \{t_{01}, t_{02}, t_{03}, t_{11}, \dots, t_{gf}, \dots, t_{92}, t_{93}\}.$$

Элементами множества позиций P являются: p_0 - разделяемая среда (ресурс хоста); p_{01}-p_{03}, p_{11}–p_{13},…p_{91}–p_{93}- состояниеВМ0-9:p_{01}, p_{11}, …, p_{91}- предоставление ресурсов; p_{02}, p_{12}, … , p_{92}- освобождение ресурсов; p_{03}, p_{13},…, p_{93}- ожидание ресурсов хоста ; p_{0c}, p_{1c}, … , p_{9c}- счетчики операций.

Элементами множества позиций T являются: t_{01} –t_{03} , t_{11} –t_{13} , … t_{91}- t_{93}- процессы распределения ресурсов хоста и формирования запросов ВМ0-9: t_{01} , t_{11} ,…, t_{91} - выделение ресурсов; t_{02} , t_{12} , …, t_{92}- работа с предоставленными ресурсами; t_{03} , t_{13} , …, t_{93} - возвращение ресурсов хосту.

Процесс моделирования работы ВК в терминах сетей Петри определяется срабатыванием переходов и изменением маркировки позиций в соответствии с (2.2) и (2.3): при срабатывании перехода изменяется маркировка его входной и выходной позиций. Таким образом, для ВК с ресурсом SRC=10 динамическая модель состояний определится системой уравнений (2.4) [102]:

Входная и выходная матрицы переходов системы, отражающие их связь с позициями, представлены в таблицах 2.3 и 2.4.

$$
\begin{cases}
\mu'(p_0) = \mu(p_0) + 1\big(\#\big(p_0, I(t_{03})\big) = 1\big) + 1\big(\#\big(p_0, I(t_{13})\big) = 1\big) \\
+1\big(\#\big(p_0, I(t_{23})\big) = 1\big) + 1\big(\#\big(p_0, I(t_{33})\big) = 1\big) + 1\big(\#\big(p_0, I(t_{43})\big) = 1\big) \\
+1\big(\#\big(p_0, I(t_{53})\big) = 1\big) + 1\big(\#\big(p_0, I(t_{63})\big) = 1\big) + 1\big(\#\big(p_0, I(t_{73})\big) = 1\big) \\
+1\big(\#\big(p_0, I(t_{83})\big) = 1\big) + 1\big(\#\big(p_0, I(t_{93})\big) = 1\big) - 1\big(\#\big(p_0, O(t_{01})\big) = 1\big) \\
-1\big(\#\big(p_0, O(t_{11})\big) = 1\big) - 1\big(\#\big(p_0, O(t_{21})\big) = 1\big) - 1\big(\#\big(p_0, O(t_{31})\big) = 1\big) \\
-1\big(\#\big(p_0, O(t_{41})\big) = 1\big) - 1\big(\#\big(p_0, O(t_{51})\big) = 1\big) - 1\big(\#\big(p_0, O(t_{61})\big) = 1\big) \\
-1\big(\#\big(p_0, O(t_{71})\big) = 1\big) - 1\big(\#\big(p_0, O(t_{81})\big) = 1\big) - 1\big(\#\big(p_0, O(t_{91})\big) = 1\big); \\
t_{01}: \mu(p_0) \geq \#\big(p_0, I(t_{01})\big)\ u\ \mu(p_{03}) \geq \#\big(p_{03}, I(t_{01})\big); \\
\mu'(p_{01}) = \mu(p_{01}) + 1\big(\#\big(p_{01}, I(t_{01})\big) = 1\big) - 1\big(\#\big(p_{01}, O(t_{02})\big) = 1\big); \\
t_{02}: \mu(p_{01}) \geq \#\big(p_{01}, I(t_{02})\big); \\
\mu'(p_{02}) = \mu(p_{02}) + 1\big(\#\big(p_{02}, I(t_{02})\big) = 1\big) - 1\big(\#\big(p_{02}, O(t_{03})\big) = 1\big); \\
t_{03}: \mu(p_{02}) \geq \#\big(p_{02}, I(t_{03})\big); \\
\mu'(p_{03}) = \mu(p_{03}) + 1\big(\#\big(p_{03}, I(t_{03})\big) = 1\big) - 1\big(\#\big(p_{03}, O(t_{01})\big) = 1\big); \\
\mu'(p_{0c}) = \mu(p_{0c}) + 1\big(\#\big(p_{0c}, I(t_{02})\big) = 1\big); \\
t_{11}: \mu(p_0) \geq \#\big(p_0, I(t_{11})\big)\ u\ \mu(p_{13}) \geq \#\big(p_{13}, I(t_{11})\big); \\
\mu'(p_{11}) = \mu(p_{11}) + 1\big(\#\big(p_{11}, I(t_{11})\big) = 1\big) - 1\big(\#\big(p_{11}, O(t_{12})\big) = 1\big); \\
t_{12}: \mu(p_{11}) \geq \#\big(p_{11}, I(t_{12})\big); \\
\mu'(p_{12}) = \mu(p_{12}) + 1\big(\#\big(p_{12}, I(t_{12})\big) = 1\big) - 1\big(\#\big(p_{12}, O(t_{13})\big) = 1\big); \\
t_{13}: \mu(p_{12}) \geq \#\big(p_{12}, I(t_{13})\big); \\
\mu'(p_{13}) = \mu(p_{13}) + 1\big(\#\big(p_{13}, I(t_{13})\big) = 1\big) - 1\big(\#\big(p_{13}, O(t_{11})\big) = 1\big); \\
\mu'(p_{1c}) = \mu(p_{1c}) + 1\big(\#\big(p_{1c}, I(t_{12})\big) = 1\big); \\
t_{21}: \mu(p_0) \geq \#\big(p_0, I(t_{21})\big)\ u\ \mu(p_{23}) \geq \#\big(p_{23}, I(t_{21})\big); \\
\mu'(p_{21}) = \mu(p_{21}) + 1\big(\#\big(p_{21}, I(t_{21})\big) = 1\big) - 1\big(\#\big(p_{21}, O(t_{22})\big) = 1\big); \\
t_{22}: \mu(p_{21}) \geq \#\big(p_{21}, I(t_{22})\big); \\
\mu'(p_{22}) = \mu(p_{22}) + 1\big(\#\big(p_{22}, I(t_{22})\big) = 1\big) - 1\big(\#\big(p_{22}, O(t_{23})\big) = 1\big); \\
t_{23}: \mu(p_{22}) \geq \#\big(p_{22}, I(t_{23})\big); \\
\mu'(p_{23}) = \mu(p_{23}) + 1\big(\#\big(p_{23}, I(t_{23})\big) = 1\big) - 1\big(\#\big(p_{23}, O(t_{21})\big) = 1\big); \\
\mu'(p_{2c}) = \mu(p_{2c}) + 1\big(\#\big(p_{2c}, I(t_{22})\big) = 1\big); \\
t_{31}: \mu(p_0) \geq \#\big(p_0, I(t_{31})\big)\ u\ \mu(p_{33}) \geq \#\big(p_{33}, I(t_{31})\big); \\
\mu'(p_{31}) = \mu(p_{31}) + 1\big(\#\big(p_{31}, I(t_{31})\big) = 1\big) - 1\big(\#\big(p_{31}, O(t_{32})\big) = 1\big); \\
t_{32}: \mu(p_{31}) \geq \#\big(p_{31}, I(t_{32})\big); \\
\mu'(p_{32}) = \mu(p_{32}) + 1\big(\#\big(p_{32}, I(t_{32})\big) = 1\big) - 1\big(\#\big(p_{32}, O(t_{33})\big) = 1\big); \\
t_{33}: \mu(p_{32}) \geq \#\big(p_{32}, I(t_{33})\big); \\
\mu'(p_{33}) = \mu(p_{33}) + 1\big(\#\big(p_{33}, I(t_{33})\big) = 1\big) - 1\big(\#\big(p_{33}, O(t_{31})\big) = 1\big); \\
\mu'(p_{3c}) = \mu(p_{3c}) + 1\big(\#\big(p_{3c}, I(t_{32})\big) = 1\big); \\
t_{41}: \mu(p_0) \geq \#\big(p_0, I(t_{41})\big)\ u\ \mu(p_{43}) \geq \#\big(p_{43}, I(t_{41})\big); \\
\mu'(p_{41}) = \mu(p_{41}) + 1\big(\#\big(p_{41}, I(t_{41})\big) = 1\big) - 1\big(\#\big(p_{41}, O(t_{42})\big) = 1\big); \\
t_{42}: \mu(p_{41}) \geq \#\big(p_{41}, I(t_{42})\big);
\end{cases}
\tag{2.4}
$$

$$
\begin{cases}
\mu'(p_{42}) = \mu(p_{42}) + 1\big(\#\big(p_{42}, I(t_{42})\big) = 1\big) - 1\big(\#\big(p_{42}, O(t_{43})\big) = 1\big); \\
t_{43}: \mu(p_{42}) \geq \#\big(p_{42}, I(t_{43})\big); \\
\mu'(p_{43}) = \mu(p_{43}) + 1\big(\#\big(p_{43}, I(t_{43})\big) = 1\big) - 1\big(\#\big(p_{43}, O(t_{41})\big) = 1\big); \\
\mu'(p_{4c}) = \mu(p_{4c}) + 1\big(\#\big(p_{4c}, I(t_{42})\big) = 1\big); \\
t_{51}: \mu(p_0) \geq \#\big(p_0, I(t_{51})\big)\ u\ \mu(p_{53}) \geq \#\big(p_{53}, I(t_{51})\big); \\
\mu'(p_{51}) = \mu(p_{51}) + 1\big(\#\big(p_{51}, I(t_{51})\big) = 1\big) - 1\big(\#\big(p_{51}, O(t_{52})\big) = 1\big); \\
t_{52}: \mu(p_{51}) \geq \#\big(p_{51}, I(t_{52})\big). \\
\mu'(p_{52}) = \mu(p_{52}) + 1\big(\#\big(p_{52}, I(t_{52})\big) = 1\big) - 1\big(\#\big(p_{52}, O(t_{53})\big) = 1\big); \\
t_{53}: \mu(p_{52}) \geq \#\big(p_{52}, I(t_{53})\big); \\
\mu'(p_{53}) = \mu(p_{53}) + 1\big(\#\big(p_{53}, I(t_{53})\big) = 1\big) - 1\big(\#\big(p_{53}, O(t_{51})\big) = 1\big); \\
\mu'(p_{5c}) = \mu(p_{5c}) + 1\big(\#\big(p_{5c}, I(t_{52})\big) = 1\big); \\
t_{61}: \mu(p_0) \geq \#\big(p_0, I(t_{61})\big)\ u\ \mu(p_{63}) \geq \#\big(p_{63}, I(t_{61})\big); \\
\mu'(p_{61}) = \mu(p_{61}) + 1\big(\#\big(p_{61}, I(t_{61})\big) = 1\big) - 1\big(\#\big(p_{61}, O(t_{62})\big) = 1\big); \\
t_{62}: \mu(p_{61}) \geq \#\big(p_{61}, I(t_{62})\big); \\
\mu'(p_{62}) = \mu(p_{62}) + 1\big(\#\big(p_{62}, I(t_{62})\big) = 1\big) - 1\big(\#\big(p_{62}, O(t_{63})\big) = 1\big); \\
t_{63}: \mu(p_{62}) \geq \#\big(p_{62}, I(t_{63})\big); \\
\mu'(p_{63}) = \mu(p_{63}) + 1\big(\#\big(p_{63}, I(t_{63})\big) = 1\big) - 1\big(\#\big(p_{63}, O(t_{61})\big) = 1\big); \\
\mu'(p_{6c}) = \mu(p_{6c}) + 1\big(\#\big(p_{6c}, I(t_{62})\big) = 1\big); \\
t_{71}: \mu(p_0) \geq \#\big(p_0, I(t_{71})\big)\ u\ \mu(p_{73}) \geq \#\big(p_{73}, I(t_{71})\big); \\
\mu'(p_{71}) = \mu(p_{71}) + 1\big(\#\big(p_{71}, I(t_{71})\big) = 1\big) - 1\big(\#\big(p_{71}, O(t_{72})\big) = 1\big); \\
t_{72}: \mu(p_{71}) \geq \#\big(p_{71}, I(t_{72})\big); \\
\mu'(p_{72}) = \mu(p_{72}) + 1\big(\#\big(p_{72}, I(t_{72})\big) = 1\big) - 1\big(\#\big(p_{72}, O(t_{73})\big) = 1\big); \\
t_{73}: \mu(p_{72}) \geq \#\big(p_{72}, I(t_{73})\big); \\
\mu'(p_{73}) = \mu(p_{73}) + 1\big(\#\big(p_{73}, I(t_{73})\big) = 1\big) - 1\big(\#\big(p_{73}, O(t_{71})\big) = 1\big); \\
\mu'(p_{7c}) = \mu(p_{7c}) + 1\big(\#\big(p_{7c}, I(t_{72})\big) = 1\big); \\
t_{81}: \mu(p_0) \geq \#\big(p_0, I(t_{81})\big)\ u\ \mu(p_{83}) \geq \#\big(p_{83}, I(t_{81})\big); \\
\mu'(p_{81}) = \mu(p_{81}) + 1\big(\#\big(p_{81}, I(t_{81})\big) = 1\big) - 1\big(\#\big(p_{81}, O(t_{82})\big) = 1\big); \\
t_{82}: \mu(p_{81}) \geq \#\big(p_{81}, I(t_{82})\big); \\
\mu'(p_{82}) = \mu(p_{82}) + 1\big(\#\big(p_{82}, I(t_{82})\big) = 1\big) - 1\big(\#\big(p_{82}, O(t_{83})\big) = 1\big); \\
t_{83}: \mu(p_{82}) \geq \#\big(p_{82}, I(t_{83})\big); \\
\mu'(p_{83}) = \mu(p_{83}) + 1\big(\#\big(p_{83}, I(t_{83})\big) = 1\big) - 1\big(\#\big(p_{83}, O(t_{81})\big) = 1\big); \\
\mu'(p_{8c}) = \mu(p_{8c}) + 1\big(\#\big(p_{8c}, I(t_{82})\big) = 1\big); \\
t_{91}: \mu(p_0) \geq \#\big(p_0, I(t_{91})\big)\ u\ \mu(p_{93}) \geq \#\big(p_{93}, I(t_{91})\big); \\
\mu'(p_{91}) = \mu(p_{91}) + 1\big(\#\big(p_{91}, I(t_{91})\big) = 1\big) - 1\big(\#\big(p_{91}, O(t_{92})\big) = 1\big); \\
t_{92}: \mu(p_{91}) \geq \#\big(p_{91}, I(t_{92})\big); \\
\mu'(p_{92}) = \mu(p_{92}) + 1\big(\#\big(p_{92}, I(t_{92})\big) = 1\big) - 1\big(\#\big(p_{92}, O(t_{93})\big) = 1\big); \\
t_{93}: \mu(p_{92}) \geq \#\big(p_{92}, I(t_{93})\big); \\
\mu'(p_{93}) = \mu(p_{93}) + 1\big(\#\big(p_{93}, I(t_{93})\big) = 1\big) - 1\big(\#\big(p_{93}, O(t_{91})\big) = 1\big); \\
\mu'(p_{9c}) = \mu(p_{9c}) + 1\big(\#\big(p_{9c}, I(t_{92})\big) = 1\big).
\end{cases}
\tag{2.4}
$$

Таблица 2.3

Входная матрица переходов системы, отражающая их связь с позициями

	t_{11}	t_{12}	t_{13}	t_{21}	t_{22}	t_{23}	t_{31}	t_{32}	t_{33}	t_{41}	t_{42}	t_{43}	t_{51}	t_{52}	t_{53}	t_{61}	t_{62}	t_{63}	t_{71}	t_{72}	t_{73}	t_{81}	t_{82}	t_{83}	t_{91}	t_{92}	t_{93}	t_{101}	t_{102}	t_{103}
p_0	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0
p_{11}	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_{12}	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_{13}	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_{1c}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_{21}	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_{22}	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_{23}	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_{2c}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_{31}	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_{32}	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_{33}	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_{3c}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_{41}	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_{42}	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_{43}	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_{4c}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_{51}	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_{52}	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_{53}	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_{5c}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_{61}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_{62}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
p_{63}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_{6c}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_{71}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
p_{72}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
p_{73}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
p_{7c}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_{81}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
p_{82}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
p_{83}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
p_{8c}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_{91}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_{91}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
p_{93}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
p_{9c}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
p_{101}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
p_{102}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
p_{103}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
p_{10c}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Таблица 2.4

Выходная матрица переходов системы, отражающая их связь с позициями

	t_{11}	t_{12}	t_{13}	t_{21}	t_{22}	t_{23}	t_{31}	t_{32}	t_{33}	t_{41}	t_{42}	t_{43}	t_{51}	t_{52}	t_{53}	t_{61}	t_{62}	t_{63}	t_{71}	t_{72}	t_{73}	t_{81}	t_{82}	t_{83}	t_{91}	t_{92}	t_{93}	t_{101}	t_{102}	t_{103}
p_0	0	0	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0	1
p_{11}	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_{12}	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_{13}	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_{1c}	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_{21}	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_{22}	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_{23}	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_{2c}	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_{31}	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_{32}	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_{33}	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_{3c}	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_{41}	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_{42}	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_{43}	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_{4c}	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_{51}	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_{52}	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_{53}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_{5c}	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_{61}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
p_{62}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
p_{63}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
p_{6c}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
p_{71}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
p_{72}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
p_{73}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
p_{7c}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
p_{81}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
p_{82}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
p_{83}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
p_{8c}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
p_{91}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
p_{91}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
p_{93}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
p_{9c}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
p_{101}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
p_{102}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
p_{103}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
p_{10c}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

В основе алгоритма моделью ВК лежит алгоритм управления объектами и потоками данных физического ВК для решения задачи управления поездами на участке ж.д., контролируемом ДЦ «Сетунь» (рисунок 1.4). В момент получения запроса от системы автоведения поезда ВК на ВМ «шлюз» загружает необходимые данные от самого локомотива и ДЦ «Сетунь». Там эти данные распределяются по пакетам и последовательно передаются на ВМ1, ВМ2, ВМ3, ВМ6 (см. таблицу 2.1). После того как данные указанными ВМ получены начинает работать ВМ4, рассчитывая текущую мощность агрегатов и систем тепловоза. После завершения этих вычислений результаты передаются на ВМ7, где они обрабатываются для получения прогноза по показателям надежности локомотива и одновременно начинает работать ВМ5, рассчитывающая оптимальный алгоритм управления локомотива. После завершения расчета данные должны через ВМ «шлюз» передаться на систему автоведения локомотива. Скорость передачи информации по каналам связи принималась 1Гбит/с на основании [103, 104].

Алгоритм моделирования динамических процессов в ВК в терминах сетей Петри представлен на рисунке 2.2. Разработанная для реализации алгоритма программа расчетов процессов в ВК базируется на объектно-ориентированном подходе, для чего были созданы специализированные классы, описывающие состояния, переходы, дуги и функционирование сети в целом.

Верификация разработанной модели выполнялась с точки зрения выполнения алгоритма функционирования ВК и по показателю использования его ресурса.

На рисунке 2.3 представлена диаграмма результатов моделирования функционирования ВК при получении запроса от системы автоведения локомотива. Из диаграммы видно, при что τ=0,00 с первой начинает работать ВМ «шлюз», причем информация на нее приходит двумя пакетами – от локомотива и от ДЦ. Затем последовательно в работу включается ВМ1, ВМ2, ВМ3 и ВМ6. Информация на них поступает пакетами данных, а интервалы их активизации соответствуют времени передаваемой информации (с учетом ее объема).

После того, как все информация передана на ВМ, формирующие базы данных, начинает работать ВМ4, которая рассчитывает текущею скорость тепловоза и передает информацию на ВМ5, которая рассчитывает режим управления локомотивом и на ВМ7, которая диагностирует состояние агрегатов и систем тепловоза. Таким образом, полученная диаграмма алгоритма управления моделью ВК соответствует ее физической реализации с учетом времени передачи информации между отдельными элементами системы.

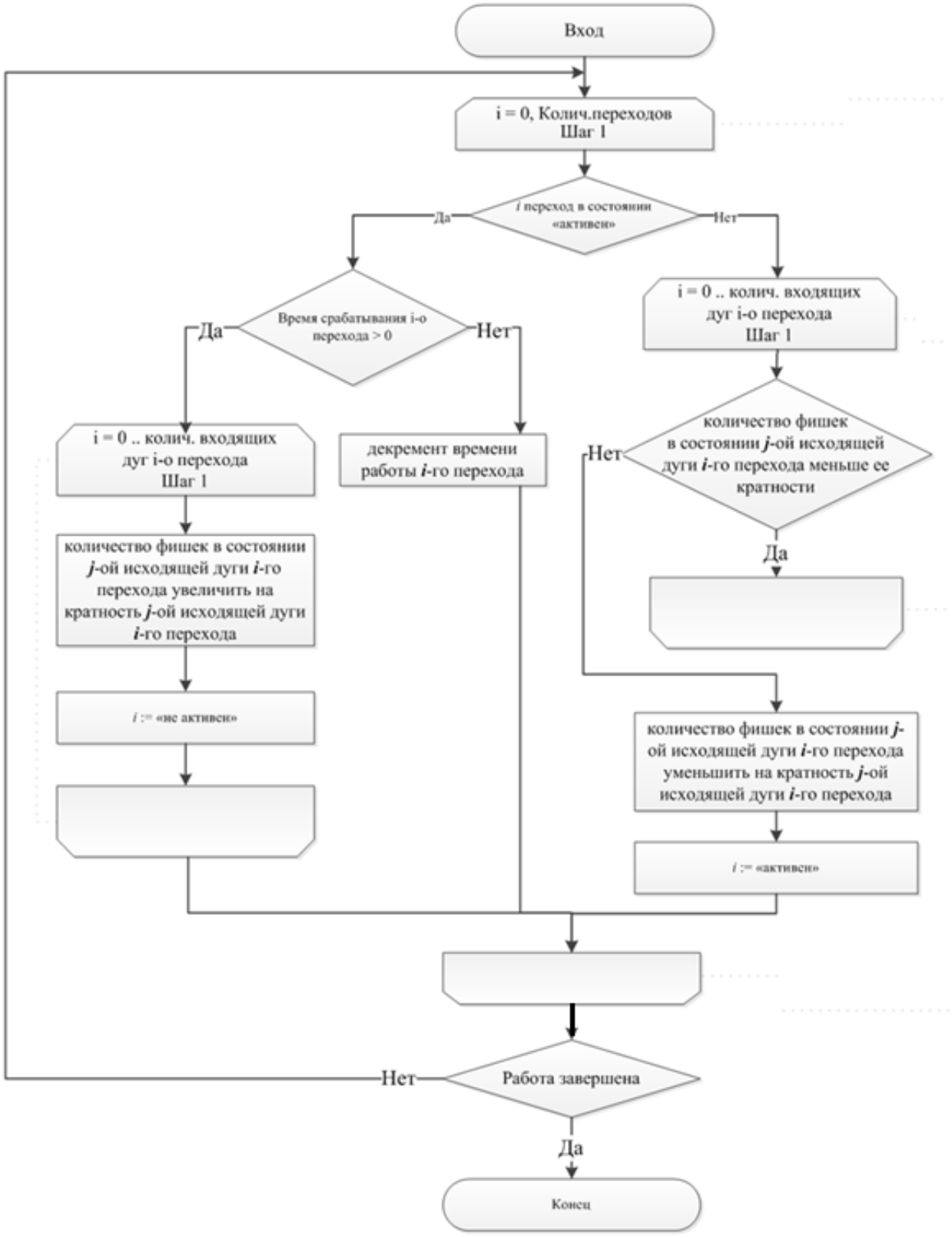


Рисунок 2.2. Блок-схема алгоритма моделирования работы ВК в терминах сетей Петри

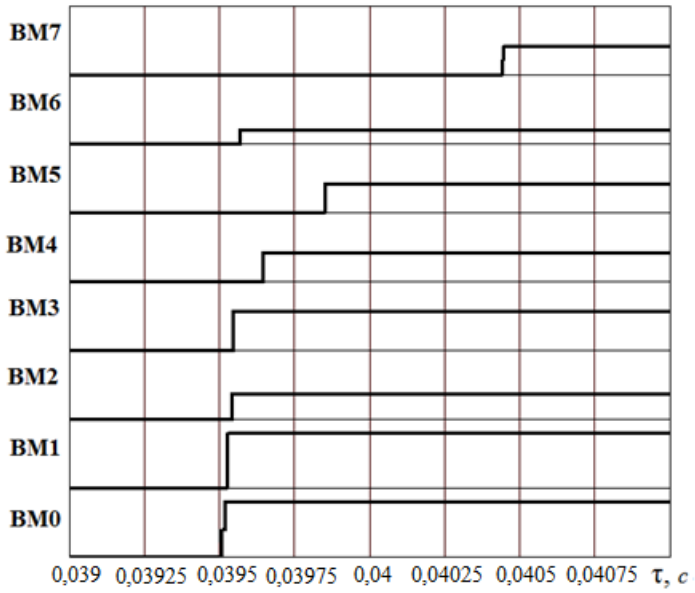


Рисунок 2.3. Результаты моделирования управления ВК при получении запроса от системы автоведения локомотива

Моделирование функционирования ВК на событийном уровне с использованием модели (2.4) в терминах сетей Петри представлено на рисунке 2.4. Диаграмма отражает процесс взаимодействия виртуальных машин с ресурсом при управлении локомотивом: с интервалом T2=100 мс ресурс по запросу передается сначала ВМ0 (позиция p_{01}), затем ВМ1, ВМ2, ВМ3, ВМ6, ВМ4,ВМ6 и ВМ7 (позиция p_{11}, p_{21}, p_{31}, p_{61}, p_{41}, p_{51}, p_{71}). По истечении нормированного времени работы системы автоведения локомотива ресурс возвращается от каждой из ВМ (p_{02}, p_{12}, p_{22}, p_{32}, p_{62}, p_{42}, p_{52}, p_{72}). Поскольку ресурс рассчитан на одновременную работу всех ВМ срабатывают переходы t_{01},t_{11},t_{21},t_{31},t_{61},t_{41},t_{51},t_{71}, изымая маркеры из позиций p_{03}, p_{13}, p_{23}, p_{33}, p_{63}, p_{43}, p_{53}, p_{73}, т.е. время ожидания ресурса каждой ВМ равно нулю.

Таким образом, результаты динамического моделирования изменения состояний позиций и переходов в модели ВК отражают заданный алгоритм управления физическим вычислительным комплексом.

Верификация модели ВК при расчете нагрузки на ресурс выполнялась при двух режимах работы комплексной системы управления движением поездов - при минимальной нагрузке и максимальной нагрузке.

В первом случае выполнялось моделирование процесса функционирования ВК при его взаимодействии с одной секцией локомотива поезда, движущегося на участке, контролируемом ДЦ «Сетунь» (рисунок 2.5).

Условиями моделирования предполагалось, что запросы от локомотива на ВК поступают при $\tau_з$=(14+T2) мс от начала отсчета, а время для обработки текущей информации и расчет режима работы локомотива составляет $\tau_р$=20 мс. Такая нагрузка на ресурс возможна, если

в передаваемых пакетах изменилась небольшая часть данных (например, не изменились характеристики профиля участка и поездная ситуация).

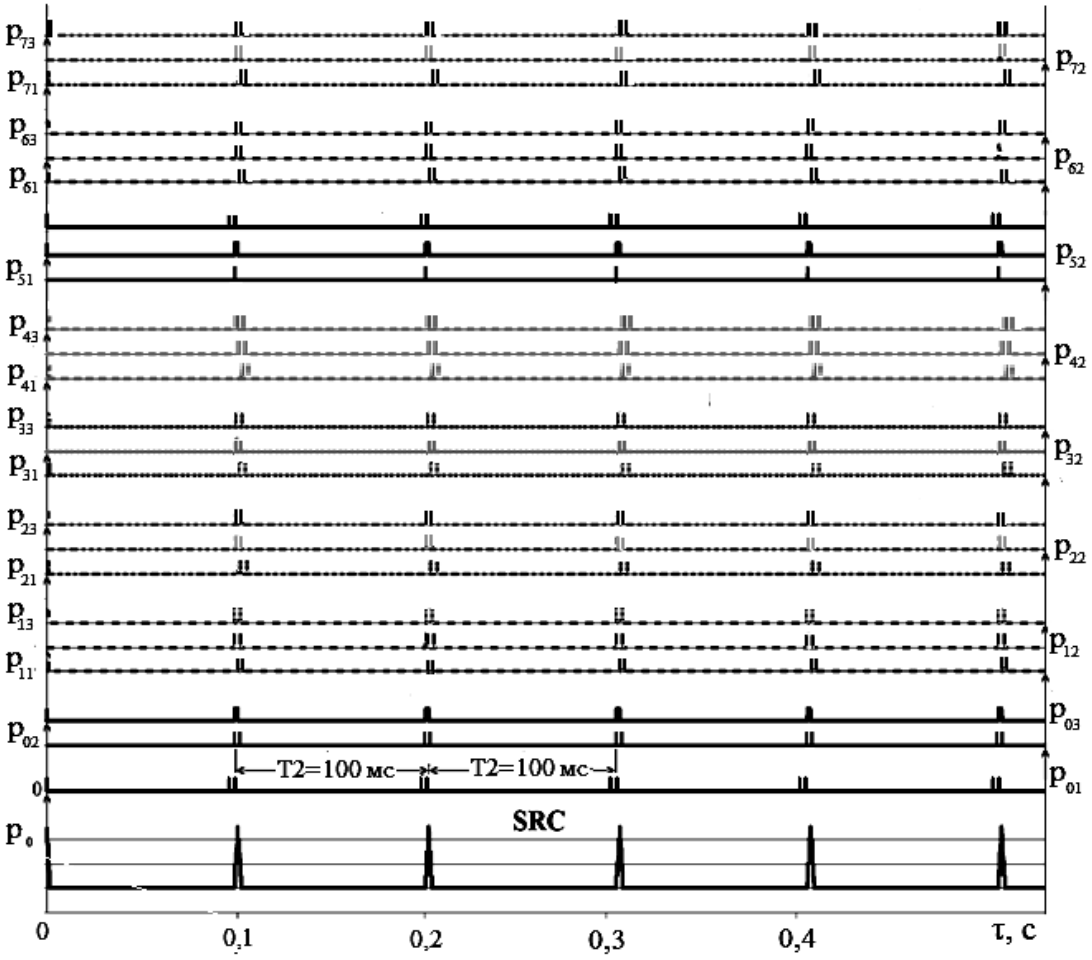


Рисунок 2.4. Моделирование динамических процессов в ВК в терминах сетей Петри

Полученные данные показывают, что нагрузка на ресурс соответствует расчетной от одной секции SRC=2532 КБ, причем основная часть нагрузки приходится на ВМ5, которая вычисляет режим движения локомотива, а большую часть времени ресурс остается свободным. Кроме ВМ5 значительный ресурс потребляет ВМ0 «шлюз», через который проходят пакеты информации от локомотива и ДЦ «Сетунь» на ВК и обратно. Нагрузки от остальных ВМ составляют менее 100 КБ. При моделировании получено, что значения нагрузок от ВМ, соответствуют расчетным (см. таблицу 2.1) и синхронизированы по времени, что отвечает условиям функционирования ВК.

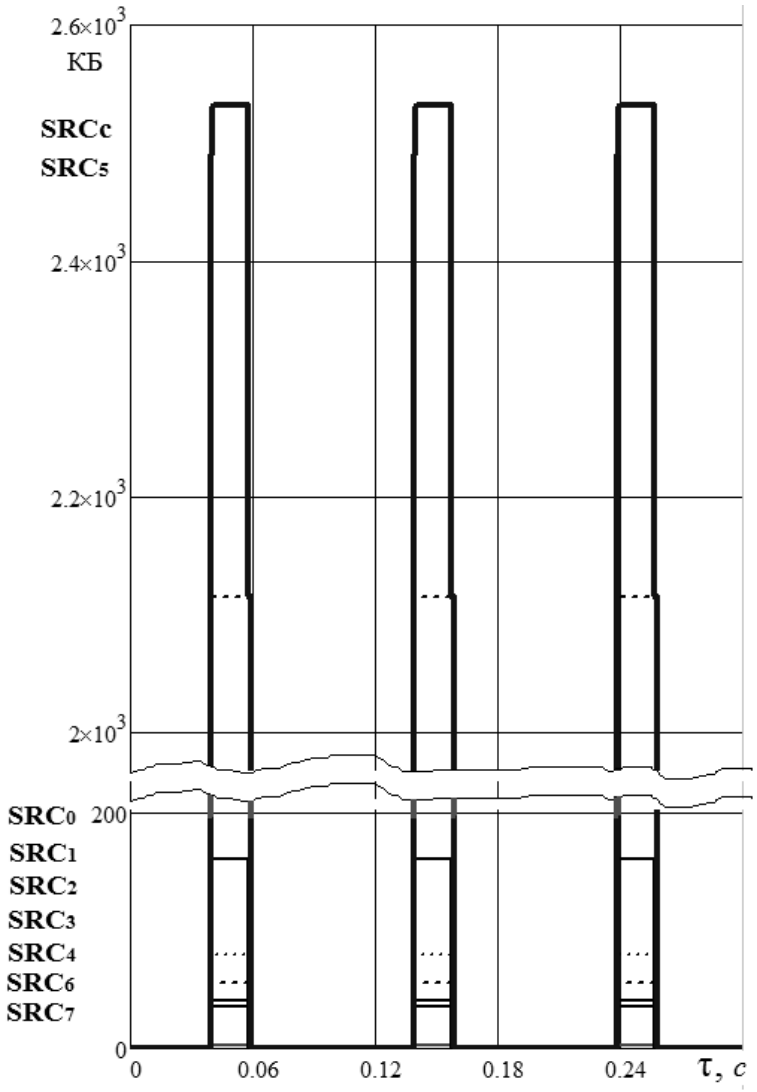


Рисунок 2.5. Диаграмма нагрузки на ресурс ВК от системы автоведения одного локомотива

Наибольшая нагрузка на ресурс ВК будет иметь место, если на контролируемом участке находится максимально допустимое число поездов, которое в соответствии с [95] для участка протяженностью 200 км составляет 68 единиц, а запросы, отправляемые от систем автоведения локомотивов этих поездов, оказались синхронизированы по времени и требуют максимального времени проводимых вычислений.

Результаты моделирования такого режима представлены на рисунке 2.6, из которых следует, что в этом случае ресурс ВК, предназначенный для работы комплексной системой управления движением используется полностью и соответствует расчетному SRC=517 Мб (см. таблицу 2.2). Резкое снижение нагрузки на ресурс при текущем времени τ=0; 0,1; 0,2; 0,3 мс соответствует режимам передачи пакетов информации по внутренним каналам связи ВК.

Таким образом, результаты верификации разработанной модели ВК показали возможность ее использования для расчета характеристик и исследования процессов при нормальной работе и внештатных ситуациях.

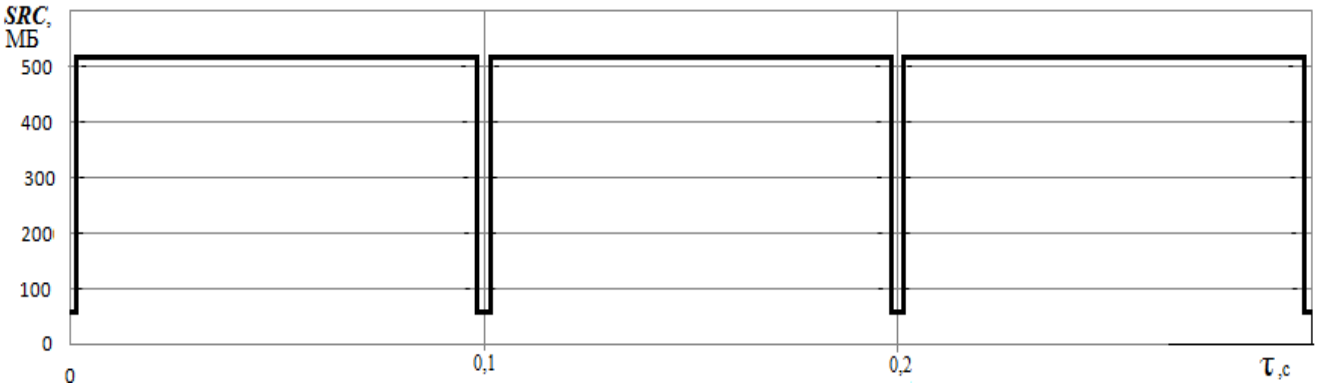


Рисунок 2.6. Диаграмма нагрузки на ресурс ВК от систем автоведения 68 поездов при синхронных заявках на обслуживание с максимальным временем расчета режима работы

2.4. Расчет характеристик работы вычислительного комплекса при работе в системе управления движением

Разработанная модель ВК в терминах расширенных сетей Петри позволяет моделировать динамические асинхронные процессы, происходящие в системе и определять ее характеристики. В связи с этим были определены нагрузка на ресурс при нормальной работе ВК и ограничениях по времени выполнения программы расчета параметров режимов управления локомотивами в соответствии с требованиями алгоритма работы системы автоведения поезда.

В реальных условиях эксплуатации железных дорог следует ожидать, что заявки на обслуживание систем автоведения поездов будут поступать на ВК в разные моменты времени. Кроме того необходимо учитывать, что характеристики профиля, поездная ситуация и режим работы локомотива каждые 100 мс не меняются, поэтому массивы данных о параметрах и ограничениях движения могут в течение секунды многократно повторяться, что сокращает время использования ресурса ВК.

На рисунке 2.7 представлена диаграмма моделирования взаимодействия шлюза (ВМ0) с ресурсом ВК при случайном времени запросов, поступающих от систем автоведения 15 локомотивов при общем числе поездов на линии - 68. Время поступления заявок на обслуживание локомотивов всех поездов задавалось равномерным законом распределения. Запросы на ресурс от шлюза соответствуют состояниям позиций p_{01}в модели ВК (2.4) (см. рисунок 2.1):p_{01}^{0} – для первого локомотива; p_{01}^{1} – для второго локомотива;…; p_{01}^{14} – для пятнадцатого локомо-

тива. Из диаграммы видно, что интервалы запросов от каждого локомотива составляют T2=100 мс, а нагрузка на ресурс имеет случайный характер. Поскольку на диаграмме приведены результаты только для 15 локомотивов из 68 поездов, представленная нагрузка на ресурс не отражает равномерного характера распределения запросов. При этом важно отметить, что из-за наличия строгого периода заявок T2 от систем автоведения, использование ресурса также имеет периодичность в 100 мс.

Этот процесс был рассчитан с использованием разработанной модели, когда текущее время предоставления ресурса хоста задавалось с использованием генератора псевдослучайных чисел. Алгоритмом моделирования выполнялось дискретное разбиение временной оси τ и задавалось распределение количества событий λ на каждом промежутке времени $\Delta\tau$ в предположении, что λ и τ являются независимыми величинами, т.е. работа ВК рассматривалась как процесс со случайными интенсивностями событий $\lambda=\lambda(\tau)$.

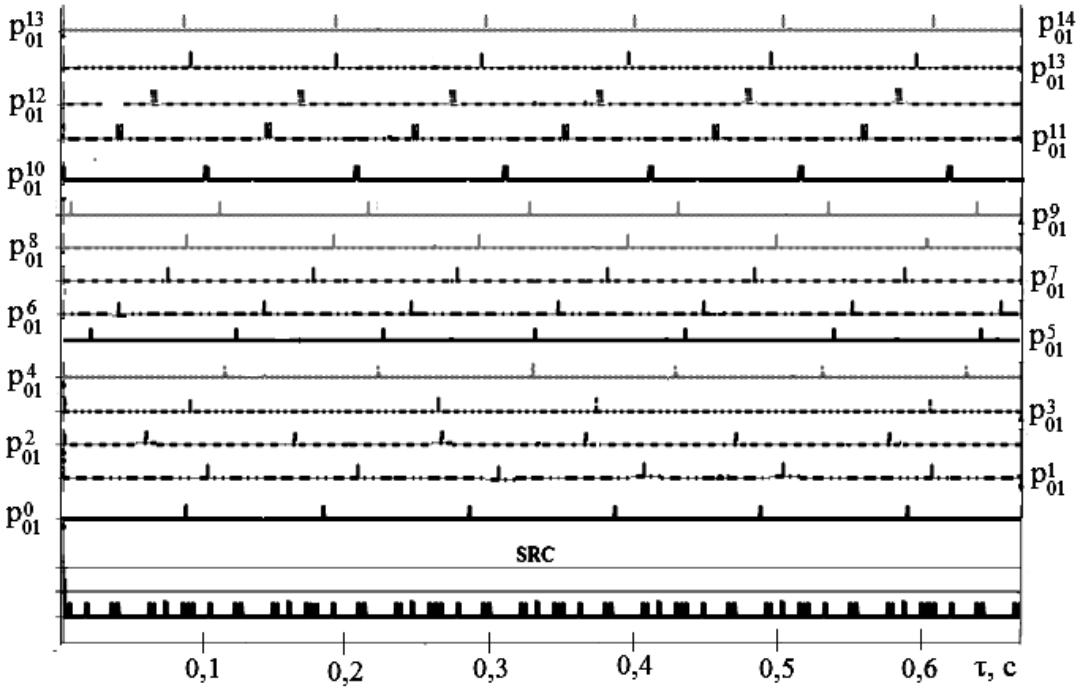


Рисунок 2.7. Моделирование динамического процесса поступления запросов на ресурс ВК от 15 локомотивов при общем числе поездов на линии - 68

На рисунке 2.8 приведена нагрузка на ресурс ВК от систем автоведения при обслуживании 68 поездов, если время работы в каждом цикле составляет τ_p= 15 мс, а запросы от каждого локомотива распределены по равномерному закону с периодом T2=100 мс.

Как видно из представленной диаграммы при таком режиме нагрузка на ресурс ВК представляет собой периодическую функцию с периодом Tн=100 мс (поскольку заявки на обслуживание от систем автоведения поступают с интервалом T2=100 мс), а шестикратное со-

кращение времени обработки заявки от системы автоведения относительно допустимого также в шесть раз сокращает интегральную нагрузку на ресурс.

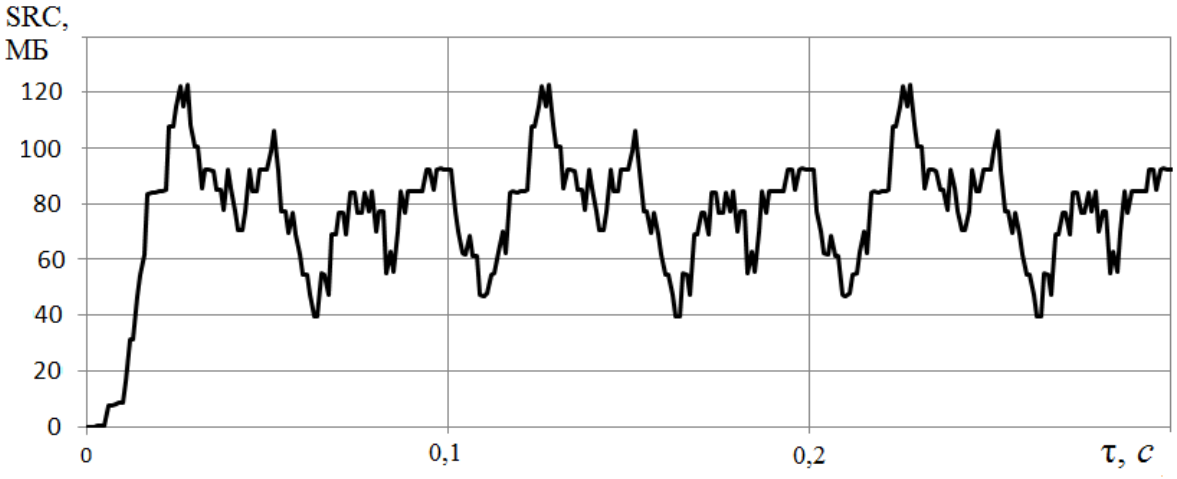


Рисунок 2.8. Нагрузка на ресурс ВК от систем автоведения 68 поездов при заявках на обслуживание с равномерным распределением и временем расчета режима работы $\tau_р$= 15 мс

Если и время работы ВК в каждом цикле определять как равномерно распределенную случайную величину с математическим ожиданием $\tau_р$= 15 мс нагрузка на ресурс теряет периодичность, но интегральная нагрузка на ресурс остается прежней (рисунок 2.9).

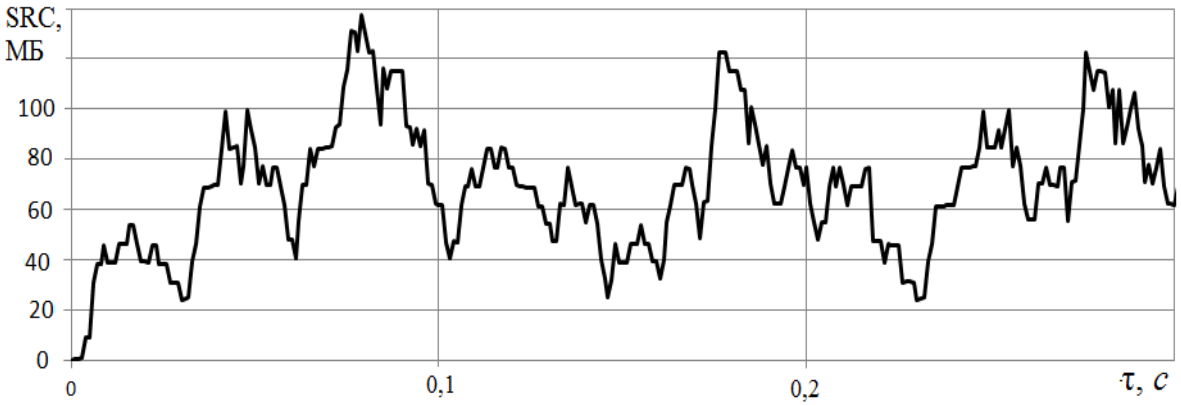


Рисунок 2.9. Нагрузка на ресурс ВК от систем автоведения 68 поездов при заявках на обслуживание с равномерным распределением и случайным временем расчета режима работы с математическим ожиданием $\tau_р$= 15 мс

При увеличении времени обработки заявок до максимально допустимого значения $\tau_р$=100 мс нагрузка на ресурс возрастает, но и в это случае не достигает расчетного значения, т. е. 517 МБ. (рисунок 2.10).

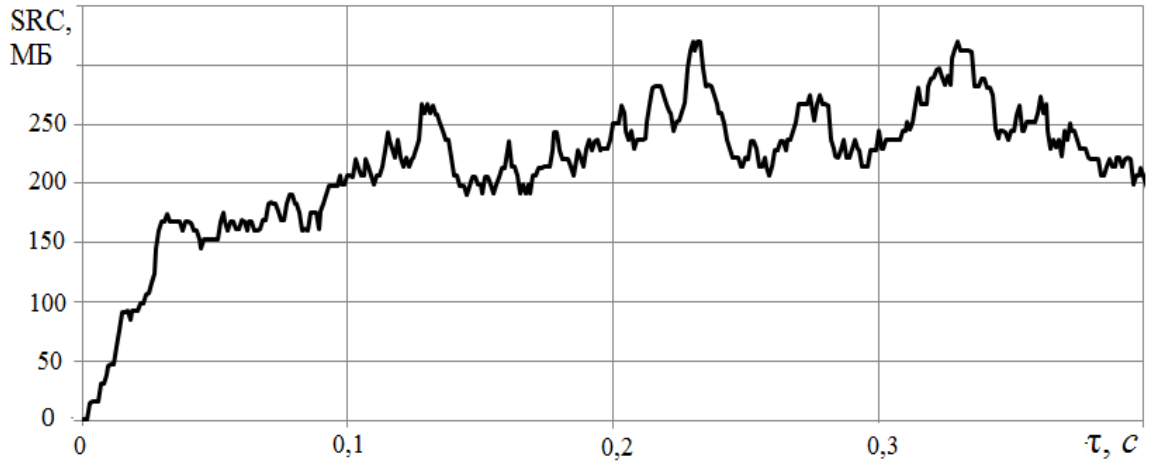


Рисунок 2.10. Нагрузка на ресурс ВК при равномерных распределениях заявок от каждого поезда с интервалом Т2=100мс и времени загрузки вычислительного ресурса ВМ5 в диапазоне $0 \leq \tau_{\text{ВМ5}} \leq 99$ мс

Таким образом, проведенные исследования показали, что при эксплуатации ВК системы управления движением в среднем его ресурс только на обслуживание систем автоведения будет использоваться на 50%. Однако, учитывая нагрузку от системы мониторинга, удельные показатели использования ресурса ВК возрастают. Расчет показал, что при учете нагрузки от системы мониторинга ВК эффективность использования его ресурса возрастает до 73% (рисунок 2.11).

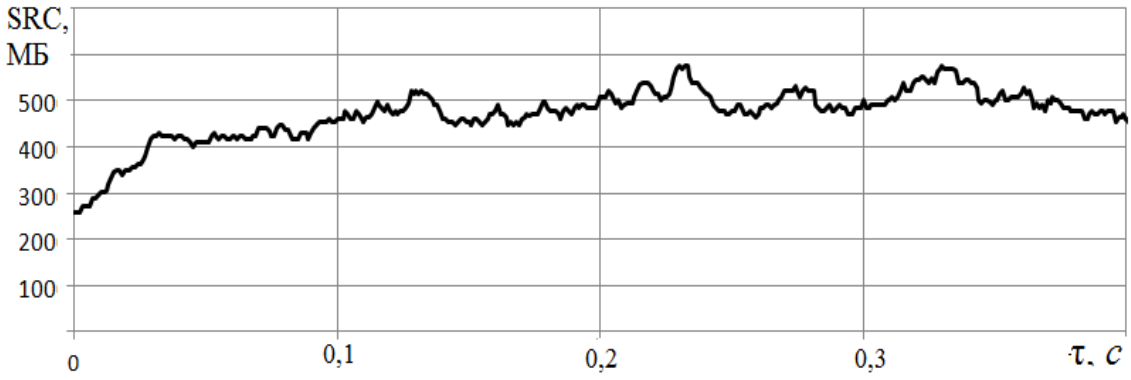


Рисунок 2.11. Нагрузка на ресурс ВК при равномерных распределениях заявок на обслуживание поездов, времени загрузки вычислительного ресурса ВМ5 в диапазоне $0 \leq \tau_{\text{в}} \leq 96$ мс и с учетом работы системы мониторинга

Разработанная модель работы ВК системы управления движением позволила установить требования по допустимому времени работы циклической программы расчета режима управления поездом. Поскольку рассчитанные параметры режима работы должны быть переданы на локомотив с учетом интервального времени цикла работы системы автоведеня, скоро-

сти передачи информации по канала связи ВК 1 Гбит/с и алгоритма управления всеми ВМ, максимально допустимое время работы программы ВМ5 составило τ_{BM5}=99,5 мс (рисунок 2.12).

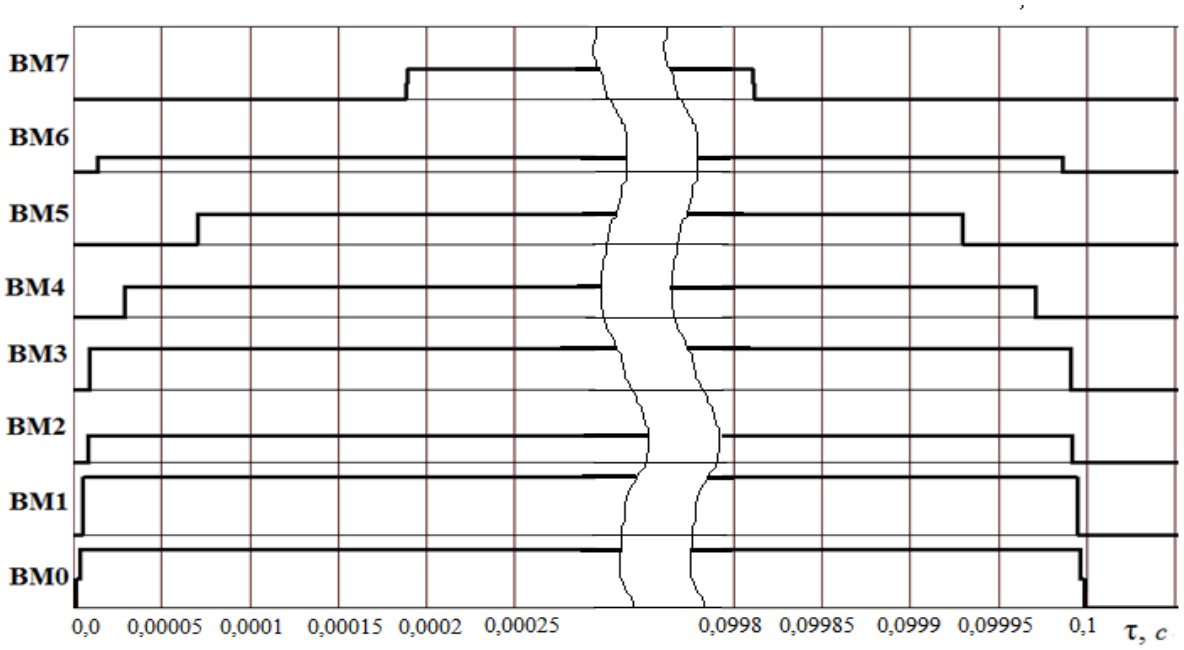


Рисунок 2.12. Полный цикл работы ВК по одному запросу системы автоведения локомотива

2.5. Определение эффективности использования вычислительного комплекса

Полученные результаты показали, что затраты ресурса ВК на обслуживание заявок комплексной системы управления движением на участке 200 км в общем расходе ресурса ВК составляет менее 10% (см. таблицу 2.2). Это нельзя рассматривать как эффективное использование ресурса ВК для решения основной задачи. Поэтому важно определить при какой длине участка обслуживаемого комплексной системой управления движения ресурс ВК будет использоваться наиболее эффективно.

Для реализации разрабатываемого ВК предлагается использовать сервер IBM Flex System x240 с встроенной фабрикой IBM® Virtual Fabric, которая обеспечивает высокую гибкость ввода-вывода. В настоящее время 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) опти-

мизирован 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.

Вычислительный узел Flex System x240 обеспечивает максимальную производительность (на 50% выше производительности серверов предыдущего поколения). Благодаря этому потребители могут эффективно использовать вычислительную среду для широкого спектра рабочих нагрузок. В таблице 2.3. приведены цены сервера IBM Flex System x240 разной комплектации.

Очевидно, что при использовании любого высокотехнологичного оборудования целесообразно оптимизировать его производительность и цену.

Таблица 2.3

Цена сервера IBM Flex System x240 различной комплектации

Процессор	Оперативная память, ГБ	Цена, руб.
Xeon 8C E5-2670 115W 2.6GHz/1600MHz/20MB	4 GB	198 425
	8GB	202 725
	3x4=12GB	207 025
	2x8=16GB	211 325

Это приводит к решению задачи оптимизации с векторной целевой функцией [105, 106, 107]:

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

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 выступает ресурс, необходимый для обслуживания систем автоведения поездов, находящихся на контролируемом участке, и его цена, а качестве параметра управления – возможное число обслуживаемых локомотивов G на этом же участке.

$$\begin{cases} K_1(G) \to \min \\ K_2(G) \to \max \end{cases}, \quad . \qquad (2.5)$$

где: K_l – цена сервера;

K_2 – ресурс сервера, необходимый для обслуживания заявок локомотивов.

Поиск оптимального распределения ресурсов такой системы сводится к определению множества неулучшаемых решений (оптимизации по Парето), т.е. приближению параметров

управления системой к значению, при котором обеспечивается приближение $Ц(u)$ к утопической точке $K_{ут}$ [108, 109, 110] (рисунок 2.13).

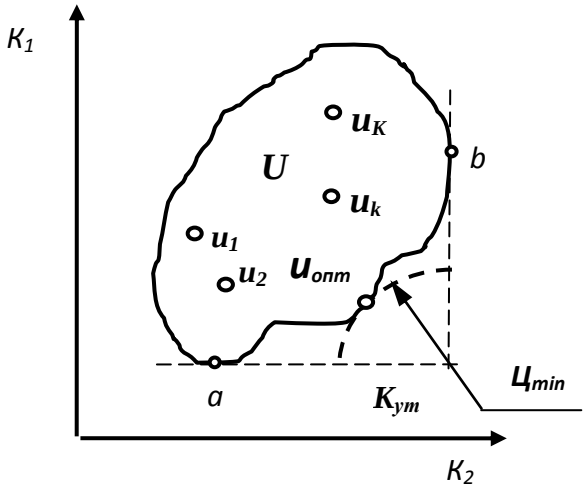


Рисунок 2.13. К определению оптимальной структуры ВК

В данном случае множеству неулучшаемых решений соответствует отрезок $[a,b]$ функции $K_1(u) = f(K_2(u))$, а оптимальное решение определяется приближением значений K_1 и K_2 к утопической точке $K_{ут}$, которая по определению не принадлежит к множеству неулучшаемых решений и поэтому достигнута быть не может.

В задачах векторной оптимизации для отыскания вектора управлений, обеспечивающих парето-оптимальные решения, используется обобщенный критерий [111,112]

$$\sum_{l=1}^{L} a_l K_l(u) = \min_{u \in U}, \qquad (2.6)$$

где a_l - весовой коэффициент l-го критерия ($a_l > 0$, если согласно условию задачи критерий K_l должен минимизироваться, $a_l < 0$ если критерий K_l должен максимизироваться).

Для принятых критериях оптимизации применительно к решаемой задаче обобщенный критерий оптимального управления ВК в соответствии с (2.6) имеет вид:

$$a_1 K_1(G) - a_2 K_2(G) \to \min. \qquad (2.7)$$

При анализе работы ВК существует неопределенность при выборе значений весовых коэффициентов для зависимости (2.7) в линейной комбинации критериев. Поэтому, в данном случае целесообразно использовать минимаксное решение задачи оптимизации, когда минимизируется наибольшее из отклонений каждого критерия от утопической точки (минимаксное чебышевское решение) [111, 112] :

$$\max\left|K_l(u) - K_{ут}\right| \to \min_{u \in U}.$$

Поскольку в данном случае эффективность использования ВК определяется двумя конфликтующими критериями $Ц(K_1, K_2, G)$ оптимизацию целесообразно выполнять с использованием стратегии взвешенных сумм [112]. Использование этой стратегии позволяет многокритериальную задачу минимизации длины вектора $Ц(u)$ преобразовать в скалярную величину, представляющую собой взвешенную сумму для используемых критериев

$$minimize_{u \in U} Ц(u) = \sum_{l=1}^{L} w_l [K_l(u)]^2 \qquad (2.8)$$

где w_l - взвешенные коэффициенты, которые должны соответствовать относительной значимости частных критериев.

Применительно к ВК с учетом (2.8) оптимальное решение находится минимизацией расстояния до точки $K_{ут}$ на плоскости критериев $(K_1, 0, K_2)$ (рисунок.2.13):

$$\begin{cases} Ц(G) = \min ; \\ Ц^2(G) = \left[K_1(G) - K_{1\min}\right]^2 + \left[K_2(G) - K_{2\max}\right]^2 . \end{cases} \qquad (2.9)$$

Таким образом, целевая функция для определения эффективности работы ВК в соответствии с (2.9) по принятым критериям определиться как минимизация радиус-вектора неулучшаемых решений от $K_{ут}$ (рисунок 2.13)

$$Ц(G) = \sqrt{\left[K_1(G) - K_{1\min}\right]^2 + \left[K_2(G) - K_{2\max}\right]} \to \min \qquad (2.10)$$

Поскольку значения критериев, принятых в соответствии с (2.5), могут отличаться на несколько порядков (в зависимости от масштабов измерения значений K_1 и K_2), целевую функцию для определения эффективности работы ВК целесообразно определить через их относительные величины:

$$\begin{cases} \overline{K}_1(G) = \dfrac{K_1(G) - K_1^*}{K_1^{**} - K_1^*} ; \\ \overline{K}_2(G) = \dfrac{K_2(G) - K_2^{**}}{K_2^{**} - K_2^*} , \end{cases}$$

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.

С учетом (2.10) при равной значимости принятых критериев эффективности использования ресурса ВК, целевую функцию целесообразно представить как кратчайшее расстояние до утопической точки в относительной системе координат:

$$Ц(G)=\sqrt{\left(\frac{K_1(G)-K_1^{*}}{K_1^{**}-K_1^{*}}\right)^2+\left(\frac{K_2(G)-K_2^{**}}{K_2^{**}-K_2^{*}}\right)^2}\rightarrow \min . \qquad (2.11)$$

В соответствии с (2.11) были рассчитаны значения $Ц(G)$ в диапазоне 68≤ G≤ 1088 (шестнадцать участков протяженностью 200 км) для полигона ж.д. Ярославского направления при допустимом интервале следования поездов (рисунок 2.12).

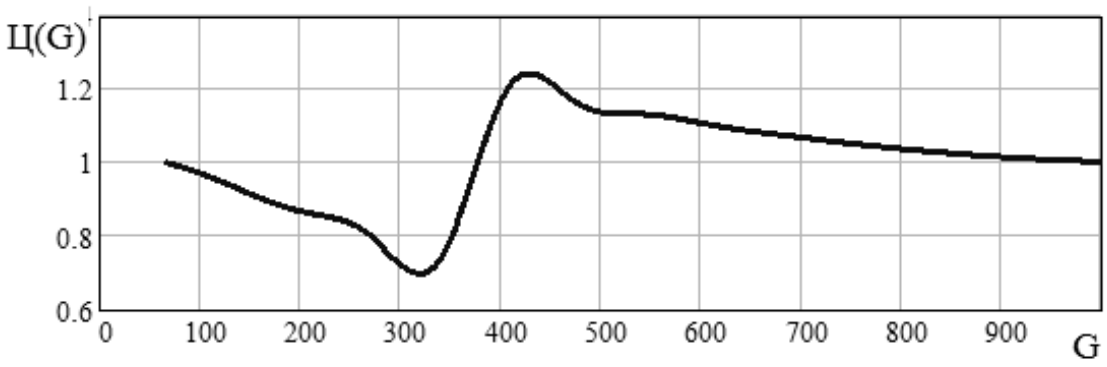


Рисунок 2.12. Значения целевой функции эффективности использования ресурса ВК в зависимости от числа локомотивов на обслуживаемом участке ж.д.

Результаты расчетов показали, что при равной значимости частных критериев эффективности $\overline{K}_1(G)$ и $\overline{K}_2(G)$ ресурс ВК будет использоваться наиболее эффективно, если комплексная система управления движением будет обслуживать 320 поездов, т.е. участок ж.д. протяженностью 950 км

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 организации каналов взаимодействия этих приложений. (ПРИЛОЖЕНИЕ А). Материалы работы были частично опубликованы в журнале «Информационные технологии в проектировании и производстве» 2013г., № 2 [113].

2.6. Выводы по главе II

Для расчета требуемого ресурса вычислительного комплекса и исследования его функционирования в системе управления движением:

1. 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 ди-

намический процесс распределения ресурса между приложениями в виртуальной инфраструктуре с учетом параллельных и асинхронных процессов их взаимодействия и рассчитывать количественные показатели работы системы, в том числе, при моделировании сценариев использования резервных элементов комплекса.

2. Верификация математической модели вычислительного комплекса выполнялась при имитации процессов взаимодействия приложений по заявке на обслуживание системы автоведения одного локомотива и по заявкам локомотивов, движущихся на контролируемом участке с допустимым интервалом следования (режим максимальной нагрузки на ресурс) путем соответствия ТУ на функционирование систем автоведения поезда, устройств безопасности движения и диспетчерской централизации.

3. Рассчитана нагрузка на ресурс хоста при различных характеристиках потока заявок от локомотивов и времени обработки каждой заявки.

4. Разработана методика расчета оптимальной длинны участка ж.д., контролируемого системой управления движением, на базе метода векторной оптимизации по противоречивым частным критериям, в качестве которых выступают ресурс и цена сервера, и имитационной модели функционирования вычислительного комплекса.

5. Для обеспечения требований стандартов ОАО «РЖД» 1.18.002-2009 к системам управления движением на сети ж.д. должны быть разработаны мероприятия, гарантирующие функционирование вычислительного комплекса при внезапном отказе одного из его элементов, и определены уязвимости с целью выбора эффективной защиты.

III. ВОЗМОЖНЫЕ УЯЗВИМОСТИ ВЫЧИСЛИТЕЛЬНОГО КОМПЛЕКСА И МЕТОД БОРЬБЫ С НИМИ

3.1. Использование средств резервирования ВК для повышения надежности его функционирования

При разработке любой высокотехнологичной системы, особенно системы связанной с безопасностью движения, должны быть предусмотрены меры по сохранению ее работоспособности в случае внезапных частичных отказов. Применительно к виртуальному ВК таким частичным отказом является потеря работоспособности одной из ВМ. Поэтому в ходе выполнения работы была проанализирована возможность разворачивания резервной ВМ (ВМ9) при ограничениях на функционирование комплексной системы управления движением поездов.

Для расчета динамических характеристик ВК при отказе одной ВМ была разработана его модель, отражающая динамический процесс разворачивания резервной ВМ на хосте (рисунок 3.1).

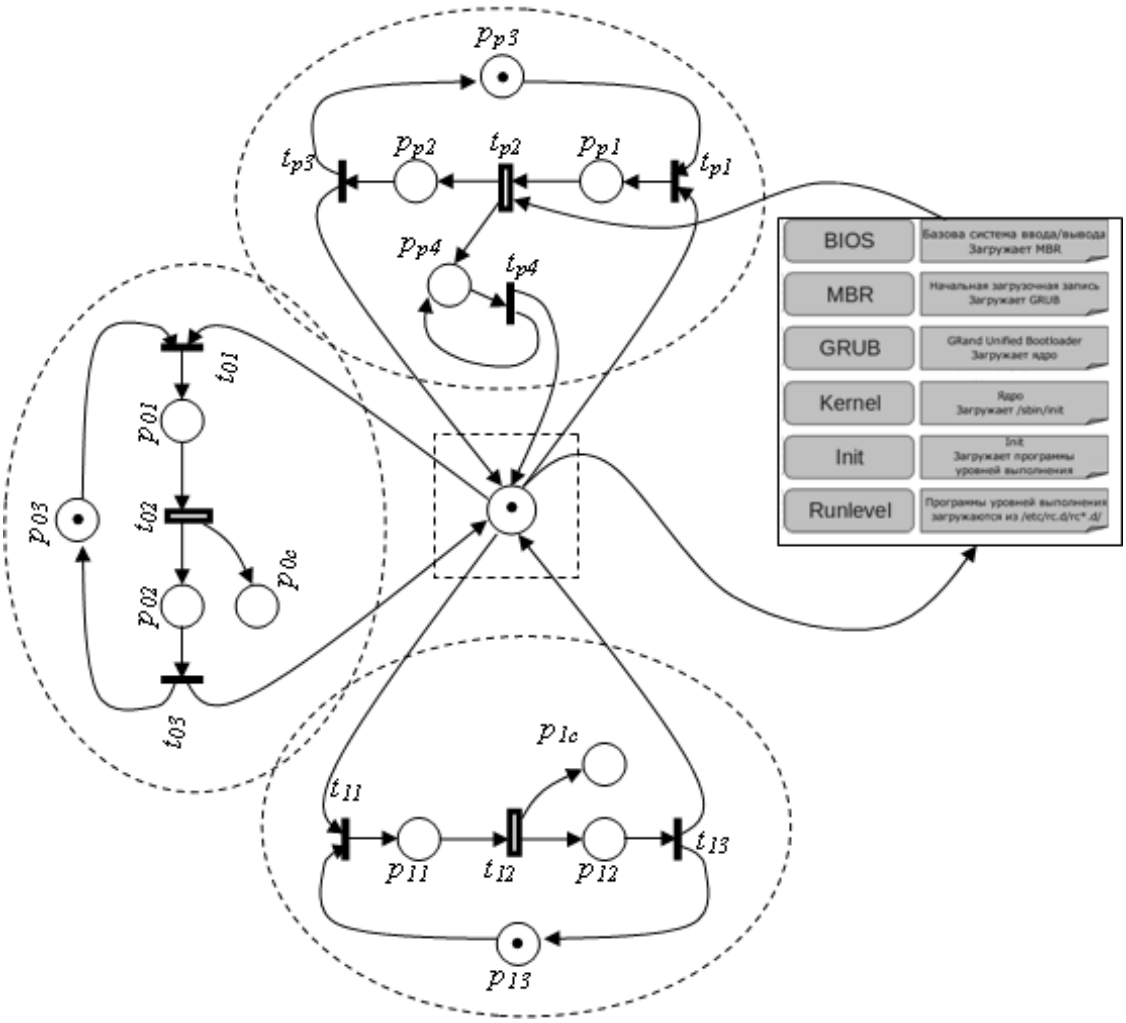


Рисунок 3.1 Модель функционирования ВК при разворачивании на хосте резервной $ВМ_р$

Модуль разворачиваемой $ВМ_р$ содержит дополнительную позицию p_{p4}, функциональное назначение которой - сформировать пакет ПО, обеспечивающего работу требуемой $ВМ_р$. В память $ВМ_р$ последовательно загружаются модули ОС: BIOS, MBR, GRUB, Kernel, Init, Runlevel; этот процесс отражается переходом $t_{p2.}$ Время загрузки каждого модуля принималось исходя из времени загрузки ОС ВМ. После того как все необходимое ПО для работы разворачиваемой $ВМ_р$ загружено срабатывает переход t_{p4} и делает дополнительную связь между ресурсом и уже развернутой $ВМ_р$ неактивной. С этого момента вновь развернутая $ВМ_р$ начинает функционировать в нормальном режиме и ей начинают передаваться потоки данных отказавшей ВМ. При этом предполагалось, что исправные ВМ вычислительного комплекса работают в штатном режиме, создавая соответствующую нагрузку на ресурс.

Разработанная модель внештатной работы ВК в терминах сетей Петри, построенная на базе (2.4) , была использована для моделирования динамического процесса отказа одной из его ВМ и разворачивания резервной $ВМ_р$. По условиям моделирования заявки на обслуживание систем автоведения поездов и время загрузки вычислительного ресурса ВМ5 имели равномерное распределение в соответствии с ограничениями Т2=100мс и ($\tau_{BM5)max}$=99,5 мс.

Результаты моделирования этого процесса приведены на рисунке 3.2. Диаграмма рисунка 3.2а иллюстрирует функционирование ВК в терминах сетей Петри: изменение количества операций, выполнимых каждой ВМ, изменение состояний позиций (p_{ij}) ВМ0-ВМ9 и значение свободного ресурса ВК**.** Моделирование было проведено при разворачивании снапшота ВМ.

Результаты моделирования показали, что время загрузки снапшота составляет 15,0 с. Эксперименты по разворачиванию снапшота на физическом хосте дали близкий результат (рисунок 3.2б). В зависимости от степени загрузки ресурса хоста это время может составлять от 11 до 17 с. Таким образом сопоставление полученных результатов показывает их хорошую сходимость

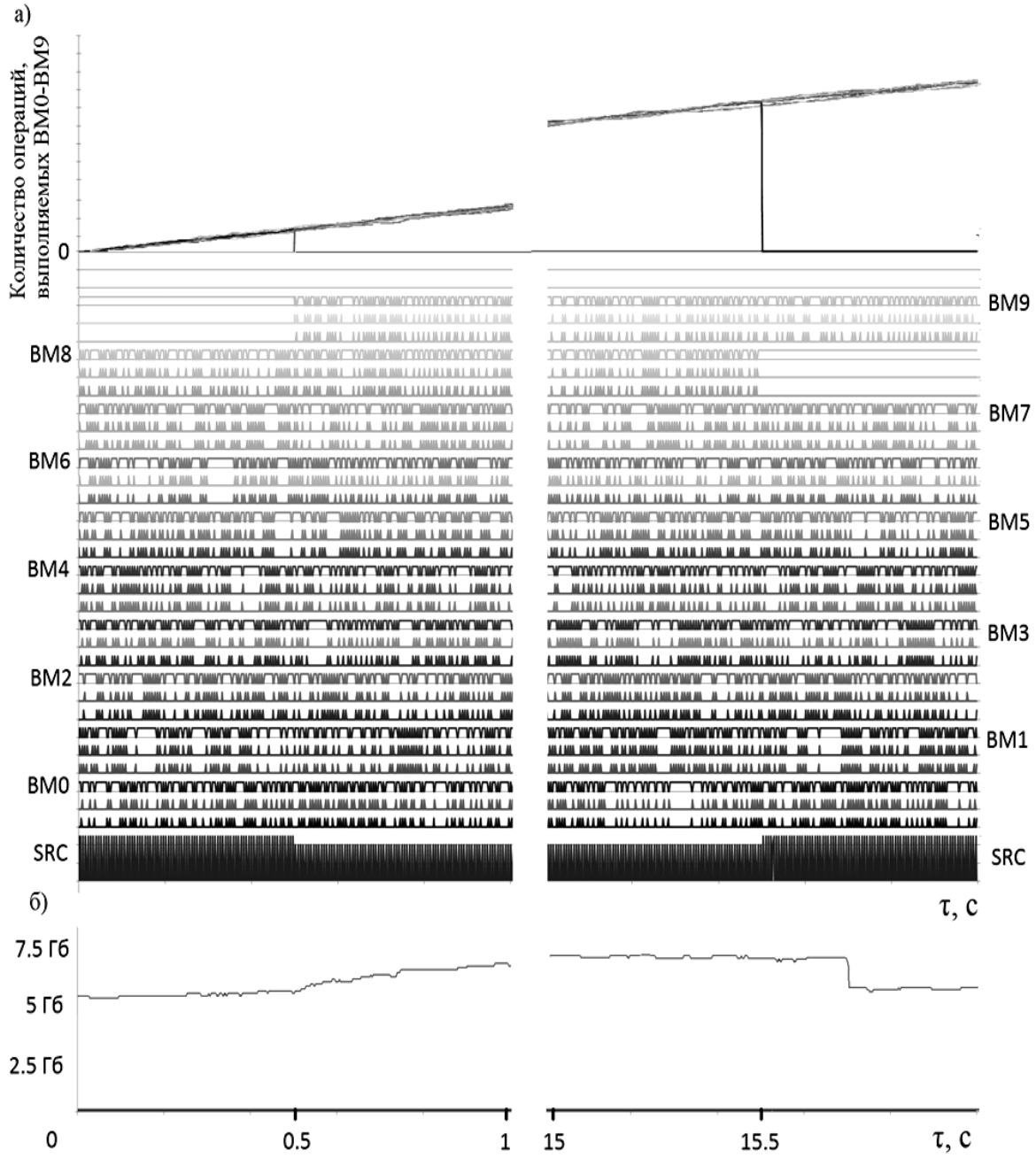


Рисунок 3.2. Процесс разворачивания резервной ВМ9 со снапшотаом: расчетный процесс (а); экспериментальный процесс (б)

Аналогичные эксперименты были проведены при загрузке на хостовую систему ВМ только с базовой ОС. Было получено, что в этом случае время разворачивания ВМ составляет от 7 до 12 секунд. Расчетные и экспериментальные результаты разворачивания ВМ с базовой ОС приведены на рисунке 3.3.

Результаты расчета времени разворачивания резервных ВМ показали, что минимальное значение не может составлять менее 5 с, что не отвечает требованиям алгоритма работы системы автоведения поезда (таблица 3.1).

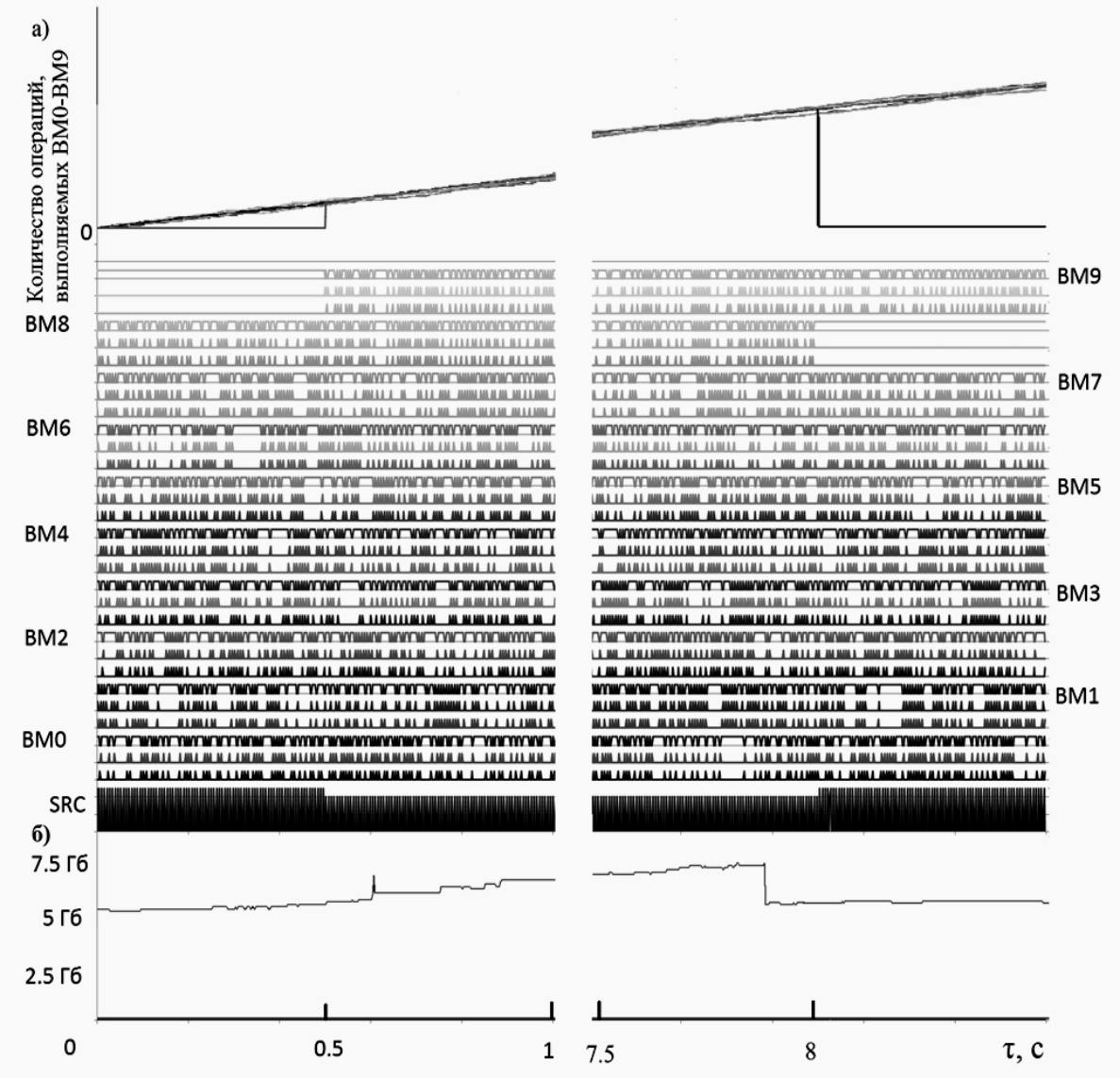


Рисунок 3.3. Процесс разворачивания резервной ВМ9 с базовой ОС: расчетный процесс (а); экспериментальный процесс (б)

Таблица 3.1

Значения времени разворачивания резервных ВМ и загрузки необходимого программного обеспечения

Программное обеспечение	Время, с
Загрузка виртуальной машины с базовой ОС	7-12 с.
Загрузка виртуальной машины со снапшотом	11-17 с.
Загрузка баз данных	8-12 с.
Загрузка ПО системы автоведения	4-6 с.

Таким образом получено, что при отказе одной из ВМ использование резерва ресурса не позволит развернуть на хосте дополнительную ВМ и передать ей функции управления за Т2=100 мс.

3.2. Резервирование вычислительного комплекса

В современных условиях интенсивного движения железнодорожного транспорта и, особенно, с началом эксплуатации скоростных поездов, вопросам безопасности и надежности управления перевозочным процессом придается особое внимание.

В ОАО «РЖД» действуют стандарты обеспечения надежности функционирования систем автоматики, телемеханики и связи, осуществляющих управление движением на сети ж.д. В этих стандартах отказы современных релейных систем железнодорожной автоматики подразделяются на защитные и опасные. Появление сложных микропроцессорных систем привело к выделению нового класса отказов – маскируемых, которые не приводят непосредственно к нарушению функционирования системы, но вызывают накопление отказов и, как следствие, изменяют ее работу. Для контроля работоспособности системы используются такие параметры и события, как целостность линий связи с модулями ввода-вывода, ошибка контрольной суммы, ошибка памяти, «зависание» процессора и т. п. Перечень процедур контроля приведен в [114].

Необходимые показатели безотказности, контролепригодности и безопасности микропроцессорных систем железнодорожной автоматики и телемеханики достигаются за счет использования аппаратного или программного резервирования. Для контроля правильности работы каналов обработки информации используется аппаратное или программное сравнение результатов выполнения отдельных команд или решения отдельных задач.

Используемые методы резервирования и контроля в системах железнодорожной автоматики, отвечающие требованиям безопасности, должны обеспечивать:

- независимость отказов в однотипных элементах функционально избыточных структур;

- защиту системы от сбоев и отказов, исключение накопления отказов;

- контроль правильности функционирования программного обеспечения.

При структурном резервировании критическими узлами с точки зрения независимости отказов в различных вычислительных каналах являются входная и выходная информация, питание, достоверность работы устройств контроля, однотипные ошибки программного обеспечения.

Программные методы резервирования и контроля требуют большего, чем аппаратные, времени обнаружения отказов, и при их использовании трудно обеспечить принципы независимости отказов в различных программах обработки информации.

Архитектура резервирования микропроцессорных систем, в том числе используемых в системах железнодорожной автоматики, может быть представлена в двух вариантах:

- резервирование замещением;

- мажоритарное резервирование.

В общем случае резервирование замещением может быть реализовано в трех различных видах получивших наименование: «холодное», «горячее» и «теплое»» резервирование замещением.

При «холодном» резервировании замещением резервное устройство имеется в наличии, но отключено, в том числе и от источника питания; для приведения его в рабочее состояние требуется достаточно продолжительное время. Поэтому «холодное» резервирование применяется в системах, не требующих высокого быстродействия.

В системах требующих высокой оперативности резервирования применяются системы «горячего» и «теплого» резервирования. Отличительной чертой «горячего» резервированием замещением является принципиальная необходимость в подсистеме контроля работоспособности как основного, так и резервного элементов, наличие блока переключения на резерв (обычно переключение выполняется программно), а также шины для синхронизации работы между процессорами (последнее относится только к резервированию процессоров). Основным параметром систем с резервированием замещением является время переключения на резерв. Переход на резерв выполняется в пределах одного или нескольких контроллерных циклов и занимает время от единиц миллисекунд до долей секунды.

Системы с более медленным переключением на резерв (от долей до единиц секунд) относят к системам с «теплым» резервом. Отличие «теплого» резервирования от «горячего» заключается в отсутствии высокоскоростного канала синхронизации между процессорами; вместо него используется стандартная низкоскоростная промышленная сеть или другой последовательный канал обмена.

Диагностическая информация о состоянии системы должна выводиться на пульт оператора и одновременно может использоваться для переключения на резерв. В системе ДЦ «Сетунь» устройства ЛВС включают в себя по два выделенных файл-сервера для всех автоматизированных рабочих мест АРМ одного района управления с учетом 100% резервирования (рис. 1.4).

Конфигурация АРМ ДНЦ включает одну рабочую станцию «Схема» в «холодном» резерве. Но рабочая станция резервного комплекта может отсутствовать, если система охвачена

100-%-ным «горячим» резервированием, при котором каждый компонент архитектуры может функционально брать на себя вышедшую из строя рабочую станцию. При наличии района управления, включающего в себя до восьми АРМ, допускается иметь в «холодном резерве» одну РС «Схема» и одну РС «Табло» на район управления. В случае выхода из строя одной из РС «Табло» ее функция будет реализовываться на оставшихся исправных рабочих станциях. Каждая ПЭВМ имеет источник бесперебойного электропитания.

Для исключения ошибочного перехода на резерв по причине сбоя в системе контроля используют временной фильтр, который разрешает переключение только при условии, что состояние неисправности длится не менее установленного времени (например, 1...100 мс).

Вместе с тем, наряду с относительной простотой систем резервирования замещением им присущи следующие недостатки: сложность коммутации и перерыв в работе системы по основной программе при замене отказавшего элемента или комплекта исправным.

С учетом этого в особо ответственных системах, к которым относятся системы автоведения поездов, применяется мажоритарное резервирование (резервирование с голосованием) [115].

Основным отличительным признаком систем резервирования с голосованием является невозможность выделения в системе основных элементов и резервных, поскольку все они равноправны, работают одновременно и выполняют одну и ту же функцию. Выбор одного сигнала из нескольких осуществляется схемой голосования, которая в частном случае нечетного числа голосов называется мажоритарной системой.

Мажоритарные системы не требуют контроля работоспособности элементов для своего функционирования, но используют подсистему диагностики для сокращения времени восстановления отказавших элементов. Наличие системы диагностики снижает также вероятность накопления скрытых неисправностей, которые со временем могут явиться причиной отказа. Мажоритарное резервирование позволяет защититься не только от постоянных отказов, но и от перемежающихся, в том числе от воздействия помех, т.к. они обычно проявляются неодинаково в резервированных каналах обработки информации.

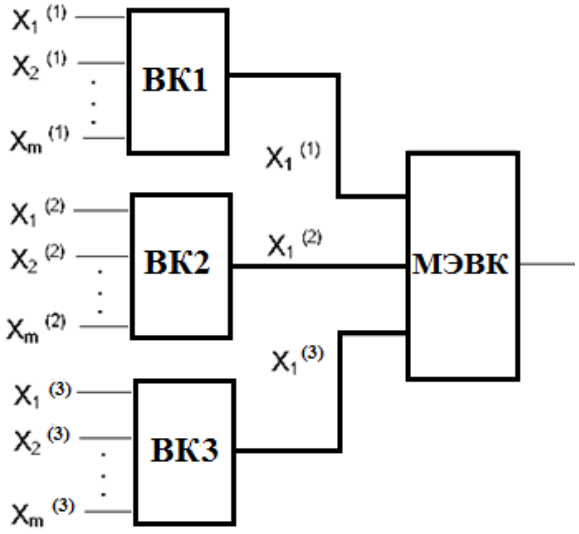
С учетом сказанного для комплексной системы управления движением принимаем мажоритарное резервирование ВК (рис. 3.4).

В этом случае организуется нечетное число каналов обработки информации элементов ВК, выходные сигналы которых объединяются с помощью восстанавливающего органа (мажоритарного элемента вычислительного комплекса МЭВК).

Сигнал на выходе МЭВК (мажоритарного элемента) определяется большинством выходных сигналов; отказ или сбой каналов обработки информации не приводит к отказу системы в целом. Поэтому работоспособность отдельных каналов можно восстанавливать без пре-

рывания работы системы, что позволяет значительно увеличить ее коэффициент готовности. При работе МЭВК с голосованием «2 из 3» (МЭВК состоит из трех элементов, для корректной работы системы 2 из них должны быть исправны) отказ наступает при неисправно работе любых двух элементов.

Для повышения надежности работы комплексной системы управления движением, а также снижения времени восстановления неисправных элементов ВК необходимо увеличение кратности мажоритарного резервирования. При высокой кратности резервирования структуры МЭВК отказ одного ВК позволяет сохранить работоспособность системы путем снижения кратности резервирования. Такого рода преобразование может быть выполнено путем понижения порога в мажоритарном элементе.



ВК1, ВК2, ВК3 – вычислительные комплексы системы резервирования; МЭВК- мажоритарный элемент системы резервирования

Рис. 3.4. Блок-схема мажоритарного резервирования ВК комплексной системы управления движением

Работа ВК связанна с безопасностью движения, поэтому важно оценить надежность системы, получаемой при использовании принципа мажоритарного резервированияс голосованием«2 из 3».

Поскольку в работе находятся одновременно три ВК, событие, определяющее работоспособность системы с МЭВК, определится выражением [116]:

$$A_{\Sigma} = A_1 \cdot A_2 \cdot \overline{A_3} + A_1 \cdot \overline{A_2} \cdot A_3 + \overline{A_1} \cdot A_2 \cdot A_3 + A_1 \cdot A_2 \cdot A_3, \qquad (3.1)$$

где A_1, A_2, A_3– события, определяющие работоспособность первого, второго и третьего ВК ;$\overline{A_1}, \overline{A_2}, \overline{A_3}$–события, определяющие отказ первого, второго и третьего ВК.

По условию обеспечения надежности в комплексной системе управлением движением поездов не могут использоваться вычислительные средства, достигшие своего износа. Анормальная эксплуатация технического средства, прошедшего период приработки, может сопровождаться внезапными отказами, когда интенсивность отказов в среднем приблизительно постоянная величина [117]. Соответственно для одного ВК интенсивность отказов определится как

$$\lambda_0 \approx \frac{1}{\mathrm{T}_0}, \qquad (3.2)$$

а вероятность его работоспособного состояния

$$P_0(\tau) = exp\left(-\int_0^\tau \lambda_0(\tau)d\tau\right) = e^{-\lambda_0\tau}, \qquad (3.3)$$

где $\mathrm{T}_0 = 1{,}0 \cdot 10^5 - 1{,}25 \cdot 10^5$часов - среднее время наработки до первого отказа одного ВК [118].

Переходя от событий к их вероятностям, и считая, что все ВК имеют одинаковые параметры надежности, т.е.

$$P(A_1) = P(A_2) = P(A_3) = P_0$$

получаем выражение для вероятности безотказной работы ВК с мажоритарным резервированием «2 из 3»

$$P_\Sigma = P_0^2(1-P_0) + P_0^2(1-P_0) + P_0^2(1-P_0) + P_0^3 = 3P_0^2 - 2P_0^3 \qquad (3.4)$$

Плотность распределения времени безотказной работы ВК с мажоритарным резервированием (плотность отказов)

$$f_\Sigma(\tau) = 6\lambda_0(e^{-2\lambda_0\tau} - e^{-3\lambda_0\tau}), \qquad (3.5)$$

а среднее время

$$T_{\text{ср}} = \int_0^\infty \tau\, f_\Sigma(\tau)d\tau = 6\lambda_0 \int_0^\infty \left(e^{-2\lambda_0\tau} - e^{-3\lambda_0\tau}\right)d\tau = \frac{5}{6\lambda_0} = 0{,}833\, T_0. \qquad (3.6)$$

Таким образом, среднее время работоспособного состояния ВК с мажоритарным резервированием с голосованием «2 из 3» составит 93700 часов при среднем времени наработки до первого отказа одного ВК $1{,}125 \cdot 10^5$ часов [118].

Снижение времени безотказной работы ВК с мажоритарным резервированием относительно ВК без резервирования объясняется тем, что система с *тремя* ВК и голосованием «2 из 3» имеет дробную кратность резервирования 1: 2, т.к. в ней резервный элемент – один, а резервируемых – два, и только наличие двух работоспособных ВК обеспечивает работоспособность всей системы. Поэтому эффект снижения безотказности вследствие нарастания числа элементов в системе при больших наработках оказывается сильнее эффекта резервирования.

На (рисунке 3.5) представлены графики безотказной работы одного ВК и ВК с мажоритарным резервированием. График зависимости вероятности безотказной работы для системы с

голосованием, начиная со значения $\tau=0{,}78104\cdot10^5$ часов, идёт ниже, чем для системы без резервирования, а средняя наработка до отказа получается меньше.

Однако, при $\tau<0{,}78104\cdot10^5$ часов, т.е. для наработки менее 8,9 лет, ВК с мажоритарным резервированием имеет более высокие показатели надежности.

Таким образом, для ВК системы управления движением поездов рекомендуется использовать мажоритарное резервирование с голосованием «2 из 3», которое обеспечит не только высокую степень достоверности определения поездной ситуации на контролируемом участке железной дороги, состояния каждого локомотива и соответствующего алгоритма управления им, но и высокую степень надежности самого ВК на интервале времени $0 < \tau \leq 0{,}833T_0$.

В общем случае адаптивные мажоритарные системы позволяют значительно повысить показатели безотказности ВК даже без восстановления отказавших каналов обработки информации. Однако увеличение параллельно работающего числа элементов ведет к увеличению стоимости системы и поэтому во многих случаях ограничиваются применением мажоритарных системы в составе трех параллельно работающих ВК.

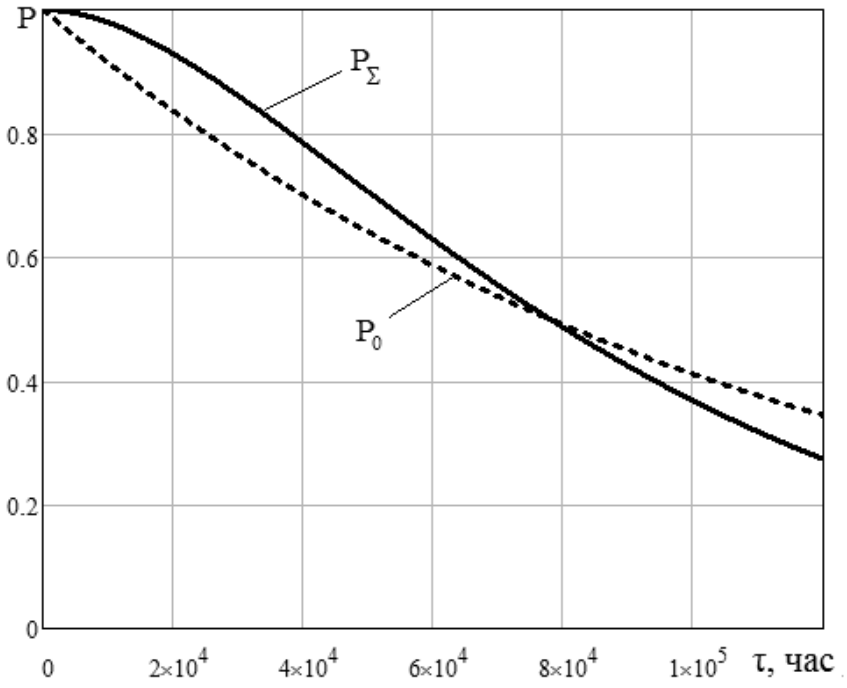


Рисунок 3.5 Вероятность безотказной работы ВК без резервирования (P_0) и ВК с мажоритарным резервированием с голосованием «2 из 3» (P_Σ)

Практическую реализацию адаптивных мажоритарных элементов наиболее целесообразно выполнять программно, т.к. в аппаратном выполнении они получаются довольно слож-

ными и, следовательно, имеют невысокие показатели безотказности, что соответственно снижает эффективность резервирования.

.

3.3. Моделирование работы вычислительного комплекса в условиях проведения информационной атаки

В настоящее время наибольшее распространение среди информационных атак получил так называемый «отказ в обслуживании» - Denial of Service (DoS-атака). Этот класс объединяет атаки, направленные на блокирование доступа к информационному ресурсу легитимных пользователей. Однако, структура комплексной системы управления движением поездов делает маловероятной проведение DoS-атаки вследствие ее закрытости и малого числа узлов. Поэтому MITM-атака - наиболее вероятный метод нелегитимного воздействия на систему.

Анализ взаимодействия элементов комплексной системы управления движением по каналам связи показал, что наиболее уязвимой точкой для несанкционированного подключения является радиоканал между системой автоведения и ВК, образуя канал взаимодействия «система автоведения – атакующий – ВК» (рисунок 1.4).

Для анализа функционирования ВК во внештатном режиме и выбора эффективной системы защиты от MITM-атаки разработана обобщенная математическая модель на базе математического аппарата расширенных сетей Петри. Модель представляет собой направленный маркированный граф, включающий в себя 14 состояний и 18 переходов (рисунок 3.6):

$$P = \{p_1, p_2, p_{10}, p_{11}, p_{12}, p_{13}, p_{14}, p_{15}, p_{20}, p_{21}, p_{30}, p_{31}, p_{40}, p_{41}\};$$

$$T = \left\{ \begin{matrix} t_{10}, t_{20}, t_{40}, t_{50}, t_{100}, t_{110}, t_{120}, t_{130}, t_{140}, t_{150} t_{160}, t_{170}, t_{180}, t_{190}, \\ t_{510}, t_{520}, t_{530}, t_{540} \end{matrix} \right\}.$$

Элементами множества позиций P являются: p_1 - состояние буфера передаваемой информации ВМ; p_2- состояние буфера принимаемой информации ВМ; p_{10}, p_{12}, p_{13}, p_{15} - состояния процесса передачи информации между ВМ и ресурсом до устройства маршрутизации; p_{11}, p_{14}, - состояния штатного процесса передачи информации; p_{20}, p_{21}- состояние буферов передаваемой и принимаемой информации ресурса; p_{30}- состояние устройства маршрутизации, при которой информация передается по штатному маршруту; p_{31} - состояние устройства маршрутизации, при которой информация передается через нарушителя; p_{40},p_{41}- состояния передачи информации через нарушителя.

Элементами множества позиций T являются: t_{100}, t_{180},t_{130}, t_{180} - передача информации до устройства маршрутизации, t_{110}, t_{120},t_{160}, t_{170} - передача информации по штатному маршруту; t_{510}, t_{520},t_{530}, t_{540} - передача информации через нарушителя; t_{10}, t_{20} - начало атаки; t_{40}, t_{50} - завершение атаки; t_{140}, t_{190}-получение запроса и формирование ответа.

При штатном функционировании ресурса осуществляется передача трафика между ВМ (состояния p_1,p_2) и ресурсом (состояния p_{20}, p_{21}). При пассивном переходе t_{10} в состоянии p_{30} присутствует маркер, а передача трафика перенаправляется через промежуточные состояния системы p_{10}, p_{11}, p_{12} и p_{13}, p_{14}, p_{15}.

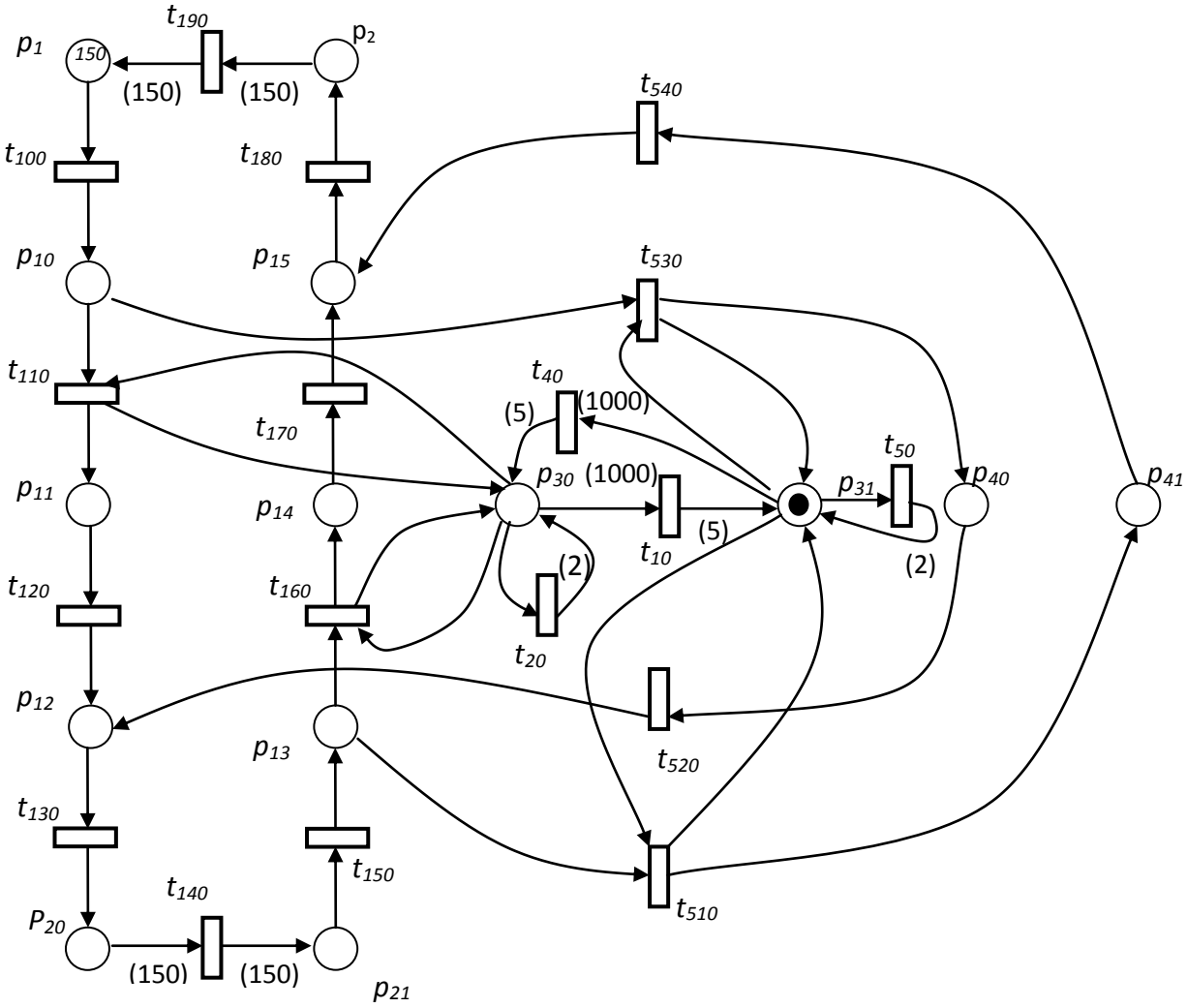


Рисунок 3.6. Модель MITM-атаки на ВК в терминах сетей Петри

В случайный момент времени нарушитель воздействует на устройство сетевой маршрутизации для перенаправления трафика и перехватывает его. При этом активизируется переход t_{10} и изменяет маркировку сети: маркеры из состояния p_{30} переходят в состояние p_{31} и закрывают переходы t_{110} и t_{160}. Это эквивалентно закрытию прямого канала передачи информации между ВМ и ресурсом.

Одновременно с этим маркеры, перемещаясь по замкнутым дугам из состояния p_{31},открывают переходы t_{510} и t_{530}. Результатом этого является переход маркеров из состояния p_{13} в p_{41} и из p_{41}в p_{15}, а также из состояния p_{10} в p_{40} и из p_{40} в p_{12}. Срабатывание переходов t_{510} и t_{530}, приводящее к открытию канала передачи информации p_{10}-p_{40}-p_{12}, эквивалентно перена-

правлению трафика от ВМ к ресурсу через нарушителя (состояние p_{40}). Срабатывание переходов t_{520} и t_{430}, приводящее к открытию канала передачи информации p_{13}-p_{41}-p_{15}, эквивалентно перенаправлению трафику от ресурса к ВМ через атакующего (состояние p_{41}).

Таким образом, в результате изменений активности переходов и маркировки состояний сети весь трафик между ВМ и ресурсом будет проходить через нарушителя, обеспечивая ему доступ к потоку данных.

При завершении атаки активизируется переход t_{50} и маркеры из состояния p_{31} возвращаются в состояние p_{30}. Это приводит к тому, что число маркеров в состоянии p_{31} становится меньше чем кратность входных дуг переходов t_{510}, t_{530} и эти переходы закрываются.

Одновременно увеличение количества маркеров в состоянии p_{30} открывает переходы t_{110} и t_{160}. Это эквивалентно восстановлению канала прямой связи между ВМ и ресурсом.

Управление системой при MITM-атаке осуществляется переходами t_{20} и t_{40}.

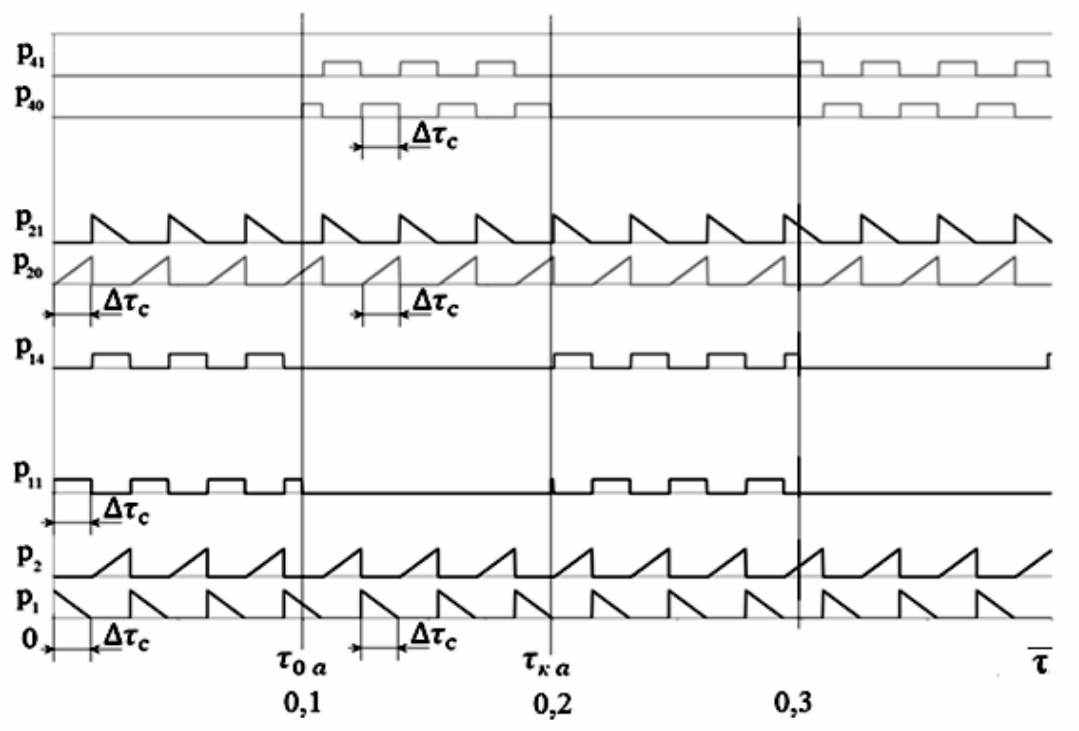
Переход t_{20} замкнут на состояние p_{30}: он имеет входную дугу с кратностью 1 и выходную дугу с кратностью 2. Его функционирование приводит к увеличению количества маркеров в состоянии p_{30}, что необходимо для срабатывания перехода t_{10}, который имеет входную дугу кратностью 1000.

Переход t_{50} замкнут на состояние p_{31}, имеет входную дугу с кратностью 1 и выходную дугу с кратностью 2. Его функционирование приводит к увеличению количества маркеров в состоянии p_{31},что необходимо для срабатывания перехода t_{40}, который также имеет входную дугу кратностью 1000 . Значительная разница в кратности дуг переходов t_{20}-t_{10} и t_{40}-t_{50} обеспечивает адекватность разработанного алгоритма и физического процесса в ВК по времени τ при моделировании MITM-атаки.

Математическая модель, описывающая разработанный алгоритм проведения MITM-атаки на ВК, представляет собой систему из следующих логических уравнений (3.7):

$$
\begin{cases}
\mu'(p_1) = \mu(p_1) + 150\big(\#\big(p_1, O(t_{190})\big) = 150\big) - 1\big(\#\big(p_1, I(t_{100})\big) = 1\big)\ ; \\
t_{100}: \mu(p_1) \geq \#\big(p_1, I(t_{100})\big)\ ; \\
\mu'(p_{10}) = \mu(p_{10}) + 1\big(\#\big(p_{10}, O(t_{100})\big) = 1\big) - 1\big(\#\big(p_{10}, I(t_{110})\big) = 1\big) \\
-1\big(\#\big(p_{10}, I(t_{530})\big) = 1\big)\ ; \\
t_{110}: \mu(p_{10}) \geq \#\big(p_{10}, I(t_{110})\big) \text{и} \mu(p_{30}) \geq \#\big(p_{30}, I(t_{110})\big)\ ; \\
\mu'(p_{11}) = \mu(p_{11}) + 1\big(\#\big(p_{11}, O(t_{110})\big) = 1\big) - 1\big(\#\big(p_{11}, I(t_{120})\big) = 1\big)\ ; \\
t_{120}: \mu(p_{11}) \geq \#\big(p_{11}, I(t_{120})\big)\ ; \\
\mu'(p_{12}) = \mu(p_{12}) + 1\big(\#\big(p_{12}, O(t_{120})\big) = 1\big) + 1\big(\#\big(p_{12}, O(t_{520})\big) = 1\big) \\
-1\big(\#\big(p_{12}, I(t_{130})\big) = 1\big); \\
t_{130}: \mu(p_{12}) \geq \#\big(p_{12}, I(t_{130})\big)\ ; \\
\mu'(p_{20}) = \mu(p_{20}) + 1\big(\#\big(p_{20}, O(t_{130})\big) = 1\big) - 150\big(\#\big(p_{20}, I(t_{140})\big) = 1\big)\ ; \\
t_{140}: \mu(p_{20}) \geq \#\big(p_{20}, I(t_{140})\big)\ ; \\
\mu'(p_{21}) = \mu(p_{21}) + 150\big(\#\big(p_{21}, O(t_{140})\big) = 150\big) - 1\big(\#\big(p_{21}, I(t_{150})\big) = 1\big)\ ; \\
t_{150}: \mu(p_{21}) \geq \#\big(p_{21}, I(t_{150})\big)\ ; \\
\mu'(p_{13}) = \mu(p_{13}) + 1\big(\#\big(p_{13}, O(t_{150})\big) = 1\big) - 1\big(\#\big(p_{13}, I(t_{160})\big) = 1\big) \\
-1\big(\#\big(p_{13}, I(t_{510})\big) = 1\big)\ ; \\
t_{160}: \mu(p_{13}) \geq \#\big(p_{13}, I(t_{160})\big) \text{и} \mu(p_{30}) \geq \#\big(p_{30}, I(t_{160})\big)\ ; \\
\mu'(p_{14}) = \mu(p_{14}) + 1\big(\#\big(p_{14}, O(t_{160})\big) = 1\big) - 1\big(\#\big(p_{14}, I(t_{170})\big) = 1\big)\ ; \\
t_{170}: \mu(p_{14}) \geq \#\big(p_{14}, I(t_{170})\big)\ ; \\
\mu'(p_{15}) = \mu(p_{15}) + 1\big(\#\big(p_{15}, O(t_{170})\big) = 1\big) + 1\big(\#\big(p_{15}, O(t_{540})\big) = 1\big) \\
-1\big(\#\big(p_{15}, I(t_{180})\big) = 1\big)\ ; \\
t_{180}: \mu(p_{15}) \geq \#\big(p_{15}, I(t_{180})\big)\ ; \\
\mu'(p_2) = \mu(p_2) + 1\big(\#\big(p_2, O(t_{180})\big) = 1\big) - 150\big(\#\big(p_2, I(t_{190})\big) = 150\big)\ ; \\
t_{190}: \mu(p_{21}) \geq \#\big(p_2, I(t_{190})\big); \\
\mu'(p_{30}) = \mu(p_{30}) + 1\big(\#\big(p_{30}, O(t_{110})\big) = 1\big) + 1\big(\#\big(p_{30}, O(t_{160})\big) = 1\big) \\
+2\big(\#\big(p_{30}, O(t_{20})\big) = 2\big) - 1\big(\#\big(p_{30}, I(t_{110})\big) = 1\big) - 1\big(\#\big(p_{30}, I(t_{160})\big) = 1\big) \\
-1\big(\#\big(p_{30}, I(t_{20})\big) = 1\big) - 1000\big(\#\big(p_{30}, I(t_{10})\big) = 1000\big) + 5\big(\#\big(p_{30}, O(t_{50})\big) = 5\big)\ ; \\
t_{20}: \mu(p_{30}) \geq \#\big(p_{30}, I(t_{20})\big); \\
\mu'(p_{31}) = \mu(p_{31}) + 1\big(\#\big(p_{31}, O(t_{530})\big) = 1\big) - 1000\big(\#\big(p_{31}, O(t_{40})\big) = 1000\big) \\
+1\big(\#\big(p_{31}, O(t_{510})\big) = 1\big) + 5\big(\#\big(p_{31}, O(t_{10})\big) = 5\big) \\
-1\big(\#\big(p_{31}, I(t_{530})\big) = 1\big) - 1\big(\#\big(p_{31}, I(t_{530})\big) = 1\big) \\
-1\big(\#\big(p_{31}, I(t_{50})\big) = 1\big) + 2\big(\#\big(p_{31}, O(t_{50})\big) = 2\big)\ ; \\
\mu'(p_{40}) = \mu(p_{40}) + 1\big(\#\big(p_{40}, O(t_{530})\big) = 1\big) - 1\big(\#\big(p_{40}, I(t_{520})\big) = 1\big)\ ; \\
\mu'(p_{41}) = \mu(p_{41}) + 1\big(\#\big(p_{41}, O(t_{510})\big) = 1\big) - 1\big(\#\big(p_{410}, I(t_{540})\big) = 1\big)\ ; \\
t_{510}: \mu(p_{31}) \geq \#\big(p_{31}, I(t_{510})\big) \text{и} \mu(p_{13}) \geq \#\big(p_{13}, I(t_{510})\big)\ ; \\
t_{520}: \mu(p_{31}) \geq \#\big(p_{31}, I(t_{520})\big)\ ; \\
t_{540}: \mu(p_{31}) \geq \#\big(p_{31}, I(t_{540})\big)\ ; \\
t_{530}: \mu(p_{31}) \geq \#\big(p_{31}, I(t_{530})\big) \text{и} \mu(p_{10}) \geq \#\big(p_{10}, I(t_{530})\big)\ ; \\
t_{40}: \mu(p_{31}) \geq \#\big(p_{31}, I(t_{40})\big)\ ; \\
t_{50}: \mu(p_{31}) \geq \#\big(p_{31}, I(t_{50})\big)\ .
\end{cases}
\tag{3.7}
$$

Результаты моделирования работы ВК по разработанному алгоритму представляют процессы штатного функционирования, начала атаки, перехвата трафика и завершения атаки. На рисунке 3.7 приведены диаграммы функционирования ВМ и ресурса; информация между участниками сессии передается пакетами: каждое сообщение - за интервал времени $\Delta\tau_c$. Диаграммы состояний буферов p_1 и p_2 отражают функционирование ВМ: p_1 -передача информации, p_2 - получение информации. Аналогичным образом диаграммы состояний буферов p_{20} и p_{21} отражают функционирование ресурса: p_{20}- получение информации, p_{21}- передача информации.



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

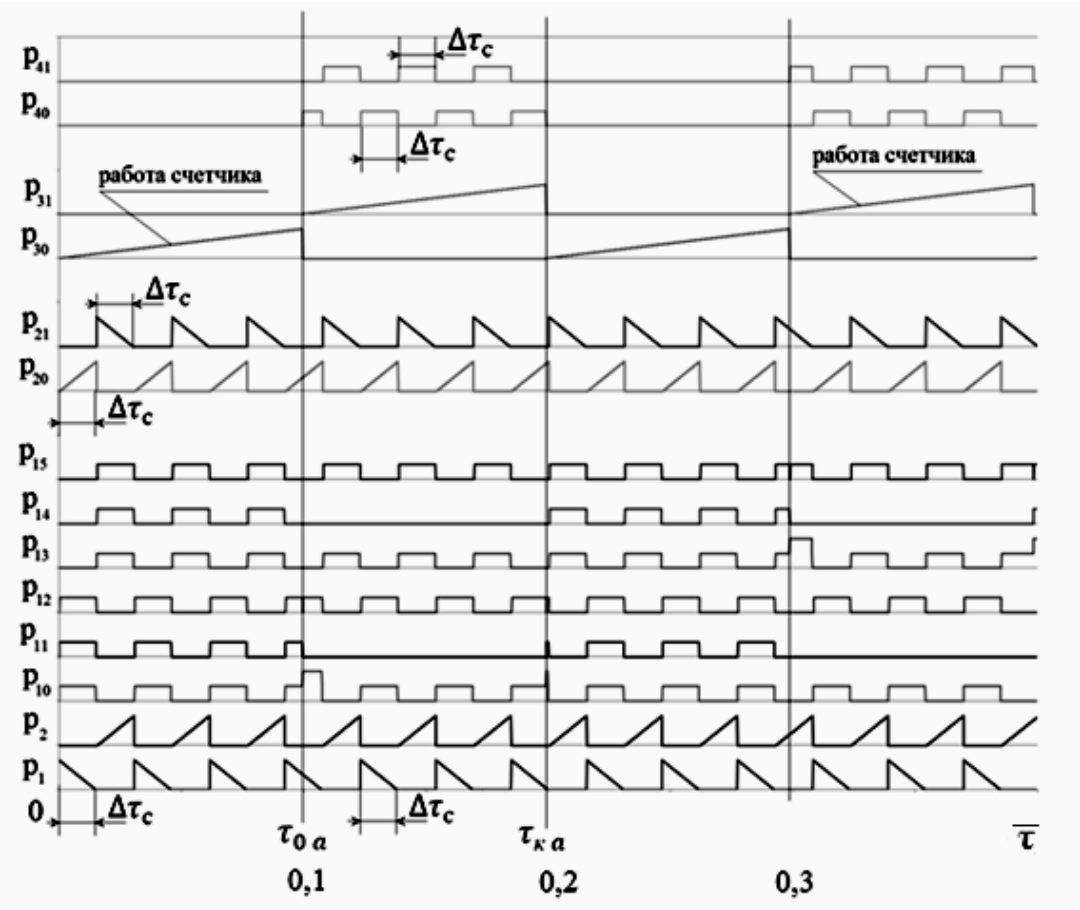
Рисунок 3.7. Моделирование работы каналов передачи информации при MITM-атаке на ВК

В начальный момент времени $\tau = 0$ запрос передается к ресурсу по каналу p_1-p_{11}-p_{20}: объем информации в буфере p_1 уменьшается, в буфереp_{20} – увеличивается. После получения всего запроса, ресурс генерирует ответ в буфере p_{21} и передает его по каналу p_{21}-p_{14}-p_2 за интервал времени $\Delta\tau_c$. Как видно, характер этого процесса не меняется на протяжении всего интервала моделирования.

В момент времени $\tau_{0\,a}$ в сеть включается нарушитель. При этом обрываются штатные каналы передачи информации p_{11} и p_{14}, а вместо них начинают работать каналы p_{40} и p_{41}. Нарушитель считывает пакеты передаваемой информации через состояния $p_{40,}$ и p_{41}, а штатные

каналы передачи информации не используются. Характер передачи информации не меняется ни для ВМ, ни для ресурса, т.е. нарушитель перенаправляет трафик, оставаясь незамеченным для легитимных участников сессии. В произвольный момент времени $\tau_{к\,a}$ нарушитель покидает сессию, штатные каналы передачи информации восстанавливаются, что также не отражается на характере передачи и получения информации для ВМ и ресурса.

Результаты моделирования всех процессов, происходящих при MITM-атаке, приведены на рисунке 3.8.



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

Рисунок 3.8. Результаты моделирования MITM-атаки на ВК

Диаграмма отражает изменение множества P всех состояний системы, представленной на рисунке 3.6. Кроме процессов, приведенных на рисунке 3.7, диаграмма иллюстрирует работу счетчиков системы, имитирующих действия атакующего: момент подключения к каналам передачи информации $\tau_{0\,a}$ и отключения $\tau_{к\,a}$.

3.4. Определение маршрутов возможных атак на вычислительный комплекс

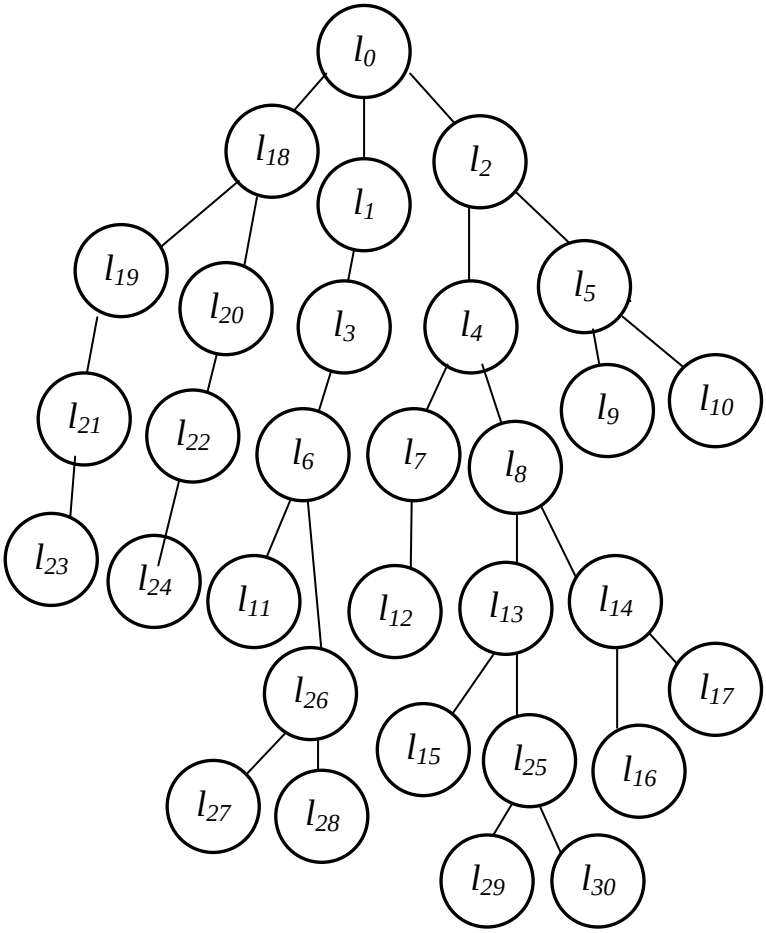
Для выявления общей тенденции атак на ВК была использована методика создания формализованных моделей информационных атак, разработанная Б. Шнайером [119]. Основой данной методики является иерархическое дерево атак $G=<L,E>$, где L - множество вершин, E -множество дуг. Дерево G представляет собой множество маршрутов g_p, где каждый $g_p \in G$ является последовательностью дуг $(e_{p1}, e_{p2}, ..., e_{pn})$ и вершин $(l_{p1}, l_{p2}, ..., l_{pm})$; при этом конечная вершина дуги e_{pk} является начальной вершиной дуги e_{pk+1}. В качестве начальных вершин выступают листья дерева G, а в качестве конечной вершины - его корень. Каждая вершина дерева G соответствует определенному действию атакующего, а корень представляет конечный результат атаки.

В виртуальной среде атака на ресурс может быть проведена путем получения доступа к хосту, гипервизору или непосредственно самой ВМ. Эта специфика должна быть отражена в дереве атак (рисунок 3.9) [120, 121].

Угрозы в отношении хоста могут быть реализованы любым доступным способом взлома - заражением, фишингом и т.д. ($l_{10}, l_{11}, l_{15}, l_{17}$). Результатом этих действий является доступ к терминалу хоста l_6, возможность установки на хост сниффера или анализатора трафика l_3 и, соответственно, доступ к сетевому интерфейсу l_1.

Угрозы в отношении гипервизора могут быть достигнуты либо после взлома хоста, что позволяет получить доступ к средствам управления гипервизором или модифицировать его файлы, либо путем несанкционированного удаленного управления гипервизором l_9, l_{16}. Взлом гипервизора позволит получить контроль над эмуляцией сетевого интерфейса и соответственно перехватить входящий и исходящий трафик l_5.

Угрозы в отношении ВМ могут быть реализованы путем взлома физических аппаратных средств (хоста или репозитория) или гипервизора, что позволит модифицировать его файлы l_{13} и файлы ВМ l_8, l_{14}. Также возможно рассматривать ВМ как независимое физическое устройство; соответственно возможен ее непосредственный взлом любым доступным способом - заражением, фишингом и т.д l_{12}. Это опять же открывает доступ к терминалу ВМ l_7, т.к. позволяет установить сниффер или анализатор трафика l_4, и в свою очередь откроет доступ к сетевому интерфейсу ВМ l_2.



l_0 -прослушивание трафика ВМ; l_1- доступ к сетевому интерфейсу хоста; l_2 - доступ к сетевому интерфейсу ВМ; l_3- установка сниффера или анализатора трафика на хост; l_4 - установка сниффера или анализатора трафика на ВМ; l_5 - доступ к гипервизору; l_6 - доступ к терминалу хоста; l_7 - доступ к терминалу ВМ; l_8-доступ к файлам ВМ; l_9, l_{16} - удаленный доступ к гипервизору; l_{10}, l_{11}, l_{15}, l_{17} доступ к хосту (заражение, фишинг и т.д.); l_{12}- доступ к ВМ (заражение, фишинг и т.д.); l_{13} - доступ к файлам хоста; l_{14}- доступ к гипервизору (управление жесткими дисками ВМ); l_{18}– перенаправление компрометируемого трафика; l_{19} - ARP-компрометация; l_{20} - DNS-компрометация; l_{21} - доступ к LAN; l_{22} - доступ к DNS-службе; l_{23},l_{24} –анализ структуры LAN; l_{25}, l_{26}- развертывание скомпрометированной и целевой ВМ на одном хосте; l_{27}, l_{29}- доступ к любой ВМ инфраструктуры как к независимому объекту (заражение, фишинг и т.д.); l_{28}, l_{30}- доступ к репозиторию ВМ

Рисунок 3.9. Дерево атаки, направленной на прослушивание трафика ВК

Угроза безопасности всему ВК может быть реализована атакующим через доступную ему ВМ l_{27}, l_{29} или репозиторий l_{28},l_{30} . После развертывания скомпрметированной ВМ l_{25},l_{26} она используется для атаки на целевую ВМ.

Виртуальную машину можно рассматривать как независимый объект и провести на нее типовую MITM-атаку, используя ARP-poising или через DNS-службу. Для этого необходимо проанализировать структуру компрометируемой локальной сети (LAN) l_{23},l_{24}, после чего провести атаку на любой ее элемент (l_{21}) или используемый DNS-сервер l_{22}. Это позволяет осуществить ARP-poising l_{19} или переопределение службы DNS l_{20} за счет чего компрометируемый трафик перенаправляется через атакующего.

Очевидно, что вес каждой ветви дерева атак определится вероятностями реализации конкретной последовательности угроз.

Особенностью дерева атак виртуальной инфраструктуры является наличие ветви (l_{11}, l_6, l_3, l_1, l_0), 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.

3.5. Выводы по главе III

1. В соответствии с требованиями стандарта СТО РЖД 1.18.002-2009 «Управление информационной безопасностью. Общие положения» для повышения надежности функционирования системы управления движением поездов разработана структура вычислительного комплекса, предусматривающая мажоритарное резервирование с голосованием «2 из 3».

2. Проанализированы возможные алгоритмы проведения атак на вычислительный комплекс с учетом топологии каналов связи системы управления движением; наибольшую уязвимость вычислительный комплекс имеет при проведении MITM-атаки, а точкой для несанкционированного подключения будет являться радиоканал между системой автоведения поезда и вычислительным комплексом.

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 проведении атаки.

4. С целью выбора эффективной защиты вычислительного комплекса от информационных атак должна быть разработана методика расчета его защищенности, учитывающая структуру комплекса и возможные алгоритмы проведения атак.

IV. РАЗРАБОТКА МЕТОДИКИ ОЦЕНКИ ЗАЩИЩЕННОСТИ ВЫЧИСЛИТЕЛЬНОГО КОМПЛЕКСА И ЕГО ПРИЛОЖЕНИЙ

4.1. Статистика уязвимостей и эффективности систем защиты информационных систем

Выбор мер защиты информации ВК должно осуществляться в соответствии с техническим заданием и структурой ИС, учитывающий физические, логические, функциональные и технологические взаимосвязи между ее сегментами [122]. Правила и процедуры по реализации требований ИБ в конкретной ИС определяются в эксплуатационной документации на систему защиты информации и организационно-распорядительных документах по защите информации, которая разрабатывается с учетом национальных стандартов. Определение класса защищенности информационной системы проводится в соответствии с пунктом 14.2 «Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденных приказом ФСТЭК России от 11 февраля 2013 г. № 17.

Устанавливаются четыре класса защищенности информационной системы К1-К4; нижний класс - четвертый, высший класс - первый. Класс защищенности ИС определяется в зависимости от уровня значимости информации, обрабатываемой в ИС, и масштаба самой ИС (федеральный, региональный, объектовый).

Уровень значимости информации определяется возможным ущербом для обладателя информации от нарушения конфиденциальности и зависит от степени негативности последствий в социальной, политической, международной, экономической, финансовой или иных областях деятельности. Уровень значимости информации может быть:

- высокий, если в результате нарушения одного из свойств безопасности информации возможны существенные негативные последствия, а обладатель информации не может выполнять возложенные на него функции;

- средний, если в результате нарушения одного из свойств безопасности информации возможны умеренные негативные последствия, а обладатель информации не может выполнять хотя бы одну из возложенных на него функций;

- низкий, если в результате нарушения одного из свойств безопасности информации возможны незначительные негативные последствия, а обладатель информации может выполнять возложенные на него функции с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств.

Для определения степени возможного ущерба от нарушения конфиденциальности, целостности или доступности могут применяться национальные стандарты и (или) методические документы, разработанные и утвержденные ФСТЭК России в соответствии с подпунктом 4 пункта 8 «Положения о Федеральной службе по техническому и экспортному контролю»

№1085, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. (с изменениями и дополнениями 2005 г., 2006г., 2008г., 2012г. и 20013г.).

Адекватность мер защиты оценивается расчетом риска, как сопоставление субъективной оценки потенциальной угрозы с объективным расчетом затрат на внедрение механизма защиты [123].

В 2011—2012 компания Positive Technologies провела тестирование на проникновение в информационные системы наиболее крупных государственных и коммерческих компаний (в том числе, входящих в рейтинг 400 крупнейших компаний России в 2012 г. по объему реализации продукции по версии агентства «Эксперт») [124]. Для исследования в каждом году было выбрано по 10 систем (по просьбе владельцев систем тестирование проводились на ограниченном количестве узлов).

В результате проведенных работ в 75% случаев специалистам Positive Technologies удалось получить полный контроль над критическими ресурсами тестируемых систем, при этом почти в половине случаев (45%) подобный уровень доступа мог быть получен со стороны любого внешнего нарушителя [124]. Практически все системы оказались подвержены уязвимостям высокой степени риска, и только в 5% систем не было выявлено критических уязвимостей, однако присутствовали уязвимости среднего уровня риска. Три четверти рассмотренных систем содержали уязвимости высокого уровня риска, связанные с недостатками конфигурации; еще в 25% систем были выявлены недостатки среднего уровня риска.

Не всегда эффективны и применяемые стратегии защиты [124]. Анализ уязвимостей показал, что для 74% тестируемых систем внешний атакующий, не имеющий никаких привилегий и дополнительных данных о сети, способен преодолеть сетевой периметр и попасть во внутреннюю сеть. Для этого требуется последовательная эксплуатация в среднем трех различных уязвимостей: словарного пароля, веб-приложения и версии ПО. Почти в половине случаев (47%) первым этапом служит подбор словарных паролей, далее осуществляется расширение привилегий и получение контроля над каким-либо из ресурсов, относящихся ко внутренней сети. В каждой третьей системе первым этапом преодоления защиты служит эксплуатация уязвимостей веб-приложений. Далее, в зависимости от полученного уровня доступа, атака распространяется до получения контроля над операционной системой уязвимого сервера.

В тройку лидеров уязвимостей, встречающихся на ресурсах сетевого периметра, вошли (рисунок 4.1):

- использование словарных паролей (в том числе — установленных производителями по умолчанию);

- внедрение операторов SQL;

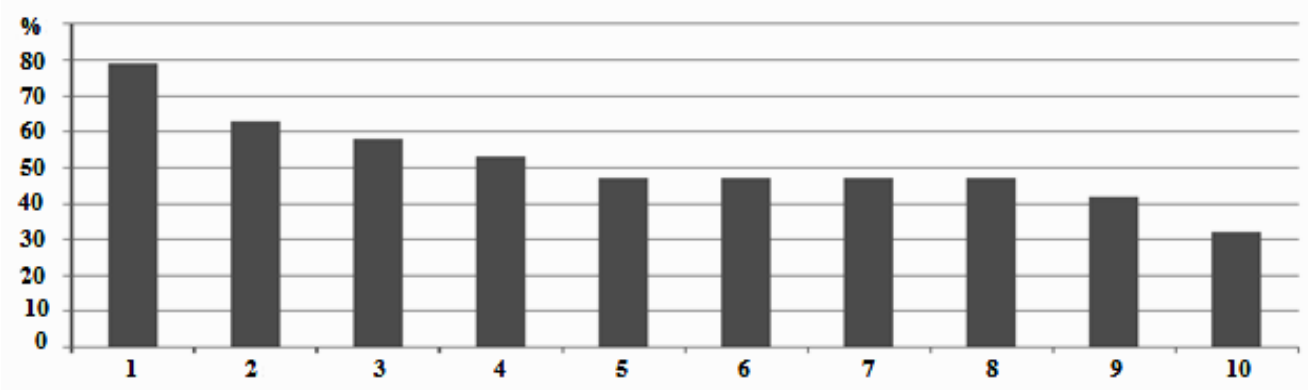
- наличие на сетевом периметре интерфейсов удаленного доступа и управление сетевым оборудованием и серверами, которые должны быть доступны только ограниченному числу администраторов.

Еще хуже обстоят дела в сфере защиты ресурса от внутреннего нарушителя. Из [124] следует, что непривилегированный внутренний нарушитель, находящийся в пользовательском сегменте сети, в 67% случаях может получить полный контроль над всей информационной инфраструктурой организации. В среднем, при наличии доступа во внутреннюю сеть, для получения контроля над критическими ресурсами, атакующему требуется эксплуатация 7 различных уязвимостей. Самая короткая проведенная атака включала три шага:

- получение доступа к файлам конфигурации сетевого оборудования Cisco, хранящимся на общедоступных сетевых ресурсах;

- восстановление паролей, хранящихся в файлах конфигурации с использованием обратимого алгоритма кодирования Type 7;

- успешный подбор паролей привилегированных пользователей для множества критических ресурсов с использованием словаря, включающего пароли, восстановленные на предыдущем этапе.



1 - словарные пароли пользователей; 2 - внедрение операторов SQL; 3 –доступные интерфейсы управления оборудованием ; 4 - межсайтовое выполнение сценариев; 5 - хранение важных данных в открытом виде; 6 - раскрытие конфигурационной информации в веб-приложениях; 7 - недостаточная защита от подбора учетных данных; 8 - использование открытых протоколов передачи данных; 9 - выход за пределы каталога (Path Traversal); 10 - раскрытие информации об идентификаторах

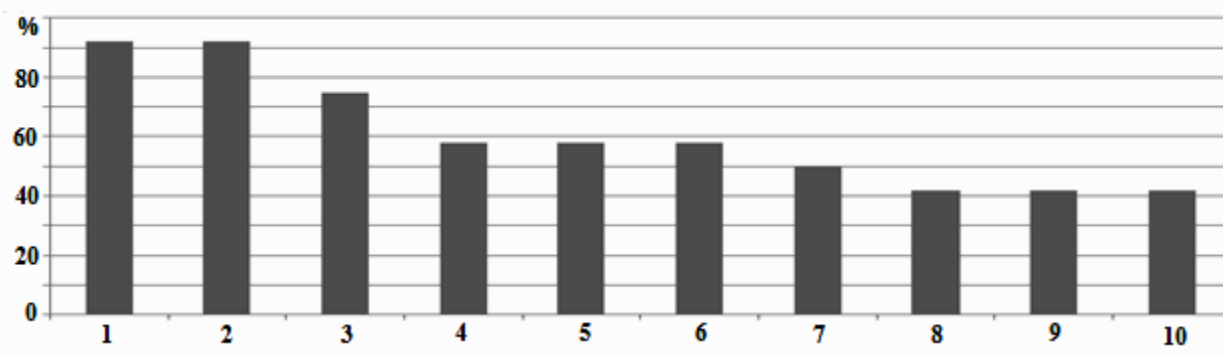
Рисунок 4.1. Наиболее распространенные уязвимости сетевого периметра

Самая длинная атака во внутренней сети одного из филиалов крупной корпорации насчитывала 13 шагов и заключалась в поэтапном расширении привилегий от рядового пользо-

вателя на веб-сервере до получения полного контроля над головным офисом и всеми ресурсами предприятия в целом.

Только в 30% случаях внутренний атакующий должен обладать высокой квалификацией для получения доступа к критическим ресурсам, тогда как для 10% систем успешные атаки возможны со стороны любого неквалифицированного пользователя внутренней сети.

Наиболее распространенными уязвимостями ресурсов внутренней сети являются использование слабых паролей и недостатки фильтрации и защиты служебных протоколов канального и сетевого уровней, таких как ARP, STP, DHCP, CDP (рисунок 4.2). Обе этих уязвимости встречаются в 92% систем. Следующий по распространенности недостаток — использование открытых протоколов передачи данных, таких как Telnet, FTP, HTTP, которое встречается в 75% случаев.



1- словарные пароли пользователей; 2- недостатки защиты служебных протоколов канального и сетевого уровней; 3-использование открытых протоколов передачи данных; 4 – хранение важной информации в открытом виде; 5-стандартное значение SNMP Community String с правами на чтение (public); 6 - возможность подключения стороннего оборудования без его предварительной авторизации; 7 - стандартное значение SNMP Community String с правами на чтение и запись (private); 8 -использование слабых алгоритмов шифрования при хранении паролей; 9 - интерфейсы управления оборудованием доступны любому пользователю локальной сети; 10 - недостаточная защита от подбора учетных данных

Рисунок. 4.2. Наиболее распространенные уязвимости во внутренней сети

Использование открытых протоколов во внутренней сети для 75% систем позволяет реализовать MITM–атаку и осуществить перехват информации, в том числе учетных данных администраторов.

В рамках проведенного исследования была дана средняя оценка уровня защищенности рассмотренных систем относительно различных векторов проникновения [124]. Векторы проникновения были классифицированы в зависимости от компонентов системы, когда эксплуатация уязвимостей позволяла получить несанкционированный доступ к ресурсам. Оценка

уровня защищенности по каждому направлению рассчитывалась по пятибалльной системе, где «0» соответствует крайне низкому уровню защищенности (уязвимость позволяет напрямую получить доступ к ресурсу), а оценка «5» соответствует приемлемому уровню защищенности (уязвимостей не обнаружено, средства защиты реализованы корректно).

Анализ средних уровней защищенности всех исследованных компонентов системы по итогам 2011, 2012 гг. показывает значения «ниже среднего» (рисунок 4.3) [124].

Рисунок 4.3. Средние уровни защищенности различных компонентов систем

Согласно статистическим данным, наиболее распространенными являются уязвимости «использование слабых паролей», низкий уровень защищенности имеют серверы и веб-приложения. В большинстве случаев получение доступа к критическим ресурсам на серверах, рабочих станциях и в системах управления базами данных (СУБД) связано именно с подбором простых паролей.

Аналогичные исследования были выполнены с точки зрения выявления недостатков в реализации защиты (рисунок 4.4) [124].

Наиболее серьезные недостатки были выявлены для механизмов управления учетными записями и паролями. Кроме того, во множестве систем были выявлены серьезные недостатки реализации механизмов разграничения доступа, отсутствия актуальных обновлений безопасности и снижения уровня криптографической защиты. В отчете отмечается, что в 2012 году средний уровень защищенности систем относительно механизмов криптографической защиты снизился до крайне низкой отметки: практически везде используются открытые протоколы передачи данных, а важная информация хранится в открытом виде [124].

Несмотря на принимаемые меры защиты, широкое распространение специального и сложного ПО неизбежно приводит к появлению новых уязвимостей. Так, в 2010 году IBM зарегистрировала свыше 8000 новых уязвимостей, что на 27% больше, чем было зарегистриро-

вано в 2009 году [125, 126]. За период с 2009 по 2010 год отмечен 21%-ный рост числа эксплоитов, выложенных в свободном доступе. В 2011г. по данным IBM ситуация несколько улучшилась, однако атакующая сторона продолжает приспосабливать средства атаки к отмеченным улучшениям ИБ и за отчетный период ежедневно происходило 13 млрд. событий безопасности [127]. Эти данные свидетельствуют о неблагоприятной ситуации высокого уровня угроз, когда все более сложные вычислительные среды подвергаются все более изощренным атакам.

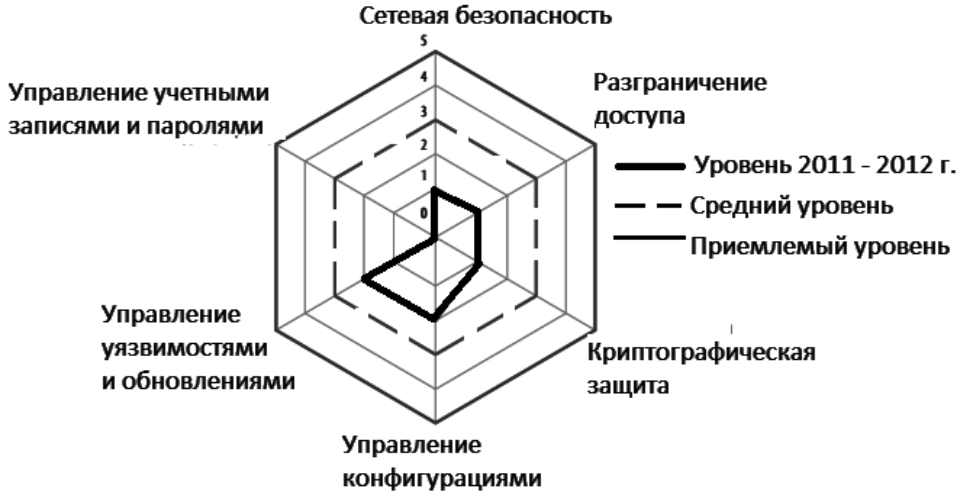


Рисунок 4.4. Уровни защищенности систем в зависимости от механизма защиты

Аналогичные данные получены OSVDB (Open Source Vulnerability Database) в 2012 г. при анализе статистических данных по росту уязвимостей ИС за последние двенадцать лет (рисунок 4.5) [128, 129].

Анализ уязвимостей с точки зрения конечной цели реализации атаки показывает их широкий спектр.

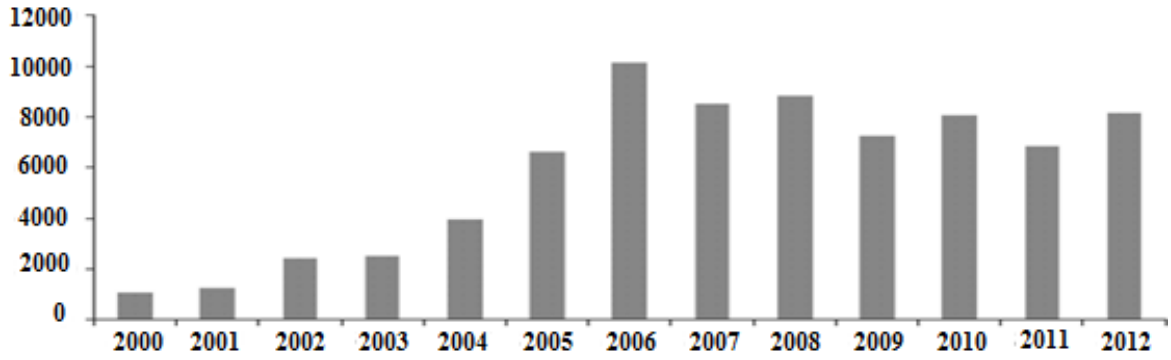


Рисунок 4.5. Число уязвимостей, зарегистрированные OSVDB в 2000–2012гг.

Как указано в [128] к основным целям атак на уязвимости приложений можно отнести: установку и запуск вредоносной программы (28%), кражу информации (в том числе кража денег, в совокупности, 37%), дезинформацию, либо несанкционированную модификацию информации (19%) (рисунок 4.6). Важно отметить, что это атаки, связанные с несанкционированными записью и чтением информации (которые равновероятны), а их последствия следует минимизировать в первую очередь.

Рисунок 4.6. Классификация целей проводимых сетевых атак

При уязвимости приложений защита должна в первую очередь реализовываться разграничительной политикой доступа к ресурсам - файловым объектам. Однако в данном случае субъектом доступа является процесс (приложение), идентифицируемый именем своего исполняемого файла. Как следствие, защита должна реализовываться контролем доступа (разграничением прав доступа) процессов (приложений) к файловым объектам.

Из отчета Security Lab за февраль 2012 г следует, что 56.3% от общего числа составили уязвимости в Web - приложениях, 28.2% - уязвимости в клиентском ПО,14.6% - уязвимости в серверном ПО, и 1% -уязвимости в компонентах операционных систем (рисунок 4.7) [128].

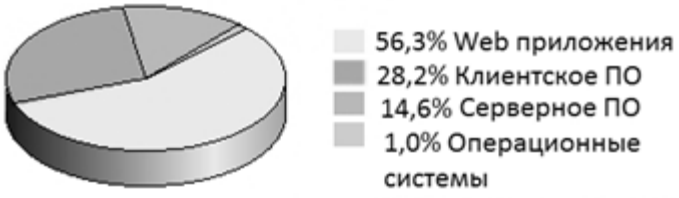


Рисунок 4.7. Распределение уязвимостей по типам ПО за февраль 2012г.

Анализ уведомлений ИБ за этот же период показал, что подавляющее число эксплуатаций уязвимостей приходится на векторы удаленных атак – 93,2%, и всего лишь 6,8% на векторы локальных атак (рисунок 4.8) [128].

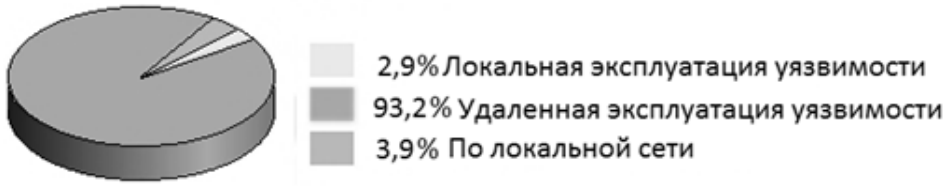
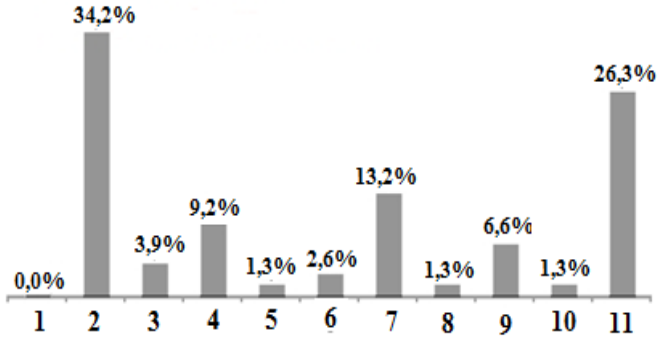


Рисунок 4.8. Распределение уязвимостей по векторам атак в феврале 2012г.

По типу воздействия наибольшее число атак были направлены на компрометацию систем – 26,3% и на неавторизованное изменение данных – 13,2% (рисунок 4.9), а высокий уровень опасности приходился на долю 15,9% атак (рисунок 4.10) [128].



1. Брут-форс атака (0,0%)
2. Межсайтовый скрипинг (34,2%)
3. Отказ в обслуживании (3,9%)
4. Раскрытие важных данных (9,2%)
5. Раскрытие системных данных (1,3%)
6. Внедрение в сессию пользователя (2,6%)
7. Неавторизованное изменение данных (13,2%)
8. Повышение привилегий (1,3%)
9. Обход ограничений безопасности (6,6%)
10. Спуфинг-атака (1,3%)
11. Компрометация системы (26,3%)

Рисунок. 4.9. Распределение атак по типу воздействия в феврале 2012г.

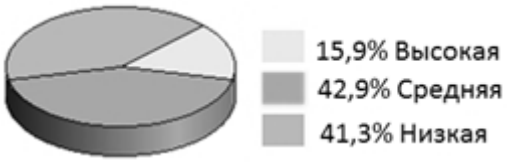


Рисунок 4.10. Распределение уязвимостей по уровню опасности в феврале 2012г.

При этом только около 50% уязвимостей были устранены производителями ПО (рисунок 4.11) [128].

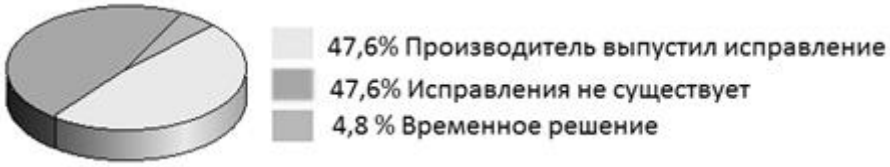


Рисунок 4.11. Наличие исправлений к уязвимостям на конец февраля 2012г.

Таким образом, проведенный анализ уязвимостей ИС показывает, что абсолютной защиты не существует. С определенной степенью вероятности при наличии необходимого времени атакующий может получить доступ к ценному ресурсу. Причем, как и для большинства сложных систем, успех атакующего во многом определяется «человеческим фактором» в системе защиты – использование словарных паролей, недостатки реализации механизмов разграничения доступа, отсутствие обновлений безопасности и снижение уровня криптографической защиты. Поэтому целью систем защиты является разработка ее структуры с учетом структуры информационной сети, обеспечивающей снижение вероятности доступа к охраняемому ресурсу за время, достаточное для обнаружения совершаемой атаки.

4.2. Анализ алгоритмов и моделей безопасности компьютерных сетей

Выбор типа математического аппарата для моделирования алгоритмов защиты ИС определяется решаемой задачей, однако большинство алгоритмов используют методы теории вероятности, математической статистики, теории множеств и теории автоматов. Обосновывается это случайным характером нагрузки системы и неопределенностью характера проведения атак на ее ресурсы. Основой моделей безопасности ИС является теория графов [130, 131, 132, 133].

Теоретическим основам решения задач безопасности посвящены работы Безрукова Н.Н., [134], Борисова А.Н. [135, 136], Бородакия Ю.В. [137], Водолазкого В.В. [138], Гераси-менко В.А. [139, 140], Грушо А.А. [141], П.Н. Девянина [142, 143], Домарева В. В. [144], Зегжды П.Д. [145], Касперского К. [146], Корниенко А.А. [147, 148], Лукацкого А.Г. [149], Машкиной И.В. [150], Молдовяна А.А. [151], Тимониной Е.Е. [141], Щербакова А.Ю. [152], Bell D.E. [153], Berman F. [154], Bishop M. [155], Bragg R. [156], Cullum J. [157], Dacier M. [158], Fox G. [154], Jajodia S. [159], Jensen Ch.D. [160], Hey T. [154] , Hoffman L. [161], LaPadula L.J. [153], McLean J. [162], McNab C. [163], Sandhu R. [164,165],, Shiller C.A. [166], Vitek J. [160].

Одним из основных видов атак на компьютерные системы являются DoS-атаки (атаки типа «отказ в обслуживании»), цель которых затруднить или исключить доступ легитимных пользователей к системе; или DDoS-атаки, когда такая атака проводится одновременно с большого числа компьютеров. Межсетевые экраны не позволяют защитить систему от DDoS-атак, особенно если атака проводится трафиком большого объема. Системы защиты от таких атак строятся на поиске аномалий в структуре трафика, поскольку приводят к потери запросов и ответов, т.е. отказам веб-серверов на основе Microsoft IIS, Apache и др. В [167,168] для решения задачи защиты от низкоактивных распределенных DDoS-атак предложена модель, базирующаяся на расчете вероятностей потери пакетов или запросов в сети, которая рассматривается как система массового обслуживания с пуассоновским распределением заявок и экспо-

ненциальным характером распределений длительностей их обслуживания в узлах сети (сеть Джексона).

Разновидностью вероятностной модели является сценарная логико-вероятностная модель оценки риска ИБ в инфокоммуникационной системе [169,170, 171, 172, 173]. Модель, представленная в [170] реализует сценарии DoS-атак, направленных на генерирование и внедрение новых объектов сетевого взаимодействия в сегменты системы, и атак несанкционированного сбора информации о сегментах системы. Кроме того, в [173] предложен метод выполнения экспертной оценки рисков ИБ с использованием логико-вероятностной модели, а в [173] разработан логико-сценарный анализатор сетевой безопасности.

Широкий класс моделей для анализа защищенности информационных сетей, учитывающих их топологию, использует теорию графов [174, 175, 176, 177]. В [174] разработан граф атак, который строится на алгоритме поведения нарушителя с учетом конфигурации сети и результатов сканирования сети. Графо-вероятностная модель обнаружения нелегитимного программного обеспечения, использующего технологию аппаратной виртуализации, позволяющая выявить особенности статистических характеристик длительности выполнения трассы при получении несанкционированного доступа к структуре, представлена в [175, 176]. Критерий присутствия нелегитимного программного обеспечения в защищаемой системе синтезирован на основе расчетных значений моментов 2-го и 4-го порядков, а также длины вариационного ряда длительности выполнения трассы.

Ряд работ, посвященных вопросам ИБ, используют поведенческие модели, использующие математические аппараты теории графов и теории конечных автоматов. Так, в [178, 179] разработана поведенческая модель защиты автоматизированных систем, предназначенная для выявления атак на Web-серверы, взаимодействие с которыми осуществляется по протоколу HTTP. С использованием данной модели был разработан конечный автомат, распознающий язык штатных HTTP–запросов, которые могут быть корректно обработаны защищенным Web-сервером; в противном случае запрос рассматривается как атака. В [180] отмечается, что разработанная модель позволяет выявлять как известные, так и новые типы атак экспертами в области ИБ путем определения вероятности ее реализации. В [181] предложены принципы формального моделирования автоматизированного поиска уязвимостей защищенной вычислительной системы в процессе сертификационных испытаний, где вычислительная машина представлена автоматом, изменяющим свое состояние в зависимости от поведения нарушителя.

В формальных моделях анализа состояния компьютерных систем используется математический аппарат теории конечных автоматов, а компьютерная система представляется абстрактной иерархической системой, состоящей из сущностей, каждое состояние которой пред-

ставляется графом доступов. Переход компьютерной системы из состояния в состояние выполняется по правилам преобразования графа доступа. С использованием этого алгоритма разработаны формальные модели для исследования компьютерных систем: Take-Grant–модель [181] и ДП-модель [142, 143, 182, 183]. С помощью ДП-моделей анализируются условия передачи прав доступа к информационным потокам, а также методы предотвращения несанкционированных доступов. Разработанная в [184, 185]. ДП-модель с функционально-ассоциированными сущностями (ФАС ДП-модель) позволяет анализировать условия получения прав доступа к объекту при реализации информационных потоков по памяти.

Аналогичный математический аппарат используется в формализованной модели функционирования ИС в условиях снижения безопасности [186]. Данная модель представлена ориентированным графом, а для исследования состояния системы в ней применяется метод причинно-следственных связей между показателями (в виде симмантических связей). Оценка уровня безопасности ИС в модели выполняется с использованием теории численных экспериментов.

Теоретические основы управления корпоративной ИС на основе интеллектуальных технологий разработаны в [150, 187], где обосновывается, что в условиях неполноты, противоречивости и неопределенности данных о состоянии информационной среды целесообразно использовать механизм нечеткого логического вывода. По признакам аномальных событий, соответствующих процессам в сети, система нечеткого логического вывода рассчитывает вероятность события, что их совокупность является атакой. Модель выбора рационального варианта реагирования на атаку построена в виде графа связи вариантов реагирования на события безопасности и получаемых экономически обоснованных исходов.

Основным недостатком рассмотренных выше моделей является определение состояния ИС по предельным вероятностям, т.к. используемый математический аппарат описывает дискретный переход системы из штатного режима работы в режим несанкционированного доступа. Однако работа ИС представляет собой динамический процесс, а всякая атака на информационный ресурс обладает протяженностью во времени, и только после ее успешного завершения атакуемый ресурс становится доступен для нарушителя. Поэтому для создания эффективных систем защиты нужно иметь динамическую модель ИС, которая позволяла бы обнаруживать несанкционированное вторжение на его начальной стадии по изменяющимся характеристикам работы системы.

В ряде работ, посвященных безопасности ИС, в качестве средства защиты рассматривается тестирование используемого программного обеспечения на предмет уязвимости. Так в [188] предложена вероятностная модель функционирования информационной телекоммуникационной сети, которая позволяет с учетом структуры сети определить размер матрицы по-

крытия ее средствами защиты.

Практическая реализация поиска уязвимостей программного обеспечения в условиях отсутствия исходного кода предложена в [44]. В основе данного метода лежит алгоритм обеспечения покрытия тестами программного обеспечения с целью исследования его на наличие уязвимостей по исполняемым файлам. Данный алгоритм позволяет автоматически выбрать точку внедрения специального кода, обеспечить покрытие участков программного обеспечения, ответственных за обработку аварийных ситуаций, получить количественную характеристику завершения тестовых испытаний. Для количественной оценки программного обеспечения на предмет уязвимостей разработанный алгоритм использует математический аппарат теории графов. Использование метода тестирования для защиты от сетевых атак предлагается и в [189].

В [46] разработана обобщенная вероятностная модель обнаружения вторжений на основе динамических байесовских сетей. Особенность данной модели в пространстве состояний заключается в том, что ее структура сохраняется неизменной во всех временных срезах при изменяющемся (динамическом) процессе моделирования. В основе модели лежит метод анализа информативных характеристик сетевого трафика для обучающих наборов данных и метод поиска новых типов вторжений с использованием вероятностного вывода в динамических байесовских сетях, что позволяет прогнозировать вторжение в условиях нехватки данных.

Использование статистики инцидентов в модели оценки безопасности информационной системы предлагается в [54]. Разработанная модель базируется на расчете вероятностей реализаций угроз путем анализа статистики инцидентов и мотиваций противника. По полученным значениям вероятностей угроз ИБ автор работы выполняет экспертную оценку рисков, стоимости потерь от нарушения конфиденциальности и стоимости внедрения соответствующих средств защиты. Для обработки экспертных оценок в работе использован алгоритм вычисления коэффициентов информационной компетентности экспертов, а в качестве объектов рассматриваются методы реализации угроз.

В [190] разработана модель социотехнической ИС при воздействии дестабилизирующих факторов, построенная на использовании теории чувствительности и аппарата математической статистики, которая по значениям математического ожидания, дисперсии и коэффициента корреляции дестабилизирующих факторов выполняет оценку защищенности системы.

Главным недостатком моделей, основанных на тестировании используемого программного обеспечения, заключается в невозможности выявления новых типов атак с неизвестным кодом. Кроме того, в данных моделях факт атаки определяется по предельным вероятностям состояний системы или с использованием метода динамики средних, что не позволяет создавать эффективные средства защиты.

Управление ИС в условиях воздействия компьютерных атак выполняется на основе априорной информации о характеристиках информационного ресурса, ценности ресурса, средств противодействия атакам и характеристиках известных атак [151-154]. На практике для решения этой задачи необходимо оценить показатели функционирования ИС по экспериментальным данным. Однако, ввиду наличия факторов неопределенности в реализации конкретного сценария атаки определять требуемые характеристики функционирования можно лишь с определенной вероятностью или экспертным путем [139, 142, 143].

Для анализа функционирования ВК во внештатном режиме должна быть разработана методика расчета вероятных характеристик его работы при MITM-атаке. Полученные вероятностные значения параметров функционирования ВК позволят выполнять объективную оценку его состояния в количественных показателях.

4.3. Моделирование атаки на виртуальный комплекс при условии криптографической защиты информации

В настоящее время для защиты конфиденциальной информации, передаваемой через сеть, применяются методы криптографии. Поэтому поиск эффективной защиты ВК должен учитывать ее шифрованный характер. Тем не менее, опыт показывает, что даже в этом случае информация может оказаться доступной атакующему.

Для дальнейшего определения вероятности доступа к ВК разработана математическая модель в терминах цветных сетей Петри, описывающая динамические процессы в системе с шифрованной информацией при проведении атаки (рисунок 4.12):

$$\Pi = \{P, T, I, O, \mu\},$$

где $$P = \begin{Bmatrix} p_1, p_2, p_{10}, p_{11}, p_{12}, p_{13}, p_{14}, p_{15}, p_{20}, p_{21}, p_{30}, \\ p_{31}, p_{140}, p_{150}, p_{160}, p_{170}, p_{180}, p_{190} \end{Bmatrix};$$

$$T = \begin{Bmatrix} t_{10}, t_{20}, t_{40}, t_{50}, t_{95}, t_{100}, t_{105}, t_{110}, t_{115}, t_{120}, t_{125}, t_{130}, t_{135},, \\ t_{140}, t_{145}, t_{150}, t_{155}, t_{160}, t_{165}, t_{170}, t_{175}, t_{180}, t_{185}, t_{190}, \\ t_{505}, t_{510}, t_{515}, t_{520}, t_{525}, t_{530}, t_{545}, t_{550}, t_{600}, t_{610}, t_{620}, \\ t_{650}, t_{660}, t_{670} \end{Bmatrix}.$$

Элементами множества позиций P являются: p_1, p_2 – передача и получение клиентом информации; p_{30}, p_{31}- - легитимные и скомпрометированные настройки систем маршрутизации; p_{20}, p_{21} – получение и передача ресурсом информации; p_{10}, p_{11}, p_{12} - легитимный канал передачи данных от клиента к ресурсу; p_{13}, p_{14}, p_{15} - легитимный канал передачи данных от ресурса к клиенту; p_{140} - получение атакующим зашифрованного пакета от клиента; p_{150} - пакет клиента расшифрован атакующим; p_{160}- пакет клиента зашифрован нарушителем; p_{170}- получение атакующим зашифрованного пакета от ресурса; p_{180}, p_{190}- пакет ресурса расшифрован и зашифрован атакующим.

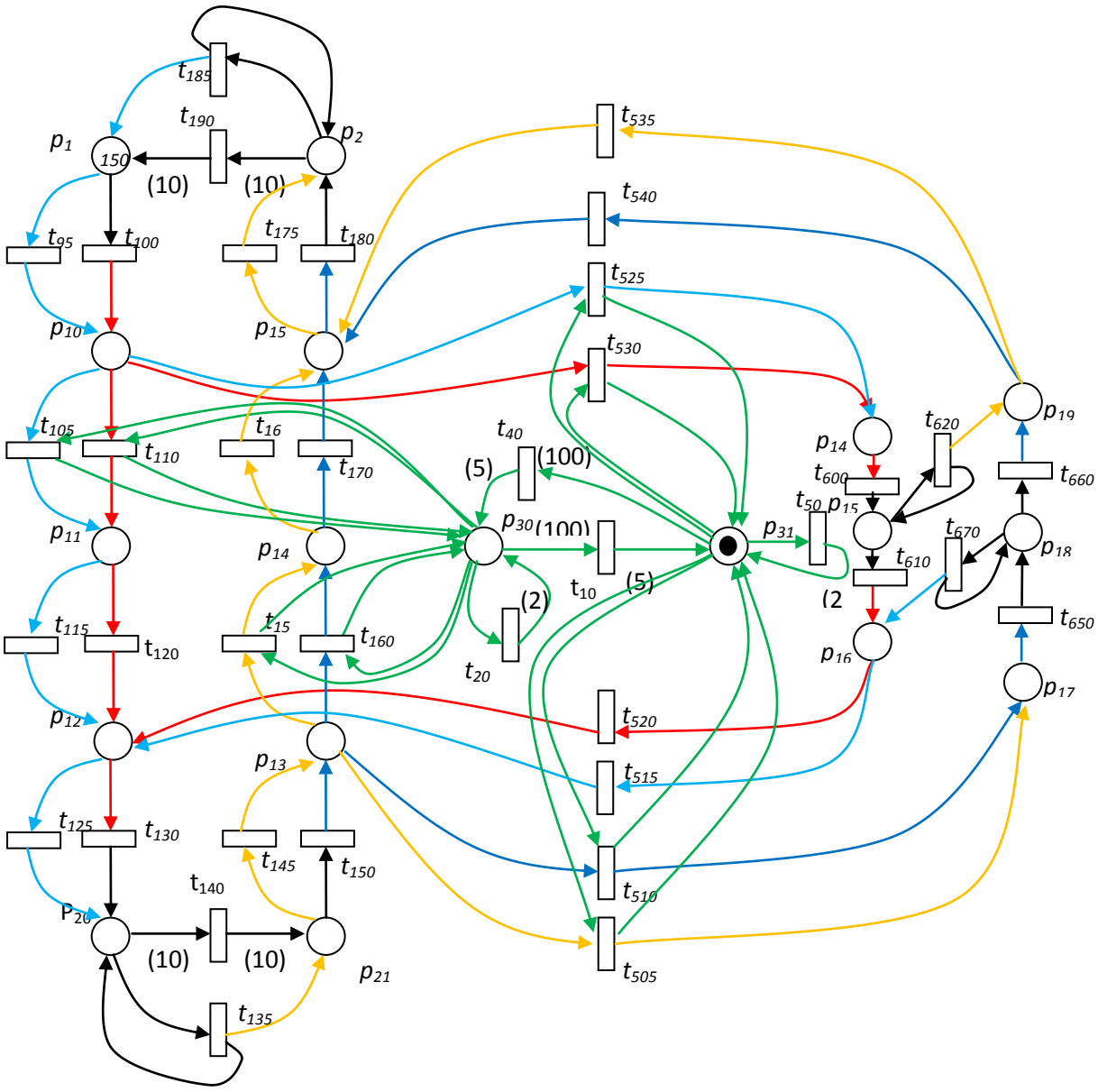


Рисунок 4.12 . Модель атаки на ВК в терминах цветных сетей Петри при условии криптографической защиты информации

Элементами множества позиций *T* являются: t_{10} - перенаправление трафика через атакующего; t_{40} - перенаправление трафика через легитимные каналы связи; t_{20}, t_{50} - воздействие на средства маршрутизации атакующим; t_{100}- шифрование информации клиентом и передача его ресурсу; t_{110}, t_{120} - передача зашифрованной информации по легитимному каналу от клиента к ресурсу; t_{130} - дешифрование информации ресурсом; t_{140} - формирование ответа ресурсом; t_{150}- шифрование информации ресурсом и передача его клиенту; t_{95}, t_{105}, t_{115}, t_{125} - передача подтверждения получения пакета информации клиентом; t_{135}- формирование подтверждения получения пакета ресурсом; t_{145}, t_{155}, t_{165}, t_{175}- передача подтверждения получения пакета информации ресурсом; t_{160}, t_{170} - передача зашифрованной информации по легитимному каналу от ресурса

клиенту; t_{180}- дешифрование информации клиентом; t_{185} - формирование подтверждения получения пакета клиентом; t_{190} - формирование ответа клиентом; t_{505} - передача подтверждения получения пакета от ресурса к атакующему; t_{510} - передача пакета информации от ресурса к атакующему; t_{515} - передача подтверждения получения пакета клиентом, сфальсифицированное атакущим; t_{520} - передача информации от нарушителя к ресурсу; t_{525}- передача подтверждения получения пакета от клиента к атакующему; t_{530}- передача информации от клиента к атакующему; t_{535} - передача подтверждения получения пакета ресурсом, сфальсифицированное атакующим; t_{540} - передача информации от атакующего к клиенту; t_{600}, t_{610} - расшифровка и шифрование пакета информации клиента атакующим; t_{620}- фальсификация получения пакета ресурсом; t_{650} , t_{660} - расшифровка и шифрование пакета ресурса атакующим; t_{670}- фальсификация получения пакета клиентом.

Графически, в терминах расширенных цветных сетей Петри, модель ВК представляется как ориентированный маркированный граф, состоящий из позиций и переходов, соединенных между собой цветными дугами.

Моделирование маршрутов в маркированном графе цветных сетей Петри удовлетворят условиями:

$$|I(p_i)| = \left|\left\{t_j \middle| p_i : color \in O : color\left(t_j\right)\right\}\right| = 1;$$

$$|O(p_i)| = \left|\left\{t_j \middle| p_i : color \in I : color\left(t_j\right)\right\}\right| = 1,$$

где $\left\{t_j \middle| p_i : color \in O : color\left(t_j\right)\right\}$ - множество переходов с дугами соответствующих цветов, для которых p_i является выходом;

$\left\{t_j \middle| p_i : color \in I : color\left(t_j\right)\right\}$ - множество переходов с дугами соответствующих цветов, для которых p_i является входом.

Разрешение на переход $t_i \in T$ определяется условием [99, 100]

$$t_j : \mu : (p_i) \geq \#(p_i : color, I : color(t_j)) \qquad (4.1)$$

для всех $p_i \in P$, где $(p_i : color, I : color(t_j))$ - кратность входной позиции p_i соответствующего цвета для дуги перехода t_j этого же цвета; т.е. переход t_j разрешен при некоторой маркировке $\mu : (p_i)$, если позиция $p_i \in P$ имеет разметку соответствующего цвета не меньшую, чем кратность дуги этого же цвета, соединяющей p_i и t_j .

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

$$\mu'(p_i) = \mu(p_i) - \#: color(p_i, I(t_j)) + \#: color(p_i, O(t_j)) \; . \qquad (4.2)$$

В итоге, динамические процессы в защищенном ВК при совершении атаки описываются системой, состоящей из 57–ми логических уравнений вида (4.1) и (4.2), определяющих условия изменений состояний системы при срабатывании переходов (4.3). Модель описывает алгоритм

взаимодействия клиента и ресурса при работе с шифрованной информацией в штатном режиме функционирования ВИ и при проведении MITM-атаки.

$$
\begin{cases}
\mu'(p_1) = \mu(p_1) + 10{:}\,black\big(\#\big(p_1, O(t_{190})\big) = 10{:}\,black\big) - \\
1{:}\,black\big(\#\big(p_1, I(t_{100})\big) = 1{:}\,black\big) + 1{:}\,cyan\big(\#\big(p_1, O(t_{185})\big) = 1{:}\,cyan\big) - \\
1{:}\,cyan\big(\#\big(p_1, I(t_{95})\big) = 1{:}\,cyan\big); \\
t_{95}{:}\,\mu(p_1) \geq \#\big(p_1, I(t_{95})\big); \\
t_{100}{:}\,\mu(p_1) \geq \#\big(p_1, I(t_{100})\big); \\
\mu'(p_{10}) = \mu(p_{10}) + 1{:}\,red\big(\#\big(p_{10}, O(t_{100})\big) = 1{:}\,red\big) + \\
1{:}\,red\big(\#\big(p_{10}, O(t_{110})\big) = 1{:}\,red\big) + 1{:}\,cyan\big(\#\big(p_{10}, O(t_{95})\big) = 1{:}\,cyan\big) - \\
1{:}\,cyan\big(\#\big(p_{10}, I(t_{105})\big) = 1{:}\,cyan\big) - 1{:}\,red\big(\#\big(p_{10}, I(t_{530})\big) = 1{:}\,red\big) - \\
1{:}\,cyan\big(\#\big(p_{10}, I(t_{525})\big) = 1{:}\,cyan\big); \\
t_{105}{:}\,\mu(p_{10}) \geq \#\big(p_{10}, I(t_{105})\big)\ u\ \ \mu(p_{30}) \geq \#\big(p_{30}, I(t_{105})\big); \\
t_{110}{:}\,\mu(p_{10}) \geq \#\big(p_{10}, I(t_{110})\big)\ u\ \ \mu(p_{30}) \geq \#\big(p_{30}, I(t_{110})\big); \\
\mu'(p_{11}) = \mu(p_{11}) + 1{:}\,red\big(\#\big(p_{11}, O(t_{110})\big) = 1{:}\,red\big) + \\
1{:}\,cyan\big(\#\big(p_{11}, O(t_{105})\big) = 1{:}\,cyan\big) - 1{:}\,red\big(\#\big(p_{11}, I(t_{120})\big) = 1{:}\,red\big) - \\
1{:}\,cyan\big(\#\big(p_{11}, I(t_{115})\big) = 1{:}\,cyan\big); \\
t_{115}{:}\,\mu(p_{11}) \geq \#\big(p_{11}, I(t_{115})\big); \\
t_{120}{:}\,\mu(p_{11}) \geq \#\big(p_{11}, I(t_{120})\big); \\
\mu'(p_{20}) = \mu(p_{20}) + 1{:}\,black\big(\#\big(p_{20}, O(t_{130})\big) = 1{:}\,black\big) + \\
1{:}\,cyan\big(\#\big(p_{20}, O(t_{125})\big) = 1{:}\,cyan\big) + 1{:}\,black\big(\#\big(p_{20}, O(t_{135})\big) = 1{:}\,black\big) - \\
10{:}\,black\big(\#\big(p_{20}, I(t_{140})\big) = 10{:}\,black\big) - 1{:}\,black\big(\#\big(p_{20}, I(t_{135})\big) = 1{:}\,black\big); \\
t_{135}{:}\,\mu(p_{20}) \geq \#\big(p_{20}, I(t_{135})\big); \\
t_{140}{:}\,\mu(p_{20}) \geq \#\big(p_{20}, I(t_{140})\big); \\
\mu'(p_{21}) = \mu(p_{21}) + 10{:}\,black\big(\#\big(p_{21}, O(t_{140})\big) = 10{:}\,black\big) + \\
1{:}\,orange\big(\#\big(p_{21}, O(t_{135})\big) = 1{:}\,orange\big) - 1{:}\,black\big(\#\big(p_{21}, I(t_{150})\big) = 1{:}\,black\big) - \\
1{:}\,orange\big(\#\big(p_{21}, I(t_{145})\big) = 1{:}\,orange\big); \\
t_{145}{:}\,\mu(p_{21}) \geq \#\big(p_{21}, I(t_{145})\big); \\
t_{150}{:}\,\mu(p_{21}) \geq \#\big(p_{21}, I(t_{150})\big); \\
\mu'(p_{13}) = \mu(p_{13}) + 1{:}\,blue\big(\#\big(p_{13}, O(t_{150})\big) = 1{:}\,blue\big) + \\
1{:}\,orange\big(\#\big(p_{13}, O(t_{145})\big) = 1{:}\,orange\big) - 1{:}\,blue\big(\#\big(p_{13}, I(t_{160})\big) = 1{:}\,blue\big) - \\
1{:}\,orange\big(\#\big(p_{13}, I(t_{155})\big) = 1{:}\,orange\big) - 1{:}\,blue\big(\#\big(p_{13}, I(t_{510})\big) = 1{:}\,blue\big) \\
-1{:}\,orange\big(\#\big(p_{13}, I(t_{505})\big) = 1{:}\,orange\big); \\
t_{155}{:}\,\mu(p_{13}) \geq \#\big(p_{13}, I(t_{155})\big)\ u\ \ \mu(p_{30}) \geq \#\big(p_{30}, I(t_{155})\big); \\
t_{160}{:}\,\mu(p_{13}) \geq \#\big(p_{13}, I(t_{160})\big)\ u\ \ \mu(p_{30}) \geq \#\big(p_{30}, I(t_{160})\big); \\
\mu'(p_{14}) = \mu(p_{14}) + 1{:}\,blue\big(\#\big(p_{14}, O(t_{160})\big) = 1{:}\,blue\big) + \\
1{:}\,orange\big(\#\big(p_{14}, O(t_{155})\big) = 1{:}\,orange\big) - 1{:}\,blue\big(\#\big(p_{14}, I(t_{170})\big) = 1{:}\,blue\big) - \\
1{:}\,orange\big(\#\big(p_{14}, I(t_{165})\big) = 1{:}\,orange\big);
\end{cases}
\tag{4.3}
$$

$$
\begin{cases}
t_{165}\colon \mu(p_{14}) \geq \#\left(p_{14}, I(t_{165})\right); \\
t_{170}\colon \mu(p_{14}) \geq \#\left(p_{14}, I(t_{170})\right); \\
\mu'(p_{15}) = \mu(p_{15}) + 1\colon blue\left(\#\left(p_{15}, O(t_{170})\right) = 1\colon blue\right) + \\
1\colon orange\left(\#\left(p_{15}, O(t_{165})\right) = 1\colon orange\right) + 1\colon blue\left(\#\left(p_{15}, O(t_{540})\right) = 1\colon blue\right) + \\
1\colon orange\left(\#\left(p_{15}, O(t_{535})\right) = 1\colon orange\right) - 1\colon blue\left(\#\left(p_{15}, I(t_{180})\right) = 1\colon blue\right) - \\
1\colon orange\left(\#\left(p_{15}, I(t_{175})\right) = 1\colon orange\right); \\
t_{175}\colon \mu(p_{15}) \geq \#\left(p_{15}, I(t_{175})\right); \\
t_{180}\colon \mu(p_{15}) \geq \#\left(p_{15}, I(t_{180})\right); \\
\mu'(p_2) = \mu(p_2) + 1\colon black\left(\#\left(p_2, O(t_{180})\right) = 1\colon black\right) + \\
1\colon orange\left(\#\left(p_2, O(t_{175})\right) = 1\colon orange\right) + 1\colon black\left(\#\left(p_2, O(t_{185})\right) = 1\colon black\right) - \\
1\colon black\left(\#\left(p_2, I(t_{185})\right) = 1\colon black\right) - 10\colon black\left(\#\left(p_2, I(t_{190})\right) = 10\colon black\right); \\
t_{185}\colon \mu(p_2) \geq \#\left(p_2, I(t_{185})\right); \\
t_{190}\colon \mu(p_2) \geq \#\left(p_2, I(t_{190})\right); \\
\mu'(p_{30}) = \mu(p_{30}) + 1\colon green\left(\#\left(p_{30}, O(t_{105})\right) = 1\colon green\right) + \\
1\colon green\left(\#\left(p_{30}, O(t_{110})\right) = 1\colon green\right) - 1\colon green\left(\#\left(p_{30}, I(t_{105})\right) = 1\colon green\right) - \\
1\colon green\left(\#\left(p_{30}, I(t_{110})\right) = 1\colon green\right) + 1\colon green\left(\#\left(p_{30}, O(t_{155})\right) = 1\colon green\right) + \\
1\colon green\left(\#\left(p_{30}, O(t_{160})\right) = 1\colon green\right) - 1\colon green\left(\#\left(p_{30}, I(t_{155})\right) = 1\colon green\right) - \\
1\colon green\left(\#\left(p_{30}, I(t_{160})\right) = 1\colon green\right) + 2\colon green\left(\#\left(p_{30}, O(t_{20})\right) = 2\colon green\right) - \\
2\colon green\left(\#\left(p_{30}, I(t_{20})\right) = 1\colon green\right) - 100\colon green\left(\#\left(p_{30}, I(t_{10})\right) = 100\colon green\right) + \\
100\colon green\left(\#\left(p_{30}, O(t_{40})\right) = 100\colon green\right); \\
t_{10}\colon \mu(p_{30}) \geq \#\left(p_{30}, I(t_{10})\right); \\
t_{20}\colon \mu(p_{30}) \geq \#\left(p_{30}, I(t_{20})\right); \\
\mu'(p_{31}) = \mu(p_{31}) + 100\colon green\left(\#\left(p_{31}, O(t_{10})\right) = 100\colon green\right) + \\
1\colon green\left(\#\left(p_{31}, O(t_{510})\right) = 1\colon green\right) - 1\colon green\left(\#\left(p_{31}, I(t_{510})\right) = 1\colon green\right) + \\
1\colon green\left(\#\left(p_{31}, O(t_{505})\right) = 1\colon green\right) - 1\colon green\left(\#\left(p_{31}, I(t_{505})\right) = 1\colon green\right) + \\
1\colon green\left(\#\left(p_{31}, O(t_{525})\right) = 1\colon green\right) - 1\colon green\left(\#\left(p_{31}, I(t_{525})\right) = 1\colon green\right) + \\
1\colon green\left(\#\left(p_{31}, O(t_{530})\right) = 1\colon green\right) - 1\colon green\left(\#\left(p_{31}, I(t_{530})\right) = 1\colon green\right) + \\
1\colon green\left(\#\left(p_{31}, O(t_{50})\right) = 1\colon green\right) - 1\colon green\left(\#\left(p_{31}, I(t_{50})\right) = 1\colon green\right) - \\
100\colon green\left(\#\left(p_{31}, I(t_{40})\right) = 100\colon green\right); \\
t_{40}\colon \mu(p_{31}) \geq \#\left(p_{31}, I(t_{40})\right); \\
t_{50}\colon \mu(p_{31}) \geq \#\left(p_{31}, I(t_{50})\right); \\
t_{505}\colon \mu(p_{31}) \geq \#\left(p_{31}, I(t_{505})\right) \text{и} \mu(p_{13}) \geq \#\left(p_{13}, I(t_{505})\right); \\
t_{510}\colon \mu(p_{31}) \geq \#\left(p_{31}, I(t_{505})\right) \text{и} \mu(p_{13}) \geq \#\left(p_{13}, I(t_{510})\right); \\
t_{515}\colon \mu(p_{160}) \geq \#\left(p_{160}, I(t_{515})\right); \\
t_{520}\colon \mu(p_{160}) \geq \#\left(p_{160}, I(t_{520})\right);
\end{cases}
\tag{4.3}
$$

$$
\begin{cases}
t_{525}: \mu(p_{31}) \geq \#\big(p_{31}, I(t_{505})\big) \text{и} \mu(p_{10}) \geq \#\big(p_{10}, I(t_{525})\big); \\
t_{525}: \mu(p_{31}) \geq \#\big(p_{31}, I(t_{530})\big) \text{и} \mu(p_{10}) \geq \#\big(p_{10}, I(t_{530})\big); \\
t_{535}: \mu(p_{190}) \geq \#\big(p_{190}, I(t_{535})\big); \\
t_{540}: \mu(p_{190}) \geq \#\big(p_{190}, I(t_{540})\big); \\
\mu'(p_{140}) = \mu(p_{140}) + 1: cyan\big(\#\big(p_{140}, O(t_{525})\big) = 1: cyan\big) \\
+1: red\big(\#\big(p_{140}, O(t_{530})\big) = 1: red\big) - 1: red\big(\#\big(p_{140}, I(t_{600})\big) = 1: red\big); \\
t_{600}: \mu(p_{140}) \geq \#\big(p_{140}, I(t_{600})\big); \\
\mu'(p_{150}) = \mu(p_{150}) + 1: black\big(\#\big(p_{150}, O(t_{600})\big) = 1: black\big) - \\
1: black\big(\#\big(p_{150}, I(t_{610})\big) = 1: black\big) + 1: black\big(\#\big(p_{150}, O(t_{620})\big) = 1: black\big) - \\
1: black\big(\#\big(p_{150}, I(t_{620})\big) = 1: black\big); \\
t_{610}: \mu(p_{150}) \geq \#\big(p_{150}, I(t_{610})\big); \\
\mu'(p_{160}) = \mu(p_{160}) + 1: red\big(\#\big(p_{160}, O(t_{610})\big) = 1: red\big) + \\
1: cyan\big(\#\big(p_{160}, O(t_{670})\big) = 1: cyan\big) - 1: red\big(\#\big(p_{160}, I(t_{520})\big) = 1: red\big) - \\
1: cyan\big(\#\big(p_{160}, I(t_{515})\big) = 1: cyan\big); \\
t_{620}: \mu(p_{150}) \geq \#\big(p_{150}, I(t_{620})\big); \\
\mu'(p_{170}) = \mu(p_{170}) + 1: blue\big(\#\big(p_{170}, O(t_{510})\big) = 1: blue\big) + \\
1: orange\big(\#\big(p_{170}, O(t_{505})\big) = 1: red\big) - 1: blue\big(\#\big(p_{170}, I(t_{650})\big) = 1: blue\big); \\
t_{650}: \mu(p_{170}) \geq \#\big(p_{170}, I(t_{650})\big); \\
\mu'(p_{180}) = \mu(p_{180}) + 1: black\big(\#\big(p_{180}, O(t_{650})\big) = 1: black\big) - \\
1: black\big(\#\big(p_{180}, I(t_{660})\big) = 1: black\big) + 1: black\big(\#\big(p_{180}, O(t_{670})\big) = 1: black\big) - \\
1: black\big(\#\big(p_{180}, I(t_{670})\big) = 1: black\big); \\
t_{660}: \mu(p_{180}) \geq \#\big(p_{180}, I(t_{660})\big); \\
\mu'(p_{190}) = \mu(p_{190}) + 1: blue\big(\#\big(p_{190}, O(t_{660})\big) = 1: blue\big) + \\
1: orange\big(\#\big(p_{190}, O(t_{620})\big) = 1: orange\big) - 1: blue\big(\#\big(p_{190}, I(t_{540})\big) = 1: blue\big) - \\
1: orange\big(\#\big(p_{190}, I(t_{535})\big) = 1: orange\big); \\
t_{670}: \mu(p_{180}) \geq \#\big(p_{180}, I(t_{670})\big).
\end{cases}
\tag{4.3}
$$

Клиент формирует запрос (состояние p_1), и передает его ресурсу; при этом каждый пакет информации шифруется (переход t_{100}). Получение ресурсом шифрованного пакета идентифицируется состоянием p_{12}. После этого информация пакета дешифруется (переход t_{130}) и передается ресурсу (состояние p_{20}).

После получения клиентом каждого шифрованного пакета (состояниеp_{15}), он дешифруется (переход t_{180}) в открытый текст (состояние p_2). Клиент формирует подтверждение получения каждого пакета (переход t_{185}) и передает его ресурсу (переходы t_{95}, t_{105}, t_{115}, t_{125}). После получения клиентом всего пакета информации (состояние p_2), он формирует новый запрос ресурсу (переход t_{190}) .

Ресурс формирует подтверждение получения пакета (переход t_{135}). Передача клиенту подтверждения получения ресурсом каждого пакета информации осуществляется через перехо-

ды t_{145}, t_{155}, t_{165}, t_{175}. После получения ресурсом исходного сообщения (всех пакетов информации), он формирует ответ, что идентифицируется состоянием p_{21}, и передает его клиенту (состояние p_{15}), шифруя при этом каждый пакет. Процедуре шифрования каждого пакета информации соответствует переход t_{150}.

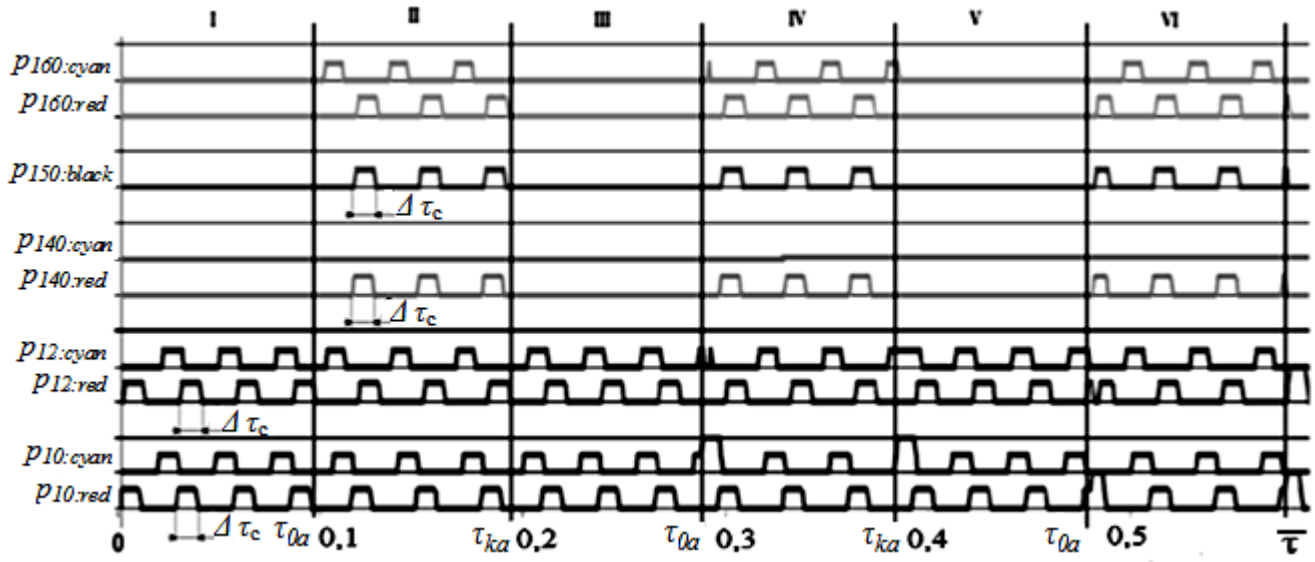
В штатном режиме работы системы маркеры, отображающие функционирование средств маршрутизации, находятся в состоянии p_{30}, при этом передача информации осуществляется через легитимные каналы (состояния p_{11} и p_{14}).

В случайный момент времени атакующий воздействует на средства маршрутизации (переход t_{20}) и, в случае успеха, перенаправляет информацию через себя (переход t_{10}, состояние p_{31}). В результате, трафик между клиентом и ресурсом проходит через атакующего (переходы t_{505}, t_{510}, t_{525}, t_{530}, состояния p_{140} и p_{170}). Атакующий дешифрует полученные пакеты (переходы t_{600}, t_{650}), получая при этом доступ к информации (состояния p_{150} и p_{180}), затем фальсифицирует подтверждения о получении соответствующих пакетов (переходы t_{620}, t_{670}) и передает их клиенту (переход t_{535}) или ресурсу (переход t_{515}). «Прочитав» каждый пакет, атакующий снова шифрует его (переходы t_{610}, t_{660}), и передает ресурсу или клиенту (переходы t_{540}, t_{520}). Время прослушивания информации определяется функционированием перехода t_{50}. Собрав необходимую информацию, нарушитель уходит из сети и легитимные каналы передачи информации восстанавливаются, что соответствует срабатыванию перехода t_{40}.

Для технической реализации данной модели был разработан конструктор цветных сетей Петри на языке C++. Результаты моделирования динамических процессов в ВК в условиях MITM-атаки на ресурс при наличии криптографической зашиты приведены на рисунках 4.13 - 4.14.

Рисунок 4.13 отражает процесс передачи информации между клиентом и ресурсом в штатном режиме работы системы и при проведении атаки.

На участке I рисунка 4.13 передача информации между клиентом и ресурсом идет по легитимным каналам (активны состояния p_{11} и p_{14}). В случайный момент $\tau_{0\alpha}$ (участок II) атакующий перенаправляет трафик через себя: это соответствует тому, что легитимный канал связи обрывается и трафик передается через атакующего (активны состояния p_{11}, p_{14} и p_{140}, p_{150}, p_{160}). Однако характер передачи трафика не нарушается ни с точки зрения клиента, ни с точки зрения ресурса, а атакующий получает все пакеты информации, проходящие между ними. После того как сообщение прочитано, в случайный момент $\tau_{k\alpha}$ атакующий, также незаметно для легитимных пользователей, уходит из сети.



$\tau_{0\alpha}$, $\tau_{k\alpha}$ – моменты начала и окончания атаки; $\Delta\tau_c$ – время передачи сообщения; $p_{10:red}$, $p_{12:red}$ – получение клиентом и ресурсом шифрованной информации; $p_{10:cyan}$, $p_{12:cyan}$– получение клиентом и ресурсом подтверждения о передаче пакетов информации; $p_{140:red}$ – получение атакующим шифрованного пакета; $p_{140:cyan}$ – получение атакующим подтверждения о передаче шифрованного пакета; $p_{150:black}$, $p_{160:red}$- пакет клиента расшифрован и зашифрован атакующим; $p_{160:cyan}$- фальсификация атакующим подтверждения о получении шифрованного пакета

Рисунок 4.13. Результаты моделирования MITM-атаки на ВК при условии криптографической защиты информации

На участке IV диаграммы атакующий перехватил только последнюю часть пакетов, относящихся к сообщению $\Delta\tau_c$ и соответственно, не смог его прочесть.

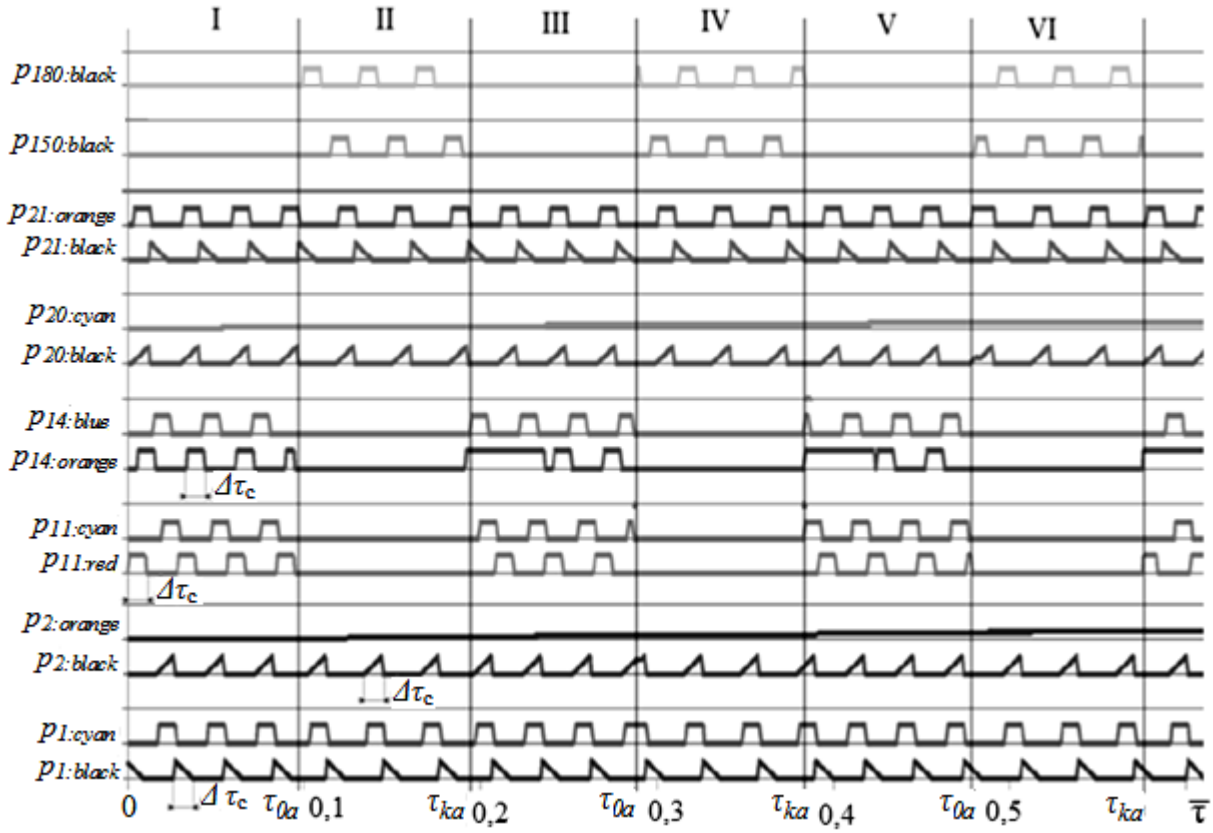
Такой “закрытый” процесс проникновения атакующего в канал связи между ресурсом и клиентом соответствует проведению реальной MITM-атаки, поэтому можно считать, что разработанная модель адекватно отражает процессы нарушения конфиденциальности криптографически защищенной информации в ВК.

Динамический процесс функционирования всего ВК в штатном режиме и при проведении MITM-атаки представлен на рисунке 4.14. Кроме действий клиента, ресурса и атакующего в текущем относительном времени здесь отражены процессы получения подтверждений о передаче пакетов информации от клиента ресурсу $p_{2:orange}$ и от ресурса клиенту $p_{20:cyan}$.

При штатном функционировании ВК переход t_{10} пассивен и маркер присутствует в состоянии p_{30} . Это соответствует тому, что передача трафика между ВМ (состояния p_1,p_2) и ресурсом (состояния p_{20} , p_{21}) осуществляется по легитимному каналу связи через промежуточные состояния системы p_{10}, p_{11},p_{12} и p_{13}, p_{14},p_{15}.

В случайный момент времени атакующий воздействует на устройство сетевой маршрутизации для перенаправления трафика, что дает возможность осуществить его перехват. При этом активизируется переход t_{10} и изменяет маркировку сети: маркеры из состояния p_{30} переходят в состояние p_{31}, в результате чего закрываются переходы t_{110} и t_{160}.

Это эквивалентно закрытию легитимного канала передачи информации между ВМ и ресурсом и открытию канала через атакующего, обеспечивающего «перехват» и «прослушивание» конфиденциальной шифрованной информации.



$\tau_{0\alpha}$ – момент начала атаки, $\tau_{k\alpha}$ – момент окончания атаки, $\Delta\tau_c$ – время передачи сообщения, $p_{1:black}$, $p_{2:black}$ – передача и получение клиентом информации; $p_{1:cyan}$ – передача клиентом подтверждения о получении пакета информации; $p_{2:orange}$ – получение клиентом подтверждения от ресурса о получении пакета; $p_{20:black}$, $p_{21:black}$ – получение и передача ресурсом информации; $p_{20:cyan}$ – получение ресурсом подтверждения от клиента о получении пакета; $p_{21:orange}$ – передача ресурсом подтверждения о получении пакета; $p_{11:red,cyan}$ - легитимный канал передачи данных от клиента к ресурсу; $p_{14:blue,orange}$ - легитимный канал передачи данных от ресурса к клиенту; $p_{150:black}$ - пакет клиента расшифрован атакующим; $p_{180:black}$ - пакет ресурса расшифрован атакующим

Рисунок 4.14. Результаты моделирования MITM-атаки на виртуальный комплекс при условии криптографической защиты передаваемой информации

Таким образом, на базе математического аппарата расширенных цветных сетей Петри разработана динамическая модель функционирования ВК, предусматривающая процессы шифрования и дешифрования информации и случайный характер перенаправления трафика с легитимных каналов связи на канал связи через атакующего при совершении MITM-атаки.

4.4. Разработка метода определения эффективности системы защиты вычислительного комплекса

Взаимодействие атакующего и системы защиты относятся к конфликтным ситуациям, поэтому для прогнозирования эффективности применяемой защиты зачастую используется математический аппарат теории игр [130, 195, 196]. Задача, которую решает система защиты с точки зрения теории игр – определить оптимальную стратегию, использование которой приведет к минимальным рискам со стороны легитимных пользователей ВК, поэтому преимущественно используется мини-максная стратегия. Однако в области построения систем защиты применение мини-максной стратегии не всегда оправдано, так как вполне вероятно, что атакующий имеет цели отличные от целей и приоритетов системы защиты [196]. Кроме того, атакующий не всегда имеет полную информацию относительно конфигурации системы защиты, что значительно усложняет для него возможность определить свою оптимальную стратегию.

В настоящее время для моделирования случайных процессов широко применяется метод статистических испытаний (метод Монте-Карло), базирующийся на законе больших чисел (теореме Чебышева). Его преимуществом является возможность получения адекватного результата, когда построение аналитической модели объекта является трудноосуществимым, т.к. согласно теореме Чебышева при большом числе независимых опытов математическое ожидание случайной величины может быть представлено ее средним арифметическим значением [130]. Кроме того, метод Монте-Карло справедлив для описания функционирования систем, случайные процессы в которых не являются марковскими.

На основании указанных причин в основе алгоритма определения эффективности защиты ВК использовался метод Монте-Карло. В данном случае задача решалась для дерева атак на ВК, разработанного в п. 3.3 (рис. 3.7). При этом, каждая реализация процесса «атака-защита» выполнялась при случайном характере его параметров, а вероятность успешной атаки на ресурс в соответствии с теоремой Бернули определялась частотой совершения этого события.

Для определения эффективной конфигурации системы защиты ВК был разработан метод, в основу которого положена модель MITM-атаки на ресурс с криптографической защитой трафика, представленная в п. 4.3. В алгоритме моделирования процесса «MITM-атака-защита» учитывалась разветвленная конфигурация системы защиты и случайный характер параметров системы защиты и параметров проведения атаки. Для расчета вероятности успешной атаки на

защищенный ресурс использовались статистические данные о совершении атак на информационные системы, приведенные в п. 4.1.

В соответствии с алгоритмом разработанного метода начало атаки может реализовываться воздействием на одну из начальных (листовых) вершин дерева атак (рис. 4.15), множество которых

$$P(P_{0,m}) = \{P_{0,1}, P_{0,2}, P_{0,3}, P_{0,4}, P_{0,5}, P_{0,6}, P_{0,7}, P_{0,8}, P_{0,9}\}, \qquad (4.4)$$

где: «*0*» – индекс вектора исходных вершин маршрутов атак; $m = R0$ – номер маршрута проведения атаки;

$R0$– случайное число с равномерным распределением, $R0 \in \{1,2,\dots,9\}$, т.е. выбор начальной вершины маршрута атаки имеет случайный характер и задается генератором случайных чисел. Распределение типов атак принималось на основании [128] и диаграмм, приведенных на рис. 4.2,4.6.

Разработанный алгоритм проведения атак учитывает случайное значение базовой квалификации атакующего. Параметр квалификации атакующего для каждой моделируемой атаки в терминах цветных сетей Петри задается количеством маркеров в исходной вершине маршрута $\mu_{0,m}$. В соответствии с принятым алгоритмом работы системы

$$\mu_{0,m} = R1_m\ , \qquad (4.5)$$

где: $R1_m$- случайная величина с нормальным распределением: $1 \leq R1_m \leq 100$ и шагом $\Delta R1_m = 1$.

В соответствии с [128] (рис. 4.10) атакующие по степени квалификации распределяются следующим образом: 41% имеют низкую квалификацию, 43% - среднюю, а 16% - высокую. Это было учтено при создании алгоритма моделирования: при $1 \leq R1_m \leq 41$ предполагалось, что атакующий имеет низкую квалификацию; при $42 \leq R1_m \leq 84$ - среднюю квалификацию; при $85 \leq R1_m \leq 100$ - высокую квалификацию. Разыгранное значение параметра $R1_m$ для каждого маршрута атаки с индексом «*m*» функционально влияет на время срабатывания переходов данного маршрута $\tau_{j,m}$, где j – индекс перехода по маршруту

Таким образом, исходное состояние для проведения атаки по маршруту с индексом «*m*» определяется комбинацией двух случайных чисел: $P_{0,m}(R0, R1_m)$. Попадая на случайную листовую вершину дерева, атакующий, с учетом своей квалификации, может реализовать успешную атаку пройдя по определенному маршруту до его корня.

В соответствии с алгоритмом работы модели для совершения перехода от одной вершины дерева к другой атакующему необходимо выполнить ряд действий некоторой сложности, занимающих определенное время. Результирующее время срабатывания каждого перехода $\tau_{j,m}$

определяется значениями трех параметров: сложностью проводимой атаки, квалификацией атакующего и собственно временем проведения атаки:

$$\tau_{j,m} = k2_{j,m} \cdot R2_{j,m} + k3_{j,m} \cdot R3_{j,m} + k4_{j,m} \cdot R4_{j,m}\ , \qquad (4.6)$$

где $R2_{j,m}$, $R3_{j,m}$, $R4_{j,m}$ - случайные величины, определяющие сложность проводимой атаки, квалификацию атакующего с точки зрения решения текущей задачи и процедуру эксплуатации уязвимости; $k2_{j,m}$, $k3_{j,m}$, $k4_{j,m}$- коэффициенты размерности.

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

Сложность проводимой атаки, задается случайной величиной $R2_{j,m}$, в соответствии с рисунком 4.6; при этом в режиме работы ВК без использования средств информационной защиты на данном переходе $1 \leq R2_{j,m} \leq 100$ с шагом $\Delta R2_{j,m} = 1$. В том случае, если переход снабжен средствами защиты $1 \leq R2_{j,m} \leq 10000$ с шагом $\Delta R2_{j,m} = 1$.

Возможность эксплуатации атакующим каждой уязвимости маршрута определяется его квалификацией. В связи с этим диапазон случайной величины $R3_{j,m}$ характеризуется квалификацией атакующего, определенной в начале маршрута, и задается как $1 \leq R3_{j,m} \leq R1_m$ с шагом $\Delta R3_{j,m} = 1$.

Эксплуатация уязвимости каждого перехода определяется количеством необходимых процедур. Для характеристики эксплуатации уязвимости был принят диапазон изменения $0 \leq R4_{j,m} \leq 1000$ с шагом $\Delta R4_{j,m} = 1$.

Коэффициенты $k2_{j,m}$, $k3_{j,m}$, $k4_{j,m}$ зависимости (4.6) позволяют перевести ны $R2_{j,m}$, , $R3_{j,m}$, $R3_{j,m}$ в масштаб времени.

Проведенный анализ статистической информации о получении несанкционированного доступа к информационным системам показывает, что экономически оправданное время, затрачиваемое на компрометацию ресурса, в среднем составляет 7 рабочих дней; а в результате тестирования информационных систем было получено, что в 75% случаев, специалистам Positive Technologies удалось получить полный контроль над критическими ресурсами [124]. Статистика, приведенная в [124] была использована для определения масштаба времени при моделировании процессов компрометации ВК с защищенным ресурсом

Процедура отыскания и эксплуатации уязвимости на переходе $t_{\mathrm{j,m}}$ дерева атак в математической модели, описывающей динамические процессы в ВК с использованием математического аппарата цветных сетей Петри, соответствует срабатыванию перехода $t_{j,m}$. При этом сложность атаки характеризуется кратностью входной дуги этого перехода$I(t_{j,m})$

$$|I(p_{j,m})| = |\{t_{j,m}|p_{j,m} \in O(t_{j,m})\}|, \qquad (4.7)$$

где: $I(p_{j,m})$ – кратность входной дуги состояния;

$p_{j,m}$, $O(t_{j,m})$ - кратность выходной дуги перехода $t_{j,m}$.

Квалификация атакующего определяется кратностью выходной дуги каждого да$O(t_{j,m})$, а процедура эксплуатации уязвимости – срабатыванием перехода $t_{j,m}$. Срабатывание перехода $t_{j,m}$ в динамической модели функционирования ВК может быть реализовано только при выполнении условия

$$\mu(p_{i,m}) \geq \#(p_{j,m}, I(t_{j,m})), \qquad (4.8)$$

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

Кратность входной дуги перехода $I(t_{j,m})$ задается генератором случайных чисел $R2_{j,m}$, т.е.

$$\mathrm{I}(t_{j,m}) = R2_{j,m}, \qquad (4.9)$$

а кратность выходной дуги перехода $\mathrm{O}(\mathrm{t_{j,m}})$ зависит от квалификации атакующего:

$$O(t_{j,m}) = R3_{j,m}. \quad . \qquad (4.10)$$

Количество необходимых процедур $N_{\text{п}}$ для выполнения условия (4.8)

$$N_{\text{п}} = R4_{j,m}\ . \qquad (4.10)$$

Таким образом, разработана методика определения количественных показателей эффективности защиты ВК с учетом структуры дерева атак, основу которой составляют метод статистических испытаний Монте-Карло и закон больших чисел (теорема Чебышева), когда характеристики маршрутов проводимых атак и эксплуатаций уязвимостей могут задаваться случайными числами с любыми распределениями в соответствии с результатами анализа работы ИС. Данная методика при большом числе испытаний позволит сравнить эффективность различных систем защиты ВК по количественным показателям вероятности и времени доступа к ресурсу.

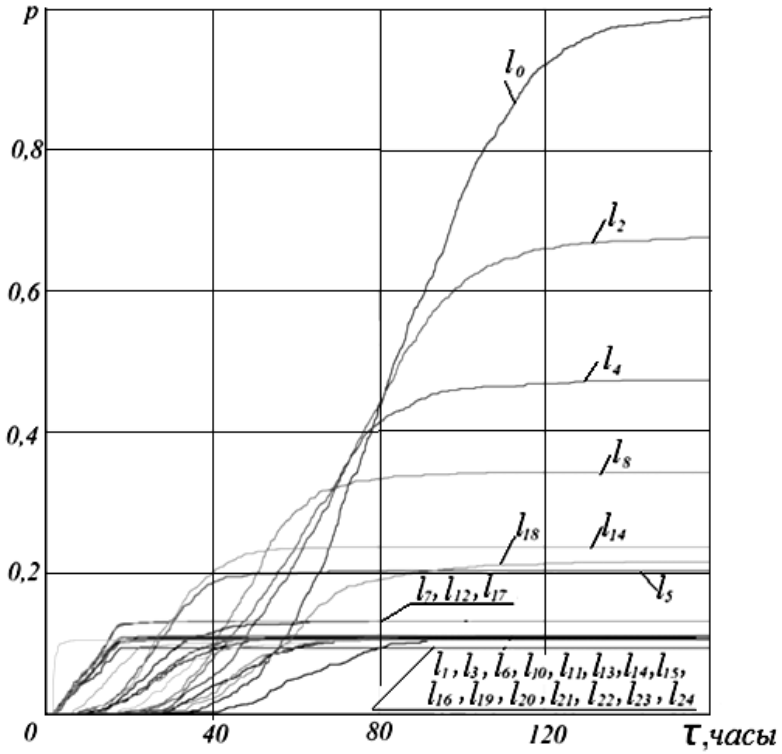
4.5. Результаты расчета эффективности системы защиты вычислительного комплекса

В соответствии с приведенным алгоритмом выполнено моделирование динамического процесса атаки на ВК при различны вариантах защиты. Поскольку алгоритм расчета вероятности успешной атаки базируется на использовании метода Монте-Карло, из центральной предельной теоремы теории вероятностей следует, что полученные частные результаты распределятся приближенно по нормальному закону [130]. При моделировании была принята погрешность расчета $\varepsilon = 0{,}03$, что допустимо при решении технических задач. При соответствующим

значении "уровня доверия" число розыгрышей в каждом варианте защиты должно было составлять $L = 65250$.

В качестве базовой системы защиты, успешная атака которой может быть реализована за 168 часов, принят стандартный комплекс мер на основе мониторинга сетевых процессов и разграничения прав доступа к ресурсам без использования специализированного анализирующего или защитного ПО (рисунки 4.3, 4.4) [124].

Результаты моделирования показывают, что при любом алгоритме MITM-атаки, реализуемым соответствующим маршрутом дерева (рисунок 3.7), гарантированный доступ к хосту будет получен через 61 час (рисунок 4.15). Гипервизор станет доступен атакующему через 87 часов, а информация ресурса - через 159 часов.



l_0 - прослушивание трафика ВМ; l_1 - доступ к сетевому интерфейсу хоста; l_2 - доступ к сетевому интерфейсу ВМ; l_3 - установка сниффера или анализатора трафика на хост; l_4 - установка сниффера или анализатора трафика на ВМ; l_5 - доступ к гипервизору (эмулятору сетевых интерфейсов); l_6 - доступ к терминалу хоста; l_7 - доступ к терминалу ВМ; l_8 - доступ к файлам ВМ; l_9, l_{16} - удаленный доступ к гипервизору; l_{10}, l_{11}, l_{15}, l_{17} - доступ к хосту (заражение, фишинг и т.д.); l_{12} - доступ к ВМ (заражение, фишинг и т.д.); l_{13} - доступ к файлам хоста; l_{14}- доступ к гипервизору (управление жесткими дисками ВМ); l_{18}- перенаправление трафика через атакующего; l_{19}- ARP-компрометация; l_{20}- DNS-компрометация; l_{21}- доступ к LAN; l_{22}- доступ к DNS-службе; l_{23}, l_{24}- заражение, фишинг и т.д.

Рисунок 4.15. Расчетные вероятности получения несанкционированного доступа к элементам ВК с базовой защитой при проведении MITM – атаки

В том случае, если MITM-атака направлена на ресурс как на независимое устройство, не учитывая его виртуальную реализацию, то он будет скомпрометирован через это же время.

Таким образом, анализ статистических результатов атак на ресурс показал адекватность разработанного алгоритма определения эффективности защиты по значению времени компрометации ресурса.

Подтверждением верности разработанного алгоритма является тот факт, что в случае успешного проведения этапа атаки на элемент ВК сумма предельных вероятностей состояния его по всем маршрутам $\sum_{m=1}^{9} p_{j,m} = 1$.

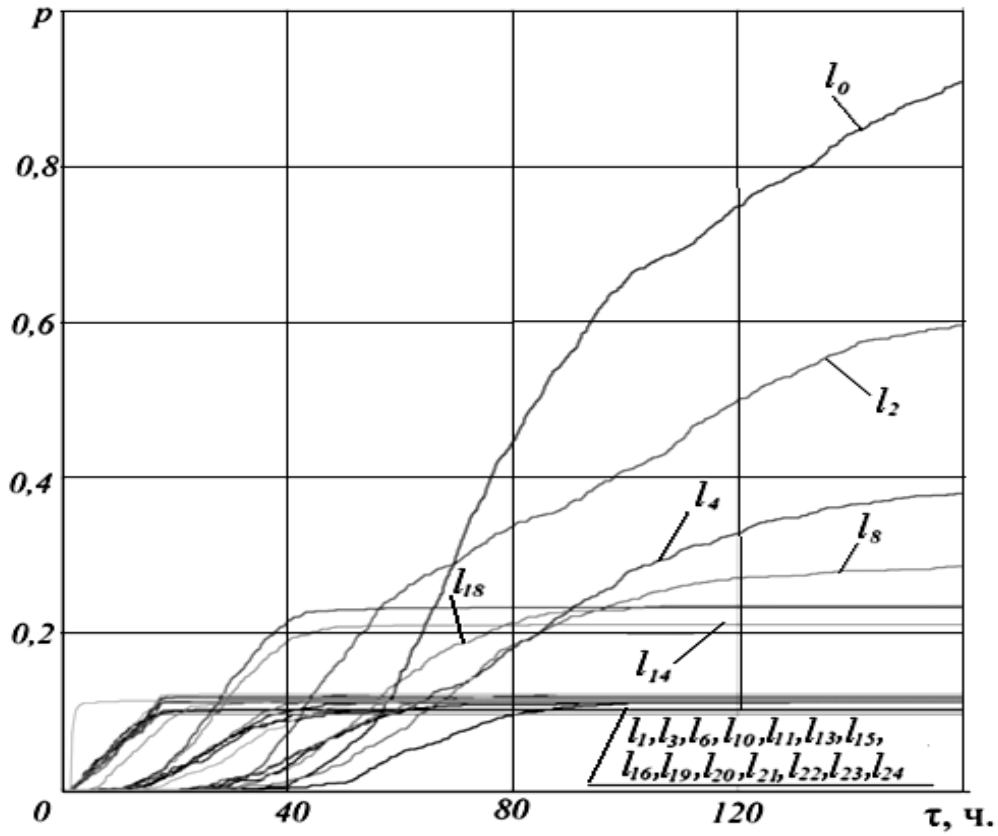
С использованием разработанного метода были определены расчетные значения вероятностей несанкционированного доступа к информации ресурса при использовании четырех типов защит:

- 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 (рисунки 4.16, 4.20). Поскольку хост и гипервизор ВК не получили дополнительной защиты время доступа к ним не меняется по сравнению с базовой системой защиты.

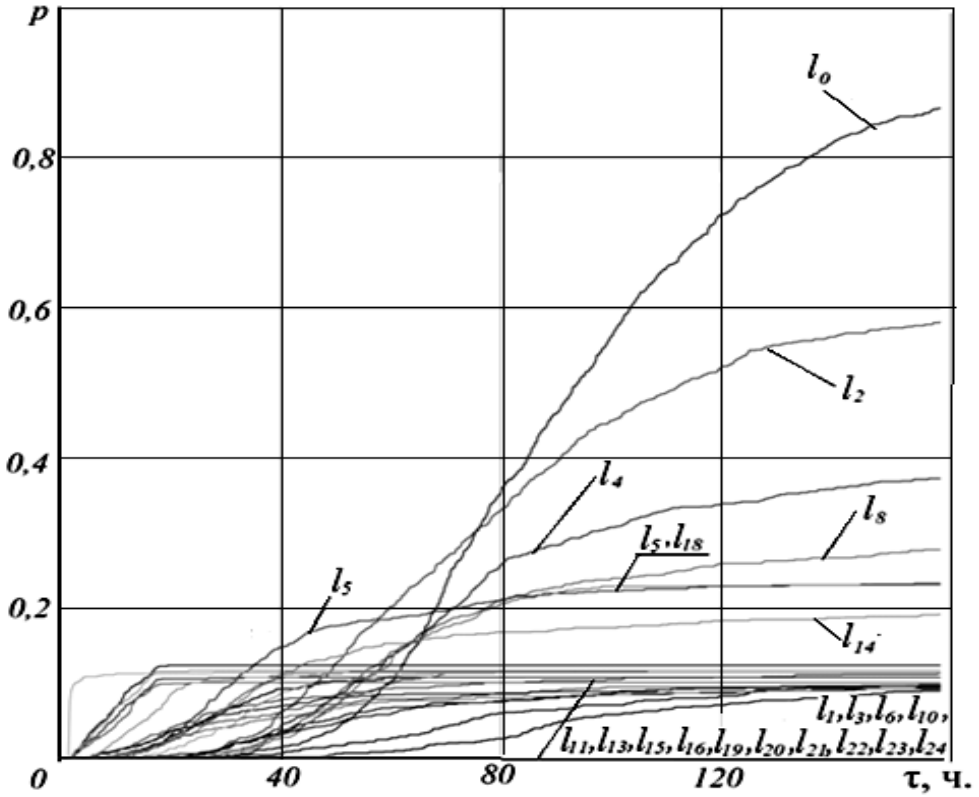
В том случае, если в ВК используются комплекс защитных средств и ПО для обеспечения конфиденциальности «диска» ВМ, на момент контрольного времени вероятность защиты от несанкционированного доступа к информации составила 0,12 (рисунки 4.17, 4.20), а время доступа к гипервизору увеличилось на 2 часа (3%) по сравнению с базовой системой защиты.

Наиболее эффективной системой для защиты ресурса ВК оказывается комплекс защитного ПО для хоста (рисунки 4.18, 4.20). Его использование снижает вероятность защиты за контрольное время (168 ч.) 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.



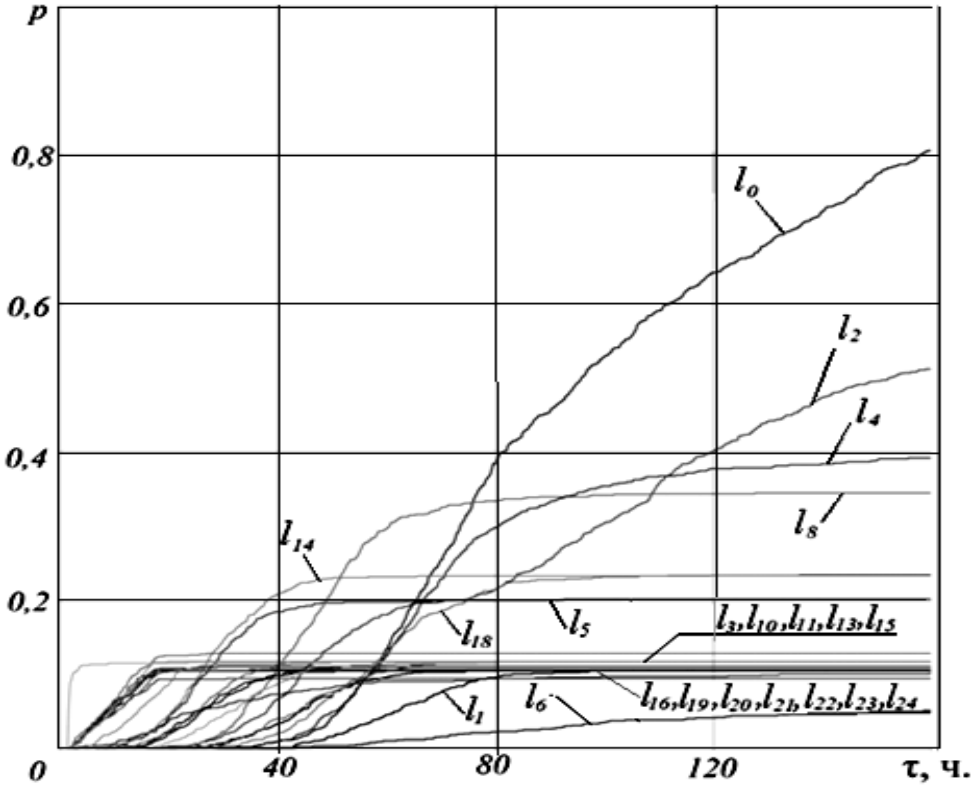
l_0 - прослушивание трафика ВМ; l_1 - доступ к сетевому интерфейсу хоста; l_2 - доступ к сетевому интерфейсу ВМ; l_3 - установка сниффера или анализатора трафика на хост; l_4 - установка сниффера или анализатора трафика на ВМ; l_5 - доступ к гипервизору; l_6 - доступ к терминалу хоста; l_7 - доступ к терминалу ВМ; l_8 - доступ к файлам ВМ; l_9, l_{16} - удаленный доступ к гипервизору; l_{10}, l_{11}, l_{15}, l_{17} - доступ к хосту (заражение, фишинг и т.д.); l_{12} - доступ к ВМ (заражение, фишинг и т.д.); l_{13} - доступ к файлам хоста; l_{14}- доступ к гипервизору (управление жесткими дисками ВМ); l_{18}- перенаправление трафика через атакующего; l_{19}- ARP-компрометация; l_{20}- DNS-компрометация; l_{21}- доступ к LAN; l_{22}- доступ к DNS-службе; l_{23}, l_{24}- заражение, фишинг и т.д.

Рисунок 4.16. Расчетные вероятности получения несанкционированного доступа к элементам ВК с защитой ВМ при проведении MITM - атаки



l_0 - прослушивание трафика ВМ; l_1 - доступ к сетевому интерфейсу хоста; l_2 - доступ к сетевому интерфейсу ВМ; l_3 - установка сниффера или анализатора трафика на хост; l_4 - установка сниффера или анализатора трафика на ВМ; l_5 - доступ к гипервизору; l_6 - доступ к терминалу хоста; l_7 - доступ к терминалу ВМ; l_8 - доступ к файлам ВМ; l_9, l_{16} - удаленный доступ к гипервизору; l_{10}, l_{11}, l_{15}, l_{17} - доступ к хосту (заражение, фишинг и т.д.); l_{12} - доступ к ВМ (заражение, фишинг и т.д.); l_{13} - доступ к файлам хоста; l_{14}- доступ к гипервизору (управление жесткими дисками ВМ); l_{18}- перенаправление трафика через атакующего; l_{19}- ARP-компрометация; l_{20}- DNS-компрометация; l_{21}- доступ к LAN; l_{22}- доступ к DNS-службе; l_{23}, l_{24}- заражение, фишинг и т.д.

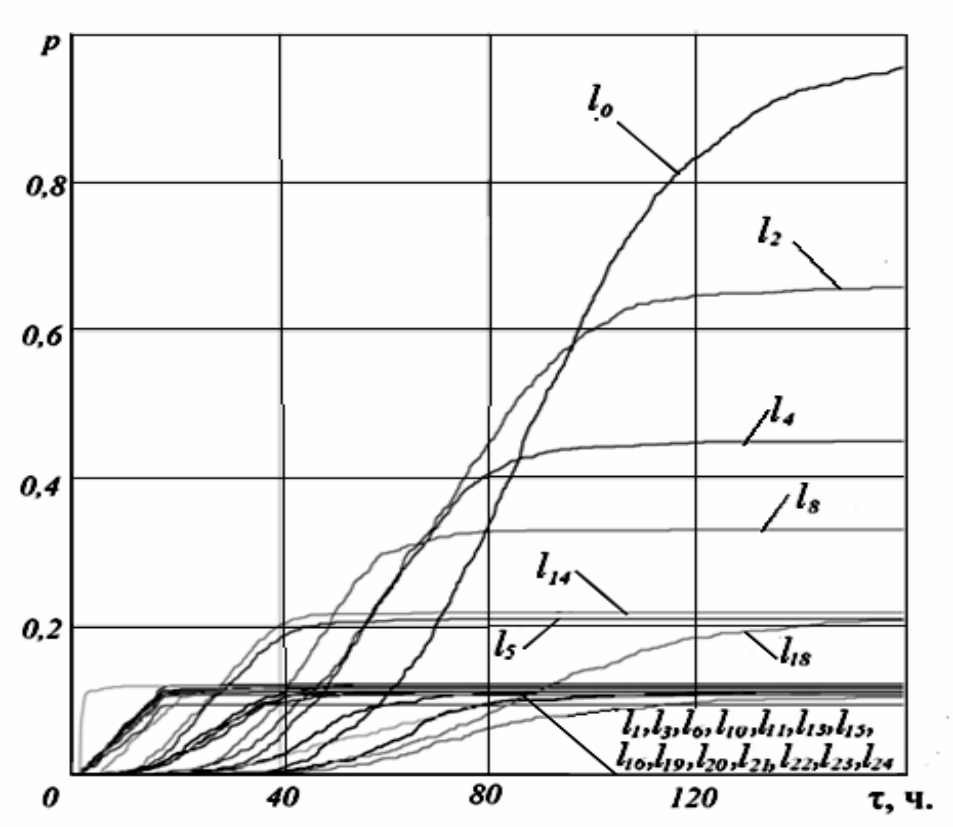
Рисунок 4.17. Расчетные вероятности получения несанкционированного доступа к элементам ВК с защитой «диска» ВМ при проведении MITM -атаки



l_0 - прослушивание трафика ВМ; l_1 - доступ к сетевому интерфейсу хоста; l_2 - доступ к сетевому интерфейсу ВМ; l_3 - установка сниффера или анализатора трафика на хост; l_4 - установка сниффера или анализатора трафика на ВМ; l_5 - доступ к гипервизору; l_6 - доступ к терминалу хоста; l_7 - доступ к терминалу ВМ; l_8 - доступ к файлам ВМ; l_9, l_{16} - удаленный доступ к гипервизору; l_{10}, l_{11}, l_{15}, l_{17} - доступ к хосту (заражение, фишинг и т.д.); l_{12} - доступ к ВМ (заражение, фишинг и т.д.); l_{13} - доступ к файлам хоста; l_{14}- доступ к гипервизору (управление жесткими дисками ВМ); l_{18}- перенаправление трафика через атакующего; l_{19}- ARP-компрометация; l_{20}- DNS-компрометация; l_{21}- доступ к LAN; l_{22}- доступ к DNS-службе; l_{23}, l_{24}- заражение, фишинг и т.д.

Рисунок 4.18. Расчетные вероятности получения несанкционированного доступа к элементам ВК с защитой хостовой системы при проведении MITM-атаки

Использование средств обеспечения безопасности сетевой инфраструктуры ВК оказалось наименее эффективным средством защиты (рис. 4.19, 4.20). К контрольному времени информация будет защищена с вероятностью 0,1; время доступа к хосту составит 67 ч., а к гипервизору - 90 ч.



l_0 - прослушивание трафика ВМ; l_1 - доступ к сетевому интерфейсу хоста; l_2 - доступ к сетевому интерфейсу ВМ; l_3 - установка сниффера или анализатора трафика на хост; l_4 - установка сниффера или анализатора трафика на ВМ; l_5 - доступ к гипервизору; l_6 - доступ к терминалу хоста; l_7 - доступ к терминалу ВМ; l_8 - доступ к файлам ВМ; l_9, l_{16} - удаленный доступ к гипервизору; l_{10}, l_{11}, l_{15}, l_{17} - доступ к хосту (заражение, фишинг и т.д.); l_{12} - доступ к ВМ (заражение, фишинг и т.д.); l_{13} - доступ к файлам хоста; l_{14}- доступ к гипервизору (управление жесткими дисками ВМ); l_{18}- перенаправление трафика через атакующего; l_{19}- ARP-компрометация; l_{20}- DNS-компрометация; l_{21}-доступ к LAN; l_{22}- доступ к DNS-службе; l_{23}, l_{24}- заражение, фишинг и т.д.

Рисунок 4.19. Расчетные вероятности получения несанкционированного доступа к элементам ВК со средствами обеспечения безопасности сетевой инфраструктуры при проведении MITM - атаки

На диаграммах рисунка 4.20 представлены вероятностные характеристики защищенности информации ВК при использовании указанных типах защит и проведении MITM-атак. 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 4.20). Результаты показали, что в этом случае за контрольное время информация будет защищена с вероятностью 65%.

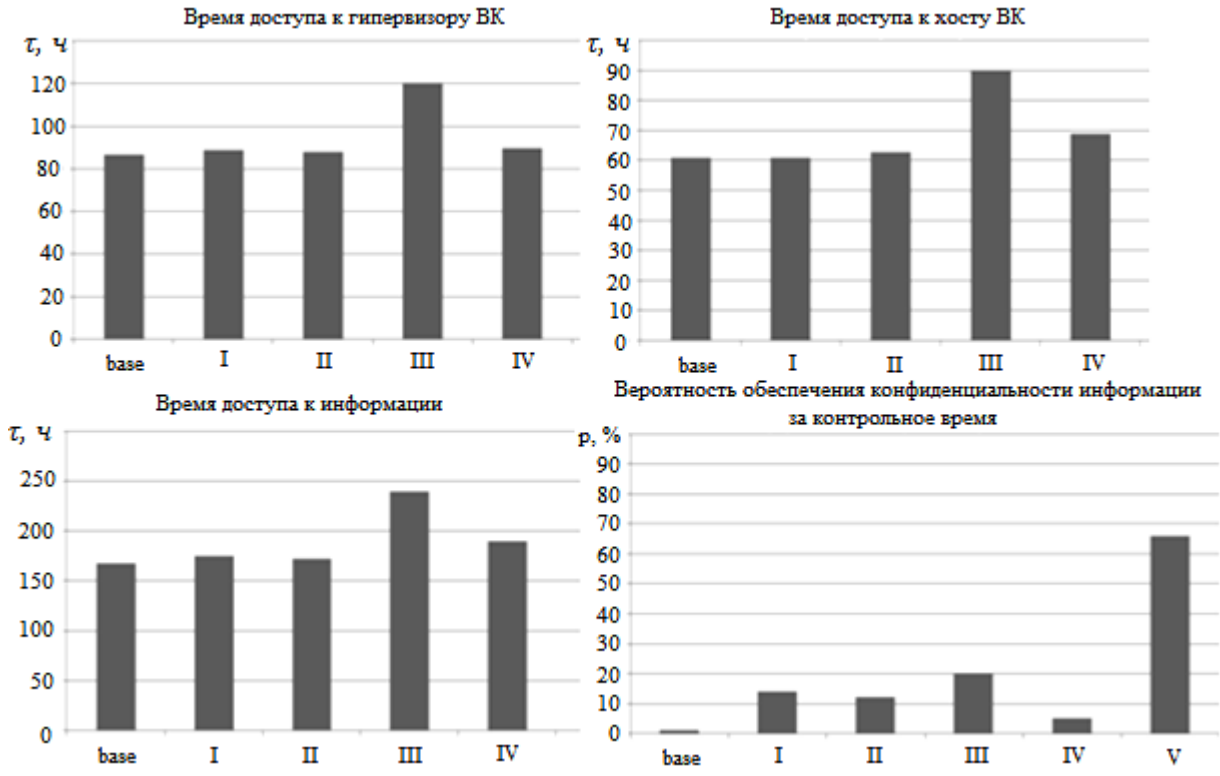


Рисунок 4.20. Вероятностные характеристики защищенности информации ВК с различными системами защиты при проведении MITM-атаки: base - стандартные меры на основе мониторинга сетевых процессов и разграничения прав доступа к ресурсам без использования специализированного анализирующего или защитного ПО; 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

На основании полученных результатов для ВК системы управления движением поездов целесообразно использование интегральной системы защиты, обеспечивающей вероятность сохранения конфиденциальности информации за контрольное время доступа 0,65.

Для возможности оценки эффективности применяемых средств защиты виртуального вычислительного комплекса системы управления движением разработана программа, использующая CLI интерфейс (ПРИЛОЖЕНИЕ Б).

4.6. Выводы по главе IV

1. Анализ результатов тестирования на проникновение в информационные системы наиболее крупных государственных и коммерческих компаний, проведенного компанией Positive Technologies в 2011—2012, позволил установить основные характеристики проводимых атак,

которые были использованы при расчете эффективности систем защиты по фактору времени получения несанкционированного доступа к защищаемому ресурсу.

2. 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.

3. Разработанный метод позволил рассчитать значения вероятностей и времени несанкционированного доступа к информации ресурса при использовании четырех типов защит: ВМ; «диска» ВМ; хостовой системы; сетевой инфраструктуры. Полученные результаты показали, что по сравнению со стандартным комплексом мер защиты вычислительного комплекса защита сетевой инфраструктуры снижает вероятность получения доступа к информации до 0,95, защита "диска" ВМ – до 0,88, защита ВМ – до 0, 86, защита хостовой системы - до 0,8 и увеличивает время доступа в полтора раза .

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

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 несанкциониро-

ванного доступа к информации ресурса при случайных параметрах атак и уровней защиты его элементов.

8. Получено, 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.

СПИСОК ЛИТЕРАТУРЫ

1. Высокоскоростной интеллектуальный железнодорожный транспорт. Сайт РЖД. - URL: http: // rzd.ru.

2. Интеграция ПУ ДЦ «Сетунь» и КП «Круг» ДЦ «Юг». Технические решения. Утверждено Главным инженером Департамента Автоматики и телемеханики ОАО «РЖД» Г.Д. Казиевым, 2010, 23 с.

3. Системы автоведения: высокие технологии, эффективность, безопасность. / АВП «Технология» // Наука и транспорт. Модернизация железнодорожного транспорта.- 2013. - № 2 .- С. 24-25.

4. Тормасов, А.Г. Математическое моделирование средств управления ресурсами и данными в распределенных и виртуализованных средах: дис. ... док. физ.-мат. наук: 05.13.19 / А.Г. Тормасов - М.:, 2008. -233 с.

5. Брижак, Е.П. Система телеуправления на железнодорожном транспорте / Е.П. Брижак. - М.: Маршрут, 2005. - 467 с.

6. Валиев, Р.Ш. Возможности системы протоколирования в диспетчерской централизации «Сетунь» / Р.Ш. Валиев, Е.С. Ходневич // Современные информационные технологии, электронные системы и приборы железнодорожного транспорта: Сб. науч. трудов. - Екатеринбург: УрГУПС, 2005.- С. 124-132.

7. Система диспетчерской централизации «Сетунь»: Презентация – URL:http://www.docme.ru/doc/452355/sistema-dispetcherskoj-centralizacii.

8. Универсальная система автоведения тепловозов УСАПВ-Т. Руководство по эксплуатации. АЮПВ. 468382. 015 РЭ.

9. УСАПВ-Т. Универсальная система автоведения магистральных тепловозов /АВП «Технология». - URL: http://avpt.ru/sa/usavp-t.

10. Донской, А.Л. Системы автоведения и регистрации для электровозов пассажирского движения/ А.Л. Донской, Е.Е. Завьялов - URL: http://www.zdt-magazine.ru/publik/spezproekt/2005/september-05-09/donskoy-pri.htm.

11. Комплексное локомотивное устройство безопасности унифицированное (КЛУБ-У): пат. 2248899 Рос. Федерация: МПК7 B61L25/04/ А.Ю. Елагин [и др.] ; ООО «СБ-ТРАНС-АЛС». - № 2003129732/11; заявл. 08.10.2003; опубл. 27.03.2005. – 4 с.: ил.

12. Астраханов, В.И. Унифицированное комплексное устройство обеспечения безопасности (КЛУБ-У): учебное пособие / В.И. Астраханов, В.И. Зорин; под ред. В.И. Зорина. - М.: ГОУ «Учебно-методический центр по образованию на железнодорожном транспорте», - 2008. - 177 с.

13. Грищенко, А.В. Микропроцессорные системы автоматического регулирования электропередачи тепловозов. Учебное пособие для студентов вузов железнодорожного транспорта/ А.В. Грищенко, В.В. Грачев, С.И. Ким и др.: под ред. А.В. Грищенко. – М.: Маршрут, 2004. – 172 с.

14. Баранов, Л.А. Системы автоматического и телемеханического управления электроподвижным составом / Л.А Баранов, В.И Астрахан, Я.М Головичер; под ред. Л.А. Баранова. - М. : Транспорт, 1984.-с. 311.

15. Шалабаев, Б.Р. Имитационное моделирование систем управления движением поездов на линии метрополитена: дисс. … канд. техн. наук: 05.13.07/ Б.Р. Шалабаев. - М. - 1994.- 159 с.

16. Воробьева, Л.Н. Алгоритмы централизованного управления движением поездов на линии метрополитена: дисс. … канд. техн. наук: 05.13.07/ Л.Н. Воробьева. – М. – 2008. - 202 с.

17. Мелёшин, И.С.Алгоритмы управления временем хода поезда «русич» на перегонах метрополитен: дисс. … канд. техн. наук: 05.13.07/ И.С. Мелешин. - М. -2011. -173 с.

18. Система управления движением поездов: пат. 2388637 Рос. Федерация: МПК7 B61L27/04 / В.И. Якунин и др. ; ОАО "РЖД". - 2008147832/11; заявл. 05.12.2008 ; опубл. 10.05.2010. – 2 с.: ил.

19. Филонов, С.П. Тепловоз 2ТЭ116 / С.П. Филонов, А.И. Гибалов, Е.А.Никитин и др. 3-е изд., перераб. и доп. – М.: Транспорт, 1996. -334 с.: ил.

20. Бычков, Д. А. Система автоматического управления силовой установкой тепловоза, совместимая с существующими системами автоведения/ Д. А. Бычков // Проблемы железнодорожного транспорта/ Сборник трудов ВНИИЖТ.- М.: Интекст.- 1999 г.- С. 72-75.

21. Автоматизированне рабочее место поездного диспетчера (АРМ «ДНЦ-Сетунь»). Программное обеспечение. Руководство электромеханика, 04841021.21001 - 01 92 01, 1998г., 16 с.

22. Блок Шлюз CAN-485. Руководство по эксплуатации ЦВИЯ.468152.053 РЭ. Подписано к печати 07.12.2012г. Ижевский радиозавод. 28 с.

23. Самойленко, А. Виртуализация: новый подход к построению IT-инфраструктуры / А. Самойленко. – URL: http://www.ixbt.com/cm/virtualization.shtml (дата обращения 16.04.2007) .

24. Евсеев, И. Система виртуализации OpenVZ : Часть 1/ И. Евсеев. - URL: http://www.ibm.com/developerworks/ru/library/l-openvz_1/#authorN10021.

25. Tulloch, M. Understanding Microsoft Virtualization Solutions (Second Edition) / Mitch Tulloch - Microsoft Press Library of Congress Control Number: 2010920178, 2010. – P. 466.

26. Черешкин, Д.С. Принципы таксономии угроз безопасности информационных систем/ Д.С. Черешкин, А.А., Коконов, Д.В. Тищенко // Вести РФФИ. – 1999. - №3. - С. 68-72.

27. Preliminary, A Classification Scheme for Information System Threats, Attacks, and Defenses; A Cause and Effect Model; and Some Analysis Based on That Model/ Sandia National Laboratories; Cohen Fred & Associates Specializing in Information Protection Since. - 1998.- URL: http://all.net/journal/ntb/cause-and-effect.html .

28. Krsul, I.V. Software Vulnerability Analysis: A Thesis of the Requirements for the Degree of Doctor of Philosophy/ Ivan Victor Krsul. - Purdue University, 1998. – P. 188.

29. Howard, J.D. An Analysis of Security Incidents on the Internet: 1989-1995: Ph.D. Dissertation/ J. D. Howard— Carnegie Mellon University, Pittsburgh, PA. 1997. – URL: http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=52454 .

30. Longstaff, T. Update: CERT/CC Vulnerability Knowledgebase/ T. Longstaff- Savannah, Georgia, USA: DARPA, 1997.- URL: https://www.yumpu.com/en/document/view/16960149/detection-of-recurring-software-vulnerabilities-by-researchgate/57.

31. Марков, А.С. Систематика уязвимостей и дефектов безопасности программных ресурсов/ А.С. Марков, А.А. Фадин// Безопасность компьютерных систем. – 2013. - № 3. – С. 2-7.

32. Климовский, А.А. Таксономия кибератак и ее применение к задаче формирования сценариев их проведения/ А. А. Климовский // Труды Института системного анализа Российской академии наук. – М.: 2006, т. 27. - С. 74–107.

33. Williams, J.G. Modeling External Consistency of Automated Systems/ J. G. Williamsand, L. J. LaPadula // Journal of High-Integrity Systems, Vol. 1. – 1995. - № 3. P. 249-267.

34. ISO/IEC 15408:2005. Common Criteria for Information Technology Security Evaluation. - Second edition 2005-08 .

35. Демидов, Н.Е. Математические модели и методы анализа иерархий в системах обеспечения информационной безопасности: дис. … канд. техн. наук: 05.13.01/ Н.Е. Деминов. – Тверь, 2004.- 113 с.

36. Эддоус, М. Методы принятия решений / М. Эддоус, Р. Стэнсфилд; пер. с англ. под ред. член-корр. РАН И.И. Елисеевой – М.: Аудит, ЮНИТИ, 1997. – 590с.: ил.

37. Ларичев, О.И. Качественные методы принятия решений. Вербальный анализ решений / О.И. Ларичев, Е.М. Мошкович. - М.: Нука, 1996. – 208с.: ил.

38. Ногин, В.Д. Принятие решений в многокритериальной среде: количественный подход / В.Д. Ногин. – М.:Физматлит, 2002. -175с.: ил.

39. Литвак, Б.Г. Экспертные оценки и принятие решений / Б.Г. Литвак. – М.:Патент, 1996.- 271с.: ил.

40. Месарович, М. Теория иерархических многоуровневых систем/ М. Месарович, Д. Мако, И. Такахара; пер. с англ. Б.И. Копылова.- М.:Мир,1973.-344с.: ил.

41. Ширманов, А. Безопасность виртуальной инфраструктуры // Открытые системы. СУБД.- 2009. - № 6.- С. 30-31.

42. Самойленко, А. Защита виртуальной инфраструктуры VMware vSphere от специфических типов угроз с помощью решения vGate R2/ А. Самойленко. – URL: http://www.vmgu.ru/articles/vgate-r2-against-treats (дата обращения 29.07.2012).

43. Писарев, А. Виртуализация и безопасность: риска нет?/ А. Писарев. – URL: http://www.cnews.ru/reviews/free/security2012/articles/article17.shtml

44. Благодаренко, А.В. Разработка метода, алгоритмов и программ для автоматического поиска уязвимостей программного обеспечения в условиях отсутствия исходного кода: дис. ... канд. техн. наук: 05.13.19 / А.В. Благодаренко. - Таганрог, 2011.- 129 с.

45. Аверченков, В.И. Служба защиты информации: организация и управление: учеб. пособие для вузов [электронный ресурс] / В.И. Аверченков, М.Ю. Рытов. – 2-е изд., стереотип. – М.:ФЛИНТА, 2011.- 186 с.

46. Дайнеко, В.Ю. Разработка модели и алгоритмов обнаружения вторжений на основе динамических байесовских сетей: дис. … канд. техн. наук: 05.13.19/ В.Ю. Дайнеко.– СПб. – 2013.-130 с.

47. Sandu, Ravi S. Access Control: Principles and Practice// Ravi S. Sandu, Pierangela Samarati // IEEE Communications Magazine.- September 1994. - 32(9). – P. 40–48.

48. Osborn, S. Configuring Role-based Access Control to Enforce Mandatory and Discretionary Access Control Policies [J]/ S.Osborn, R. Sandhu, Q. Nunawer// ACM Trans on Info Syst Security.- 2000.- 3(2):- P. 85-106.

49. Implementation of Mandatory Access Control in Role-based Security System CSE367 / Final Project Report Professor Demurjian Steve - Computer Science & Engineering The University of Connecticut Storrs, CT 06269-3155 - Fall 2001.-P. 19.

50. Sandhu, R. S. Role - based Access Control Models/ R. S. Sandhu, E. J. Coyne, H. L. Feinstein, C. E. Youman// IEEE Computer, 29..- Feb. 1996. – P. 38–47.

51. Грушо, А.А. Теоретические основы защиты информации/ А.А. Грушо, Е.Е. Тимонина. – М.:Яхтсмен, 1996. -192с.: ил.

52. Симонов, С.В. Методология анализа рисков в информационных системах/ С.В. Симонов// Защита информации. Конфидент. – 2002. - №2. – С.16-21.

53. Аграновоvский, А.В. Теоретико-графовый подход к анализу рисков в вычислительных сетях/ А.В. Аграновоvский, Р.А. и др. // Защита информации. Конфидент.- 2002.-№2.- С.50-

54. Львова, А.И. Метод анализа и управления рисками безопасности защищенной информационной системы: дис. … канд. техн. наук: 05.13.01; 05.13.19 / А.И. Львова.- М., 2009.- 168 с.

55. ISO/IEC 17799:2005. Information technology - Security techniques - Code of practice for information security management. - Second edition 2005-06-15 .-P. 108

56. ISO/IEC 27002:2005. Information technology —Security techniques —Code of practice for information security management . - BS ISO/IEC 27002:2005 BS 7799-1:2005; Second edition 2005-06-15 . – P. 130.

57. ISO/IEC 27001:2013. Information technology — Security techniques — Information security management systems — Requirements. - BS ISO/IEC 27001:2013 BS 7799-2:2013; Second edition 2013-09-P. 25 .

58. ISO/IEC 27005 :2008. Information technology — Security techniques —Information security risk management . - BS ISO/IEC 27005:2008 ; First edition 2008-06. – P. 64 .

59. Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutzhandbuch . - Bundesamt für Sicherheit in der Informationstechnik (BSI) – P. 93.

60. Trusted Computer System Evaluation Criteria.- Department of Defense Standard.-1985-P. 12.

61. NIST SP800-30. Guide for Conducting Risk Assessments . - Computer Security Division Information Technology Laboratory National Institute of Standards and Technology .-Gaithersburg, MD 20899-8930.- 2012-09.- P. 95

62. NIST SP800-35. Guide to Information Technology Security Services. - Computer Security Division Information Technology Laboratory National Institute of Standards and Technology.- Gaithersburg, MD 20899-8930.- 2003-10.-P. 84.

63. NIST SP800-39. Managing Information Security Risk . - Computer Security Division Information Technology Laboratory National Institute of Standards and Technology.- Gaithersburg, MD 20899-8930.- 2011-03.- P. 84.

64. ГОСТ Р ИСО/МЭК 15408-1-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.- Введ. 2008–12–18. – М.: ФГУП «Стандартинформ», 2009. – 41 с.

65. ГОСТ Р ИСО/МЭК 15408-2-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. - Введ. 2009-10-01. – М.: Национальные стандарты, 2007. – 174 с.

66. ГОСТ Р ИСО/МЭК 15408-3-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. - *Введ.* 2008-12-18. – М.: ФГУП «Стандартинформ», 2009. – 119 с.

67. ГОСТ Р ИСО/МЭК 17799-2005 — Информационные технологии. Практические правила управления информационной безопасностью. - Введ. 2005-12-25. – М.: ФГУП «Стандартинформ», 2006. – 56 с.

68. ГОСТ Р ИСО/МЭК ТО 15446-2008 — Информационные технологии. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности. - Введ. 2008-12-18. – М.: ФГУП «Стандартинформ», 2006. – 108 с.

69. ГОСТ Р ИСО/МЭК 18044-2007— Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. - Введ. 2007-12-27. – М.: ФГУП «Стандартинформ», 2009. – 50 с.

70. ГОСТ Р ИСО/МЭК 27033-1-2011— Информационные технологии. Методы и средства обеспечения безопасности. Часть 1. Безопасность сетей. - Введ. 2011-12-01. – М.: ФГУП «Стандартинформ», 2012. – 65 с.

71. ГОСТ Р 53113.1-2008 - Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения. - Введ. 2008-12-18. – М.: ФГУП «Стандартинформ», 2012. – 13 с.

72. ГОСТ Р 53113.2-2009 — Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов». Часть 2. «Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов. - Введ. 2009-12-15. – М.: ФГУП «Стандартинформ», 2010. – 13 с.

73. ГОСТ Р 53704-2009— Системы безопасности комплексные и интегрированные. Общие технические требования. - Введ. 2009-12-15. – М.: ФГУП «Стандартинформ», 2010. – 13 с.

74. Астахов, А. Искусство управления информационными рисками. – М.: ДМК Пресс, 2010. – 312 с., ил.

75. СТО РЖД 1.18.002-2009 - Управление информационной безопасностью. Общие положения» - Введ. 2009-03-11. – М.:ОАО «РЖД», 2009. – 30 с.

76. СТО БР ИББС-1.0-2006 - Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения. - Введ. 2006-01-26. – М.: Банк России, 2009. – 27 с.

77. Дубинин, В.Н., Заикин С.А. Сетевые модели распределенных систем обработки, хранения и передачи данных: монография / В.Н Дубинин, С.А Заикин. – Пенза: Приволжский Дом знаний, 2013. – 452 с. ISBN 978-5-8356-1351-9.

78. Росляков, А. В. Виртуальные частные сети. Основы построения и применения. М.: Эко-Трендз, 2006 - 304 с.; ISBN 5-88405-078-X, 978-5-88405-078-5.

79. Barrett, D., Kipper, G., Virtualization and Forensics: A Digital Forensic Investigator's Guide to Virtual Environments. Burlington, Ma [etc.]: Syngress: Elsevier, 2010. - XVII, ISBN 978-1-59749-557-8-254 P.

80. Microsoft virtualization. Master microsoft server, desktop, application, and presentation virtualization [Text] : монография / Olzak, T.; Boomer, J.; Keefer, R. M.; Sabovik, J. - Burlington, Ma [etc.] : Syngress: Elsevier, 2010. - XX, 486 p. : ill. - Указ.: с. 479-486. - ISBN 978-1-59749-431-1.

81. Ларсон, Р., Платформа виртуализации Hyper-V / Р. Ларсон, Ж. Карбон Ресурсы WindowsServer 2008. М.: Русская Редакция, 2010. - 800 с.

82. Chris Takemura, Luca S. Crawford. The Book of Xen. A Practical Guide for the System Administrator- No Starch Press, 2009, 312 P.

83. Von Hagen W. Professional Xen Virtualization/ William von Hagen - Wrox, 2008.- 55 P.

84. Haletky, E., VMware ESX and ESXi in the Enterprise: Planning Deployment of Virtualization Servers. Boston: Prentice Hall, 2011. – 587 P.

85. Chris Wolf, Erick M. Halter Virtualization: From the Desktop to the Enterprise – Apress, 2005, 600 P.

86. Лоу, С., VMware vSphere 4. Полное руководство. М.: Диалектика, 2010 -800 с.; ISBN 978-5-8459-1651-8, 978-0-470-48138-7.

87. Зинкин, С. А. Развитие теоретических основ и методов функционально-структурной организации систем и сетей внешнего хранения и обработки данных: дис. … докт. техн. наук: 05.13.15, 05.13.13 / С.А. Зинкин.- Пенза, 2009.- 544 с.: ил.

88. Тормасов, А.Г. Модель потребления ресурсов вычислительной системы // Вестник НГУ.Серия: Информационные технологии.- 2006.- т.4, вып.1- С. 63-72.

89. Луковников, А.В. Математическая модель двухуровневого управления ресурсами в операционных системах с закрытым исходным кодом: дис. … канд. техн. наук: 05.13.18 / А.В Луковников– М.:2006. - 110 с.

90. Первин, А.Ю. Система управления специализированными инструментами с механизмами оптимального распределения вычислительных ресурсов : дис. … канд. техн. наук: 05.13.11 / А.Ю. Первин – Переславль-Залесский.:2009. - 104 с.

91. Козловский, А.Л. Модели, методы и алгоритмы распределения ресурсов виртуализованных вычислительных кластеров: дис. … канд. техн. наук: 05.13.05 / А.Л. Козловский– М..:2012. - 163 с.

92. Потрясаев, С.А. Динамическая модель и алгоритмы комплексного планирования операций и распределения ресурсов в корпоративной информационной системе: дис. … канд. техн. наук: 05.13.01 / С.А. Потрясаев– СПБ:2009. - 145 с.

93. Федосин, М.Е. Виртуализация многокомпонентной системной архитектуры предметно-ориентированной облачной вычислительной среды: дис. … канд. техн. наук: 05.13.15/ М.Е. Федосин– Пенза: 2009. - 166 с.

94. Zabbix Documentation 2.0. - URL: https://www.zabbix.com/documentation/2.0/manual/installation/requirements.

95. Инструкция по определению станционных и межпоездных интервалов № ЦД-361. 1995г. 51стр.

96. Заоблачны ли облачные ИТ инфраструктуры?//Storage News – 2010. - № 2 (42). URL: www.storagenews.ru.

97. Руководство по установке DebianGNU/Linux. – URL: http://d-i.alioth.debian.org/manual/ru.i386/index.html .

98. Коновалов, М.Г. Модели и методы управления заданиями в системах распределенных вычислительных ресурсов/ М.Г. Коновалов, Ю.Е Малашенко., И.А. Назарова// Российская академия наук. Вычислительный центр. – М., 2009. -127 с.

99. Котов, В.Е. Сети Петри/ В.Е. Котов. - М.: Наука: Главная редакция физико-математической литературы, 1984. - 160 с.

100. Лескин, А.А. Сети Петри в моделировании и управлении/ А.А. Лескин, П.А. Мальцев, А.М. Спиридонов. - Л.: Наука, 1989.- 133 с.

101. Наумов, В.С. Использование сетей Петри при моделировании процесса транспортно-экспедиционного обслуживания/ В.С. Наумов// Автомобильный транспорт: сб. науч. тр.- Харьков,2009.- № 24.- С. 120-125.

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

103. Oracle VM Virtual Box Technical Documentation. – URL: https://www.virtualbox.org/wiki/Technical_documentation

104. Oracle VM Virtual Box User Manual. – URL: https://www.virtualbox.org/manual/UserManual.html

105. Соболь, И.М. Выбор оптимальных параметров в задачах со многими критериями/ И.М. Соболь.- М.: Дрофа, 2006. - 175 с.

106. Кини, Р.Л. Принятие решений при многих критериях: предпочтения и замещения/ Р.Л. Кини, Х. Райфа. - М.: Радио и связь, 1981. - 560 с.

107. Nocedal, J. Numerical Optimization; Springer Series in Operations Research / J. Nocedal, S.J. Wright.- Springer Verlag, 2006.- 653 c.

108. Zadeh, L.A. Optimality and Non-scalar-valued Performance Criteria/ L.A. Zadeh // IEEE Trans. on Automatik Control.-1963.- Vol. 8 (1).- P. 59-60.

109. Censor, Y. Pareto Optimality in Multiobjective Problems/ Y. Censor // Applied Mathematics and Optimization.- 1977.- Vol. 4.- P. 41-59.

110. Da Cunha, N.O. Constrained Minimization Under Vector-valued Criteria in Finite Dimensional Spaces/ N.O. Da Cunha, E. Polak, // Of Mathematical Analysis and Applications.- 1967.- Vol. 19.- P. 103-124.

111. Нетушил, А.В. Теория автоматического управления: Нелинейные системы/ А.В. Нетушил и др.; ред. А.В. Нетушила. – 2-е изд., перераб. и доп. – М.: Высшая школа, 1983. – 432 с.

112. Трифонов, А.Г. Многокритериальная оптимизация/, А.Г. Трифонов. - URL: http://matlab.exponenta.ru/optimiz/book_1/16.php.

113. 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.

114. ГОСТ Р 51841-2001 Программируемые контроллеры. Общие технические требования и методы испытаний. 73 стр.

115. Памятка Организации сотрудничества железных дорог (ОСЖД) Р585 Основные принципы обеспечения безопасности и безотказности микропроцессорных систем железнодорожной автоматики и телемеханики. Варшава 2006г. 24 стр.

116. Денисенко, В. Аппаратное резервирование в промышленной автоматизации/ СТА 2008. № 2,4. – URL: wwwcta.ru

117. Александровская, Л.Н. Безопасность и надежность технических систем: Учебное пособие/ Л.Н. Александровская, И.З. Аронов, В.И. Круглов. –М. : Логос, 2008. - 376с.

118. Захаров, О.Г. Корректировка требований к надежности цифровых устройств релейной защиты, автоматики и сигнализации. – URL: http://olgezaharov.narod.ru/RD/nadezhnostj.htm.

119. Schneier, B. Breaking Up Is Hard to Do: Modeling Security Threats for Smart Cards/ B. Schneier and A Shostack // USENIX Workshop on Smart Card Technology.- USENIX Press: 1999.- P. 175-185.

120. 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» / Моск. гос. ун-т путей сообщения.- М.: МИИТ, 2013.- С.17.

121. 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» /Днепропетровский национальный университет железнодорожного транспорта.- Днепропетровск.: ДНУЖТ, 2014.- С.68-69.

122. Меры защиты информации в государственных информационных системах: методический документ. - Утв. Федеральной службой по техническому и экспортному контролю 11.02.2014.-ИА «ГАРАНТ». – URL: http://www.garant.ru/products/ipo/prime/doc/70491518/#ixzz324GKcuON.

123. ISO 13335 Международные стандарты безопасности информационных технологий: ISO13335-1:2004 Information technology. Guidelines for the management of IT security. Consepts and models for information and communications technology security management; ISO13335-3:1998 Information technology. Guidelines for the management of IT security. Techniques for the management of IT security; ISO13335-4:2000 Information technology. Guidelines for the management of IT security. Selection of safeguards; ISO13335-5:2001 Information technology. Guidelines for the management of IT security. Management guidance of network security.- Веден 19.12.2006. - М.: Стандартинформ.-URL: http://www.iso27000.ru/standarty/iso-13335-mezhdunarodnye-standarty-bezopasnosti-informacionnyh-tehnologii**.**

124. Статистика уязвимостей корпоративных информационных систем за 2011-2012 годы: аналитический отчет – М.:Positive Technologies, 2013.- URL: http://www.ptsecurity.ru/download/Analitika_pentest.pdf.

125. 2010 Trend and Risk Report: аналитическийотчет. – New York: IBM, 2011. – URL: http://www-03.ibm.com/press/ru/ru/pressrelease/36296.wss. (датаобращения 31.03.2011).

126. Щеглов, К.А., Защита от атак на уязвимости приложений. Модели контроля доступа/ К.А. Щеглов, А.Ю. Щеглов. – URL: http://www.securitylab.ru/blog/personal/Information-security/34883.php. (дата обращения 20.11.2013).

127. 2011 TrendandRiskReport: аналитический отчет. – NewYork: IBM, 2012. – URL: http://www-03.ibm.com/press/ru/ru/pressrelease/37275.wss. (дата обращения 23.03.2012).

128.Отчеты по уязвимостям 20.02-26.02 2012: аналитический отчет. Security Lab, 2012. - URL:/ http://www.securitylab.ru/vulnerability/reports/420676.php.

129. Семенов, Ю.А. Обзор по материалам ведущих фирм, работающих в сфере сетевой безопасности/ Ю.А. Семенов.- URL: http://book.itep.ru/10/2013.htm. (дата обращения 2013)

130. Вентцель, Е.С. Исследование операций/ Е.С. Вентцель. - М.: Советское радио, 1972.- 552 с.

131. Хемди А. Введение в исследование операций/ Хемди А. Таха.— 8 изд. — М.: Вильямс, 2007. —912с.

132. Кнут, Д. Искусство программирования для ЭВМ. т. 1 Основные алгоритмы / Д. Кнут.- 3-е изд.—М.:«Вильямс», 2006.— 720 с.

133. Lippmann, R.P. Evaluating and Strengthening Enterprise Network Security Using Attack Graphs: Technical Report ESC-TR-2005-064/ R.P. Lippmann, K.W. Ingols. - Lexington.: MIT Lincoln Laboratory, 2005. - P. 96

134. Безруков, Н.Н. Компьютерная вирусология. ч. 1. Общие принципы функционирования, классификации и каталог наиболее распространенных вирусов в операционной системе MS DOS/ Н.Н. Безруков. - Редакция 5.5 .- Киев: Украинская Советская Энциклопедия, 1991 – 416 с.

135. Борисов, А.Н. Обработка нечеткой информации в системах принятия решений/ А.Н. Борисов и др.- М.: Радио и , 1989.- 304 с.

136. Борисов, А.Н. Принятие решений на основе нечетких моделей: примеры использования/ А.Н. Борисов, О.А. Крумберг, И.П. Федоров.- Рига.: Знание, 1990.- 184 с.

137. Бородакий, Ю.В. Эволюция информационных систем (современное состояние и перспективы)/ Ю.В. Бородакий, Ю.Г. Лободинский. - М.:Горячая линия – Телеком, 2011.- 368 с.- ISBN: 978-5-9912-0199-5.

138. Водолазкий, В. В. Современные технологии безопасности. Интегральный подход/ В. С. Барсуков, В. В. Водолазкий.- М.: Нолидж, 2000г.- 496 с.

139. Герасименко, В.А. Защита информации в автоматизированных системах обработки данных: Книга 1 и 2./ В.А. Герасименко. - М.: Энергоатомиздат, 1994. -576 с.

140. Герасименко, В.А. Основы защиты информации/ В.А. Герасименко, А.А. Малюк.- М.: МОПО РФ МГИФИ, 1997. - 500 с.

141. Грушо, А.А.Теоретические основы защиты информации/ А.А. Грушо, Е.Е. Тимонина.– М.: Издательство Агентства «Яхтсмен», 1996.- 192 с.

142. Девянин, П.Н. Анализ безопасности управления доступом и информационными потоками компьютерных систем/ П.Н. Девянин.– М.: Радио и связь, 2006. - 176 с.

143. Девянин, П.Н. Теоретические основы компьютерной безопасности / П.Н. Девянин и др. – М.: Радио и связь, 2000.- 192 с.

144. Домарев В. В. Безопасность информационных технологий. Системный подход / В.В. Домарев.- К.: ООО «ТИД» «ДС», 2002 – 688 с.- ISBN 966-7992-02-0.

145. Зегжда, Д.П. Основы безопасности информационных систем/ Д.П. Зегжда, А.М. Ивашко. - М.: Горячая Линия - Телеком, 2000.- 452 с.

146. Касперский, К. Техника сетевых атак. Том I: Приемы противодействия / К. Касперский. – М.: СОЛОН-пресс, 2001.-400 с.

147. Корниенко, А. А. Средства защиты информации на железнодорожном транспорте (криптографические методы и средства) : учебное пособие / А.А. Корниенко, М. А. Еремеев, С. Е. Ададуров; под общ. ред. проф. А. А. Корниенко. - М.: Маршрут, 2005. - 254 с.

148. Яковлев, В.В. Информационная безопасность и защита информации в корпоративных сетях железнодорожного транспорта/ В.В. Яковлев, А.А. Корниенко. - М.:УМК МПС РФ , 2002. - 328 с.

149. Лукацкий, А.Г. Обнаружение атак / А.Г. Лукацкий.- СПб.:БХВ-Петербург, 2001.- 624 с.- ISBN: 5-94157-054-6450.

150. Машкина, И.В. Управление защитой информации в сегменте корпоративной информационной системы на основе интеллектуальных технологий: дис. … докт. техн. наук: 05.13.19/ И.В. Машкина. –Уфа, 2009.- 340 с.

151. Молдовян, А.А. Безопасность глобальных сетевых технологий/ А.А. Молдовян.- СПб.: БХВ-Петербург, 2003. - 368 с.

152. Щербаков, А.Ю. Введение в теорию и практику компьютерной безопасности / А.Ю. Щербаков.– М.: Издатель Молгачева С.В., 2001.- 352 с.

153. Bell, D.E. Secure Computer Systems: Unified Exposition and Multics Interpretation/ D.E. Bell, L.J. LaPadula.– Bedford, Mass.: MITRE Corp., 1976. – MTR – 2997 Rev. 1.- P. 129.

154. Berman, F. Grid Computing: Making the Global Infrastructure a Reality/ F. Berman, G. Fox, T. Hey. - Chichester: John Wiley & Sons, 2005. – P. 974

155. Bishop, M. Computer Security : Art and Science / M. Bishop. - Addison-Wesley Professional, 2002.- P. 1084 - ISBN 0-20144099-7.

156. Брагг, Р. Система безопасности Windows 2000/ Р. Брагг пер. с англ. – М.: Издательский дом “Вильямс”, 2001. – 592 с.

157. Cullum, J. Performance Analysis of Automated Attack Graph Generation Software: Master’s Thesis / J. Cullum.- Monterey. California: Nival Postgraduate School.- 2006.- P.143.

158. Dacier, M. A Petri Net Representation of the Take-Grant Model/ M. Dacier //6th IEEE Computer Security Foundations Workshop CSFW’93.- Franconia, New Hampshire, USA.- 1994.

159. Jajodia S. Topological Analysis of Network Attack Vulnerability / S. Jajodia, S. Noel, B. O’Berry // Managing Cyber Threats: Issues, Approaches and Challenges, 2003.-20 P.

160. Vitek, J.Secure Internet Programming. Security Issues for Mobile and Distributed Objects/ J. Vitek, Ch. D Jensen. – Berlin, Heidelberg, New York; Barcelona; Hong Kong; London; Milan; Paris; Singapore; Tokyo: Springer, 1999 , - P. 509. - ISBN 3-540- 66130-1.

161. Хоффман, Л.Дж. Современные методы защиты информации / Л.Дж. Хоффман.; пер. с англ. – М.: Сов. радио, 1980.- 264 с.

162. McLean J. Security Models and Information Flow, Proceedings of 1990/ J. McLean// IEEE Symposium on Research in Security and Privacy. – IEEE Press, 1990.-URL: http://www.cs.cornell.edu/andru/cs711/2003fa/reading/1990mclean-sp.pdf.

163. McNab C. Network Security Assessment. Second edition / C. McNab. – ISBN-10:0-596-51030-6, 2007.- 478 P.

164. Sandhu, R. Rationale for the RBC96 family of access control models/ R. Sandhu // In Proceeding of the 1st ACM Workshop on Role-Based Access Control. – ACM. 1997.

165. Sandhu, R. Role-Based Access Control? Advanced in Computers/ R. Sandhu, Edvard J. Coyne, Hal L. Feinstein, Charles E. Youman. – Academic Press. 1998.-P. 38-47.

166. Shiller, C.A. The Killer Web Applications / C.A. Shiller. - Paperback, 2007.- P. 459. - ISBN-10: 1-59749-135-7.

167. Щерба, М.В. Обнаружение низкоактивных распределенных атак типа «отказ в обслуживании» в компьютерных сетях: дисс. … канд. техн. наук: 05.13.19/ М.В. Щерба. – Омск. - 2012. -123 с.

168. Щерба, М.В. Методика разработки системы защиты информации комплекса муниципальных информационных систем/ М.В. Щерба// Информационные технологии управления и моделирования. – 2009. – Выпуск 6. – С. 850-854.

169. Уткин, Л.В. Методы и модели анализа надежности и безопасности информационных систем при неполной информации : дис. … док. техн. наук: 05.13.18/ Л.В. Уткин.- СПб.- 2004. – 300 с.

170. Котенко, Д.А. Метод оценки риска информационной безопасности на основе сценарного логико-вероятностного моделирования: дис. … канд. техн. наук: 05.13.19/ Д.А. Котенко. – СПб. 2010.- 115 с.

171. Котенко, А.Г. Анализ риска в инфокоммуникационной системе/ А.Г. Котенко, Д.А Котенко // Автоматика, связь, информатика.- 2010. - № 8. - С. 16-18.

172. Danforth M. Models for Threat Assessment in Networks: PhD dissertation / M. Danforth.- University of California, 2006.-P. 176.

173. Ou, X. , Govindavajhal S., Appel A. A Logic-based Network Security Analyzer / X. Ou, S.Govindavajhal, A. Appel/ X. Ou, S. Govindavajhal, A. Appel // In 14th USENIX Security Symposium.- Baltimore, MD, USA.-2005.-URL: http://www.tzi.de/~edelkamp/secart/IntSec.pdf.

174. Коллегов, Д.Н. Проблемы синтеза и анализа графов атак/ Д.Н. Коллегов, // Вестник Томского ун-та. Приложение.- 2007. - № 23. - С. 180 - 188.

175. Коркин, И.Ю. Методика обнаружения нелегитимного программного обеспечения, использующего технологию аппаратной виртуализации: дис. … канд. техн. наук: 05.13.19 / И.Ю. Коркин.- М.,2011.- 140 с.

176. Коркин, И.Ю. Выявление вложенных мониторов виртуальных машин/ И.Ю. Коркин // Системы высокой доступности.-2011.- № 2, т.6. – С. 76-77.

177. Sheyner, O. Scenario Graphs and Attack Graphs : Ph.D. dissertation / O. Sheyner; Carnegie Mellon University. – Pittsburgh, 2004. –P. 132.

178. Сердюк, В.А. Разработка и исследование математических моделей защиты автоматизированных систем от информационных атак: дис. … канд. техн. наук: 05.13.19/ В.А. Сердюк.–М.,2004.- 171 с.

179. Сердюк, В.А. Анализ современных тенденций построения моделей информационных атак/ В.А. Сердюк // Информационные технологии. -2004. -№5. - С.20-26.

180. Корт, С.С. Разработка методов и средств поиска уязвимостей при сертификационных испытаниях защищенных вычислительных систем: дис. … канд. техн. наук: 05.13.16; 05.13.19/ Корт С.С.- СПб, 1998.- 120 с.

181. Shahriary, H.R. Network Vulnerability Analysis through Vulnerability Take-Grant Model (VTG)/ H. R. Shahriari, R. Sadoddin, R. Jalili, M. R. Zakerinasab, et.al.// In Proc. Of 7th International Conference on Information and Communication Security (ICICS2005).- China, 2005.-P. 256-268.

182. Колегов, Д.Н. Применение ДП-моделей для анализа защищенности сетей / Д.Н. Колегов // Прикладная дискретная математика. -2008 - №1. – С. 71-88.

183. Буренин, П.В. Подходы к построению ДП-модели файловых систем / П.В. Буренин // Прикладная дискретная математика. -2009. -№ 1 (3).- С. 93-112.

184. Коллегов, Д.Н. Дискреционная модель безопасности управления доступом и информационными потоками в компьютерных системах с функционально или параметрически ассоциированными сущностями: дис. … канд. техн. наук: 05.13.01/Д.Н. Коллегов– Томск, 2009. -132 с.

185. Колегов, Д.Н. Об использовании формальных моделей для анализа уязвимостей / Д.Н. Колегов // Прикладная дискретная математика. -2009. -№1. - С. 113-116.

186. Дмитриев, Ю.В. Исследование и разработка алгоритмов интегральной оценки безопасности информационной системы на основе рациональной структуры частных показателей защиты: дис. … канд. техн. наук: 05.13.19/ Ю.В. Дмитриев. – Воронеж, 2001. - 154 с.

187. Машкина, И.В. Методы разработки функциональной модели управления защитой информации / И.В. Машкина, М.Б. Гузаиров // Безопасность информационных технологий. М.: МИФИ.- 2008. -№ 2. - С.105-110.

188. Аль-Хаммуд, И. Модели и алгоритмы повышения уровня информационной безопасности корпоративных информационно-телекоммуникационных сетей: дис. … канд. техн. наук: 05.12.13/ Ибрахим Аль-Хаммуд. - Владимир, 2007. – 164 с.

189. Templeton, S. A Requires/Provides Model for Computer Attacks / S. Templeton, K.Levitt // Workshop on New Security Paradigms of the 2000 / New York, ACM, 2001. – P. 15-21.

190. Морева, О.Д. Разработка методики оценки информационной защищенности социо-технических систем с использованием функций чувствительности: дис. … канд. техн. наук: 05.13.19/ О.Д. Морева. - Воронеж, 2006. – 162 с.

191. Климов, С.М. Противодействие компьютерным атакам. Технологические основы: электронное учебное издание (С)/ С.М. Климов, М.П. Сычев, А.В. Астрахов- М.: МГТУ им Н.Э. Баумана, 2013г.- 108 с.

192. Корнев, Д.А. Моделирование атак на информационную систему в терминах сетей Петри. Интеллектуальные системы на транспорте/ IV международная научно-практическая конференция «ИнтеллектТранс-2014»/ Под ред. А.А. Корниенко.- СПб.: ПГУПС.- С. 243-249.

193. О некоторых приемах атаки Man in the middle.- URL: http://habrahabr.ru/post/131710/ (дата обращения 03.11.2011).

194. Sanders, C. Understanding Man-in-the-Middle Attacks – ARP Cache Poisoning (Part 1)/ Chris Sanders. - URL: http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part1.html (дата обращения 17.03.2010).

195.Чуев, Ю.В. Основы исследования операций в военной технике/ Ю.В. Чуев и др.- М.: «Советское радио», 1965.- 253 с.

196.Чибров, О.М. Об одной проблеме, возникающей при использовании теории игр в области защиты информации/ Труды XII Всероссийской научно-практической конференции «Проблемы информационной безопасности в системе высшей школы».- М.:МИФИ, 2013.- С.92-93. ISBN 5-7262—0557-X.

ПРИЛОЖЕНИЕ А

ВИРТУАЛЬНЫЙ КОМПЛЕКС ЗАДАНИЯ ПАРАМЕТРОВ ДВИЖЕНИЯ АВТОНОМНОГО ПОДВИЖНОГО СОСТАВА С ИСПОЛЬЗОВАНИЕМ СИГНАЛОВ GPS - НАВИГАТОРА

Для тестирования и отладки в лабораторных условиях систем безопасности и контроля движения поездов был разработан симулятор, имитирующий работу основных локомотивных и напольных систем, взаимодействующий с комплексным локомотивным устройством безопасности (КЛУБ), широко используемым на отечественных железных дорогах, а также позволяющий осуществлять формирование сигналов бортовой и станционной аппаратуры безопасности движения. Структурная схема симулятора показана на рис. П.А.1.

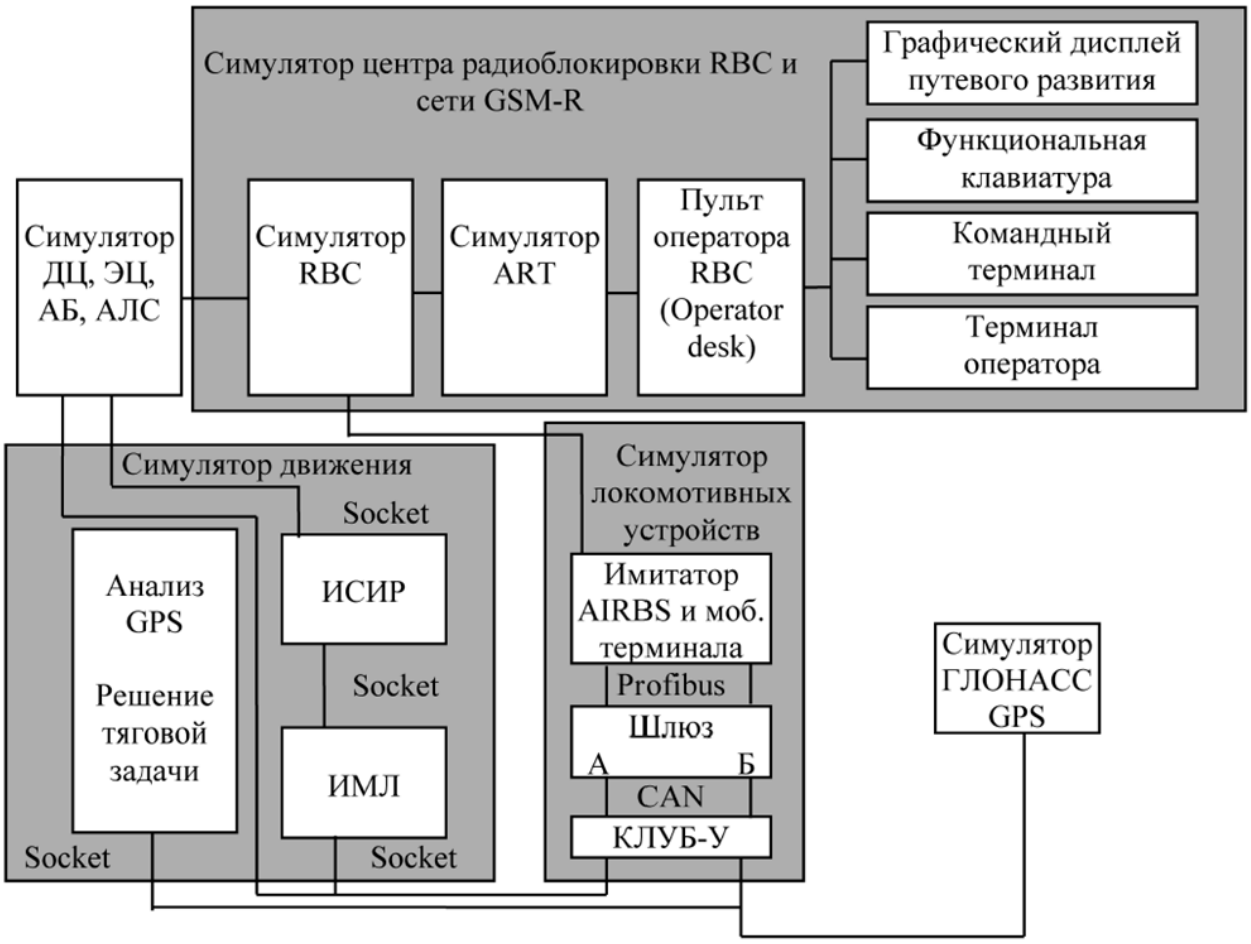


Рисунок П.А.1. Основные компоненты симулятора ITARUS-ATC

ДЦ - диспетчерская централизация, ЭЦ - электроцентрализация, АБ - автоблокировка, ИНУ - имитатор состояния напольных устройств, ИМЛ - имитатор состояния локомотивных устройств, RBC - центр радиоблокировки

GSM-R стационарную сеть мобильной радиосвязи.

Симулятор дает возможность дальнейшего развития объектов транспортной системы.

Симулятор состоит из отдельных модулей:

- модуля симулятора отечественных систем управления движения поездов ДЦ, ЭЦ, АБ;

- модуля симулятора центра радиоблокировки RBC и сети мобильной радиосвязи GSM-R, подключенный через сетевой шлюз к модулю симулятора систем ДЦ, ЭЦ, АБ;

- модуля симулятора локомотивной системы управления, включающий в себя симулятор мобильного терминала GSM-R (AIRBS), шлюз для обмена сообщениями между системами AIRBS и КЛУБ-У и натурную аппаратуру системы КЛУБ-У;

- модуля симулятора параметров движения, предназначенный для формирования сигналов, имитирующих движение поезда и работу его систем;

- модуля симулятора системы спутниковой навигации GLONASS.

Модуль симулятора параметров движения включает в себя две подсистемы:

- имитатор состояния напольных устройств (ИНУ), формирующий сигналы о состоянии рельсовых цепей, блок-участков, светофоров, положения стрелочных переводов по ходу движения поезда и т.п., передаваемые в симулятор систем управления ДЦ, ЭЦ, АБ;

- имитатор состояния локомотивных устройств (ИМЛ), предназначенный для формирования значений текущей скорости движения поезда и состояний локомотивных устройств, взаимодействующих с системой КЛУБ-У; обмен сигналами между ИМЛ и КЛУБ-У осуществляется с использованием конвертора сигналов.

- Модуль тягового расчета, позволяющий выполнять статистическую обработку данных от GPS и на их основе определять скорость, ускорение и тягу локомотива

Все компоненты разрабатываемого симулятора связаны между собой через общий сетевой коммутатор, что упрощает их взаимодействие. Сетевая структура симулятора представлена на рис. П.А.2.

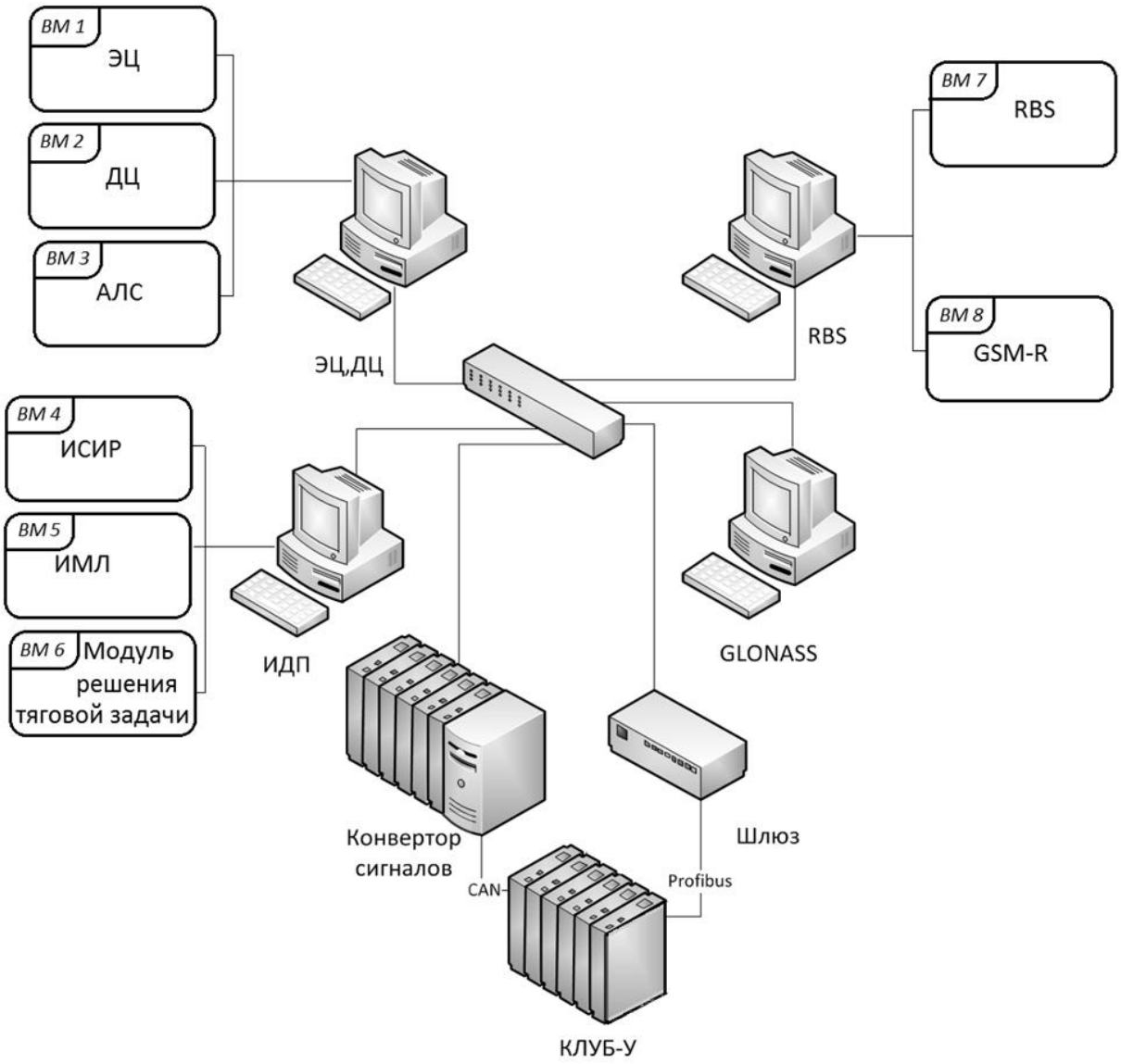


Рисунок П.А.2. Сетевая структура симулятора

ДЦ - диспетчерская централизация, ЭЦ - электроцентрализация, АБ - автоблокировка, ИНУ - имитатор состояния напольных устройств, ИМЛ - имитатор состояния локомотивных устройств, RBC - центр радиоблокировки

GSM-R стационарную сеть мобильной радиосвязи.

Обмен информацией между отдельными компонентами выполняется стандартными средствами технологии Ethernet по стеку протоколов TCP-IP с применением сетевых сокетов. Реализация практически всех компонентов симулятора осуществляется на базе стандартных ПЭВМ; конвертор сигналов выполнен с использованием модулей National Instruments. Все процессы, моделируемые различными компонентами симулятора, должны быть синхронизиро-

ваны по времени. Выполнить это можно использовав, например, локальный сервер NTP, синхронизирующий работу всех компонент.

Имитатор состояния локомотивных устройств (ИМЛ) реализуется на ПЭВМ симулятора движения; он моделирует работу основных локомотивных систем, управление которыми осуществляется через экран интерфейса машиниста (рис. П.А.3.).

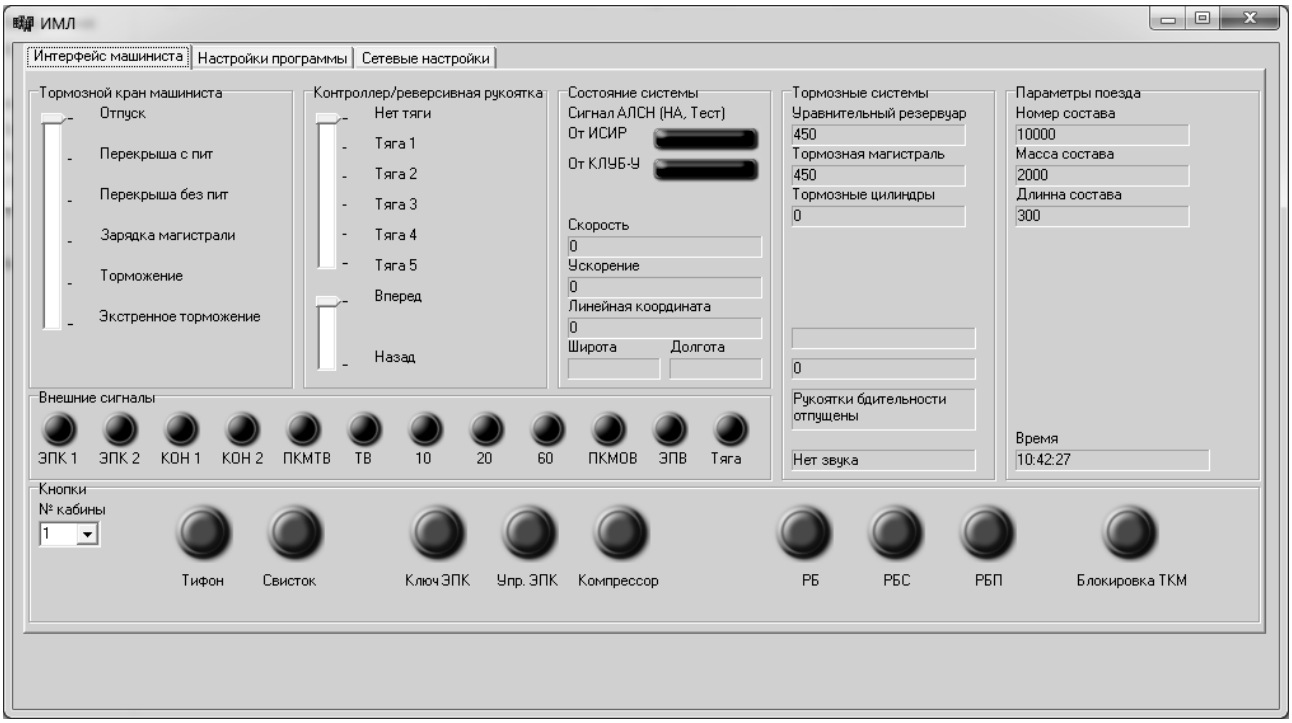


Рисунок П.А.3. Интерфейс модуля ИМЛ

Через интерфейс машиниста в симулятор вводятся следующие параметры режима работы виртуального поезда:

1) Позиция контроллера машиниста, определяющая мощность локомотива.

Виртуальный контролер машиниста реализует шесть уровней мощности, в том числе нулевой уровень, при которой тяга отсутствует. В процессе имитации режим движения поезда - сила тяги и скорость - определяются позицией контролера и соответствующей тяговой характеристикой локомотива. При получении от системы КЛУБ-У соответствующих сигналов, или при появлении сигнала о наличии давления в тормозных цилиндрах виртуального поезда энергетическая система его локомотива переводится на режим холостого хода.

2) Давление в уравнительном резервуаре, тормозной магистрали и тормозных цилиндрах, определяемые положением тормозного крана машиниста.

Имитатором предусмотрено шесть положений тормозного крана: отпуск и зарядка, поездное, перекрыша без питания, перекрыша с питанием, служебное торможение и экстренное торможение. Информация о состоянии тормозной системы отображается на экране интерфейса машиниста.

3) Скорость и ускорение поезда, определяемые силой тяги и состоянием тормозной системы.

4) Направление движения поезда, определяемое положением переключателя «вперед-назад» (положением реверсивной рукоятки).

5) Сигналы АЛСН, положение ключа электропневматического клапана, состояние блокировки тормозного крана машиниста, номер используемой кабины, сигналы включения тифона, свистка, электропневматического клапана, компрессора, рукоятки бдительности.

Помимо имитации данных, передаваемых в системы КЛУБ-У и ИНУ, имитатор ИМЛ принимает из КЛУБ-У, обрабатывает, и отображает на экране машиниста виртуального локомотива следующие параметры:

- линейные и географические координаты поезда;

- параметры поезда (номер поезда, длина, масса и т.п.);

- логические сигналы управления поездом: тяга, холостой ход, торможение и др.

Важно отметить, что в модуле ИМЛ предусмотрена возможность выбора основного или одного из вспомогательных режимов имитации.

В основном режиме имитации ИМЛ выполняет следующие действия:

- формирует направление движения и значение текущей скорости поезда с учетом положения реверсивной рукоятки, позиции контроллера и режима работы тормозной системы (давления в тормозных цилиндрах);

- получает от системы КЛУБ-У значение линейного перемещения поезда, и передает его на модуль ИНУ; получает от ИНУ коды показаний светофоров для передачи их в КЛУБ-У.

Вспомогательные режимы имитации позволяют установить:

- ручное задание сигналов АЛСН, при котором ИМЛ игнорирует данные, получаемые от модуля ИНУ; при этом коды сигналов АЛСН задаются через интерфейс машиниста модуля ИМЛ;

- расчет перемещения поезда по значению скорости вычисленной ИМЛ без учета данных, полученных от КЛУБ-У.

Закладка «Сетевые настройки» в ИМЛ позволяет задать IP - адреса и номера используемых портов модулей ИНУ и конвертора сигналов, с которыми он взаимодействует.

В процессе имитации движения, модуль ИМЛ циклически повторяет выполнение следующих операций:

- сетевое взаимодействие с конвертором сигналов и модулем ИНУ; при этом выполняется инициализация их подключения или обмен текущей информацией;

- определение значений давления в уравнительном резервуаре, тормозной магистрали и тормозных цилиндрах;

- определение направления движения, текущей скорости и ускорения поезда исходя из положения реверсивной рукоятки, позиции контроллера и состояния тормозной системы,

- формирование пакетов данных, которые передаются вначале следующей итерации в систему КЛУБ-У и ИНУ.

Имитатор состояний напольных устройств (рис. П.А.4.) позволяет при настройке симулятора загрузить электронно-цифровую карту участка железной дороги и указать положение виртуального поезда на этой карте .

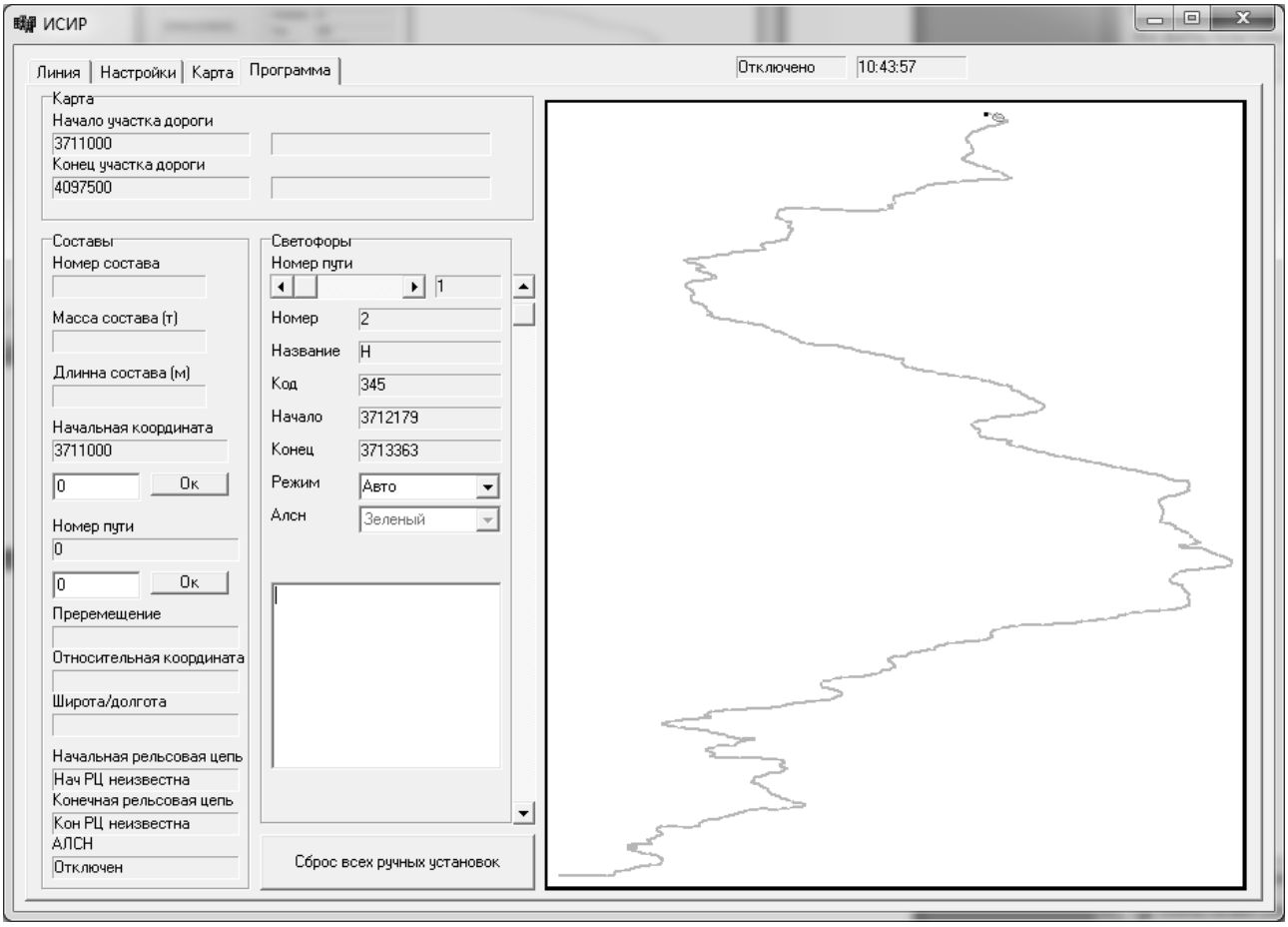


Рисунок П.А.4. Интерфейс модуля ИНУ

В процессе симуляции модуль ИНУ выполняет мониторинг состояния объектов участка железной дороги - занятость блок-участков, рельсовых цепей и т.д. Информация о занятости блок-участков передается в симулятор систем ЭЦ, ДЦ, АБ, который формирует для модуля ИНУ коды сигналов АЛСН. Если задан ручной режим работы модуля ИНУ, то оператор может задать сигнал каждого из светофоров, если автоматический - то модуль ИНУ получает эти сигналы от системы ЭЦ. Затем определяются текущие координаты поезда, занятые им рельсовые цепи и блок-участки. Исходя из этой информации, формируются сообщения для модулей ИМЛ и ЭЦ.

Взаимодействие между модулями ИМЛ и ИНУ в составе симулятора движения осуществляется через стандартные сокеты по протоколу TCPIP. Выбор этого протокола для работы симулятора обусловлен его повышенной надежностью и бесперебойностью функционирования.

Протоколы взаимодействия между модулями ИНУ, ИМЛ и конвертором сигналов системы КЛУБ-У построены по единому принципу (рис. П.А.5.).

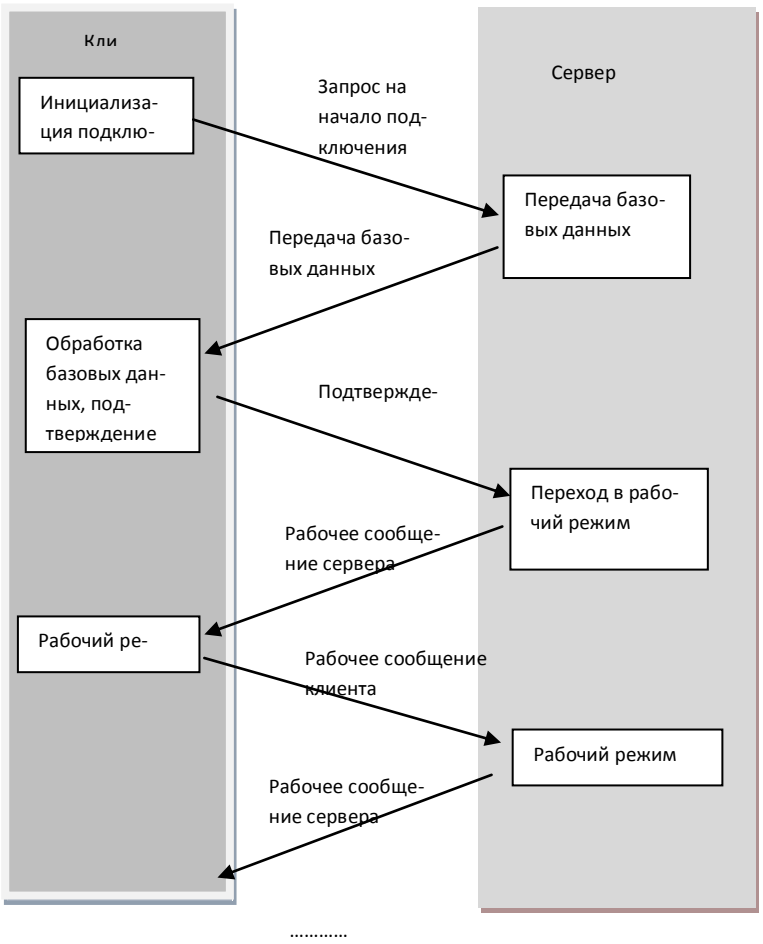


Рисунок П.А.5. Протокол взаимодействия модуля ИМЛ и конвертора сигналов

Сначала сервер прослушивает выбранный порт, ожидая подключение клиента.

Затем клиент посылает запрос на подключение, проверяя наличие сервера в сети. Получив этот запрос, сервер отвечает подтверждением, передавая при этом базовую информацию о начальном состоянии системы. Получив эту информацию, клиент должен подтвердить переход в рабочий режим.

После перехода системы в рабочий режим обе стороны клиент-сервер последовательно обмениваются сообщениями, содержащими информацию о текущем состоянии своих модулей. Различие протоколов в парах «конвертор сигналов - ИМЛ» и «ИМЛ - ИНУ» состоит в полях данных, передаваемых между ними. Для системы «конвертор сигналов – ИМЛ» - это данные о

текущем состоянии подсистем поезда, а для системы «ИМЛ – ИНУ» – данные о положении поезда на участке железной дороги, его текущей скорости, а также сигналы АЛСН.

Таким образом взаимодействие модулей ИНУ, ИМЛ и конвертора сигналов системы КЛУБ-У, включенных в состав симулятора, позволяет выполнять лабораторное тестирование системы безопасности движения поезда.

При использовании в составе симулятора предложенных программных моделей ИМЛ и ИНУ обеспечивается достаточно точная имитации процесса движения поезда по участку железной дороги, заданному электронной картой, что дает возможность проверять реакцию виртуального поезда на нештатные ситуации.

Модуль тягового расчета автономного тягового подвижного состава с гидравлической тяговой передачей используется для определения тяговых свойств подвижного состава, не имеющего электрической тяговой передачи, и вследствие этого исключающего возможность использования для расчетов зависимостей момента на валу тягового электродвигателя от тока по его обмоткам.

Модуль тягового расчета взаимодействует системой GPS с использованием протоколов MNP или NMEA и использует следующие сигналы:

- линейные и географические координаты поезда;

- параметры поезда (масса, коэффициент инерции вращающихся масс, длина);

- логические сигналы управления поездом (уровень мощности силовой установки, торможение и др.).

Для определения тяговой характеристики с помощью модуля GPS, при движении подвижного состава в режиме выбега на известном участке профиля пути, предварительно определяется его основное сопротивление движению. После этого определяется изменение скорости движения в режиме тяги, при нахождении подвижного состава на определенном участке профиля пути, что дает возможность определить его дополнительное сопротивление движению с учетом уклона и кривизны пути.

На основании полученных данных модулем выполняется аппроксимация скорости движения, и ее дифференцирование по времени, что позволяет определить ускорение подвижного состава за достаточно малый промежуток времени. Затем выполняется расчет силы тяги для данного интервала скорости движения, и затем во всем интервале скоростей движения вплоть до конструкционной и при различных значениях мощности силовой установки тягового подвижного состава.

Модуль может взаимодействовать как с физическим оборудованием, связанным с ПЭВМ по COM интерфейсу, так и с подготовленными файлами - записями с систем GPS.

Данный модуль был использован для экспериментального определения тяговых характеристик рельсовых автобусов серий РА1, РА2 и автомотрисы PESA 610M.

ПРИЛОЖЕНИЕ Б

ИНТЕРФЕЙС ПРОГРАММЫ РАСЧЕТА ЭФФЕКТИВНОСТИ СРЕДСТВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ВИРТУАЛЬНОГО КОМПЛЕКСА

На рис. П.Б.1 приведена схема структура файла, описывающего дерево атак в терминах сетей Петри.

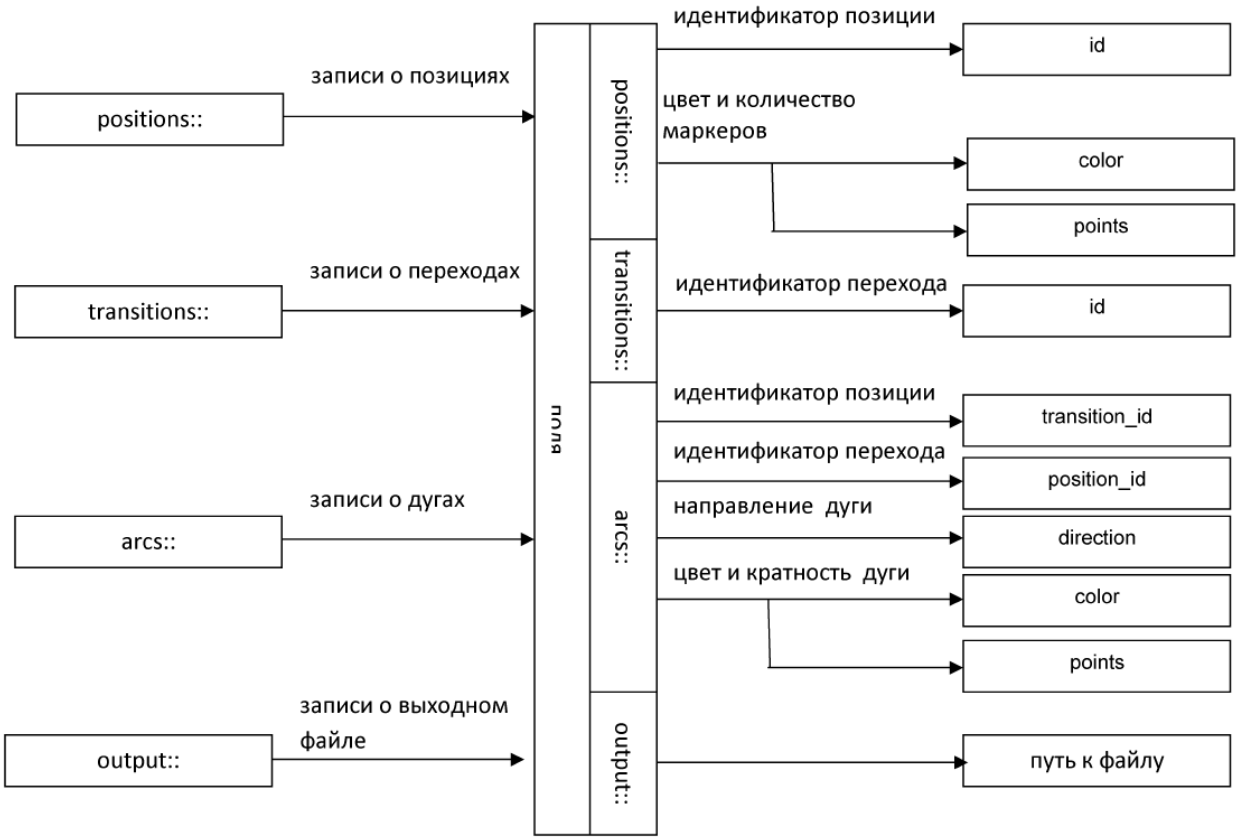


Рисунок. П.Б.1. Структура файла, описывающего дерево атаки

Файл состоит из последовательности записей, каждая из которых заключена в квадратные скобки, а поля внутри которых разделяются запятыми. Алгоритм обработки записей включает следующие этапы.

1. Считывание заголовка, описывающего блок записей, возможные значения: positions::, transitions::, arcs::, output::.

2. Заголовок вида positions:: определяет, что следующими считанными записями будут описания позиций вида:

[id = , color = , points =]

id - идентификатор позиции;

color - цвет маркеров внутри позиции;

points - количество маркеров внутри позиции;

Если позиция содержит несколько маркеров различных цветов, то все они описываются последовательно идущими парами полей color и points. Если цвет маркера явно не задан, то он определяется как черный. Такимобразом, записьвида:

[id = 10, color = red, points = 17, color = green, points = 9, points = 21]

описывает позицию с идентификатором 10, содержащую 17 красных, 9 зеленых и 21 черный маркер.

3. Заголовок вида transitions:: определяет, что следующими считанными записями будут описания переходов вида:

[id =]

id - идентификатор перехода.

Таким образом, запись вида:

[id = 8]

описывает переход с идентификатором 8

4. Заголовок вида arcs:: определяет, что следующими считанными записями будут описания дуг, соединяющих позиции и переходы вида:

[transition_id = , position_id = , direction = , color =, points =]

transition_id - идентификатор перехода;

position_id - идентификатор позиции;

direction - направление дуги, которое может принимать значения: transition_output - дуга направлена от позиции к переходу, position_output - дуга направлена от перехода к позиции;

color - цвет маркеров, используемых дугой, если цвет не указан явно, то он определяется как черный;

points - кратность дуги;

Таким образом, запись вида:

[transition_id = 8, position_id = 10, direction = transition_output, color = white, points = 30]

описывает дугу, направленную от десятой позиции к восьмому переходу и имеющую кратность, равную тридцати белым маркерам.

5. Заголовок вида output:: определяет , что следующей считанной записью будет путь для сохранения результатов моделирования

[d:\testdir\log.txt] - диск D:, директория testdir, файл log.txt

СПИСОК СОКРАЩЕНИЙ

ИТ – информационные технологии;

ИБ – информационная безопасность;

ИС – информационная система;

ВИ – виртуальная инфраструктура;

ВК – виртуальный компьютерный комплекс;

ВМ – виртуальная машина;

ОС - операционная система;

ДЦ – диспетчерская централизация;

ЛП – линейный пункт;

ИШД - общая информационная шина данных